

The Influence of Emotions on Employees' Cybersecurity Protection Motivation Behaviour: Examining the Mediating Effect of Self- Efficacy and Moderating Role of Cybersecurity Awareness

By

Abdulelah Sulaiman A Alshammari

A thesis submitted to Aston university in accordance with the
requirements of the degree of Doctor of Philosophy

Aston University

December 2024

©Abdulelah Alshammari, 2024. Abdulelah Alshammari asserts their moral right to be
identified as the author of this thesis

“This copy of the thesis has been supplied on condition that anyone who consults it
is understood to recognise that its copyright belongs to its author and that no
quotation from the thesis and no information derived from it may be published
without appropriate permission or acknowledgement.”

Thesis Abstract

Aston University

The Influence of Emotions on Employees' Cybersecurity Protection Motivation Behaviour: Examining the Mediating Effect of Self-Efficacy and Moderating Role of Cybersecurity Awareness

Abdulelah Sulaiman A Alshammari
Doctor of Philosophy
December 2024

Cyber threats at the employee level are a complex issue that needs more attention. Psychological research shows that emotions influence individuals' motivation to engage in cybersecurity practices. Most existing studies focus on how external factors affect employees' cybersecurity behaviours, including risk perception, rational decision making in cybersecurity policies, security regulations, compliance, and ethical behaviour. However, research into employees' internal capabilities and psychological factors, such as emotions, that enable them to protect organisational information assets is still in its early stages. Therefore, this thesis aims to explore the influence of employees' emotions on their cybersecurity protection motivation behaviours within Saudi Arabia's context. The research highlights self-efficacy as a mediating factor and cybersecurity awareness as a moderating factor. This thesis is underpinned by the Broaden and Build Theory (BBT) and Protection Motivation Theory (PMT) to explore the influence of negative and positive emotions on employees' cybersecurity protection motivation behaviour. Moreover, it adopted a deductive research design, employing a quantitative approach through an online survey, resulting in 383 responses from participants at King Abdulaziz University in Saudi Arabia. The data were analysed using partial least squares structural equation modelling (PLS-SEM) via SmartPLS 4 software, which included measurement and structural model assessments.

The study found that negative emotions do not influence employees' self-efficiency or motivation to protect themselves. Moreover, it found that self-efficacy does not mediate the relationship between negative emotions and employees' protection motivation behaviour. However, positive emotions positively influence employees' self-efficacy and protection motivation behaviour. In addition, self-efficacy positively mediates the relationship between positive emotions and employees' protection motivation behaviour. Regarding cybersecurity awareness, it was found that it positively influences employees' protection motivation. Moreover, it also moderates the relationships between positive emotions and self-efficacy and protection motivation behaviour, and between self-efficacy and protection motivation behaviour. The study contributes to cybersecurity by showing how emotions influence protective behaviours. It introduces a novel model based on BBT and PMT, exploring how emotions influence employees' self-efficacy and protection motivation behaviour. Moreover, the study's empirical findings address a gap by focusing on how emotions influence cybersecurity protection motivation behaviours.

Keywords: *cybersecurity, protection motivation behaviour, emotions, positive emotions, negative emotions, self-efficacy, cybersecurity awareness.*

Dedication

This thesis is dedicated to:

My parents, my father Sulaiman, my mother Hasna, my sisters and brothers, my lovely wife, and my little son may ALLAH always be generous and merciful with them.

Acknowledgements

In the name of God, the Most Merciful, the Most Compassionate, I extend my deepest gratitude to Allah for the countless blessings bestowed upon me.

I am greatly grateful to Professor Vladlena Benson for her steadfast faith in my abilities and her invaluable guidance throughout my PhD and professional journey. Your advice, support, and mentorship are beyond words, and I hold a profound respect and affection for you that I cannot fully express. I also thank Dr. Luciano Batista for his extraordinary generosity and consistent readiness to help me and address my questions.

My heartfelt thanks go to my parents, whose endless support and love have driven me to pursue excellence. From my first breath to this moment, your encouragement and prayers have been my safeguard and source of success. Words are insufficient to acknowledge the depth of your impact on my life. To my sisters and brothers, thank you for your constant support, love, and kindness. Your unwavering affection, assistance, and strength are treasures I hold dear.

I am also profoundly thankful to my beloved spouse and son for their love, patience, support, and inspiration. Your presence not only fuels my dedication but also serves as a constant reminder of the importance of family in my life, inspiring me to strive to improve myself, be a better partner, and be an outstanding father.

I am deeply grateful to King Abdulaziz University in Saudi Arabia for their generous support in funding my journey and turning my cherished dream into reality.

Lastly, I dedicate this work to the memory of my beloved brother, Ajlan. Your kindness and support continue to inspire me daily. Though you are deeply missed, your legacy drives me to honour you in all I do. May you rest in peace.

List of Publications

Alshammari, A., Benson, V., & Batista, L. (2023). Emotional Cost of Cyber Crime and Cybersecurity Protection Motivation Behaviour: A Systematic Literature Review. PACIS 2023 Proceedings, 133. <https://aisel.aisnet.org/pacis2023/133>

Alshammari, A., Benson, V., & Batista, L. (2024). The Influences of Employees' Emotions on their Cyber Security Protection Motivation Behaviour: A Theoretical Framework. In *26th International Conference on Enterprise Information Systems*.

List of Contents

Thesis Abstract	ii
Dedication	iii
Acknowledgements	iv
List of Publications	v
List of Contents	vi
List of Abbreviations	xi
List of Tables	xii
List of Figures	xiii
Chapter One: Introduction	1
1.1 Introduction	1
1.2 Research Background	1
1.3 Research Problem	4
1.4 Research Motivation	5
1.5 Research Questions	8
1.6 Research Aim and Objectives	9
1.7 Research Framework	10
1.7.1 Overview of Saudi Arabia	10
1.7.2 Saudi Arabia and Internet Connectivity	10
1.7.3 Saudi Arabia and Cybersecurity	11
1.7.4 Saudi Vision 2030 in Cybersecurity	11
1.7.5 Saudi Vision 2030 in Education	12
1.7.6 Cybersecurity Attack in Higher Education	13
1.8 Research Contributions	14
1.8.1 Contributions to Theories	14
1.8.2 Contribution to Methodology	15
1.9 Research Process and Thesis Structure	16
Chapter Two: Literature Review	18
2.1 Introduction	18
2.2 Emotions	18
2.2.1 Definitions of Emotion	18
2.2.2 Functions of Emotion	19
2.2.2.1 Adaptive Functions	20
2.2.2.2 Communicative Functions	21
2.2.2.3 Regulatory Functions	22
2.2.2.4 Motivational Functions	23
2.2.3 Components of Emotion	24
2.2.4 Categorisations of Emotions	25
2.2.4.1 Discrete Models of Emotion	25
2.2.4.2 Dimensional Model	27
2.2.4.3 Componential Model	28
2.2.4.4 Social Constructivist Models	30
2.2.4.5 Other Emotional Categories	30
2.3 Cybersecurity	33

2.3.1 Definition of Cybersecurity	33
2.3.2 Importance of Cybersecurity	35
2.3.3 Taxonomy of Cybersecurity Threats	36
2.4 Human Behaviour in Cybersecurity	40
2.5 Higher Education and Cybersecurity	44
2.6 Saudi Arabia Higher Education and Cybersecurity	44
2.7 Emotions and Cybersecurity Systematic Literature Review (SLR)	46
2.7.1 Planning the Review	47
2.7.2 Specification of the Study	47
2.7.3 Data Extraction	48
2.7.4 Data Execution: Research Profiling	50
2.7.5 Thematic Foci	52
2.7.5.1 Emotions and Cybersecurity Violations	53
2.7.5.2 Emotions and Cybersecurity Protection Motivation Behaviour	53
2.7.5.3 Emotions and Cybersecurity Policy Compliance	55
2.7.5.4 Emotions and Insider Behaviour	55
2.7.5.5 Psychological Factors and Cybersecurity	56
2.7.5.6 Emotions and Security Fatigue	57
2.7.6 Theoretical and Methodological Context	58
2.7.7 Analysis of the Literature	60
2.8 Summary	63
Chapter Three: Theoretical Framework and Hypotheses Development	64
3.1 Introduction	64
3.2 Theoretical Overview	64
3.3 Negative Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy	67
3.4 Positive Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy	71
3.6 Employees Cybersecurity Awareness	75
3.7 Differences in Employees' Cybersecurity Protection Motivation Behaviour	78
3.8 Proposed Theoretical Framework	80
3.9 Summary	80
Chapter Four: Research Methodology	82
4.1 Introduction	82
4.2 Research Philosophy	82
4.2.1 Ontology	82
4.2.2 Epistemology	83
4.2.2.1 Positivism	83
4.2.2.2 Interpretivism	83
4.2.2.3 Critical Realism	84
4.2.2.4 Pragmatism	84
4.2.3 Selected Research Philosophy	84
4.3 Research Approach	86
4.3.1 Deductive Approach	86
4.4 Methodological Choices	87
4.4.1 Quantitative Research Approach	88

4.5 Research Strategy	88
4.5.1 Survey Research Method	89
4.5.2 Cross-Sectional Design	90
4.6 Population and Sampling	90
4.6.1 Population	91
4.6.2 Sampling Techniques	91
4.6.3 The Selection of a Sampling Technique	92
4.6.4 Sampling Procedures	92
4.6.5 Sample Size	93
4.7 Instrumentation	95
4.7.1 Survey Development and Measurements	95
4.7.1.1 Demographic Profile	96
4.7.1.2 Negative Emotions	96
4.7.1.3 Positive Emotions	97
4.7.1.4 Self-efficacy	97
4.7.1.5 Cybersecurity Awareness	97
4.7.1.6 Protection Motivation Behaviour	97
4.7.1.7 Construct summary	97
4.7.2 Translation	99
4.7.3 Pilot Study Results	100
4.8 Data Collection	101
4.8.1 Ethical Considerations	101
4.8.2 Data Collection Procedures	102
4.9 Data Analysis	102
4.9.1 Data Preparation Process for Analysis	103
4.9.2 Structural Equation Modelling (SEM)	104
4.10 Summary	105
Chapter Five: Research Findings	106
5.1 Introduction	106
5.2 Data Preparation	106
5.2.1 Response Rate	106
5.2.2 Missing Data	107
5.2.3 Outliers	107
5.2.3.1 Univariate	107
5.2.3.2 Multivariate	108
5.2.4 Unengaged Responses	109
5.2.5 Normality	110
5.2.6 Common Method Bias	112
5.3 Demographic Profile	113
5.3.1 Gender	113
5.3.2 Age	114
5.3.3 Employees' Educational Level	115
5.3.4 Employees' Work Position	116
5.3.5 Employees' Years of Experience	116
5.4 Descriptive Statistics of the Constructs	117
5.5 Model Evaluation	118
5.5.1 Measurement Model	118
5.5.1.1 Indicator Reliability	119
5.5.1.2 Construct Reliability	120

5.5.1.3 Convergent Validity	121
5.5.1.4 Discriminant Validity	121
5.5.2 Structural Model Assessment	124
5.5.2.1 Collinearity	125
5.5.2.2 Path Coefficients	125
5.5.2.3 Mediation	128
5.5.2.4 Moderation Effects	129
5.5.2.5 Coefficient of Determination (R2 value)	132
5.5.2.6 Effect Size - f^2	132
5.5.2.7 Predictive Relevance	133
5.5.2.8 M Goodness-of-Fit (GoF)	135
5.5.3 Assessing Employees' Differences in Cybersecurity Protection Motivation Behaviour	135
5.5.3.1 Gender	136
5.5.3.2 Age	138
5.5.3.3 Employees' Educational Level	141
5.5.3.4 Employees' Work Position	144
5.5.3.5 Employees' Years of Experience	147
5.6 Summary	150
Chapter Six: Discussion	152
6.1 Introduction	152
6.2 Proposed Theoretical Framework	152
6.2.1 Negative Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy	153
6.2.2 Positive Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy	155
6.2.3 Self-Efficacy and Employees' Cybersecurity Protection Motivation Behaviours	158
6.2.4 Employees' Cybersecurity Awareness	162
6.3 Assessing Employees' Differences in Cybersecurity Protection Motivation Behaviour	167
6.3.1 Gender	167
6.3.2 Age	171
6.3.3 Employees' Educational Level	176
6.3.3 Employees' Work Position	180
6.3.4 Employees' Years of Experience	184
6.4 Summary	188
Chapter Seven: Conclusion	189
7.1 Introduction	189
7.2 Addressing Research Questions, Aim and Objectives	189
7.3 Research Overview and Key Findings	192
7.4 Research Contributions and Practical Implications	195
7.4.1 Contribution to Theories	196
7.4.2 Practical Implications	197
7.5 Research Limitations	202
7.6 Future Research	203
7.7 Conclusion	204
References	205

Appendix A: Questionnaire (English)	241
Appendix B: Questionnaire (Arabic)	248
Appendix C: Ethical Approval	254
Appendix D: Approvals From King Abdulaziz University	255
Appendix E: Formal Letter of King Abdulaziz University's Deanship of Scientific Research	256
Appendix F: King Abdulaziz University Email Survey	259

List of Abbreviations

ICTs	Information and Communication Technologies
BBT	Broaden and Build Theory
AET	Affective Events Theory
IT	Information Technology
CITC	Communication and Information Technology Commission
NCA	The National Cyber Security Authority
SEM	Structural Equation Modelling
CB-SEM	Covariance Based Structural Equation Modelling
PLS-SEM	Partial Least Squares Structural Equation Modelling
CIA	Confidentiality, Integrity, and Availability
NICCS	National Initiative for Cybersecurity Careers and Studies
NIST	National Institute of Standards and Technology
ISP	Information Security Policies
IS	Information Systems
SLR	Systematic Literature Review
WoS	Web of Science
PsyCap	Psychological Capital
PFC	Problem-Focused Coping
EFC	Emotion-Focused Coping
NE	Negative Emotions
PE	Positive Emotions
SE	Self-Efficacy
CSA	Cybersecurity Awareness
PMB	Protection Motivation Behaviour
D2	Mahalanobis Distance
CA	Cronbach's Alpha
CR	Composite Reliability
VIF	Variance Inflation Factor
AVE	Average Variance Extract
Q2	Cross-Validated Redundancy
R2	Coefficient of Determination
f2	Effect Size
CVPAT	Cross-Validated Predictive Ability Test
IA	Indicator Averages
LM	Linear Model
GoF	Goodness-Of-Fit
SRMR	Standardised Root Mean Square Residual
NFI	Normed Fit Index

List of Tables

Table 1: Emotional Categories.....	31
Table 2: Overview of Chosen Papers	50
Table 3: The Most Frequently Applied Theories and Methods	59
Table 4: Minimum Sample Size (Krejcie & Morgan 1970)	93
Table 5: PLS-SEM Minimum Sample Size (Hair et al., 2014; Cohen, 1992).....	94
Table 6: PLS-SEM Minimum Sample Size (Kock & Hadaya, 2018)	95
Table 7: Constructs Summary	98
Table 8: The Survey's Translators	100
Table 9: Pilot Study Construct Reliability.....	101
Table 10: Univariate Outliers	108
Table 11: Multivariate Outliers	109
Table 12: Demographic and Construct Normality	111
Table 13: Item Normality	111
Table 14: VIF	113
Table 15: Gender of Respondents.....	113
Table 16: Age of Respondents	114
Table 17: Educational Level of Respondents	115
Table 18: Work Position of Respondents	116
Table 19: Years of Experience of Respondents	116
Table 20: Descriptive Statistics.....	118
Table 21: Measurement Model Criteria	119
Table 22: Measurement Model Assessment Results	120
Table 23: Cross-Loadings	122
Table 24: Fornell-Larcker Criterion	123
Table 25: HTMT	124
Table 26: Structural Model Assessment.....	124
Table 27: Collinearity	125
Table 28: Results of Path Analysis	126
Table 29: Hypotheses' Results	127
Table 30: Mediation Effects.....	129
Table 31: Moderation Effects	130
Table 32: R-Square	132
Table 33: Effect Size	133
Table 34: CVPAT	134
Table 35: GoF	135
Table 36: Gender Measurement Model Assessment Results.....	136
Table 37: Gender Fornell-Larcker Criterion.....	137
Table 38: Hypotheses Results by Gender.....	138
Table 39: Age Measurement Model Assessment Results	139
Table 40: Age Fornell-Larcker Criterion.....	140
Table 41: Hypotheses Results by Age Group	140
Table 42: Educational Level Measurement Model Assessment Results	142
Table 43: Educational Level Fornell-Larcker Criterion	143
Table 44: Hypotheses Results by Educational Level	143
Table 45: Work Position Measurement Model Assessment Results	145
Table 46: Work Position Fornell-Larcker Criterion	146
Table 47: Hypotheses Results by Work Position	146
Table 48: Years of Experience Measurement Model Assessment Results	148
Table 49: Years of Experience Fornell-Larcker Criterion	148
Table 50: Hypotheses Results by Years of Experience	149

List of Figures

Figure 1: Research's Flowchart.....	16
Figure 2: Affective Processes and Emotions (Gross & Thompson, 2007)	25
Figure 3: Basic Emotions Model (Ekman, 1992).....	26
Figure 4: Whissell's Wheel of Emotion Representation Model (Rojas et al., 2006).....	28
Figure 5: Circumplex Theory of Affect (Watson et al., 1988).....	28
Figure 6: a) Plutchik's Colour Wheel of Emotions, b) Dyads of Emotions (Mihalinec et al., 2008)	29
Figure 7: Emotion Classifications in IT (Beaudry & Pinsonneault, 2010)	32
Figure 8: SLR Process and Protocols	49
Figure 9: Cybersecurity and Emotions Publications Over Time	51
Figure 10: List of Studies Across Journals	52
Figure 11: A Classification of Emotions Based on Systematic Analysis	62
Figure 12: Proposed Theoretical Framework.....	80
Figure 13: Research Paradigms	85
Figure 14: Methodological Choice (Saunders et al., 2019).....	87
Figure 15: Gender Distribution	114
Figure 16: Age Distribution	115
Figure 17: Educational Level Distribution	115
Figure 18: Work Position Distribution	116
Figure 19: Years of Experience Distribution.....	117
Figure 20: Theoretical Framework Results	127
Figure 21: H_{11} Slope Test Results	130
Figure 22: H_{12} Slope Test Results	131
Figure 23: H_{13} Slope Test Results	132
Figure 24: Proposed Theoretical Framework Findings	153
Figure 25: Model Findings for Male Employees.....	168
Figure 26: Model Findings for Female Employees	168
Figure 27: Model Findings for Younger Employees.....	172
Figure 28: Model Findings for Older Employees.....	172
Figure 29: Model Findings for Employees with High School/Diploma/Bachelor Qualifications	176
Figure 30: Model Findings for Employees with Master's/PhD/Other Qualifications.....	177
Figure 31: Model Findings for Administrative Employees.....	180
Figure 32: Model Findings for Academic Employees.....	181
Figure 33: Model Findings for Employees with Less than 10 Years of Experience	184
Figure 34: Model Findings for Employees with More than 10 Years of Experience.....	185
Figure 35: Significance of the Model Findings	201

Chapter One: Introduction

1.1 Introduction

This thesis explores how emotions influence employees' protection motivation behaviour by analysing the relationships between emotions, self-efficacy, cybersecurity awareness, and cybersecurity protection motivation behaviours. This chapter introduces the thesis and outlines its key components. This chapter begins by presenting the research background, motivation, and problem, providing the reasons behind the research and its broader significance. The research questions are outlined, focusing on how emotions influence employees' cybersecurity motivation behaviours, the influence of self-efficacy as a mediator and the effect of cybersecurity awareness as a moderator, followed by assessing employee differences. The research aim and objectives are clearly stated, emphasising the study's goals to understand and improve cybersecurity protection behaviours through emotional and psychological factors. The research context section offers an overview of Saudi Arabia, including internet connectivity and the country's current cybersecurity state. It also explores cybersecurity attacks in higher education, and Saudi Vision 2030, particularly in relation to education and its relationship to cybersecurity. This section establishes the relevance of the research within the broader national framework and highlights the importance of cybersecurity in achieving Saudi Arabia's strategic goals. Finally, the research process and thesis structure are discussed, detailing the methodology and strategy employed to tackle the research questions and fulfil the study's objectives, and to guide the reader through the organisation of the study.

1.2 Research Background

The rapid improvement and increased accessibility of technology have revolutionised human society by significantly changing many aspects of governments, businesses, and individuals' daily lives. Information and communication technologies (ICTs) are vital to the critical national infrastructure of every nation (Chang & Coppel, 2020; Majeed & Ayub, 2018). The growing dependence on computers, electronic devices, and information systems has resulted in innovative models such as pervasive computing and cloud environments. These models necessitate widespread and broad availability of resources related to computers (Al-Muhtadi et al., 2021). In contrast with conventional computing, the constantly changing features of technological advances and computing computational models have heightened the security risks associated with the flow of confidential and personal data (Pearson, 2013). Moreover, as systems and devices become increasingly networked and perform more functions, the

likelihood of cybersecurity vulnerabilities also increases (Hashizume et al., 2013). Cybersecurity is defined as the prevention of cyberattacks targeting internet-connected hardware, software, and data systems (Benson et al., 2016). The process of protecting information is characterised by three essential criteria: confidentiality, integrity, and availability to authorised users (Kim & Solomon, 2018).

People and organisational elements contribute to escalating security hazards in an organisation's information systems. For example, Grassegger and Nedbal (2021) state that by monitoring online behaviours on social networking sites, cybercriminals gather personal data or credentials that enable them to breach an organisation's information systems (Grassegger & Nedbal, 2021). Reviewing cybersecurity threats, Benson (2017) demonstrates that every industry sector is at risk of cyber attacks, with the public sector most frequently affected. Security breaches involving the unauthorised disclosure of sensitive information are classified as insider incidents within an organisation. These incidents are caused by negligence and failure to adhere to the organisation's policies (Lankton et al., 2019). Reports indicate that over 70% of security breaches occur due to unplanned violations of information security regulations by organisational insiders (Alshaikh et al., 2021). Out of the 874 reported security events, 86% were caused by inside employees' negligence or accidental failure to comply with security regulations. Conversely, 22% of the occurrences were considered violations by malicious insiders. Moreover, Donalds and Osei-Bryson (2020) highlight that 90% of experts argue that internal neglect has made their businesses vulnerable to security issues. Human factors in cybersecurity are essential to organisations (AL-Nuaimi, 2022; Hughes-Lartey et al., 2021). IBM (2023) revealed that data breach costs soared to an all-time high of USD 4.45 million, marking a 2.3% rise compared to the USD 4.35 million reported in 2022. The typical cost has increased by 15.3% in the long run, reaching USD 3.86 million in 2020. Most breaches were discovered to have entered firms via employees. The average cost of a data breach caused by an employee's misconduct increased by more than 20%, rising from USD 4.06 million to USD 4.87 million (IBM, 2023). Aside from the direct consequences of cyber attacks and hacks, such as financial losses, studies have revealed that these incidents also lead to a wide range of negative impacts on organisations. These include digital and physical damage, economic consequences, emotional distress, reputation damage, and interpersonal and societal harm (Agrafiotis et al., 2018; Liang et al., 2019). These data suggest that additional investigations are necessary to comprehend the causes of human-centred breaches in cybersecurity, and increasing research has focused on examining the impact of human factors on cybersecurity systems.

The research on human elements in cybersecurity primarily revolves around efforts to eliminate human involvement in the cybersecurity procedure (Goh, 2003). This can be attributed to the prevalence of security incidents assumed to originate from human actions. Research suggests that cybersecurity issues frequently involve the actions of humans (Zimmermann & Renaud, 2019). Even with the growing perception of cybersecurity's human and social potential and the significance of capable security practices, the main focus remains on managing, monitoring, and mitigating the human element (Crossler et al., 2013; Furnell et al., 2020; Nobles, 2022; Sandberg, 2015). Furthermore, technological advances have increasingly permeated organisations and employees' professional lives, rendering them more susceptible to cybersecurity risks, which are expanding at a rapid pace (Ghelani, 2022). Benson et al. (2020) believe that the effectiveness of security measures relies more on individuals than on technical controls and countermeasures.

Throughout the evolution of cybersecurity practices, humans have often been viewed as a critical weakness, impacting the overall effectiveness of security measures (Benson & McAlaney, 2019). They tend to make unreasonable choices without fully understanding the consequences of their actions (Benson & McAlaney, 2019). Psychological researchers have made a significant contribution to cybersecurity by increasing knowledge and awareness of the reasons behind users' cybersecurity behaviour. Cybersecurity studies addressing psychological and human factors have mainly been conducted within organisational frameworks and shaped by a limited range of behavioural fields. Researchers have shown interest in the debate on the various dimensions of cybersecurity involving human factors, and reported that specific characteristics of cybersecurity influence cybersecurity decisions (Frey et al., 2019; Snyman et al., 2018).

Emotions and risk comprehension are viewed as human elements of cybersecurity (McCormac et al., 2018; Beris et al., 2015). Emotional responses to cybercrime, fear of cybercrime, rationality in security policy decision making, motivations for security programmes, compliance with security regulations, ethical behaviour in cybersecurity, and consequences of avoiding technology due to adverse incidents are all crucial aspects discussed in various studies (Liang et al., 2019; Budimir et al., 2021; Brands & Van Doorn, 2022; Jansen & van Schaik, 2018; Bulgurcu et al., 2010; Weir et al., 2019; Spanaki et al., 2019; Zamani & Pouloudi, 2021). The significance of emotions and emotion-related factors in cybersecurity behaviours is a growing area of study (D'Arcy et al., 2014; Lowry & Moody, 2015; Boss et al., 2015; Warkentin et al., 2016), but the influence of emotions on human security protection motivations and actions within businesses to enhance cybersecurity is still an area of limited research. This thesis aims to explore the influences of employees' emotions on their

cybersecurity protection motivation behaviour in Saudi higher education. Moreover, this thesis adheres to the definition provided by Posey et al. (2013, 2015) of protection motivation behaviour as behaviours carried out by people inside an organisation to safeguard organisationally important information and the computer systems that store, collect, share, and manage that information and protect it from cybersecurity risks.

1.3 Research Problem

The rapid advancement of communication technologies has completely transformed numerous industries, including higher education, while concurrently bringing significant cybersecurity concerns. Higher education institutions are becoming more dependent on connected networks and digital infrastructures, which makes them more susceptible to cyber attacks and data breaches. There has been significant research on the technical aspects of cybersecurity, but there is still a considerable lack of understanding of the human factors, specifically the emotional and psychological aspects that influence employee behaviour in cybersecurity situations (Burns et al., 2019; Burns et al., 2017). Human behaviour is a critical factor in cybersecurity, as research demonstrates that a large number of security breaches are caused by human error, negligence, or intentional misconduct (Benson & McAlaney, 2019; Alshaikh et al., 2021; Donalds & Osei-Bryson, 2020). Nevertheless, the current body of literature has primarily concentrated on technological remedies and adherence to regulations, frequently neglecting the intricate relationship between employees' emotions, their belief in their capabilities, and their behaviours related to motivation for cybersecurity protection (Zimmermann & Renaud, 2019). The lack of attention to this issue is prevalent in higher education institutions, which handle sensitive data and would therefore suffer significant consequences if data security were breached (Posey et al., 2017). Furthermore, self-efficacy has been recognised as a crucial factor influencing protective behaviours, but its role in mediating the relationship between emotions and cybersecurity behaviours has not been widely investigated (Bandura et al., 1999; Moody et al., 2018). Individuals with high levels of self-efficacy are more likely to be motivated to follow cybersecurity rules. Nevertheless, individuals with low self-efficacy may engage in risky behaviours or fail to comply with these protocols, especially when experiencing negative emotions. The lack of studies on the influence of employee demographic characteristics on the relationship between emotions, self-efficacy, and cybersecurity protection motivation behaviour escalates the issue. Understanding these distinctions is an essential element of creating customised interventions that meet the specific requirements of various staff groups within higher education institutions. Given the continuing development of cybersecurity knowledge and practices in Saudi higher education, addressing the gaps is crucial (Garba et al., 2021; Masmali & Miah, 2022). The extent to which cybersecurity awareness programmes can mitigate the influence of emotions

on self-efficacy and cybersecurity behaviours has yet to be investigated. Therefore, this thesis explores the influence of emotions on employees' protective behaviour in Saudi higher education institutions.

1.4 Research Motivation

There are several motivational factors behind the decision to conduct this study. Cybersecurity needs studies addressing employee emotions and their influence on protection motivation behaviour. As mentioned earlier, most studies primarily examine the effects of external factors on employees' cybersecurity behaviours. Therefore, research on the influence of emotions on cybersecurity is required to highlight the positive and negative intensities that influence behaviour. Beaudry and Pinsonneault (2010) state that IT studies have neglected employees' emotional problems and responses, and researchers need to adopt a more complete approach to studying the influence of emotions on insiders' motivations. Therefore, it is essential to address this within the context of cybersecurity by exploring the influence of emotions on employees' self-efficacy and protection motivation behaviour. According to Moody et al. (2018), organisations should incorporate information security awareness into their cybersecurity management programmes to improve their self-efficacy. Self-efficacy is defined as an individual's confidence in their capacity to execute the actions needed to attain particular goals effectively (Bandura, 2004; Compeau & Higgins, 1995; Brooks et al., 2019). Protection motivation theory (PMT) offers a structure for comprehending the impact of self-efficacy on behaviour. Based on this, self-efficacy influences every component of behavioural change, including the beginning, level of exertion, and continuity of coping behaviours. Within the field of cybersecurity, individuals with a strong feel of self-efficacy are more likely to perceive cybersecurity measures as tasks they can manage and positively impact. As a result, they are more likely to follow security procedures diligently (Compeau et al., 1999). Self-efficacy therefore acts as a mediator in the connection between emotions and cybersecurity behaviours. Positive emotions can increase self-efficacy, which in turn promotes the adoption of protective behaviours. Training programmes that enhance employees' confidence in their cybersecurity skills can increase the probability of adhering to security regulations and reporting suspicious actions. In contrast, negative emotions can weaken self-efficacy, resulting in reduced motivation and the possibility of engaging in risky behaviours.

In addition to studying the role of emotions in self-efficacy and protection motivation behaviour, one of the possible ways to reduce cybersecurity incidences is to increase cybersecurity awareness among employees. This might makes employees more vigilant and help them understand information security risks beyond standard procedures during information security incidents (Bilal et al., 2011). Additionally, employees can be caught unawares when they

encounter a cybersecurity risk due to a lack of cybersecurity knowledge. Most employees violate cybersecurity policies or abuse or misuse work computers when encountering a cybersecurity risk (Niemimaa & Niemimaa, 2017). Moreover, it is essential to develop employees' protection motivation behaviour, and a vital aspect of this is promoting cybersecurity awareness. Awareness programmes aim to instruct employees about the nature of cyber threats and emphasise the significance of adhering to security measures. Enhanced knowledge and understanding are closely correlated with enhanced cybersecurity practices, as well-informed staff are more capable of identifying and addressing possible security risks. Furthermore, cybersecurity awareness might moderate the relationship between emotions, self-efficacy, and protection motivation behaviour. Employee awareness programmes can improve the detrimental impacts of negative emotions. They equip employees with the necessary knowledge and tools to feel self-efficacy in their ability to manage cyber threats. This might increase their belief in their skills and drive people to participate in actions that defend their well-being. Employees who possess knowledge of phishing strategies are more resistant to falling victim to such attacks, irrespective of their current emotional condition (Bada et al., 2014).

Another motivation for this research is that the existing literature has overlooked the relationship between employees' emotions and safeguarding information systems resources from threats. As a result, there is a need to focus on how organisations stimulate positive and negative emotions in employees when safeguarding its information systems resources. Furthermore, external factors such as security regulations and social norms influence the behaviours of employees with regard to information security. More studies on the influence of emotions on employees' motivation and behaviour regarding cybersecurity protection need to be conducted. Hence, to safeguard information, the research must embrace an entire strategy towards understanding the influence of emotions on the motives of individuals within the organisation. According to Burns et al. (2017), employees' behaviours are closely associated with their psychological attitudes towards information security. Emotions impact a person's beliefs, attitudes, and behaviours (Izard, 2002). Positive emotions can improve constructive behaviour and facilitate social relationships. Gulenko (2014) found that utilising positive emotions to enhance security behaviour influences security behaviour significantly more than deterrents. Conversely, negative emotions can have a detrimental impact on an employee's memory, thereby impairing their capacity to acquire new knowledge (Izard, 2002). This can negatively influence their job performance. Negative emotions can lead to combative behaviour and revenge, hindering IT-related behaviour (Beaudry & Pinsonneault, 2010). Several information security research studies have established a correlation between negative emotions and undesirable behaviours, such as using weak passwords (Gulenko 2014) and

neglecting information security precautions (Burns et al., 2019). However, the correlation between employees' emotional issues and coping mechanisms has been largely overlooked in cybersecurity research (e.g., Beaudry & Pinsonneault, 2010; Frey et al., 2019). According to Bagozzi et al. (1999), perception influences attitudes, motivation, skills, and conduct related to a specific matter, and Renaud et al. (2021) highlight that perceptions and emotions impact attitudes and behaviours in cybersecurity. Nevertheless, the investigation into the impact of emotions on the probability of computer-related aberrant behaviour has been constrained. Burns et al. (2019) calls for additional investigation into the effects of insiders' emotions on their behaviour regarding security. This study answers that call.

Another motivational factor is that there need to be more studies on employees' emotions related to their protection motivation behaviour in the higher education sector. Higher education institutions are susceptible to data breaches due to the presence of sensitive information in the systems they operate. This includes academic records, educational documents, personal information, medical records, copyrighted data, and digital assets owned by the institution (Posey et al., 2017). The implementation of remote learning at higher education institutions because of pandemic constraints has been affected by cyber attacks. According to Walton and Chinnaswamy (2022), in the past few years since the pandemic, there has been a sharp rise in cybercrime alongside the rapid growth of a cybercrime economy. While attackers once needed to develop advanced technologies for cyber attacks, modern cyber criminals increasingly rely on social engineering techniques to carry out their attacks. Recently, instances of cyber attacks targeting higher education institutions have been reported. These attacks entail the unlawful acquisition and misuse of personal information from students, professors, and staff for illegitimate purposes (Bolanio et al., 2021). Chapman et al. (2018) highlight the growing dependency on internet technologies across diverse sectors, leading to a rise in cybercrime and dynamic attacks. The authors stated that higher education institutions are vulnerable due to their wealth of sensitive personal, financial, research, and intellectual data. Chapman et al. (2018) emphasise that limited studies focus on addressing cyber incidents within universities. Therefore, it is essential to recognise that cybersecurity should not be confined to IT departments but requires a complete, institution-wide approach to manage risks effectively. In recent years, several studies have examined various aspects of cybersecurity within higher education, particularly in Saudi Arabian institutions. These include information security practices (Saeed, 2023), the effectiveness of cybersecurity systems (Alhumud et al., 2023), student understanding of cybersecurity and cybercrime (Almrezeq et al., 2021), security awareness (Alqahtani, 2022; Alharbi & Tassaddiq, 2021; Mohammed & Bamasou, 2022), the internet security awareness of students, and their attitudes towards Learning Management Systems (Alfalah, 2023), and the protection of

intellectual property (Sharabi, 2023). However, few studies investigate employees' cybersecurity behaviour in Saudi higher education (Garba et al., 2021; Masmali & Miah, 2022).

Therefore, despite the contributions of these studies, there is a need for studies to explore the influence of internal factors, such as employee emotions, and their influence on employee's cybersecurity protection motivation behaviour. The human element, mainly the emotional and psychological factors, plays a critical role in cybersecurity awareness and behaviour. Understanding how these internal factors affect employees' engagement with cybersecurity protocols could provide a more holistic understanding of the vulnerabilities within higher education institutions. Addressing this gap in the literature could lead to the development of more effective cybersecurity strategies that incorporate emotional and motivational considerations into training programmes and policy design. As a result, this thesis focuses on the influence of emotions on the motivation of Saudi Arabia's higher education employees to engage in cybersecurity protection behaviour.

1.5 Research Questions

1. How do negative and positive emotions influence employees' cybersecurity motivation behaviours and self-efficacy?
2. How does self-efficacy affect the relationship between negative and positive emotions and cybersecurity protective motivation behaviours?
3. Does cybersecurity awareness have a positive influence on employees' cybersecurity motivation behaviours? Moreover, how does cybersecurity awareness moderate the relationship between negative and positive emotions and employees' protection motivation behaviour, the relationship between negative and positive emotions and employees' self-efficacy, and the relationship between self-efficacy and protection motivation behaviour?
4. To what extent do the effects of negative and positive emotions, self-efficacy, and cybersecurity awareness on protection motivation behaviour differ between employees based on their demographic characteristics?

1.6 Research Aim and Objectives

This thesis aims to explore the influences of employees' emotions on their cybersecurity protection motivation behaviour. To accomplish the research aim, the following objectives have been set:

1. Review the existing literature to provide evidence that supports the identified gap. Conduct a broad investigation of the existing literature on the influence of emotions on cybersecurity protection motivation behaviour. The investigation will have a wide scope, including the literature on emotions and the behavioural motivation for cybersecurity protection.
2. Develop a proposed theoretical framework that includes the influence of negative and positive emotions on employees' cybersecurity protection motivation behaviour and self-efficacy; the role of self-efficacy as a mediating variable; and the influence of cybersecurity awareness on employees' cybersecurity protection motivation behaviour; cybersecurity awareness as a moderator variable in the relationship between negative and positive emotions and employees' protection motivation behaviour, in the relationship between negative and positive emotions and employees' self-efficacy, and in the relationship between self-efficacy and protection motivation behaviour.
3. To identify an appropriate measurement scale for negative and positive emotions, self-efficacy, cybersecurity awareness, and cybersecurity protection motivation behaviour.
4. Conduct empirical testing to confirm and identify whether negative and/or positive emotions affect employees' cybersecurity motivation behaviours and self-efficacy. This validation will enable the researcher to address the first research question.
5. Conduct empirical testing to explore how self-efficacy may contribute to cybersecurity protective motivation behaviours by mediating the effects of negative and positive emotions. This will answer the second research question.
6. Conduct empirical testing to examine the relationship between cybersecurity awareness and employees' cybersecurity protection motivation behaviour and how cybersecurity awareness could moderate the relationship between negative and positive emotions and employees' protection motivation behaviour, the relationship between negative and positive emotions and employees' self-efficacy, and the

relationship between self-efficacy and protection motivation behaviour. This will answer the third research question.

7. Analyse the similarities and differences in the research model among employees, considering their demographic characteristics. This contrast is crucial for addressing the fourth research question.

1.7 Research Framework

This section offers a clear overview of the study's contextual framework focusing on the Kingdom of Saudi Arabia. The main objective is to provide an overview of Saudi Arabia, internet connectivity, the current state of cybersecurity, cybersecurity attacks in higher education, and cybersecurity and higher education developments in Saudi Vision 2023.

1.7.1 Overview of Saudi Arabia

Saudi Arabia is the largest landmass on the Arabian Peninsula. The country is subdivided into 13 administrative regions, and its population has experienced notable growth, exceeding 32.1 million in 2022 (General Authority for Statistics, 2022). Arabic is the dominant and official language spoken throughout the nation. However, the English language is employed as a secondary language in commercial enterprises, educational establishments, and medical facilities. The Saudi Arabian economy is highly dependent on oil, which is the cornerstone of its economic framework. Saudi Arabia is the primary oil exporter among the Organisation of the Petroleum Exporting Countries member countries.

1.7.2 Saudi Arabia and Internet Connectivity

Saudi Arabia hosts the broadest information and communication technology market in the Middle East, and the government is continually enhancing and expanding this sector. The latest report from the Communication and Information Technology Commission (CITC) of the Kingdom of Saudi Arabia reveals that the proportion of individuals with internet connectivity increased from 98.1% in 2021 to approximately 99% in 2023. CITC (2024) reports that the distribution of internet access in Saudi Arabia was as follows: 84.7% accessed the internet from their homes, 72% accessed it while on the move, and 43.4% accessed it from their workplaces.

The report disclosed that the average download speed in Saudi Arabia for 2023 increased to 214.6 Mbps, compared to 169.52 Mbps in 2021. This places Saudi Arabia in the top 10 position globally. Furthermore, the volume of internet traffic in Saudi Arabia amounts to 42,040,695 terabytes, with 57% being local data traffic and the remaining 43% international traffic. An

increase in data traffic, prompted by the expanding use of social media platforms, content providers such as YouTube and Snapchat, and online gaming, has significantly heightened the demand for internet and broadband services. According to the 2023 annual report, spending on ICT services is projected to continue growing, with a particular emphasis on information security as a crucial aspect of digital transformation efforts in the Kingdom. Furthermore, enterprises have been expanding to adopt sophisticated and proactive information security solutions (CITC, 2024).

1.7.3 Saudi Arabia and Cybersecurity

The National Cyber Security Authority (NCA) of the KSA has provided a report on the threats faced by the country during the fourth quarter of 2020, from October 1st to December 31st. In 2020, the NCA identified five major cybercrime threats: unauthorised activity, harmful code, exploitation attempts, information leakage, and domain name impersonation (NCA, 2020). Furthermore, they specify that the top five global threats were malware (52%), account hijacking (16%), targeted attacks (10%), vulnerability (6%), malicious script injections (4%), and other unspecified threats (12%). The survey additionally indicated that the public (19%), health (14%), education (9%), technology, and trade sectors were the most frequently targeted sectors on a global scale (NCA, 2020). Computer and computer networks are growing rapidly, introducing novel and increasingly intricate technologies, such as the cloud and the internet of things. Thus, the number of cybersecurity threats is on the rise. Hence, it is imperative for the Kingdom to actively stay updated with this trend by offering suitable defence measures, technology, and guidance to safeguard its information and communication systems from cyberattacks (NCA, 2020). The Kingdom must protect its national critical assets and infrastructure's confidentiality, integrity, and availability.

In 2016, the government initiated the Saudi Vision 2030. This strategic plan aims to establish a new economic framework by reducing reliance on oil and adopting a diversified economy. One of the critical aspects of this plan is the development of digital technology (Ouassini et al., 2021). Thus, cybersecurity will play an essential role in the current change, prompting firms to allocate resources to the IT sector and establish novel positions inside their IT departments.

1.7.4 Saudi Vision 2030 in Cybersecurity

Ensuring cybersecurity is of the highest priority in safeguarding national security and maintaining economic stability, particularly in the context of Saudi Arabia's Vision 2030. This project seeks to strengthen the country's economy and promote advancements in multiple sectors, including healthcare, tourism, and e-government. Saudi Arabia has acknowledged cybersecurity's importance and implemented numerous programmes and frameworks to

enhance its cybersecurity measures (Alharbi & Tassaddiq, 2021; Alharthi et al., 2019). Saudi Arabia's emphasis on cybersecurity is noteworthy, given the frequent occurrence of cyber attacks in the Arab region. This necessitates the development of strong cybersecurity policies and frameworks in the Kingdom (Alshammari & Singh, 2018; Talib et al., 2018). Within the framework of Vision 2030, the significance of cybersecurity is emphasised as the country allocates resources to large-scale initiatives and seeks to rejuvenate its healthcare system, requiring a strong and secure cyber infrastructure (Rahman & Al-Borie, 2021). Moreover, research has focused on examining the influence of cybersecurity practices on small organisations in Saudi Arabia, and emphasises the necessity of implementing efficient security measures to minimise the harm caused by cyber attacks, particularly for small businesses (Alharbi & Tassaddiq, 2021). The importance of cybersecurity in the adoption of e-government services is evident. It is crucial to develop a cybersecurity framework for e-government projects in Saudi Arabia to ensure the security and reliability of digital government services (AlRuthia et al., 2018). In addition, the successful use of e-government tools necessitates strong cybersecurity measures. This involves overcoming challenges and obstacles to inform and direct the development of justified policy recommendations. Furthermore, it is imperative to tackle the issue of cybercrime and cybersecurity knowledge among Saudi nationals, as indicated by studies and datasets that measure cybersecurity awareness (Alharbi et al., 2021; Alotaibi et al., 2016). Creating a cybersecurity maturity assessment system for institutions highlights the need for a strategy to improve cybersecurity in different sectors (Almomani et al., 2021). Incorporating cybersecurity protocols within the Vision 2030 framework is crucial for effectively achieving Saudi Arabia's strategic objectives. The nation's dedication to establishing strong cybersecurity rules and frameworks is essential for protecting its vital infrastructure, adopting economic variety, and guaranteeing the security of digital services in many industries.

1.7.5 Saudi Vision 2030 in Education

Saudi Vision 2030 is a complete strategy designed to diminish Saudi Arabia's reliance on oil, expand its economic base, and promote the development of sectors associated with public services, such as healthcare, education, infrastructure, leisure, and tourism. Education is an essential element of this strategy, as it is crucial in equipping the Saudi workforce with an economy that relies on knowledge and promotes long-lasting development (Mitchell & Alfuraih, 2018). The Saudi government has recognised the necessity of evaluating existing educational policies and their impact on the country's economy and environment to accomplish the goals of Vision 2030 (Essa & Harvey, 2022). Moreover, the vision prioritises advancing the healthcare industry by implementing privatisation. It emphasises the significance of education in generating a proficient workforce to facilitate this transition

(Rahman & Qattan, 2021). In addition, the vision aims to advance entrepreneurship education and promote the mindset of an entrepreneurial university, highlighting the necessity for educational changes in line with the vision's goals (Faqihi & Al-Ababneh, 2022). The vision also seeks to shift the economy's dependence on oil and views education as a method to develop a knowledge-based economy more aligned with Saudi Arabia's interests. Education is emphasised as a crucial factor in achieving economic diversification development (Mitchell & Alfuraih, 2018). In addition, the vision aims to establish connections between Saudi Arabia and other nations in education, highlighting the significance of global cooperation in education to support the vision's objectives (Nadia, 2017).

Furthermore, Vision 2030 places significant emphasis on promoting sustainable development, in addition to the goal of economic diversification. The Saudi Arabian government has established objectives to elevate the standing of cities in the country to a level that rivals the finest in the world. This highlights the significance of education in promoting sustainable development and urban planning (Alharthi et al., 2019). Moreover, the vision's focus on sustainable development standards throughout many sectors of Saudi society highlights the importance of education in advancing sustainable practices and promoting environmental consciousness (Balabel & Alwetaishi, 2021). Finally, Saudi Vision 2030 has significant educational consequences, as it aims to revolutionise the Saudi economy, promote sustainable growth, and encourage the nation's international competitiveness. Education is seen as a crucial facilitator for attaining the goals of the vision, whether by generating a proficient labour force, advocating for entrepreneurial education, encouraging sustainable development, or developing global partnerships.

1.7.6 Cybersecurity Attack in Higher Education

Higher education institutions are becoming more vulnerable to cyberattacks because of their vast repositories of sensitive information, heavy reliance on digital infrastructures, and relatively open networks. This makes cybersecurity in higher education institutions a significant issue with possibly severe societal and economic concerns, as disruptions to research, learning, and operations can have severe impacts. In recent years, there has been a rise in the number of cyber incidents reported in educational institutions. According to Saeed (2023), phishing is a prevalent cyberattack, constituting over 30% of successful security breaches within higher education institutions. Such attacks capitalise on human fallibility, deceiving faculty members, staff, and students into disclosing their credentials or installing harmful software (Saeed, 2023). Ransomware represents another significant threat; in 2021, at least 44 universities and colleges across the United States were targeted by such attacks, causing widespread disruptions to research, admissions processes, and online learning. A

single ransomware incident can cost institutions millions in ransom payments and lost operational time (Ulven & Wangen, 2021). Universities are also frequently targeted by Distributed Denial of Service (DDoS) attacks, which overwhelm their networks and cause significant service disruptions. These attacks can severely impact online learning systems and administrative functions. For instance, a major European university experienced a week-long shutdown due to a DDoS attack, leading to delayed exams and lectures (Kyva, 2022). Data breaches pose a critical risk, with attackers seeking to access personal records, financial information, and proprietary research. Human error increases these cybersecurity challenges, with research indicating that over 40% of cyber incidents in higher education institutions are the result of insufficient cybersecurity awareness among students and staff. A survey in Saudi Arabia found that only 20% of university students had experienced cybersecurity training, highlighting significant absences in fundamental practices such as password management and email security (Saeed, 2023). Addressing these risks requires a broad strategy. Cybersecurity awareness programmes have been shown to reduce human error by up to 30% (Salem & Sobaih, 2023). Additionally, deploying advanced security measures, including firewalls, encryption, and intrusion detection systems, can mitigate many vulnerabilities. Developing robust incident response plans is equally vital, enabling institutions to recover more effectively from cyberattacks. For instance, universities that implemented recovery protocols experienced a 40% reduction in downtime during cyber incidents (Alharbi, 2022).

1.8 Research Contributions

This section outlines the research contributions to theories and methodology from the findings obtained and the methods employed in this study.

1.8.1 Contributions to Theories

The main contribution of this study lies in theory-building and integration. The theories underpinning this study are the Broaden and Build Theory (BBT) and the Protection Motivation Theory (PMT), which extend the BBT by integrating PMT into the model and developing a model to explore the influence of negative and positive emotions on employees' self-efficacy and protection motivation behaviour in cybersecurity. This study contributes to the theories of BBT and PMT by exploring how negative and positive emotions influence employees' self-efficacy and motivation to engage in cybersecurity protection behaviour. The proposed model aim to explore the influence of negative and positive emotions on employees' self-efficacy and protection motivation behaviour across various cultural settings. Therefore, future researchers aiming to explore the influence of negative and positive emotions on self-efficacy and protection motivation behaviour in cybersecurity could utilise the proposed framework in this study (see Section 3.8). In addition, this study could serve as an invaluable foundation for

future research and provide a broad understanding of the influence of emotions on cybersecurity protection motivation behaviour. Furthermore, this study contributes to the existing body of knowledge by providing findings that address gaps insufficiently explored in academic journal articles. Thus, researchers may use the findings of this study as a basis for exploring the heterogeneity of employees, specifically regarding protection motivation behaviour in cybersecurity.

The original and confirmatory contributions of this study manifest in multiple aspects. Firstly, this research contributes to the body of knowledge by extending and either validating or challenging existing findings on protection motivation behaviour in the cybersecurity field. Furthermore, this research confirms or denies previous knowledge related to employees' motivation to engage in cybersecurity protection behaviour in the higher education sector. Another aspect of originality in this study lies in its participants, as it uniquely explores the influence of emotions on cybersecurity protection motivation behaviour from the perspective of administrative and academic staff in the higher education sector. Moreover, to the best of the researcher's knowledge, the Systematic Literature Review (SLR) in this study is the first of its kind within the cybersecurity protection motivation behaviour field (Alshammari et al., 2023). Finally, this study is the first to explore the influence of negative and positive emotions on cybersecurity protection motivation behaviour and self-efficacy among Saudi Arabian employees in the higher education sector, based on the proposed framework.

Hence, the framework presented in this study provides a valuable tool for academics, scholars, and researchers to empirically explore the influence of emotions on cybersecurity protection motivation behaviour among employees in different sectors and contexts.

1.8.2 Contribution to Methodology

This thesis makes a significant methodological contribution by creating and verifying a novel survey instrument. This study utilised survey items sourced from several disciplines and then modified them to align with the specific cultural setting of Saudi Arabia. In addition, this research contributes to the body of knowledge by adding six more positive emotion items to the scale: interested, strong, active, determined, alert, and proud. The survey undertook multiple validation processes, including face validity with four academic experts, pilot research involving 64 employees, and an overall study with 383 employees. The survey items showed adequate levels of indicator reliability, construct reliability, convergent validity, and discriminant validity. Additionally, the instrument was translated into Arabic, the primary language of the target population. Therefore, there are two copies of this instrument, one in Arabic and one in

English, that other studies can utilise (see Appendices A and B). Hence, future studies can reproduce and authenticate the survey in diverse cultural settings

1.9 Research Process and Thesis Structure

According to Bryman and Bell (2015), the research process is the plan for the researcher's activities from study start to finish. Therefore, researchers must create a design that meets their research aim and objectives (Sekaran & Bougie, 2016). Figure 1 shows the research's flowchart.

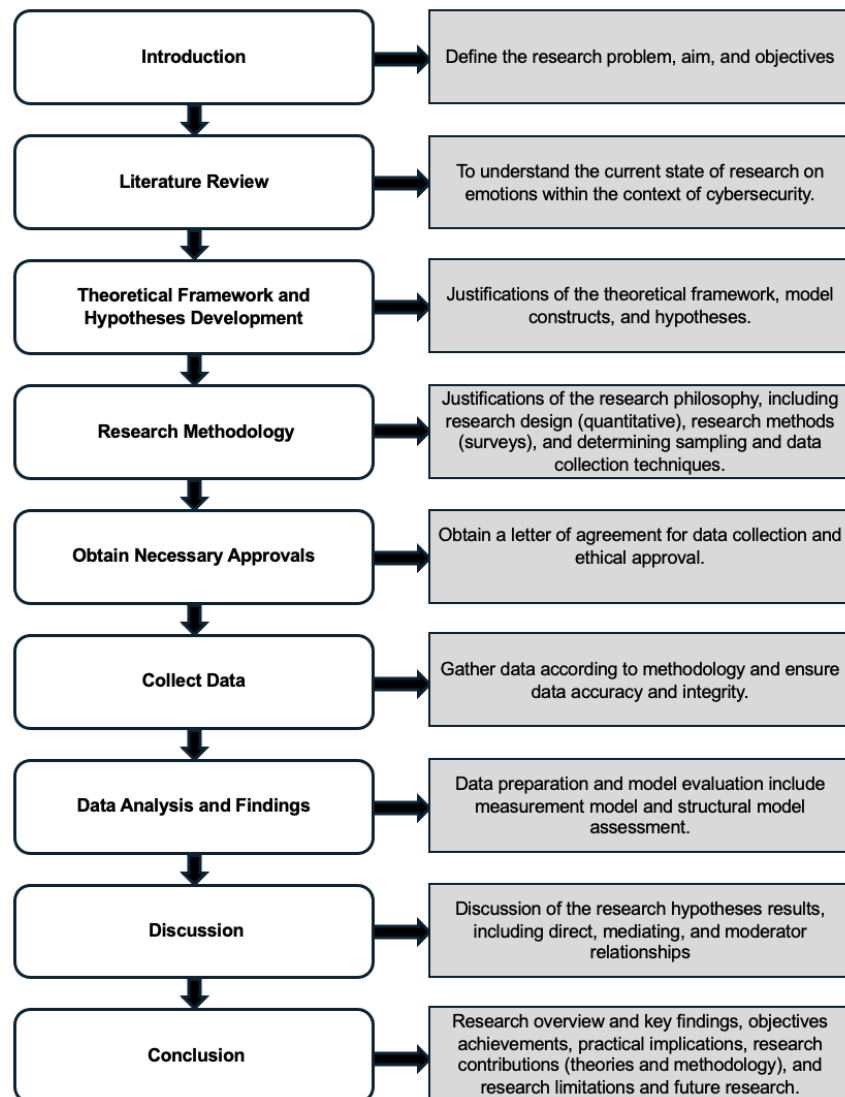


Figure 1: Research's Flowchart.

Based on the research process, this thesis is organised into seven chapters, each detailed below, ensuring a clear and logical research sequence.

Chapter One: Introduction - This chapter introduces the research by outlining its problem, motivation, questions, aims and objectives, and research process. Additionally, it explores the

study context by providing an overview of the recent changes and advancements in Saudi Arabia, focusing on education and cybersecurity.

Chapter Two: Literature Review - This chapter provides an introduction and contextual background on the core areas that form the foundation of this research: emotions, cybersecurity, and a systematic literature review about emotions and cybersecurity. The chapter began with emotions, including definition, functions, components, and categorisation. Then, it explores the literature about cybersecurity, encompassing definitions, importance, cybersecurity threats, and the classification of threats. Moreover, it presents the thorough analysis of human cybersecurity behaviour followed by cybersecurity in higher education. Finally, an SLR is conducted on emotions and cybersecurity to examine their effect and find the research gap, building a theoretical framework based on the common theories used to study protection motivation behaviour.

Chapter Three: Theoretical Framework and Hypotheses Development - This chapter aims to develop and validate the theoretical framework. The research framework is established based on the results of the SLR. The conceptual framework is established with hypotheses based on the common theories used by researchers in SLRs, which are the PMT and BBT.

Chapter Four: Research Methodology - This chapter outlines the rationale behind the selected research philosophy, approach, methodological choices, research strategy, population and sample, as well as the instruments, data collection, and analysis methods employed.

Chapter Five: Research Findings - This chapter presents the analysis and findings gathered from the data. The chapter's initial section addresses the preliminary data analysis. Additionally, it provides an overview of the participants' characteristics and the statistical analysis of the variables. Additionally, it presents the outcomes of evaluating the research conceptual model using the PLS-SEM approach with SmartPLS 4 software.

Chapter Six: Discussion - This chapter discusses the research results collected in Chapter Five and links the findings to the current body of literature. Moreover, it discusses employees' demographic differences to understand the effects clearly.

Chapter Seven: Conclusion - The final chapter addresses the research questions, aims, and objectives after the results. It summarises the research findings and discusses the research's practical implications. Moreover, it discusses the methodology. The chapter concludes with research limitations and proposes directions for further research.

Chapter Two: Literature Review

2.1 Introduction

This chapter aims to overview the existing literature on emotions and cybersecurity. Therefore, it begins with the definition, function, and components of emotions, providing the foundation for interpreting their significance in human conduct. In addition, it examines several emotion categorisation models, such as the basic emotions model, dimensional model, and componential model, as well as other emotional categories suggested in psychological studies. Following this, the chapter focuses on cybersecurity, including its definitions, importance, threats and classification. Following that, it discusses human cybersecurity behaviour and then the status of cybersecurity in higher education. Then, the chapter concludes with a systematic literature review on the relationship between emotions and cybersecurity.

2.2 Emotions

2.2.1 Definitions of Emotion

Emotional states are essential components of the human experience, impacting cognitive processes, behaviours, and relationships with other people (LeDoux, 1989). Several theories and models developed by researchers drawn to these complicated phenomena have explained their nature, function, and classification. The particular significance of emotion has been a topic of debate among academics, indicating the complex and diverse nature of emotions. Emotions are short-term psychological conditions consisting of changes in subjective perception, physiological arousal, and behavioural expression (Stanley & Burrows, 2001). Moreover, Ekman (1992) offers one of the most influential definitions of emotion, defining emotions as fleeting, mutual psychological experiences that prepare people for adaptive reactions to external cues. Scherer et al. (2001) provides another definition, defining emotions as complex, multi-systemic experiences that involve organised changes across several areas, such as cognitive evaluation, physical responses, action tendencies, and personal evaluation. Ekman (1992) indicates that emotions are inherent and universally experienced, with specific "basic emotions" such as happiness, grief, dread, rage, astonishment, and disgust acknowledged in nearly all cultures. This explanation highlights the physiological foundation of emotions and their function in supporting survival by prompt, automatic reactions to crucial situations. According to Scherer et al. (2001), the component process model of emotion emphasises the level and integrative characteristics of emotions, indicating that emotions are not restricted to affective states but include integrated activity across several systems. These emphasise the significance of cognitive appraisal in creating and differentiating emotions, indicating that the meaning given to a specific event or stimulus

is vital for influencing the emotional response. Nevertheless, several theorists explain emotions by considering their social and social functions. For instance, Averill (1980) states that emotions are social constructions that control interpersonal conduct and maintain social structure. From this point of view, emotions are not controlled by biology but are influenced by cultural norms and expectations, and they have a crucial function in regulating social interactions. Averill's (1980) definition emphasises the significance of the social environment in the perception and expression of emotions, implying that emotions are strongly linked with cultural and social events. While these definitions provide valuable understandings of the nature of emotions, they also show the wide range of angles within psychology. Several definitions highlight emotions' biological and evolutionary foundation, while others focus on their cognitive, social, or communicative functions (Shariff & Tracy, 2011). Therefore, the variety of views emphasises the complex nature of emotions and the difficulties of formulating a unified definition that includes all the elements of emotions.

2.2.2 Functions of Emotion

As a component of cognitive processing, emotions influence human interaction, including decision making (Oatley et al., 1996). In addition, emotions serve other vital purposes, including signalling the presence of events that are essential to individuals (Frijda, 1994). Emotions have several significant functions, and there is general agreement that the evolution of emotions has helped organisms survive by allowing them to effectively respond to ecological concerns such as the need for food, shelter, partners, and protection (Frijda, 1994). Emotions' motivating functions are displayed in many contexts, mainly through love, which encourages approach impulses and socialising; fear, which stimulates protective responses; and remorse or shame, which inspire pro-social behaviours, avoiding their recurrence (Carver & Harmon-Jones, 2009; Frijda, 1986; Strongman, 1996). Emotions have been recognised to encourage social communication and regulate social controllers (Ekman, 1992; Hess, 2001; Keltner & Haidt, 1999, 2001). According to Keltner and Haidt (2001), emotions develop in reaction to societal issues and serve to remedy those same problems.

It is also suggested that emotions influence how people think. Izard (1991) states that emotions constitute thoughts that drive and organise view, thinking, and behaviour, facilitating the correct response to the circumstance that provoked the emotion. Damasio (1994) emphasises the impact of emotions on cognitive functioning, especially in advanced mental activities like judgement and organising. Additionally, emotions serve to arrange objectives by making individuals pause their current actions when an emotion is experienced (Oatley & Johnson-Laird, 1987). The circumstance that triggered the emotion must be resolved. Also, emotions tell a person how to respond to their current circumstances, which helps them make

decisions (Clore, 1994; Clore & Palmer, 2009). The decision taken enables people to respond correctly to the emotionally charged scenario. It is crucial to remember that such decisions and moods are all influenced by emotions like melancholy, happiness, boredom, rage, or irritation. These feelings persist briefly, occasionally for much longer, but they are always powerful, complicated, and sometimes life changing. For example, they motivate people to behave in specific ways and with the tools and resources they need to interact successfully in their social surroundings. Engaging in emotional interactions can have significant societal consequences, such as assisting in maintaining and developing beneficial relationships or, in other situations, being the source of opposition and discord (Fredrickson, 1998).

Emotions can be expressed as individuals' subjective experiences of emotions. Individuals are consciously aware of their emotions and can perceive them as complex background emotions that might influence their mood (Barrett, 2017). From a psychological angle, emotions may have various impacts on the body. This includes changes in respiration and hormone production, which can be seen in addition to changes in blood pressure and heart rate. An individual's experience of emotions is influenced by physiological sensations or changes experienced during emotional states (Levenson, 2014). Besides body language, facial expressions, tone of voice, and gestures, emotional state is also expressed through body language. These expressive behaviours can also provide cues to ourselves about a person's emotional states and intentions (Ekman, 1992). Emotions evaluate a situation or an event's significance as part of cognitive processes as well as the meaning and relevance of a stimulus and its benefits and harms, and they determine an emotional reaction (Lazarus, 1991). Emotions perform various functions in a person's life and are integral to a person's existence, as well as their survival, social connection, and psychological health. The adaptive, communicative, regulatory, and motivational domains comprise the four basic categories into which these functions fall (Izard, 2007), and these are studied in detail in the following subsections.

2.2.2.1 Adaptive Functions

Emotions have a fundamental role in allowing adaptive reactions to environmental challenges. According to Cosmides and Tooby (2000), emotions can be viewed as distinct modes of operation that have developed over time to improve survival and the success of development. The idea behind the development of emotions like fear, anger, and disgust is that these feelings help humans to avoid dangerous substances, protect themselves against threats, and react to dangers in an effective way (LeDoux, 2012). For instance, fear is an affective state motivated by recognising potential harm and it is linked to various physiological and behavioural reactions that prepare the person to either engage in a fight or escape (LeDoux,

2012). A person's ability to react quickly and effectively to the threat is improved by these reactions, which include raised heart rate, increased vigilance, and cognitive narrowing. Anger is an emotion commonly aroused by the feeling of injustice or danger to one's social position, and it drives actions aiming to either control or solve the perceived injustice (Averill, 1983). The adaptive functions of emotions are evidence of their significance in supporting appropriate reactions to environmental challenges, hence improving survival and reproductive success. Furthermore, emotions help the immediate response to dangers and have a crucial influence on long-term behaviour and decision making. According to Keltner and Haidt (1999), feelings like pride, guilt, and shame, for instance, are believed to have evolved to promote social cooperation and compliance with cultural norms. These feelings motivate people to behave in ways that align with the requirements of their social group, which improves unity among individuals and reduces the chance of conflict. As a result, emotions work as internal drivers, encouraging behaviours that benefit the individual and the social group.

2.2.2.2 Communicative Functions

In communication, emotions are crucial as they expose an individual's internal state and intentions (Aksan et al., 2013). This is important in social contexts when the capability to identify and recognise the emotions of people is necessary for successful communication. Ekman (1992) indicates that facial expressions reveal that specific emotional displays, such as smiling, frowning, or scowling, are interpreted similarly in numerous cultures. According to Ekman (1992), these expressions are used as cultural signals to enhance group social interaction and collaboration. A smile communicates peace or approval, whereas a scowl may indicate displeasure. Expressing an individual's emotions helps to direct social interactions and promote collaboration, but facial expressions alone are insufficient to express emotions—they can also be communicated by touch, tone of voice, and body language. One's tone of voice may express various emotions, including affection and happiness, as well as anger and frustration (Mulligan & Scherer, 2012).

Likewise, language and body language may express essential details about a person's emotional state, including whether they are angry, nervous, or relaxed (Davitz, 2013). According to Hertenstein et al. (2006), physical contact is an additional powerful method of expressing emotions, with various forms of touch projecting different emotional meanings. For example, a slap may indicate violence or rage, but a warm hug may represent comfort and warmth (Hertenstein et al., 2006). Emotions have a communication function beyond interpersonal interactions and are vital for regulating social organisations. Tracy and Robins (2004) propose that emotions such as pride, shame, and guilt function as social signs that either strengthen or discourage specific actions within a group. For instance, pride might

transmit to others that an individual accomplished a highly esteemed societal goal, increasing their position within the group, while shame might indicate that an individual has violated a societal norm, resulting in societal shame or rejection (Tracy & Robins, 2004).

2.2.2.3 Regulatory Functions

Emotions are crucial for regulating cognition, behaviour, and physiological functions. Emotional regulation refers to how humans maintain control over their emotional reactions' strength, duration, and appearance (Gross, 2015). The regulatory role of emotions has implications for maintaining psychological well-being and controlling adaptive functioning in response to developing environment requirements. One mechanism through which emotions regulate cognition is their impact on attention and memory functions (Tyng et al., 2017). Empirical studies have demonstrated that emotions may enhance the technique of encoding and retrieving emotionally significant information to enhance recall for situations that generate emotion (Christianson, 1992; Chrousos et al., 2013). For instance, individuals are more susceptible to remembering events linked to intense emotions, such as a distressing tragedy or a jubilant celebration, than neutral events (Kensinger & Schacter, 2008).

Furthermore, emotions are involved in the control of decision making and problem-solving processes (Naqvi et al., 2006). Research has demonstrated that emotions can affect how people consider benefits and risks; positive emotions motivate people to consider more chances and be more positive, whereas negative emotions can render people more cautious and risk-averse (Keltner & Haidt, 1999). The regulatory purpose of emotions is to influence behaviour in a way that reflects an individual's set objectives and motivational conditions (Thompson, 1994). According to Sapolsky (2004), emotions control cognition and behaviour and regulate physiological processes. Stress and anxiety, for instance, are linked to the arousal of the adrenal gland, resulting in changes in the body, such as increased heart rate, raised blood pressure, and intensified alertness (Sapolsky, 2004). These bodily responses prime the body to react to perceived dangers or challenges, but if they are long-term or excessively high, they can have negative health implications, such as increasing the risk of heart attacks or weakening the immune system. On the other hand, the parasympathetic nervous system is activated in response to the experience of positive emotions such as joy and happiness (Fredrickson, 2001). This response results in relaxation, decreased arousal, and improved recovery from stress (Fredrickson, 2001). The regulatory role of emotions emphasises their crucial role in maintaining physiology and enhancing the quality of living and overall well-being.

2.2.2.4 Motivational Functions

Emotions are complexly linked to motivation, functioning as effective drivers of behaviour (Weiner, 2012). Moreover, Weiner (2012) indicates that the experience of emotions has the combined effect of motivating and guiding human behaviour, therefore impacting the objectives that individuals aim for and the methods they use to achieve those objectives. The motivational role of emotions is essential in both approach and avoidance behaviours, where emotions function as signals that encourage or discourage specific actions according to the expected outcomes (Pessoa, 2009). Positive affective states, such as happiness, excitement, and love, are often linked to approach behaviours (Carver & Scheier, 1990). These emotions are usually generated when persons predict or achieve positive results, and they drive actions that aim to attain or maintain these results (Elliot & Thrash, 2002). The feeling of joy resulting from accomplishing a primary objective could encourage the behaviours that played a role in that success, encouraging individuals to stay motivated when seeking similar objectives in the future (Ashby et al., 1999). Likewise, emotions of love and affection may motivate actions that enhance interpersonal relations, such as investing time in close relationships or engaging in acts of kindness (Fredrickson, 1998). Nevertheless, avoidance behaviours are linked to negative emotions like fear, anger, and disgust (Lazarus, 1991). Perceived risks or undesired outcomes trigger these emotions, motivating behaviours to minimise or prevent these effects. For example, fear may cause avoidance behaviours to avoid dangerous circumstances, but disgust can drive behaviours that prevent interaction with harmful substances or viruses (Rozin et al., 2008). Anger may sometimes result in aggressive actions in contentious situations, and it also helps to remove barriers or threats that are seen to be preventing the achievement of objectives.

Furthermore, the motivational role of emotions includes much more complex and permanent objectives in which emotions function as internal directions that coordinate actions with individual principles and goals. For instance, guilt and shame are strongly associated with moral conduct, motivating people to behave in line with ethical norms and to address violations of these norms (Tangney et al., 2007). Similarly, pride and satisfaction can inspire someone to work for success and aim for accomplishments that are highly valued personally and socially (Tracy & Robins, 2004). Through this mechanism, emotions function as natural motivations, pushing actions consistent with long-term objectives and principles. The relationship between emotion and motivation is also apparent in the "emotion regulation" concept when individuals purposefully modify their emotional reactions to achieve desired outcomes. Several emotion regulation techniques, including reappraisal, suppression, and distraction, successfully regulate emotions and enhance goals and overall well-being (Gross, 2015). For instance, appraisal is the method of revising a situation in a way that changes its emotional effect, such

as understanding a challenging attempt as a chance for personal development rather than a danger. Emotion regulation helps individuals to maintain focus on their objectives, continue in a challenging set of circumstances, and adapt to changing conditions in ways that encourage achievement and general well-being.

2.2.3 Components of Emotion

As a superordinate category, "affect" is frequently applied to various states that include relatively fast positive to negative instances of discrimination (Figure 2). These include essential stress reactions, emotions, and moods, as well as various motivating impulses related to appetite, sex, violence, and pain (Gross & Thompson, 2007). Psychologists include moods, attitudes, and affective style, including temperament, under the superordinate effect category (Davidson et al., 2009).

The terms "affective state," a specific "mood", or experiencing a given "feeling" or "emotion" appear to have numerous meanings and descriptions. Some people consider the four phrases synonymous, while others believe they differ in their level of intensity. The idea that affective states, moods, emotions, and feelings serve as indicators of and triggers for behavioural change is frequently a source of disagreement (Smith & Lazarus, 1990). The evaluation that views emotion and mood as different sorts of affective experiences appears to be the most accepted.

In some studies of emotions, terminology like mood, feelings, and affect are frequently used interchangeably. However, it remains necessary to define what constitutes an emotion and what does not. This assumes that emotions may be differentiated from concepts such as general influence and mood. Emotions are short and physiologically intense, whereas moods are longer lasting and have less intense physiological responses (Mulligan & Scherer, 2012). Moreover, moods are considered diffused and more challenging to link to a particular source, while emotions are frequently supposed to be focused on distinct things like people or events. According to Beedie et al. (2005), emotion and attitude have several significant differences. Firstly, emotions are brought on by particular events, whereas attitudes are less clearly defined. Second, feelings are strong, but moods are softer emotional experiences, and feelings are object-directed while moods typically lack objectivity. Third, emotions are assumed to be related to apparent differences in physiological response, whereas moods are not. Fourth, emotions are temporary and volatile, but moods tend to become stable over time. Finally, emotions are transient and temperamental while moods are always consistent.

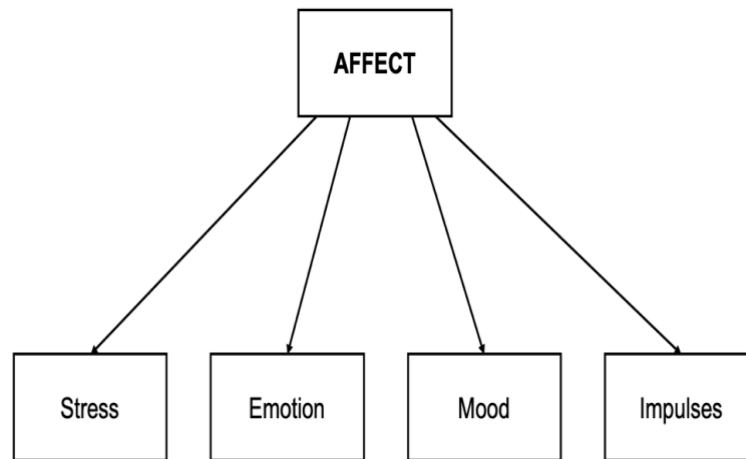


Figure 2: Affective Processes and Emotions (Gross & Thompson, 2007)

2.2.4 Categorisations of Emotions

The categorisation of emotions has been an essential topic in affective science. Several models have been suggested to categorise and differentiate a wide range of emotional experiences. Scientists have focused on understanding emotions and they have attempted to categorise several kinds of emotions. Darwin (1872) was considered the first researcher interested in studying emotions scientifically. He acknowledged that emotional expression might play a significant role in people's daily lives, such as in self-protection and continuing survival. People can effectively evaluate and respond in situations when they understand the emotional displays of others. Based on various dimensions or criteria, emotions can be classified differently. According to Borod (2000), several ways of categorising emotions exist in the literature, such as discrete emotions, which contain circuit models and basic emotions models, the dimensional model of emotions, the componential model of emotions, social constructivist models, and other emotion categories. Each model offers different perceptions of the complex nature of emotional experiences and the systematic organisation of emotions.

2.2.4.1 Discrete Models of Emotion

2.2.4.1.1 Circuit Models

Circuit models, developed from neuropsychological research, suggest that fundamental emotions and their variations are influenced by neural circuits established during evolution. The first studies on the mapping of these emotional circuits in the brain were carried out by Cannon (1927), followed by Papez (1937) and Arnold (1960). In the past, prominent researchers like Panksepp (1988) made significant contributions to this field. Panksepp (1988) categorised emotions into four main circuits, known as emotive command systems: fury, fear, expectation, and panic, each associated with specific types of behaviour. The author observed

that the relationships between these circuits can result in complex emotions that combine elements from the central sensory systems. This model adjustment becomes crucial as the focus moves from lower mammals to primates, including humans. Grey, focused on the biological foundations of attention and reinforcement.

2.2.4.1.2 Basic Emotions Model

Basic emotions are fundamental to human psychology, as they are innate and universally experienced. Physiological responses and expressive behaviours that convey these emotions share a biological basis. The concept of basic emotions forms a framework for understanding the fundamental emotional experiences that people universally experience, and this has significant influence in psychology and emotion research. According to Ekman (1992), six basic emotions may be identified from facial expressions: happiness, sadness, anger, fear, disgust, and surprise. It has been recognised that these emotions are cross-culturally universal across various cultures, as seen in Figure 3.



Figure 3: Basic Emotions Model (Ekman, 1992)

Carroll Izard has also made significant contributions to the study of basic emotions. The broader list of emotions included joy, interest, surprise, sadness, anger, disgust, contempt, fear, shame, and guilt (Izard, 1971). Izard argues that the importance of these emotions in human emotional development and functioning is biologically based. There is empirical support for the idea that basic emotions can be recognised. Researchers from different cultures have accurately identified and recognised basic emotions by analysing facial expressions (Ekman, 1992). Izard (1971) posits that these emotions emerge as early as birth and play a significant role in social interaction and communication (studies on infants and young children). In effective communication, it is essential to understand how basic emotions

are experienced. This includes physiologically and subjectively, as well as how they are expressed. For example, expressions of happiness, including laughing and smiling, are linked to positive emotions and well-being. Conversely, sadness can be expressed as tears, a depressed face, a negative valence, or disappointment or loss. Therefore, many theories and models can be applied to emotion research; however, the concept of basic emotions has played a significant role. It has been suggested that there are different sets of basic emotions or that emotions should be viewed as dimensions rather than discrete categories (Barrett, 2006). It is also possible for emotions to be experienced and expressed differently depending on culture and individuality.

2.2.4.2 Dimensional Model

Emotions can be categorised as continuous dimensions in dimensional models. Russell (1980) introduced his circumplex model, which is considered one of the most prevalent dimensional models of affect. Circumplex models are known for mapping emotions as valence (pleasantness/unpleasantness) and arousal (activation level). As a result of this two-dimensional model, emotions can be located in a broad range of locations (Russell, 1980).

Arousal and valence are continuous dimensions of emotion. Regarding valence (pleasure), which is constant, positive emotions are distinguished from negative ones. Neutral emotional states are represented by values close to zero. A zero value on the axis indicates intermediate emotional states, while a one on the axis represents active emotional states. Dimensional models represent a specific affective state by a point in dimensional space whose coordinate values range from -1 to 1 (sometimes -10 to 10 or -100 to 100). According to Whissell (2009), these two dimensions can be divided into four quadrants, as shown in Figure 4. The positive valence and positive arousal in quadrant I indicate happy, joyful, loving, contented, and satisfied emotions. In quadrant II (-V +A), anger, disgust, surprise, and fear are negative states associated with high arousal. The third quadrant (-V -A) represents a negative state of low arousal, including boredom, sadness, and depression. Positive states of low arousal are represented by quadrant IV (+V-A), including relaxation, bliss, and sleepiness.

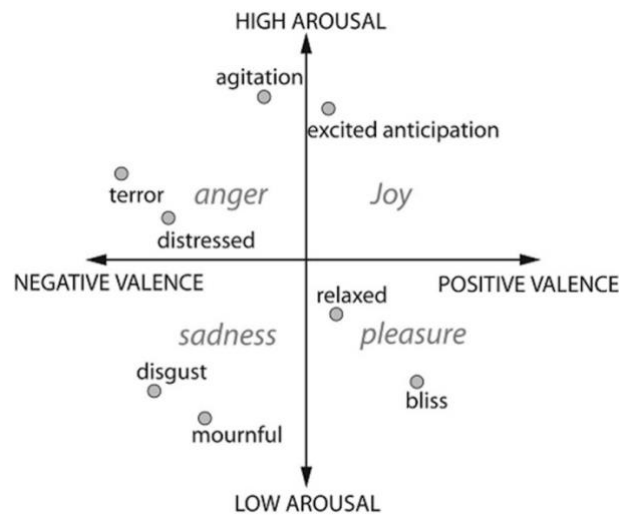


Figure 4: Whissell's Wheel of Emotion Representation Model (Rojas et al., 2006)

Moreover, valence-based categories, as seen in Figure 5, indicate that positive and negative emotions are also commonly categorised based on valence. An emotional state characterised by joy, love, or contentment has a positive valence. In contrast, an emotional state characterised by sadness, anger, and fear has a negative valence. Affective qualities of emotions are considered in this categorisation (Watson et al., 1988).

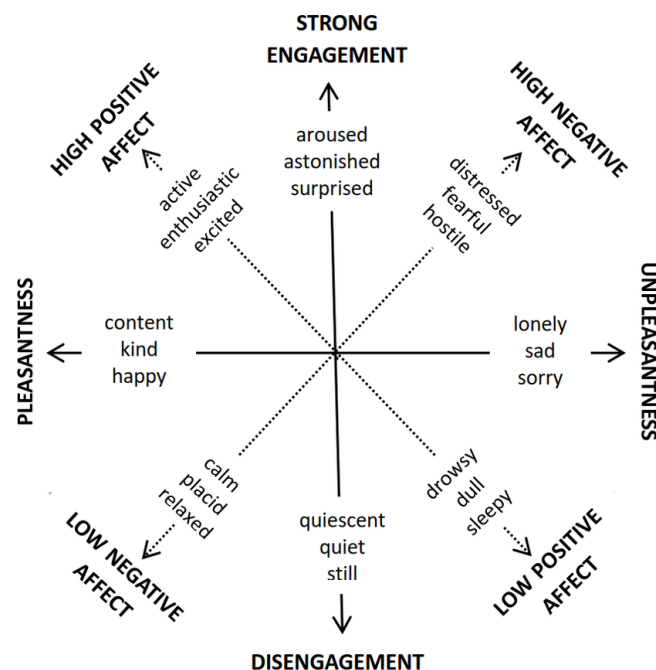


Figure 5: Circumplex Theory of Affect (Watson et al., 1988)

2.2.4.3 Componential Model

According to a component model for categorising emotions, emotions are categorised based on their underlying components. As an example of how emotions may be differentiated,

appraisal theories suggest that various factors influence them, including relevance, goal orientation, and coping capabilities (Scherer et al., 2001). Emotional experiences are analysed from the perspective of cognitive processes. Plutchik (2001) proposed that there are two types of emotions, basic and complex, in his psych-evolutionary theory of emotion. Plutchik (2001) defined eight fundamental emotions: surprise, sadness, trust, joy, anger, anticipation, disgust, and fear. In this theory, other emotions are combinations or mixtures of basic emotions, such as love, which combines joy and trust. The primary dyad of optimism is often associated with anticipation and joy, the secondary dyad of guilt is sometimes associated with joy and fear, and the tertiary dyad of pleasure is seldom connected to either emotion (Figure 7). A primary dyad is optimism, which is anticipation plus joy, a secondary dyad is guilt, which is joy and fear; and a tertiary dyad is delight, which is joy plus surprise. As a response to new-old conditions, surprise and anticipation are the most primitive emotions. Fear and anger are responses to danger, enabling one to fight or give up. Among the evolutionary emotions are joy and disgust, which motivate us to do pleasant things or protect us from unpleasant things, respectively. Sadness causes calm, and joy mobilises us to interact with others. The intensity or arousal of each emotion may differ. A visualisation is provided for the Plutchik model based on the colour wheel of emotions in Figure 6. Plutchik (2001) based the basic and advanced effects on the basic ones. Four pairs of opposites form eight basic emotions represented by the eight sectors. Emotion intensity is determined by its colour: dark shades indicate more intense emotions. In this way, the intensity of emotion increases as people approach the centre of the wheel and decreases as people move away from it. For instance, serenity would be the lowest level of joy, and ecstasy would be the highest.

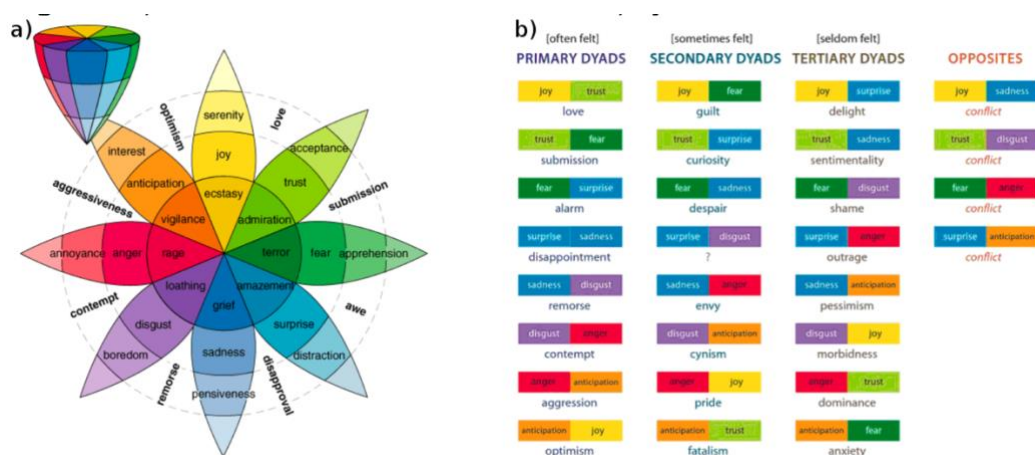


Figure 6: a) Plutchik's Colour Wheel of Emotions, b) Dyads of Emotions (Mihalinec et al., 2008)

2.2.4.4 Social Constructivist Models

An alternative method was employed by Shaver et al. (1987), building upon the research on conceptual structure (Rosch et al., 1976), to demonstrate various levels of generality in the categorisation of emotional states. They generated trees of emotion terms with varying degrees of generality by employing the cluster analysis method. The literature of theorists in this tradition needs to consistently indicate whether their primary focus is on recognising the categorisation of emotional states by those who are not experts together with the associated stereotypes or if they intend to expand the theoretical modelling to the entire emotion mechanism. Another model of emotion posits that the understanding of emotion is usually shaped by behaviour and value patterns influenced by society (Averill, 1980; Harré, 1986; Shweder et al., 2010). While recognising the psychobiological reaction components of emotion, the proponents of this approach prioritise the sociocultural context when interpreting the emotion-eliciting situation and the function of the emotional response in the individual's sense-making and social interaction. Researchers in this area are also highly interested in the emotion lexicon as they believe that the emotion labels in a language mirror the emotional meaning structures of the related culture.

2.2.4.5 Other Emotional Categories

Cultural differences in terms and concepts of emotions can also be used to categorise emotions (Mesquita & Frijda, 1992). Different cultures may categorise and conceptualise emotions differently, influencing how emotions are experienced, expressed, and valued. A sociocultural perspective on emotions highlights the influence of sociocultural factors. Experiences cannot always be neatly categorised in emotions, and categorisation does not always follow from experience. Kemper & Lazarus (1990) propose another classification of emotions, identifying ten types: shyness, fear, surprise, anger, enjoyment, sadness, interest, contempt, disgust, and shame. A similar classification is provided by Tomkins (1984), who categorises emotions into positive and negative, including surprise, fear, joy, interest, anger, distress, shame, contempt, and disgust. Frijda (1986) indicate that basic emotions are desire, happiness, interest, sorrow, surprise, and wonder. However, Johnson-Laird & Oatley (1989) emotions can be classified as anger, fear, sadness, disgust, and happiness. Similarly, Parrott (2001) state that there are different emotion classifications, which include anger, fear, joy, love, sadness and surprise. Xu et al. (2008) state that there are different emotions classifications: anger, disgust, fear, joy, like, and surprise. Based on these arguments, there is no emotional classification that has been agreed upon among many scholars, but it can be noted that the scholars have common emotions to which they have agreed. For example, fear, sadness, anger, disgust and happiness. Power (2006) indicated that there is no agreed classification for emotions, but there is a basic emotion that all scholars agreed on, such as anger, fear,

sadness, disgust, and happiness, and these five emotions might be present in other complex emotions. Table (1) summarises the classifications of emotions by among scholars.

Table 1: Emotional Categories

Author	Number	Categorisation
Izard (1971)	10	interest, enjoyment, surprise, sadness, anger, disgust, contempt, fear, shame, and shyness
Tomkins (1984)	9	anger, contempt, disgust, distress, fear, interest, joy, shame, surprise
Frijda (1986)	6	desire, happiness, interest, sorrow, surprise, wonder
Johnson-Laird & Oatley (1989)	5	Anger, fear, sadness disgust, happiness
Ortony et al. (1990)	22	fear, joy, distress, happiness, gloating, hope, pity, pride, relief, resentment, satisfaction, etc.
Ekman (1993)	6	anger, disgust, fear, joy, sadness, surprise
Plutchik (2000)	8	anger vs. fear, happiness vs. sadness, surprise vs. anticipation and trust vs. disgust.
Parrot (2001)	6	anger, fear, joy, love, sadness, surprise
Power (2006)	5 with 20 subscales	Anger, fear, sadness disgust, happiness
Xu et al. (2008)	7	anger, disgust, fear, joy, like, sadness, surprise

However, other emotions have been introduced and classified within the information technology (IT) field beyond the commonly discussed emotions. These emotions are associated with user-technological system interactions and reflect the complex mechanisms that users interact with and are impacted by in the digital environment. Beaudry and Pinsonneault (2010) introduced one of the most prominent frameworks for classifying these emotions. Their work focuses on understanding how emotions influence the use of IT during the acceptance phase of implementing new systems. Beaudry and Pinsonneault (2010) classify several emotions associated with IT usage to predict user reactions and behaviours. Furthermore, the framework examines the direct and indirect impacts of emotions on IT usage by examining the behaviours that assist users in adapting to new systems. This study extends current understanding by including emotional aspects into the conventional models of cognitive technology acceptance. The study explains emotions as cognitive states that develop from the process by which humans experience and assess events. As can be seen in Figure 7, the classification of emotions by the authors involves four primary categories: challenge emotions, which include excitement and hope, anticipation, arousal, playfulness, and flow; achievement emotions, such as happiness and satisfaction, pleasure, relief, and enjoyment; loss emotions, which include anger, dissatisfaction, disappointment, annoyance, frustration, and disgust; and deterrence emotions, including anxiety, fear, worry, and distress.

Each category reflects different emotional responses to IT experiences, which can affect user engagement and acceptance.

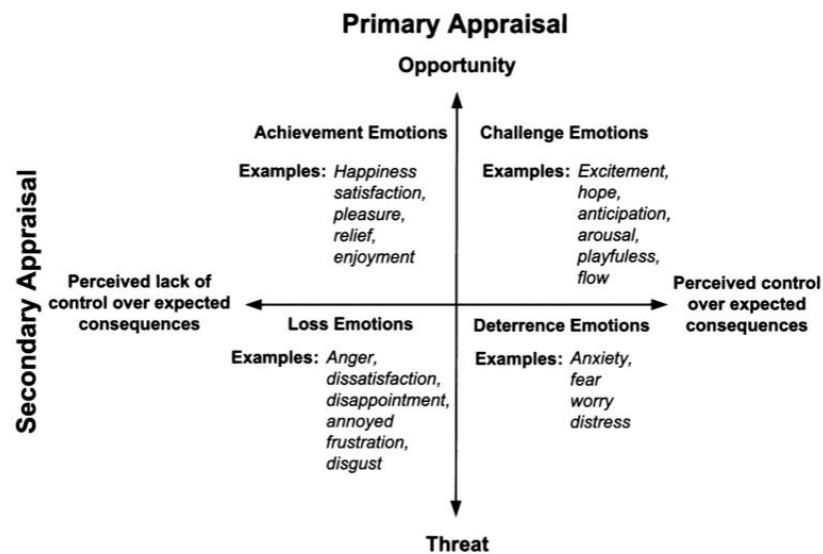


Figure 7: Emotion Classifications in IT (Beaudry & Pinsonneault, 2010)

Following the detailed examination of emotions and their influence on human behaviour, the discussion will narrow to cybersecurity. As discussed, emotions impact cognitive processes and decision making; it is therefore essential to explore emotions within cybersecurity protection motivation behaviour. Emotions have increasingly become a central focus in cybersecurity and information security research. Numerous researchers acknowledge their significant influence on decision making and behaviour, but emotions are frequently overlooked by rational approaches to understanding decision making (McAlaney et al., 2018). Research has examined the impact of emotions, including fear, anxiety, and trust, on individuals' reactions to cybersecurity threats such as data breaches, privacy issues, and phishing attempts (Boss et al., 2015; Liang et al., 2019; Vance et al., 2014). Fear appeals have been examined in security awareness research to encourage users to adopt safer online activities (Johnston et al., 2015), whereas faith in security systems may result in more complacent attitudes towards protective behaviours (Anderson & Agarwal, 2010). Positive emotions such as confidence and satisfaction are also associated with harmful online behaviours, as they may cause users to overrate the efficacy of security measures (Warkentin et al., 2011). Emotional responses to cyber threats significantly influence risk perception, as high anxiety frequently results in enhanced vigilance and defensive measures (Pfleeger et al., 2014). This research highlights the need for more studies on how emotions influence user behaviour in cybersecurity. Therefore, the following section will address cybersecurity by defining the term and emphasising the critical importance of safeguarding information and

systems. Additionally, it will explore the various threats that cybersecurity faces today. Particular attention will be directed towards the influence of emotions on cybersecurity protection motivation behaviour, thereby offering a more refined understanding of the relationship between psychological factors and security-related decisions.

2.3 Cybersecurity

2.3.1 Definition of Cybersecurity

Cybersecurity has developed from earlier fields such as information security, computer security, and data security. Information security involves protecting information from unauthorised access, disclosure, alteration, destruction, or disruption. It includes strategies, policies, and technologies designed to maintain the confidentiality, integrity, and availability (CIA) of data, whether in digital or physical form (Whitman & Mattord, 2022). As computing systems became more prevalent, computer security emerged as a key concern in the 1970s and 1980s, focusing on safeguarding hardware, software, and digital data from cyber threats such as viruses, worms, and unauthorised access (Straub & Welke, 1998). Stallings (2020) further describes computer security as "a broad field focused on protecting computing resources, ensuring data integrity, preventing unauthorised access, and mitigating potential threats to digital assets."

Cybersecurity is a broad field and has been comprehended from different perspectives since there is no universally agreed definition of cybersecurity; this is due to the numerous components that might be investigated (Wilbanks, 2007). Researchers and professionals have examined how individuals and organisations can secure their digital investments utilising internet privacy, cybersecurity, and information security. Von Solms and Van Niekerk (2013) asserted that cybersecurity and information security are frequently used interchangeably but are in fact different. There are various definitions of cybersecurity in the scientific literature and within organisations. From an educational perspective, cybersecurity is defined as a safeguard against unlawful access, utilisation, release, alterations, or deterioration of computer equipment, networks, and personal data (Gallaher et al., 2008; Yan et al., 2012). Benson et al. (2020) and Goutam (2015) define cybersecurity as protecting systems, including hardware, software and data, from cyberattacks. However, cybersecurity is defined by organisations, for instance NICCS (2022), as "the operation or procedure, abilities, or potential, or condition by which telecommunications and information systems and the information inherent therein can be safeguarded and protected from destruction, unauthorised use or alterations, or misuse."

Cybersecurity has been regarded as a component of information security strategies, covering the three required domains: data confidentiality, integrity, and availability (CIA) (Verizon, 2022).

Confidentiality is about ensuring that data is only accessible to authorised people. Encryption has become a typical strategy for maintaining confidentiality, and authenticity and permission can aid with this. Integrity guarantees that information cannot be changed by unauthorised third parties (or perhaps incorrectly altered by authorised users) and that it can be relied upon to confirm data integrity. Finally, availability guarantees that information is readily available when requested. Moreover, it ensures that the structures remain available throughout a DDoS threat, in addition to fundamental data backups. Availability also implies that vital data should be preserved from deletion, such as protecting data on an organisation's public website from being erased. By identifying vulnerabilities and lowering the likelihood of security incidents, the CIA triad model assists organisations in evaluating and improving their security measures. Additionally, it is utilised to train staff members on security best practices. A security breach indicates a breakdown in one of the principles of the CIA triad, whatever the underlying cause (Yee & Zolkipli, 2021). The model is commonly used as a standard to guide security policies and processes in cybersecurity. It has been criticised, however, for focusing too much on technological restrictions and ignoring social and behavioural aspects of security (Nicho, 2018). According to Veale and Brown (2020), it only covers a subset of organisations. Despite these criticisms, the CIA triad plays a significant role in information security and cybersecurity procedures.

The three domains above have been frequently designated by the acronym 'CIA' and function well as the security foundation. Nevertheless, Ham (2021) asserts that numerous operational and scientific papers nowadays employ the CIA triad to describe cybersecurity, despite many novel methods being available. The NIST cybersecurity framework outlines a process for managing and reducing cybersecurity risk involving identifying, protecting, detecting, responding, and recovering. Identifying consists of determining the valuables that must be adequately safeguarded and understanding the setting in which these items are located. Protect focuses on establishing and implementing asset protection procedures to secure these valuables. The detect function requires putting detectors and mechanisms in place to identify when security is violated. In the response phase, organisations must specify response procedures for when an issue is discovered, ensuring that they can quickly address and mitigate the effects of a security breach. Finally, the recovery function involves creating strategies for organisational resilience and developing recovery processes to restore normal operations following an incident.

According to Ham (2021), all organisational assets must be safeguarded. Another critical component of the identification activity is assessing the assets' context, determining which

assets must be safeguarded, and considering how the safety precautions may affect the current procedures. In the structure, safeguarding is only one of the operations, not the primary focus. This method contextualises the preventive measures, making them part of a larger picture. Detect, respond, and recover operations require understanding that security is never absolute. Some risks are too expensive to protect against, so they should be addressed through detection, incident response, and recovery activities. The method also compels one to recognise that security is never flawless. Thus, extra safeguards should be implemented to minimise the sinister implications of other precautions that may fail. According to Shen (2014), NIST implementations benefit organisations. The benefits include reconciling and explaining regulations, legislation, policy, and industry best practices. NIST reduces the risk in existing information security programs by identifying opportunities for improvement. It improves efficiency and decreases confusion with clients, collaborators, vendors, authorities, and auditors.

2.3.2 Importance of Cybersecurity

Government entities, law enforcement corporations, banking organisations, colleges, and other enterprises acquire, process, and preserve a vast quantity of confidential data and other information on computer systems, which they then transfer across computers via the Internet. The global web has provided individuals, organisations, and governments with additional authority based on continually developing internet innovations in technology. According to DataReportal (2023), 5.16 billion individuals globally were using online resources at the commencement of 2023, accounting for 64.4 per cent of the total worldwide population. Furthermore, the internet-based economy is expected to continue expanding at 10% per year, alongside emerging economies growing at 12% to 25% annually (Melnyk et al., 2019). This expansion rate raises the number of potential targets for cyberattacks. Furthermore, as IT and cyberspace skills become increasingly desirable internationally, the prospective amalgamation of attackers on the internet expands. The internet provides resources for people seeking to study and improve their hacking or attacking abilities. The pool's magnitude and competence have expanded as participants trade knowledge about hacking into systems to achieve pleasure and income (Nieles et al., 2017). Spidalieri and Kern (2014) state that civilisation's dependence on the web and technological advances has revealed emerging vulnerabilities and many cybercrimes have been committed by hacker groups, criminals, terrorists, governments, and non-government organisations. Cyber assaults have targeted public and privately owned corporations and government institutions. These have severe consequences for individuals and organisations, including financial and psychological repercussions (Liang et al., 2019). IBM Security estimated in 2021 that the median cost of a

breach of information to an organisation topped US\$3.86 million (IBM, 2023). The cost had risen to US\$4.24 million just over a year later, demonstrating the growing trend of the various losses experienced due to cybersecurity intrusions. As a result, as organisations and government departments increasingly rely on computer technology and systems to gather, analyse, safeguard, and transmit information, the expertise of cybersecurity specialists has become more critical than ever in protecting online transactions for individuals and businesses (Callen-naviglia et al., 2018). According to researchers, if security is inadequate, enterprises will face an increasing number of information intrusions ranging from minor complications to those with disastrous implications for people and companies.

2.3.3 Taxonomy of Cybersecurity Threats

Cybersecurity risks, violations, and hacking attempts have been the subject of many studies. A cybersecurity threat is the possible occurrence of an unauthorised attempt to compromise or interrupt a computer infrastructure or system (Imran et al., 2018). It describes an incident that might compromise data integrity, accessibility, and confidentiality and cause harm to information resources within the system. Jouini et al. (2014) described threats that include information destruction, fraud, vandalism, the disappearance of information, prohibited utilisation, dissemination of information, refusal of utilisation, and elevation of privilege, while differentiating between internal and external dangers, human, natural, and technological hazards, nefarious and harmless dangers, and accidental and deliberate dangers. Gerić and Hutinski (2007) divided numerous threats, including invasion of confidentiality, interruptions in infrastructural systems, and unauthorised access, into four broad categories: security of the physical environment, the safety of employees, information and communication protection, and operational safety and security. A cybersecurity intrusion is defined as the "unauthorised utilisation of delicate, safeguarded, or personally identifiable information, which leads to a violation or prospective vulnerability of the exposed data's privacy, reliability, and accessibility" (Sen & Borle, 2015). Breach tactics include malicious software, phishing, spying, sniffing, Trojan horses, DDoS, and SQL injections (Imran et al., 2018). The realisation of an imminent threat as well as taking advantage of a vulnerability can be considered a cybersecurity assault (Kumar et al., 2008). It can affect hardware, the internet, and applications, and is carried out to obtain or monitor user information, or seize an infrastructure's management (Toch et al., 2018).

Numerous security attack categorisations are used in the context of information security. Hazard categorisations are required because, to safeguard information system resources, people must first understand the root causes and dangers from which people need to defend themselves (Sweigart, 2003). Security threat categorisation writers include individuals from

global, governmental, and charitable organisations, researchers, professionals, ISS specialists, etc. The NIST categorisation by Guttman and Roback (1995) is centred on ISS threat importance criteria and distinguishes the following security threats. Firstly, errors and omissions, primarily caused by deliberate mistakes made by individuals, are the most prevalent cause of missing information. Staff who regularly input several hundred records into databases can generate this sort of security threat. However, it also has the potential to occur by users in charge of multiple information sources. Second, fraudulent activities and theft are security threats that can be accomplished by automating fraud and theft or employing more sophisticated approaches. Third, employee sabotage is a widespread cause of security hazards to technological infrastructure. The most common types of sabotage include damaging facility hardware, installing logic bombs that harm software or data, wrongly inputting data, crashing systems, erasing data, retaining data as a captive, and modifying content. Fourth, loss of physical and infrastructure support can occur in various ways, including interruptions in electrical power, interruption of communications, flooding, burning materials, earthquakes, strikes, and many more. Fifth, hackers approach and (mis)use a computerised resource in a way that is not authorised. Sixth, malware, a security threat, includes virus-like programs, worms, Trojan horse infections, logic bombs, and other undesirable software. Finally, personal privacy concerns are a new sort of security hazard. Significant amounts of personally identifiable information may be maintained in various databases (e.g., governmental and private organisations, banks, and businesses). There is a genuine risk that such sensitive information will be exploited in multiple ways.

Another security threat categorisation derived from the worldwide standard ISO/IEC 17799:2005, which differentiates security risks based on their category. Four broad categories of security threats may be identified. The first category is natural sources, including earthquakes, floods, storms, pollutants, fires, and incidents. These threats are beyond human control and can cause significant damage to physical infrastructure and data systems. The second category involves technical sources, encompassing technical failures, malfunctions, communication problems, and radiation. These are often related to information systems' hardware or software components, where failures or malfunctions can lead to operational vulnerabilities or disruptions. The third category focuses on human sources, which refer to threats from human behaviour or actions. These include disobedience, recklessness, improper software use, and unsuitable organisational practices. Human errors or intentional misconduct can significantly compromise security. The final category includes potential sources such as devastation, tampering, distraction, spying, war-related destruction, fraud, stealing, and viruses. These threats can be external or internal and often involve malicious activities to disrupt, damage, or steal information or resources.

There is another categorisation offered by Miroslav (2017). The researcher used the operation or region within which the security threats concentrate as the primary consideration for determining information systems threat categorisation. Security risks may be classified into four major categories, each with multiple subsets (Gerić & Hutinski, 2007). The first category is physical security infringement. This includes ear-tapping-related communications, a security vulnerability that uses weak or non-existent physical communication network encryption, such as cables and telecommunication lines. Another subset is DDoS, which aims to reduce the functioning and accessibility of information system components. Additionally, trash digging is a non-legal security concern focused on sifting through waste for undesired and abandoned facilities. The second category is a breach of personnel security. This includes password guessing, where an attacker attempts to guess an individual's passcode and then uses it for unlawful purposes. This kind of assault may be carried out both manually and mechanically. Impersonating, commonly referred to as false identity, is another subset where one individual assumes the identity of another to gain unauthorised access to data system infrastructures. This can occur physically by using an authorised individual's identification credentials or electronically by using a computer-generated user's identification to log into an information system. Social engineering is another method used to gain unauthorised access to critical data, such as usernames, login credentials, and corporate confidential information, which may be exploited to compromise the privacy of an information system. Extortions involve various methods of extorting individuals who have access to classified information required for an information system security breach to occur. Finally, software piracy is defined as software's illicit copying and utilisation. The third category involves interference with communication and data security. This includes data attacks, which are violations against information privacy, accessibility, and validity. Software assaults, which include varieties of malicious software such as computer viruses, worms, Trojan horses, backdoors, scheduled attacks, and fraud, are also part of this category. The fourth category is an intrusion on operational security. This includes data fraud, which can be described as the illegal modification of data input before or when the data is stored in an information system. Spoofing is another security threat where intruders obtain the desired data by exploiting internet flaws and inadequate user awareness. Sniffing is an invasion of privacy that employs malicious software to examine internet traffic in search of login credentials and passwords. Searching, another invasion of privacy, employs malicious software to search computers and networks for details that may be utilised for unwanted purposes. Finally, privileged access includes the hazard posed by administrators, privileged access granted to users, and improper application of this access.

Another taxonomy has been offered by the European Union Agency for Cybersecurity (ENISA), which provides a structured approach to identifying and mitigating cybersecurity threats across several sectors. ENISA plays an essential role in strengthening Europe's cyber resilience by conducting risk assessments, developing cybersecurity guidelines, and supporting policy initiatives. The agency categorises cyber threats into different groups based on their nature, impact, and attack vectors, offering valuable insights for organisations to enhance their security position (ENISA, 2016). ENISA's threat taxonomy focuses on various cyber threats, including malware, phishing, ransomware, DoS attacks, insider threats, data breaches, and supply chain attacks. These threats often exploit vulnerabilities in software, networks, and human behaviour to compromise systems. The agency also highlights the growing risks posed by advanced persistent threats, cyber spying, and state-sponsored attacks, which target critical infrastructure and sensitive data (ENISA, 2023). ENISA also highlights operational and technological threats, such as software vulnerabilities, hardware failures, misconfigurations, and unpatched systems. These issues create opportunities for attackers to exploit weaknesses in an organisation's digital infrastructure. Moreover, human errors and insider threats, whether intentional or unintentional, remain a significant concern for cybersecurity professionals (ENISA, 2024). ENISA recognises the impact of emerging threats, including those related to artificial intelligence, internet of things security, cloud computing, and quantum computing. The agency's threat intelligence and risk management framework benefits organisations in preparing for and responding to cyber incidents through incident response plans, cybersecurity awareness programmes, and regulatory compliance measures.

Finally, The National Institute of Standards and Technology (NIST) categorises cybersecurity threats into four primary groups: adversarial, accidental, structural, and environmental threats (NIST, 2012). Adversarial threats begin from malicious actors, such as cybercriminals, nation-state hackers, and insider threats. These adversaries employ methods like phishing, ransomware, malware, DoS attacks, and supply chain compromises to pass through and disrupt organisational systems. Advanced persistent threats represent refined challengers who maintain continued access to networks, posing significant risks to organisations (NIST, 2020). Accidental threats appear from human errors, system misconfigurations, and software failures. Examples include employees accidentally exposing sensitive data, misconfiguring security settings, or ignoring to apply essential software patches, thus increasing vulnerability to exploitation. To mitigate these risks, organisations should prioritise security awareness training, apply strict access controls, and implement automated patch management processes (NIST, 2020). Structural threats arise from essential weaknesses within an organisation's technological infrastructure, including out-of-date systems and weak security design.

Vulnerabilities such as insecure authentication methods, unsuccessful encryption protocols, and dependence on legacy systems can be misused by cyber adversaries. Therefore, addressing these concerns needs systematic system updates, the founding of strong security policies, and adherence to top practices in software development (NIST, 2020). Finally, environmental threats include external factors beyond human control, such as natural disasters, power outages, and physical security breaches. Moreover, events like earthquakes, floods, fires, or theft can compromise IT infrastructure and disrupt business operations. Organisations can safeguard against such risks by implementing comprehensive disaster recovery plans, establishing redundant systems, and enhancing physical security measures (NIST, 2020).

2.4 Human Behaviour in Cybersecurity

Security behaviours include defensive behaviours as well as the usage of security technologies. According to Kearney and Kruger (2016), human information security behaviour is complex, and technological solutions alone are insufficient to resolve security challenges. Most research has focused on the technical components of security instead of security management to study the difficulties caused by hacking attempts (Waly et al., 2012). However, user behaviour is the most common reason for information security breaches. According to Karlsson et al. (2017), users are accountable for approximately fifty per cent of all security incidents, while another study estimates that insiders contribute to over eighty per cent. Human components of information security must be addressed simultaneously with technological and organisational factors to lower the risk of information security events in an organisation (Hina & Dominic, 2017; Safa et al., 2015). Some argue that many information security programs fail to allocate sufficient resources and time to understand human behaviour fully (Liginlal et al., 2009; Parsons et al., 2014). Most companies allow employees to view, alter, and move data across devices within the same or separate networks. There should therefore be policies and systems in place to prevent indiscretions that might cost the organisation money, time, and confidence. Moreover, the absence of proper information security protocols can result in employees putting organisational assets at risk (Paulsen & Toth, 2016).

Information security policies (ISP) outline professionals' protective behaviours, but there has been no agreement on suggested workplace behaviours. Nevertheless, as detailed in various studies, numerous behaviours can help to prevent cyber attacks. Key measures include user authentication, implementing security software, regularly updating all software, remaining vigilant against cyber attacks, understanding actions that compromise privacy, and ensuring secure internet connectivity. However, many IT managers focus more on technical issues and

solutions, such as proxy servers, firewalls, intrusion detection systems, and routers, than on the users they support (Katz, 2005). The focus of ISP compliance analysis has been on security technologies, but it remains insufficient without integrating behavioural and social considerations (Han et al., 2017). Human errors can lead to the failure of technological solutions, emphasising the importance of prioritising human factors (Rhee et al., 2009; Safa et al., 2015; Scholl et al., 2018; Safa et al., 2016). The security of systems largely depends on their users, and people are often the weakest link within organisations. The unsuitable use of information system components poses an immediate threat to organisational security (Lebek et al., 2013; Tatu et al., 2018; D'Arcy & Hovav, 2009). Posey et al. (2011) found several safeguard-motivated behaviours by interviewing security specialists and employees. They contend that these are voluntary actions taken to defend the information security of the worker's organisation. They reported a wide range of security behaviours that employees may be asked to undertake in their analysis and investigation. A combination of these behaviours, or an absence of involvement, may lead to a devastating security breach. Nevertheless, the existing research has overlooked employees' emotions related to defending IT resources from internal and external threats. Furthermore, greater emphasis should be placed on the organisation's role in instilling positive and negative emotions in employees regarding safeguarding their IT resources. According to Burns et al. (2017), employee behaviours are connected with their psychological orientation towards information security, and McAlaney et al. (2024) state that psychological factors influence all users' cognitive processes and behaviours in cybersecurity. This includes the decision-making mechanisms that inform attackers' target selection and the methods employed during attacks.

Organisational employees' behaviours with regard to cybersecurity are frequently considered more significant threats than external elements, such as hackers and spyware (Moody et al., 2018; Shamsudin et al., 2019; Willison & Warkentin, 2013). Security challenges stemming from employees' non-compliance have grown in complexity and difficulty for modern firms, while many have implemented information security policies (Anderson et al., 2017; Johnston et al., 2016; Khan & AlShare, 2019). Improving the effectiveness of organisations' information security policies is only possible when employees are inspired to secure their organisations' IT assets (e.g., software, hardware, and data) (Kim, 2017). There needs to be more focus on employees' emotions and the positive emotions that businesses can generate to encourage employees to protect the organisation's technological assets. Few studies have examined the influence of employees' emotions on their engagement in protective security behaviours. Therefore, more research must be conducted to explore employees' emotions and cybersecurity motivation to engage in protection behaviour. Numerous studies have investigated employees' adherence or non-adherence to Information Security Policies (ISPs)

(Siponen et al., 2014). Previous research on employees' compliance with ISPs mainly focuses on organisational control mechanisms that effectively deter their negative behaviours. This research presents a contrasting viewpoint by asserting that if employees possess a positive disposition towards ISPs, they will be inclined to comply with ISPs and actively safeguard their employers' information resources. Many organisations prioritise safeguarding their information systems, given their increasing reliance on information systems (ISs) for achieving success (Crossler et al., 2013), and researchers have recognised and recorded the importance of implementing technical security measures (Zafar & Clark, 2009). However, an ever-increasing perspective suggests that achieving adequate information security necessitates technical measures and a behavioural component (Boss et al., 2015; Hsu et al., 2015; Vance et al., 2015). The requirement to grant employees access to organisational information systems from home and mobile devices has worsened the behavioural concerns in IS security, as this entails implementing enterprise-wide systems throughout the organisation (Vance et al., 2015). The intricate security diminishes the efficiency of an organisation's centralised response from IT personnel because devices and employees are often outside their direct control. Furthermore, access to systems cannot be entirely restricted without introducing organisational inefficiencies (Vance et al., 2015).

Hence, numerous scholars in the field of information security already acknowledge that protecting an organisation's information is becoming more reliant on the security measures taken by individuals who have authorised access to its information systems (D'Arcy & Hovav, 2007; Hsu et al., 2015; Vance et al., 2015). These include employees, as well as authorised company representatives, who have access to the organisation's data assets (Moore et al., 2011; Posey et al., 2013). The increasing impact of individuals with privileged access has resulted in the development of behavioural information security (Crossler et al., 2013). This field focuses on studying the actions of humans that affect the availability, confidentiality, and integrity of information systems (Stanton et al., 2006). Identifying the factors that drive these significant behaviours has proven difficult, leading to a discrepancy between the knowledge and actions of those within the field, commonly referred to as a "knowing-doing" gap (Burns et al., 2017). Cybersecurity concerns are significant in the rapidly developing digital world. Individuals and companies are becoming increasingly exposed to cyber burglars, attackers, and other hostile actors as internet and technological connections expand. Computer malware, ransomware, phishing, and social engineering attacks are all examples of risks. It is critical to take cybersecurity measures carefully since the implications of a breach can range from monetary losses to reputational harm and even legal proceedings. A structured strategy is required to properly guard against cybersecurity risks, including technological solutions consisting of antivirus applications, firewalls, and detection systems for intrusions, personnel,

and additional user educational materials and training. Several studies have focused on cyber security, and their investigations reveal a high level of awareness of cyber attacks, their types and causes, as well as relevant mitigation measures to counter any cyber-related attacks.

There are several limitations of the existing work within cybersecurity and IT. Existing research in cybersecurity has mainly focused on technical solutions such as encryption, firewalls, and intrusion detection systems, often neglecting the human element of security. While these technical measures are essential, they do not fully address the behavioural and psychological factors that influence employee compliance with security policies. Many studies have explored cybersecurity threats and countermeasures from a purely technological standpoint, failing to consider how emotions, self-efficacy, and awareness shape protection motivation behaviour (Rogers, 1983). Within IT more broadly, research has traditionally prioritised system functionality, network security, and software vulnerabilities, overlooking the role of human behaviour in risk mitigation. Studies examining IT user behaviour often assume rational decision making, yet employees frequently make security-related choices based on emotions, social influences, and perceived self-efficacy (Anderson & Agarwal, 2010). The lack of comprehensive research on these psychological and emotional factors has created a gap in understanding how organisations can effectively implement security policies that account for human behaviour (Von Solms & Van Niekerk, 2013).

This research addresses these gaps by integrating behavioural science with cybersecurity policy development. By examining how emotions influence cybersecurity motivation, the study extends existing models of protection motivation behaviour to incorporate psychological insights (Johnston et al., 2015). Additionally, by recognising the moderating role of cybersecurity awareness and the mediating effect of self-efficacy, this study provides a general approach to cybersecurity compliance. The findings contribute to both cybersecurity research and IT policy development by offering evidence-based recommendations for designing policies that align with employee behaviour and motivation.

Furthermore, cybersecurity has received scant attention in the context of higher education, especially concerning employees. Several studies focus on protecting student information and institutional systems, but more research is needed into the cybersecurity risks that higher education employees face, given the highly confidential nature of the information they hold and process. Employees, including academics and administrators, often access sensitive data, which, in turn, makes them easy targets for cyberattacks. Understanding the cybersecurity threats encountered and providing essential tools and training are vital for preserving the integrity and security of educational institutions in a progressively digital

environment. The following section will examine the current literature on cybersecurity in higher education, first generally and then focusing on Saudi Arabia.

2.5 Higher Education and Cybersecurity

According to Bongiovanni (2019), colleges and educational facilities have massive computational capacity and provide unrestricted access to the people they serve and the public, making them vulnerable to cyber assaults. Furthermore, university and academic institution IT infrastructure enables geographically separated scholars to collaborate and access enormous quantities of information as well as virtual resources for computing (Ulven & Wangen, 2021). Additionally, universities and educational institutions around the globe have international and national learners and personnel, and these employees and learners have respective academic accomplishments (Hina & Dominic, 2016). Causes of failure in higher education institutions to protect confidential information include the absence of awareness among learners, a shortage of knowledge about the value of information, and shortcomings in reactions to predictions of current concerns (Almrezeq et al., 2021). Higher learning institutions rely heavily on security measures and appear to disregard the final consumer's conformance with the ISP requirements to ensure the safety of their educational assets (Hina & Dominic, 2016).

From the educational perspective, Kyobe (2010) investigated the variables impacting users' willingness to comply with security regulations and university guidelines, and found that policy compliance remained a big concern. He suggested that the structure's alignment criteria be implemented with regulatory requirements that would direct users' compliance in universities. Similarly, Angraini et al. (2020) found various characteristics that influence user compliance, including habits, mindsets, moral views, self-assurance from behavioural psychology and cultural factors, dedication, incentives, and costs, which may be exploited to assess how well users comply with standards for information security. Waly et al. (2012) investigated the characteristics that impact information security behaviour in three organisational categories (education, health, and business), and they found several factors that can potentially contribute to information security breaches, including organisational factors, user behaviour, reinforcement, reward, and sanctions. Multiple educational and industrial researchers in higher learning institutions have made efforts to assess information security awareness but have concentrated solely on students rather than staff members.

2.6 Saudi Arabia Higher Education and Cybersecurity

In Saudi Arabia, Almrezeq et al. (2021) evaluated the student understanding of cybersecurity and cybercrime. Their research was targeted at students who were unfamiliar with cybercrime.

Their findings suggested a rise in cybersecurity knowledge, but there were still pupils who were unaware of the issue. Alqahtani (2022) studied cybersecurity awareness across multiple universities and found that students attending Imam Abdulrahman bin Faisal University colleges had high security awareness. Moreover, they found that having knowledge of the confidentiality of passwords, internet security, and online social networking activity significantly increased learners' understanding of cybersecurity. Learners understood the significance of cybersecurity awareness. Furthermore, Alharbi and Tassaddiq (2021) investigated and assessed the extent of knowledge about cybersecurity and adherence to rules among Majmaah University undergraduate learners by employing an analytical questionnaire incorporating several internet safety factors. They found that most students did not understand basic cybersecurity principles or recommended practices for protecting their devices from malware, viruses, and fraud. Mohammed and Bamasoud (2022) emphasise the significance of increasing cybersecurity knowledge among Saudi university students to prevent cyber attacks. The results of their investigation indicate that cybersecurity expertise is critical for safeguarding the security and confidentiality of highly confidential resources. Nevertheless, technological approaches cannot address individuals' fraudulent activity. University students should be taught about cybersecurity to give them a good basis of understanding, provide them with experience of dealing with cyber threats, and fulfil one of the objectives of Saudi Arabia's Vision 2030.

Almaliki and Safari (2023) assessed cybersecurity awareness among university employees. The findings suggest that a foundational level of awareness exists, but significant knowledge gaps persist. These gaps are evident regarding specific threats such as social engineering and malware. Moreover, the research emphasised the insufficiencies of existing training programmes, encouraging practical training to meet the needs of university employees. Alotibi (2024) established a cybersecurity awareness model for Saudi students, focusing on the security risks related to social media use. This model primarily targets students, emphasising insufficient cybersecurity education within the region. Therefore, the researcher calls for enhanced policy frameworks and training initiatives to address this deficit. Alhumud et al. (2023) examined the effectiveness of cybersecurity systems in Saudi universities and explored their integration with total quality management practices. Their findings indicate that universities often need more adequate risk assessment procedures, hold poorly defined policies, and offer insufficient training programmes. This emphasises the need for a more strategic approach to cybersecurity management. Further, Sharabi (2023) investigated the protection of intellectual property in Saudi universities, while Alfalah (2023) explored the impact of internet security awareness on students' attitudes towards learning management systems (LMSs). Both studies contribute valuable insights into the current cybersecurity

practices in higher education; however, they primarily focus on external threats and system-based risks. Saeed (2023) focused on information security practices among computing students, emphasising email management and infrastructure security. Nevertheless, the focus remains predominantly on technical practices and external risk factors.

Few studies investigate employees' cybersecurity behaviour in Saudi higher education (Garba et al., 2021; Masmali & Miah, 2022). Masmali and Miah (2022) analysed and assessed the current management of cybersecurity and regulations at 10 Saudi public universities, emphasising possible incidents related to cybersecurity. They conclude with the following proposals: (1) Universities should seek assistance from international organisations to recognise challenges and develop solutions to secure data. (2) University management should implement periodic evaluations of servers, appliances, the internet, and user approaches to safeguard information from cyber issues and formulate enhancements to the service alternatives and data oversight. (3) University management must establish an IT office to prevent cyber-related problems. These steps would help to ensure that effective cyber security measures are in place. Similarly, Garba et al. (2021), made an additional attempt to analyse the prevalence of cybersecurity awareness by utilising principal component analysis (PCA) to determine the essential issues regarding awareness about information security in Saudi academic institutions. The researchers found that 87% of the people surveyed believed that providing information on a learner's results and educational background was inappropriate since this information must be kept secret, while thirteen per cent indicated that mark data might have been shared. The responses suggest a good level of awareness, but there is still room for improvement, and academic institutions must be mindful of cybersecurity risks and the need to keep material secure and not shared.

Most studies in Saudi Arabia have investigated cybersecurity awareness among students. Furthermore, most of the study's findings focused on students' understanding of cybersecurity and its effect on their behaviour. Few research investigations have been conducted to investigate employees' cybersecurity protection motivation behaviour in Saudi Arabian higher education, and as a result, this study aims to explore the influence of emotions on employees' cybersecurity protection motivation behaviour.

2.7 Emotions and Cybersecurity Systematic Literature Review (SLR)

The present research utilised the SLR methodology, ensuring the reproducibility of the findings. An SLR requires detailed planning to identify relevant papers (Kushwah et al., 2019). During this phase, researchers select target journals, define criteria for including or excluding studies, carefully reassess the selected publications, and then document the research

findings. This SLR was conducted in four stages: choosing keywords, setting inclusion and exclusion criteria, searching databases to gather relevant papers, and finally, assessing the quality of these studies using criteria before documenting the systematic review outcomes (Kushwah et al., 2019).

2.7.1 Planning the Review

Following the methodology outlined by Kitchenham and Charters (2007), conducting an SLR involves three main stages: planning, conducting, and reporting. During this study's planning stage, a protocol for article selection was established. Researchers in fields such as Business and Management, Computer Science, and Information Systems often rely on online resources, avoiding the need for traditional print media searches. For this SLR, the researcher selected the Web of Science (WoS) because of its reliable reputation and broad coverage of reliable sources across various disciplines (Bandara et al., 2015; Fink, 2019).

The research began by identifying keywords. The researcher narrowed down the domain into three components to refine the search terms: "(‘cybersecurity’ or ‘cyber security’ or ‘information security’), trigger (‘emotions’), and action (‘behaviour’, ‘protection’)." Using these keywords, the researcher identified three significant and pertinent articles through Google Scholar (D’Arcy et al., 2014; Burns et al., 2017; Liang et al., 2019). After the initial search, the researcher included additional related keywords by repeatedly and thoroughly reviewing and revising the list of identified papers. A panel of experts was formed to ensure the depth of the SLR and minimise potential biases. This panel consisted of three specialists: two professors and a researcher. The researcher consulted this panel to reach a consensus on the final list of keywords. This process was aimed at refining the search query's accuracy by evaluating the relevance and importance of terms within each component:

(‘data security’ OR ‘cybersecurity’ OR ‘information security’) AND (‘positive emotions’ OR ‘negative emotions’ OR ‘emotions’ OR ‘psychological’) AND (‘protection motivation’ OR ‘behavior’ OR ‘protection’).

2.7.2 Specification of the Study

To define the scope of the study, it is crucial to establish criteria for including and excluding studies. These criteria help to refine the pool of studies identified through the keyword search, ensuring that the selected articles are pertinent to the research questions. In the inclusion criteria, the SLR focused on articles that explored the relationship between emotions and cybersecurity. Only articles from top-tier journals, as determined by their SJR rankings, were included to ensure a collection of high-quality studies. Additionally, the study limited its

selection to English articles covering topics related to business and management, information systems, and computer science. This was influenced by literature suggesting cybersecurity is a complex issue that includes technical and human elements affecting cybersecurity behaviour (Chowdhury et al., 2020; Warner, 2012). Regarding exclusion criteria, studies were excluded if they lacked a cybersecurity context or were editorials, brief surveys, reports, books, book chapters, and notes. Articles not written in English and duplicate studies were also ignored.

2.7.3 Data Extraction

After establishing the search keywords, the researcher initiated the first search in September 2022 using the WoS. This search identified 1,809 papers, selected without regard for journal titles but based on their titles, abstracts, and keywords. Due to the continuous addition of new publications, capturing every relevant publication was impossible. Levy and Ellis (2006) recommend continually updating the literature review to include new studies. Accordingly, the search string was run throughout September 2022, and it was updated in November 2024 to ensure the inclusion of the most recent articles. Search strings were crafted using 'OR' and 'AND' connectors to search through titles, abstracts, and keywords in the WoS databases. After applying the inclusion and exclusion criteria, this SLR identified 287 papers requiring manual review. Then, a review panel refined these articles further. The experts reviewed the titles, abstracts, and keywords against established theoretical and screening criteria. Each panel member performed this screening independently to maintain rigorous attention to detail. The panel members allocated selected articles for deeper evaluation in the third phase. Most of the articles excluded at this stage were from criminology, psychology, and education. Reverse reference chaining was applied to each selected paper to ensure complete coverage. This review yielded 61 articles. The panel then recommended excluding papers that did not meet the SLR's conceptual and scope limitations. After a review of the complete texts, 14 relevant papers were selected for the SLR. Further review of their references added three more studies to the list, totalling 17 papers. Thus, detailed profiles were created for each selected study. Figure 8 illustrates the SLR process in detail.

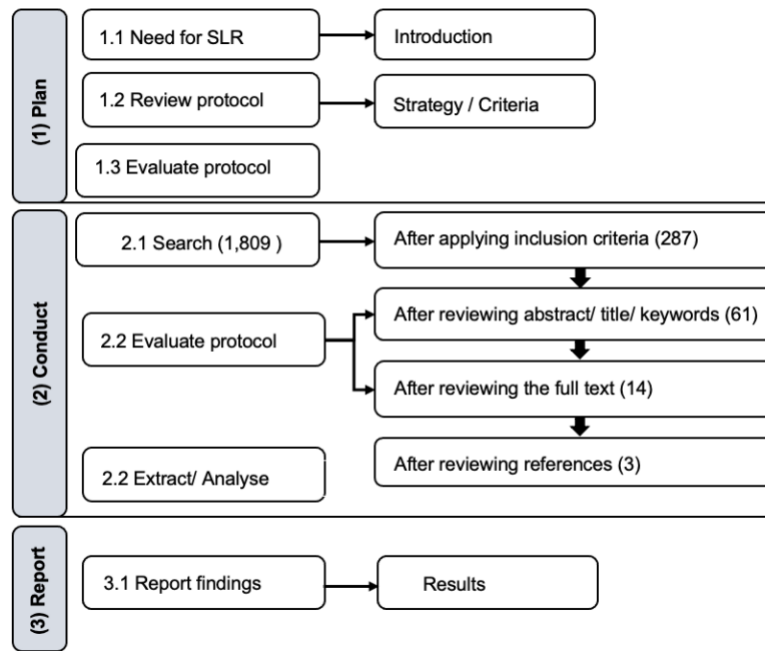


Figure 8: SLR Process and Protocols

A detailed evaluation of the selected studies was conducted, adhering to the guidelines set by Kitchenham and Charters (2007), and the quality of the primary studies was reviewed using the methodology outlined by Hosseini et al. (2017). This quality assessment was applied to five papers selected at random and included several stages.

The first stage focused on emotions, requiring each paper to examine the influence of positive and negative emotions. The second stage emphasised the importance of providing sufficient context to support the research objectives and conclusions, enabling proper analysis of the results. In the third stage, the assessment of emotions, papers needed to offer ample specific details to ensure an accurate portrayal of emotions. The fourth stage, security context, required papers to concentrate on cybersecurity or information security. The fifth stage involved the implementation of cybersecurity protective measures, assessing how emotions might affect protective behaviours. Lastly, the sixth stage, gathering data, required the methodologies used for data collection, measurement, and reporting to be clearly disclosed to ascertain data accuracy.

These quality assessment criteria were consistently applied across all the five selected studies. Additionally, the selected journals were ranked in the first and second quartiles based on SJR criteria, ensuring the inclusion of high-quality sources. The entire SLR also underwent a rigorous peer-reviewed screening process, where a secondary author evaluated the studies'

abstracts and titles. The results of the assessments, including the studies chosen for inclusion, exclusion, and quality assessment, are detailed in Table 2.

Table 2: Overview of Chosen Papers

Author	Journal	SJR
Farshadkhah et al. (2021)	Computers & Security	Q1
D'Arcy & Teh (2019)	Information & Management	Q1
Burns et al. (2017)	Computers in Human Behavior	Q1
Chen et al. (2022a)	Information & Computer Security	Q2
Zhen et al. (2020)	Journal of Business Economics and Management	Q2
Beaudry & Pinsonneault (2010)	MIS Quarterly	Q1
Gulenko (2014)	Information Management & Computer Security	Q1
Zhen et al. (2022)	Behaviour & Information Technology	Q1
Burns et al. (2019)	Information Systems Research	Q1
Liang et al. (2019)	MIS Quarterly	Q1
Xu, et al. (2020)	Information & Management	Q1
Chen et al. (2022b)	Psychology Research and Behavior Management	Q2
Menard et al. (2018)	Computers & Security	Q1
Ogbanufe & Pavur (2022)	International Journal of Information Management	Q1
Mamun et al. (2023)	Information Technology & People	Q1
Riemenschneider et al. (2023)	Information & Computer Security	Q1
Thompson et al. (2024)	Computers & Security	Q1

2.7.4 Data Execution: Research Profiling

Reviewing the number of studies published each year and their distribution across different journals provides an understanding of how research in specific fields is growing. Figure 9 shows a marked increase in studies that focus on the impact of emotions in cybersecurity. This line of inquiry started with Beaudry and Pinsonneault (2010), who authored "The Other Side of Acceptance: Investigating the Direct and Indirect Impacts of Emotions on Information Technology (IT) Usage." In 2014, Gulenko (2014) studied how emotions affect security behaviours, mainly aiming to enhance password security. In 2017 and 2018, research by Burns et al. (2017) and Menard et al. (2018) contributed two significant studies. Over the following four years, from 2019 to 2022, the field saw the addition of 10 publications. Specifically, in 2019, three papers were released by D'Arcy and Teh (2019), Burns et al. (2019), and Liang et al. (2019). The year 2020 saw the publication of two papers (Zhen et al., 2020; Xu et al., 2020).

In 2021, Farshadkhah et al. (2021) published one paper, and 2022 saw further contributions with two papers from Chen et al. (2022a, 2022b), one paper from Ogbanufe and Pavur (2022), and another from Zhen et al. (2022). In 2023, Mamun et al. (2023) and Riemenschneider et al. (2023) each published a paper, and in 2024, Thompson et al. (2024) published one paper. This trend highlights the growing awareness of the role of emotions in cybersecurity, which has attracted scholarly attention. As a result, six articles focusing on emotions in cybersecurity have been published by three different research scholars (Burns et al., 2017; Burns et al., 2019; Zhen et al., 2020; Zhen et al., 2022; Chen et al., 2022a; Chen et al., 2022b).

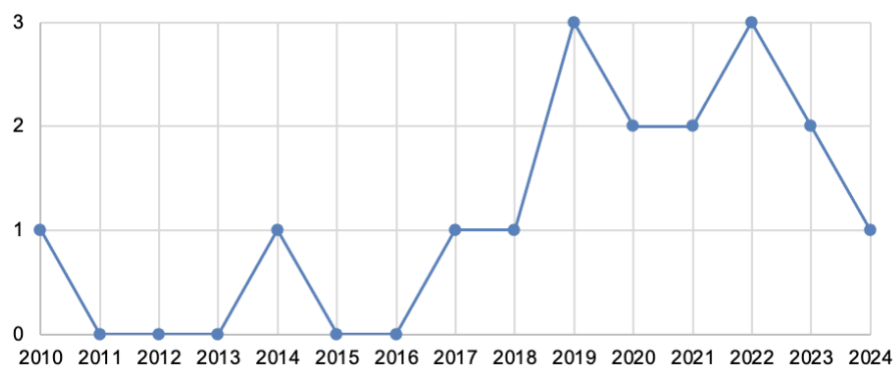


Figure 9: Cybersecurity and Emotions Publications Over Time

Figure 10 show the variety of journals that have published articles on the topic of emotions and cybersecurity. Only three journals have published more than two articles in this area. The relevant academic journals are: Computers & Security (three publications), Information & Management (two publications), MIS Quarterly (with two publications), along with Computers in Human Behavior, Information & Computer Security, Journal of Business Economics and Management, Information Management & Computer Security, Behavior & Information Technology, Information Systems Research, Psychology Research and Behavior Management, the International Journal of Information Management, and Information Technology & People.

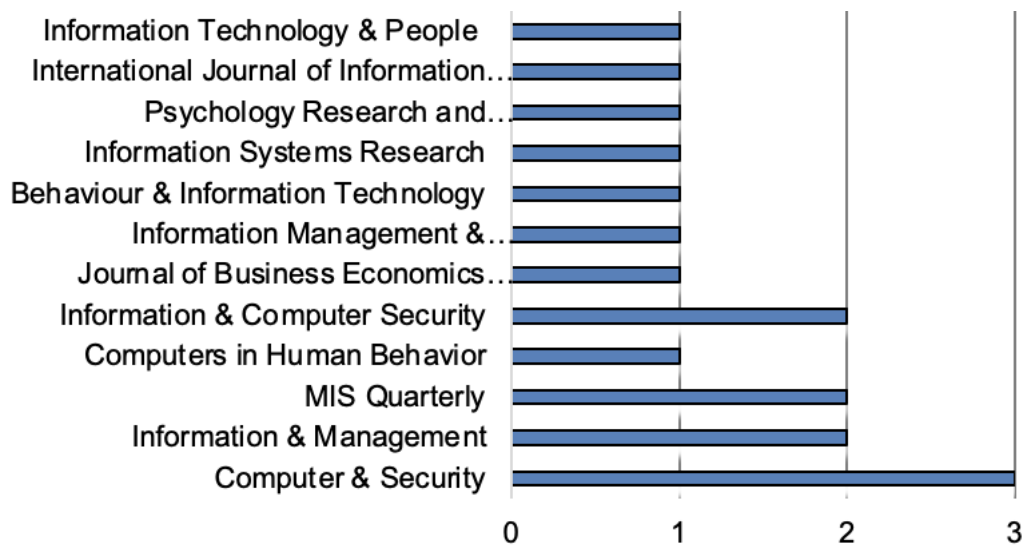


Figure 10: List of Studies Across Journals

2.7.5 Thematic Foci

The existing literature was analysed using thematic analysis, a method researchers prefer for its simplicity and flexibility for examining qualitative data. This approach facilitates identifying, categorising, and interpreting significant patterns within data sets. According to Braun and Clarke (2012), thematic analysis helps researchers to uncover common meanings and experiences by concentrating on the relevance of data. The thematic analysis aims to detect patterns that align with the study's objectives, while various patterns can be identified within each dataset. Braun and Clarke (2012) detail a six-step process for thematic analysis. The first step is to provide an initial data review, and the second step involves generating initial codes. The third step is a thorough search for recurring themes within the data, while the fourth step requires a close examination of these themes. The fifth step involves defining and naming the themes accurately. The final step is to compile and report the findings. Thematic analysis was employed in this SLR to explore key concepts and themes in the literature on cybersecurity and emotions. After an initial assessment and rapid review of selected papers, a detailed investigation was carried out to identify and analyse codes and concepts concerning the relationship between cybersecurity and emotions. During this process, the framework proposed by Webster and Watson (2002) was employed to create a table for collating the concepts extracted from each paper. The data were then rigorously evaluated, combined, and re-labelled using NVIVO 12 software to ensure uniformity. Subsequently, 'concepts' were systematically organised into 'themes' based on thematic proximity. A thematic map was then constructed to represent the identified themes visually. The thematic analysis revealed several key themes, which are discussed in the following subsections.

2.7.5.1 Emotions and Cybersecurity Violations

Studies show that emotions significantly affect the likelihood of security breaches at work. Zhen et al. (2022) found that negative emotions make employees more prone to violate information security policies, indicating that such emotions can lead to breaches. Social dynamics in the workplace also play a critical role in security issues. Research by Farshadkhah et al. (2021) reported that being observed by others might change an employee's behaviour concerning security violations. The findings suggest that the presence of observers can alter emotional responses and affect the chances of committing breaches, underlining the role of workplace interactions. Chen et al. (2022b) studied the impact of stress related to information security on compliance with security policies. Their findings reveal that stress can negatively affect employees' adherence to these policies, while positive emotions may help mitigate this effect. This indicates that positive and negative emotions influence workplace security behaviours. Psychological ownership and psychological capital (PsyCap) also affect security breaches and interpersonal dynamics at work. Menard et al. (2018) explored how collectivism and psychological ownership influence motivation to protect. They found that psychological ownership is connected to a higher motivation for protective actions, and a person's collectivist tendencies can affect their security behaviours, showing how personal and social factors at work influence these behaviours. Ogbanufe and Pavur (2022) analysed how fear and anticipated regret motivate protective behaviours against identity theft. They found that fear and regret can drive individuals to take security measures, with regret being effective across different threat levels and fear being more significant under high-threat conditions. This study highlights the complex emotions involved in responding to cybersecurity threats.

2.7.5.2 Emotions and Cybersecurity Protection Motivation Behaviour

Emotions significantly influence cybersecurity behaviour, affecting how individuals behave and make decisions. Beaudry and Pinsonneault (2010) observed that positive emotions like excitement and enjoyment increase IT use. People feeling these emotions adapt more readily to new IT applications and are more engaged in task adaptation. Zhen et al. (2020) found that positive emotions such as happiness to behaviours motivated by the desire to protect sensitive information, finding that employees with these feelings are more likely to take protective actions. Self-efficacy plays a role in this relationship, with individuals with higher self-efficacy more likely to adopt preventive behaviours. Knowledge about information security further strengthens the ties between positive emotions and self-efficacy, leading to motivated behaviour. Nevertheless, research has shown that negative emotions are associated with violations of information security policies. Zhen et al. (2022) stated that employees tend to break these rules when they feel discouraged, uncomfortable, or angry. Farshadkhah et al.

(2021) explored the effects of shame and guilt on security breaches, discovering that guilt tends to decrease the likelihood of violating information security norms. Negative emotions can also lead to information security fatigue, marked by tiredness and a lower propensity to comply with security protocols. Chen et al. (2022a) examined how stress related to information security affects adherence to protocols, finding that fatigue is directly related to stress and indirectly to social support and IT use. The perception of being watched can also affect emotional reactions and behaviours related to information security breaches. Xu et al. (2020) studied the effects of emotions like anger and fear on how employees perceive the consequences of unauthorised computer use. They aimed to better understand the link between emotions at work, perceived formal and informal penalties, and deviant behaviours involving computer use. Their findings showed a strong relation between anger and the tendency to engage in deviant computer-related behaviours, with informal penalties playing a moderating role. Awareness of both types of consequences tended to reduce these behaviours.

Negative emotions also influence how individuals assess and decide on security measures. D'Arcy and Teh (2019) found that emotions significantly affect the willingness to accept or reject security practices like software updates and password changes, shaping how individuals perceive risks and threats, mainly when messages induce fear. To mitigate the negative effects of negative emotions on information security, organisations can provide support, promote a sense of ownership, and encourage engagement at work. Zhen et al. (2022) suggested that these approaches could help to lessen negative emotional experiences among employees, improve information security awareness, and increase self-efficacy and knowledge, which could mediate the relationship between positive emotions and protective behaviours. Negative emotions significantly affect behaviour and cognitive processes in information security, leading to policy breaches and security fatigue, but strategic organisational support and enhanced security awareness can reduce these effects. Mamun et al. (2023) discuss how users' emotional attachment to the intelligent personal assistants results in continued usage intentions. Based on attachment theory, the study focuses on the quality of interaction, emotional trust, and emotional attachment in the continuance of intelligent personal assistants. Interaction quality and trust affect emotional attachment, which positively drives continuance intention. Moreover, the study highlights that emotional trust—developed by interacting with intelligent personal assistants in a human-like way—promotes emotional attachment and enhances users' continued intention to use those technologies. The quality of interaction, such as an intelligent personal assistant's responsive to users and natural communication, was essential in developing trust and attachment.

2.7.5.3 Emotions and Cybersecurity Policy Compliance

Compliance with information security policies is influenced by various factors, including emotions stemming from stress and the psychological resources available to individuals. Chen et al. (2022b) conducted research on how stress related to information security concerns affects adherence to security policies. Their findings indicate that stress negatively impacts individuals' fatigue levels concerning information security, reducing their likelihood of following security policies. Additionally, the study found that positive emotions such as interest, excitement, and pride could influence stress-related emotions and enhance compliance with regulations involving information security policies. Negative emotions also significantly affect individuals' tendencies to breach information security policies. Zhen et al. (2022) identified a clear link between negative emotions—like discouragement, discomfort, and anger—and violations of information security policies. The study also highlighted the importance of psychological ownership, perceived organisational support, and work engagement in mitigating negative emotions and promoting compliant behaviour. Psychological resources, including PsyCap, are crucial for ensuring adherence to security policies. Chen et al. (2022a) explored how information security fatigue, security-related self-efficacy, and PsyCap affect users' compliance with information security policies. Their findings revealed that while information security fatigue adversely affects compliance, PsyCap can enhance it by reducing the stress that individuals experience. Emotions also shape how individuals assess and decide on security measures. According to D'Arcy and Teh (2019), emotions influence responses to security measures like software updates and password changes. Compliance with information security policies is affected by the interaction of stress-related emotions, psychological resources, and individuals' decisions based on their emotions. Addressing these factors can help organisations enhance compliance and reduce information security risks.

4.7.5.4 Emotions and Insider Behaviour

In this SLR, several of the selected studies explored the relationship between emotions and insider behaviour, shedding light on how emotions shape individuals' decision making and compliance with information security protocols. Liang et al. (2019) examined the coping strategies that individuals deploy when confronted with information security threats. The study found that individuals use both problem-focused coping (PFC) and emotion-focused coping (EFC) strategies, with EFC involving the regulation of emotional responses such as venting. The research highlighted a complex interaction between EFC and PFC, deepening the understanding of how individuals respond to information security challenges. Thompson et al. (2024) examined the efficiency of the threat devaluation EFC strategy in responding to a phishing threat. Based on the PMT and Extended Parallel Process Model, they examined the role of perceived severity, fear, and self-efficacy in predicting EFC and PFC. The results

showed that a higher level of fear increased PFC behaviours and decreased threat devaluation. However, threat devaluation did not directly enhance PFC, thereby underlining its role in regulating emotional rather than immediate protective responses. Burns et al. (2019) investigated how the emotions of insiders influence their adherence to preventive security measures. The study identified two types of emotions: negative emotions like sorrow, avoidance, and anxiety, and positive emotions such as enjoyment and interest. It was found that negative emotions might deter an individual from engaging in preventive actions, while positive emotions could promote the adoption of safety measures. Additionally, Gulenko (2014) focused on how emotions impact the strength of passwords. The findings suggested that positive emotions lead to the creation of stronger passwords, whereas negative emotions tend to reinforce existing behaviours. Emotions also affect how individuals evaluate and decide on security measures and their overall impact on behaviour. D'Arcy and Teh (2019) showed that emotions influence individuals' perceptions and acceptance of security measures, with emotional stimuli like fear-inducing messages affecting online risk assessments. The influence of emotions on individuals with access to sensitive information is critical to understand, as emotions can enhance vigilance and awareness of cyber threats (Zhen et al., 2020).

2.7.5.5 Psychological Factors and Cybersecurity

Psychological factors such as psychological ownership, PsyCap, and self-efficacy are crucial in shaping protective behaviours within information security. Psychological ownership refers to the mental state in which an individual feels they possess a particular object or goal. Studies indicate that this sense of ownership is linked to protective motivations and decision-making processes. Additionally, self-efficacy links positive emotions and protective actions, which is the belief in one's ability to perform a task effectively. These psychological components, including emotions, ownership, self-efficacy, and PsyCap, significantly influence how individuals evaluate, decide, and act concerning information security. Addressing these psychological factors effectively can help organisations to develop a culture of information security and enhance adherence to security protocols. Psychological ownership, in particular, involves emotions and beliefs that have a rightful claim to a specific object, idea, task, or person. This concept has been explored within information security, particularly for its influence on protective motivation. For example, Menard et al. (2018) studied how psychological ownership and collectivism affect defensive motivations, finding that an individual's sense of ownership and their likelihood to engage in secure behaviour are influenced by their collectivist tendencies. Psychological ownership is tied to various protective motivations and goals. Zhen et al. (2022) examined the relationship between psychological ownership and negative emotions in scenarios involving breaches of information security

protocols. Their research showed that psychological ownership can moderate negative emotions and reduce the tendency to violate information security regulations. Moreover, PsyCap, which includes hope, resilience, optimism, and self-efficacy, has been identified as a psychological asset that enhances trust in security communications and promotes protection motivation in information security. Burns et al. (2017) analysed how PsyCap affects individuals' engagement with PMT processes within organisations, focusing on how these psychological traits influence commitment to security practices outlined in PMT. Their findings suggest that developing PsyCap with organisational security measures can strengthen protective behaviours. Riemenschneider et al. (2023) investigated perceived organisational values concerning employee commitment and information security behaviour, mediated by PsyCap. They reported that the organisational values of quality and collaboration affect employees' attitudes and proactive behaviour concerning information safety. A few key implications are that those with high psychological capital are more likely to demonstrate better alignment with organisational goals, higher commitment, and more assertive safety behaviour. These studies highlight the importance of psychological ownership in understanding individual motivations and behaviours in information security. By leveraging psychological ownership, organisations can enhance motivation for protection, mitigate negative emotions, and promote compliance with information security policies.

2.7.5.6 Emotions and Security Fatigue

The SLR highlighted analyses of how stress and fatigue influence adherence to information security policies and the reduction of violations relating to information security policies. D'Arcy & Teh (2019) found a direct link between self-reported stress levels, security-related stress, and the emotions of frustration and fatigue. However, employees often adhere to their justifications for committing these violations due to feelings of frustration and fatigue. These observations suggest that frustration and fatigue can affect an individual's willingness to follow the rules and their tendency to justify non-compliant behaviours. Chen et al. (2022a) explored the relationship between the stress from information security fatigue and the likelihood of adhering to information security policies. Their findings indicated that information security fatigue is a complete mediator between an individual's security-related self-efficacy and their likelihood of complying with policies set by information security. The study also suggests that PsyCap could reduce self-reported stress and enhance adherence to support strategies. Recognising the negative effects of stress and fatigue on compliance with information security policies is vital. These conditions can lead to irritation and fatigue, culminating in actions that do not comply with regulations and the negation of violations. Therefore, organisations must consider strategies to manage stress and fatigue among their employees effectively. This

could involve providing support and resources that promote psychological well-being and resilience.

2.7.6 Theoretical and Methodological Context

Various conclusions can be drawn from the selected studies. Table 3 demonstrates that the Protection Motivation Theory (PMT) is the most widely used theoretical framework, closely followed by the Affective Events Theory (AET) and Broaden and Build Theory (BBT) theories. A significant portion of the chosen studies (Burns et al., 2017; Zhen et al., 2020; Burns et al., 2019; Menard et al., 2018; Ogbanufe & Pavur, 2022; Thompson et al., 2024) utilised the PMT framework. Burns et al. (2017) employed PMT to investigate the impact of PsyCap on protective motivation. An assessment of vulnerabilities (including susceptibility, seriousness, and maladaptive motivations) and an estimation of the costs related to coping, self-confidence, and the efficacy of response were included in the PMT components. Furthermore, Menard et al. (2018) used all components of the PMT to evaluate the impact of psychological ownership on aspects of protective motive and intention. To investigate the influence of anticipated regret and anxiety on individuals' motivation for security, the authors employed all components of the PMT. Furthermore, Zhen et al. (2020) and Burns et al. (2019) utilised a unified theoretical framework that integrated the PMT and the BBT theories. Zhen et al. (2020) utilised both theories to examine the direct effect of positive emotions on preventative motivation, whereas Burns et al. (2019) applied both theories to evaluate the impact of emotions on the adoption of preventive actions. The independent variables were obtained from the BBT theories and included achievement emotions (happy), challenge emotions (interest), loss emotions (sadness), and avoidance emotions (anxiety). The measured variable, precaution-taking, was established using the PMT method. Thompson et al. (2024) investigated the impacts of threat devaluation as an emotion-focused coping strategy on phishing threat response based on the PMT and the Extended Parallel Process Model.

The AET emerged as the second most widely accepted theory among the examined articles (Farshadkhah et al., 2021; D'Arcy & Teh, 2019; Chen et al., 2022b). Emotional responses caused by a specific event have been quantified using the AET framework. AET assumes that emotions might emerge as a reaction to any event within an organisation. In this conceptual framework, emotions are intermediary elements that connect work occurrences with behavioural attitudes. Farshadkhah et al. (2021) used the AET to evaluate the perceived observer as an independent variable, while emotions (namely shame and guilt) were regarded as responses, and breach of security protocols were treated as the dependent variables. Feelings of shame shaped the perception of surveillance and the occurrences of security policy violations and regret experienced by individuals. D'Arcy and Teh (2019) used the AET

to predict how employees will comply with ISPs. Chen et al. (2022b) investigated the relationship between positive and negative emotions elicited by a work event, namely an information security stress test, and its influence on ISP compliance. Two studies (Zhen et al., 2020; Burns et al., 2019) utilised the BBT in combination with the PMT.

Moreover, a quantitative methodology was employed across all papers. Out of all the papers, ten relied only on surveys (D'Arcy & Teh, 2019; Burns et al., 2017; Chen et al., 2022a; Zhen et al., 2020; Beaudry & Pinsonneault, 2010; Zhen et al., 2022; Xu et al., 2020; Mamun et al., 2023; Riemenschneider et al., 2023; Thompson et al., 2024), two used surveys and experiments (Burns et al., 2019; Liang et al., 2019), and five used experiments (Farshadkhah et al., 2021; Gulenko, 2014; Chen et al., 2022b; Menard et al., 2018; Ogbanufe & Pavur, 2022).

Table 3: The Most Frequently Applied Theories and Methods

Theory	Articles	Protection motivation theory	Affective Events Theory	Broaden-and-build theory	Stressor– Emotion Model	Appraisal Tendency Framework	Social Exchange Theory	Differential Emotional Theory	Coping Theory	Psychological Ownership Theory	Regret Theory	Attachment Theory	Psychological Capital Theory	Extended Parallel Process	Method	Sample Size
	Farshadkhah et al. (2021)		•												Experiment	690
	D'Arcy and Teh (2019)		•												Survey	138
	Burns et al. (2017)	•													Survey	522
	Chen et al. (2022a)				•										Survey	488
	Zhen et al. (2020)	•		•											Survey	215
	Beaudry and Pinsonneault (2010)					•									Survey	249
	Gulenko (2014)							•							Experiment	22
	Zhen et al. (2022)						•			•					Survey	318
	Burns et al. (2019)	•		•											Survey	405
	Liang et al. (2019)								•						Experiment Survey	140 934

Xu, et al. (2020)					•									Survey	327
Chen et al. (2022b)		•												Experiment	217
Menard et al. (2018)	•													Experiment	439
Ogbanufe and Pavur (2022)	•									•				Experiment	138
Mamun et al. (2023)											•			Survey	288
Riemenschneider et al. (2023)												•		Survey	289
Thompson et al. (2024)	•												•	Survey	518

2.7.7 Analysis of the Literature

Four major points are discussed in this section. The first consideration is the impact of positive and negative emotions on the protective actions taken by employees. The second point is the variety of emotions covered in the literature. Thirdly, self-efficacy is examined, along with the role that emotions play in mediating the motivational behaviour of cybersecurity protection. Lastly, the moderating effect of cybersecurity awareness on these relationships is discussed. Pervez (2010) argues that people's ability to control their emotions significantly impacts their performance and that businesses seek employees with this skill. Negative emotions are common responses to IT threats, especially when the person experiencing them cannot change their feelings or the situation's course. Being emotionally unstable also hinders one's ability to learn and remember new material (Izard, 2002). Beaudry and Pinsonneault (2010) found that people's productivity and IT-related behaviours suffered when they were emotionally unstable because they were more likely to engage in conflicts and seek vengeance. People's emotions often cause them to act in a harmful way, such as being inconsiderate with company computers, using weak passwords, or not following all ISPs (Gulenko, 2014; Burns et al., 2019). According to Xu et al. (2020), people's negative emotions significantly impact the deployment of security measures, while positive emotions may influence people to engage in protective motivation practices. When people are determined, alert, proactive, strong, and vigilant, their positive emotions can motivate them to protect their organisation against cyber threats. Thus, people can effectively fight cyber attacks by implementing cybersecurity protocols. Managing cyber-adverse events related to cybersecurity awareness should be made more accessible (Gulenko, 2014) by integrating positive emotions into preventative measures. Because people's emotions significantly impact the results of their IT efforts, organisations should tailor their cybersecurity awareness campaigns to appeal to people's values and emotions.

A few studies highlight the need for additional research on the emotions that might inspire organisations' employees to protect their IT systems (Gulenko, 2014; Burns et al., 2017; Burns et al., 2019; Zhen et al., 2020). It has yet to be recognised that employees' positive emotions motivate them to safeguard their IT resources from cybersecurity risks. Motivating employees to take more precautions against cyber threats can be achieved by appealing to their emotions and affecting their actions and reactions to cybersecurity awareness campaigns. Accordingly, future studies should focus on measuring the direct effects of positive and negative emotions on the desire to participate in protective behaviour.

The SLR identified different emotions reported in the reviewed articles (see Figure 11). Nine studies looked at negative emotions: Farshadkhah et al. (2021) focused on the study of shame and guilt, while D'Arcy and Teh (2019) examined frustration and fatigue. Beaudry and Pinsonneault (2010) categorised negative emotions into loss emotions, including anger, deterrence emotions, and anxiety. Gulenko (2014) explored empathy and anger, and Zhen et al. (2022) stated that negative emotions encompass immersion, discouragement, uneasiness, and anger. Burns et al. (2019) used the term to describe sadness, avoidance, and emotional anxiety. Similarly, Xu, et al. (2020) studied anger or fear and Chen et al. (2022b) described negative emotions regarding hostility, irritability, distress, fear, nervousness, upset, and jitteriness. Ogbanufe and Pavur (2022) examined regret and fear. Finally, this SLR also identified various positive emotions reported by Zhen et al. (2020), Beaudry and Pinsonneault (2010), Gulenko (2014), Burns et al. (2019), and Chen et al. (2022b). Zhen et al. (2020) referred to positive emotions such as happiness and excitement, Gulenko (2014) mentioned joy and interest, and Burns et al. (2019) used happiness as an achievement emotion and interest as a challenge emotion. Chen et al. (2022b) expanded the concept of positive emotions to include interest, excitement, pride, enthusiasm, inspiration, activeness, and attentiveness. Finally, Burns et al. (2017) and Chen et al. (2022a) employed PsyCap to represent positive psychology constructs such as hope, optimism, resilience, and self-efficacy.

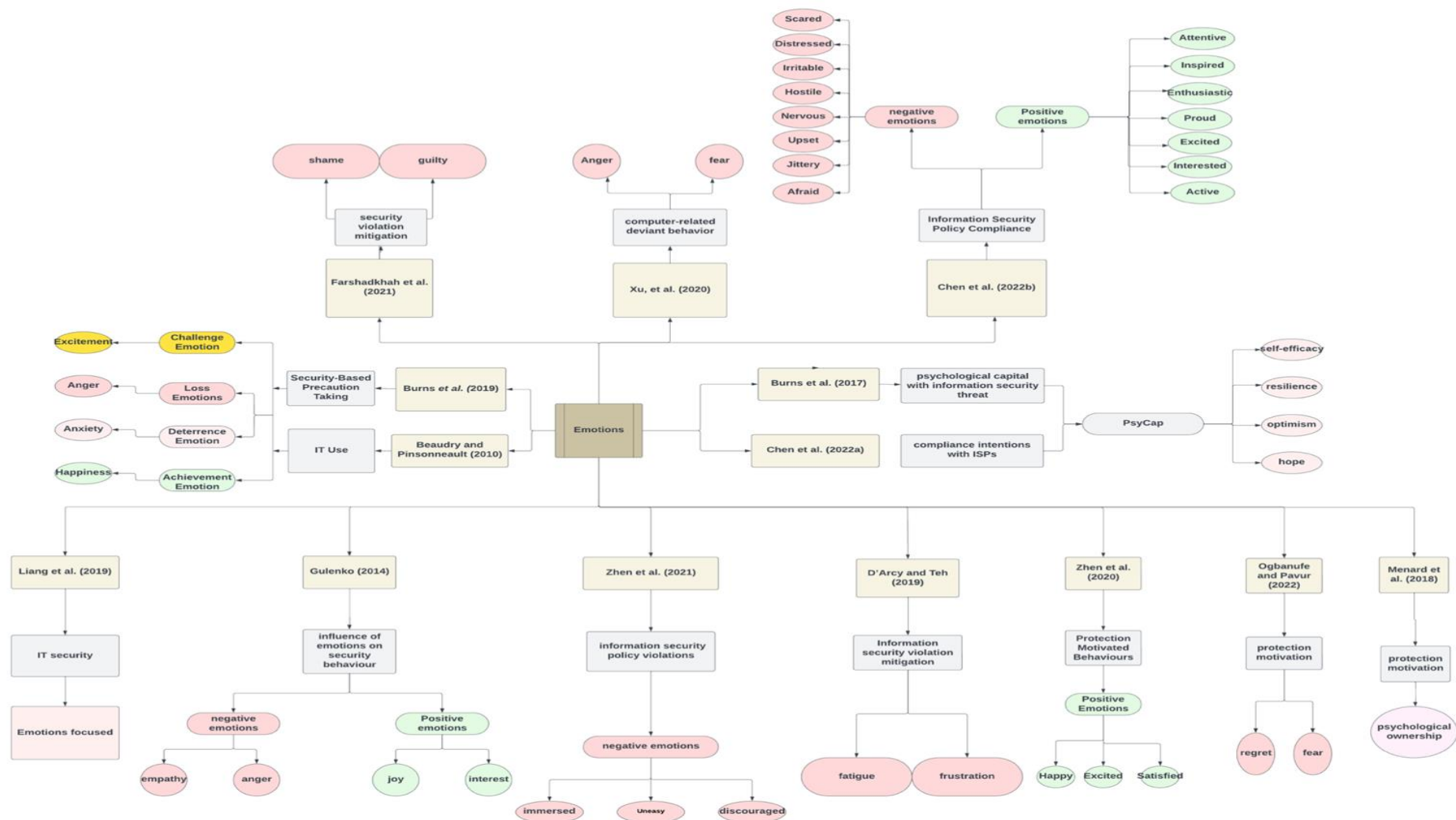


Figure 11: A Classification of Emotions Based on Systematic Analysis

Several reviewed research papers (e.g., Burns et al., 2017; Burns et al., 2019; Zhen et al., 2020; Zhen et al., 2022; Chen et al., 2022a), suggest that self-efficacy can increase the motivation to participate in protective behaviours. Beaudry and Pinsonneault (2010) examined how different emotions affected people's ability to rate their own self-efficacy. Negative emotions like fury and worry might influence a person's outlook (Gulenko 2014). Conversely, when they are feeling well, people's cognitive excitement levels rise, which helps them to think more proactively and increases self-efficacy (Zhen et al., 2020). Positive emotions are essential for increasing the acquisition and competence of new skills and knowledge (Beaudry & Pinsonneault, 2010). According to the PMT, risk factors in one's work environment determine how an individual responds to certain features. Everyone must be aware of the warning signs of potential security risks and what they can do to avoid them. As a result, people's confidence in their abilities is a significant factor in whether or not they will adopt specific protective habits. In order to raise cybersecurity awareness, it is essential to understand a company's policies and practices in order to better understand cyber vulnerabilities, threats, and incidents from diverse perspectives security awareness (Berkman et al., 2018). Zhen et al. (2020) found that people's cybersecurity knowledge is proportional to their self-efficacy and that being knowledgeable about cybersecurity can increase one's confidence and emotional well-being. Acquiring cybersecurity information can help individuals to improve their emotional health and self-esteem. As a result, people's perceptions of their cybersecurity abilities are less negatively impacted by those with more understanding in this area. Increasing individual cybersecurity knowledge can positively affect the modulation of positive emotions and self-efficacy.

2.8 Summary

This chapter provides a literature review on emotions and their impact on cybersecurity behaviour. It starts by exploring the definitions and functions of emotions, emphasising their role in human behaviour. In addition, the chapter covers several emotion categorisation models, such as the basic emotions, dimensional, and componential models, illustrating how emotions are classified and understood in psychology. The chapter then moves onto cybersecurity, discussing its definition, importance, threats, and human behaviour in cybersecurity and higher education. Finally, the chapter concludes with an SLR, synthesising key research on the relationship between emotions and cybersecurity behaviour and providing a detailed thematic analysis of relevant studies. This review forms the foundation for developing the theoretical framework and hypotheses in the next chapter, which will be built from the SLR to explore how emotions influence cybersecurity protection motivation behaviour.

Chapter Three: Theoretical Framework and Hypotheses Development

3.1 Introduction

The primary aim of this chapter is to develop a conceptual framework, along with its hypotheses, to address the gaps in the existing literature. In order to establish the theoretical framework, an SLR was conducted on the role of emotions in cybersecurity protection motivation behaviour (Alshammari et al., 2023). The SLR found that there is a critical need to explore the influences of negative and positive emotions on employees' protection motivation behaviour. Moreover, PMT and BBT were the most popular theories employed in the reviewed papers that can be used to explore the influence of emotions on human behaviour. Therefore, the following subsection will present a theoretical overview of PMT and BBT theories and proceed with the research hypotheses.

3.2 Theoretical Overview

As mentioned earlier, this research adopted two theories, PMT and BBT. The establishment of the PMT was driven by the necessity to forecast behaviour changes through fear appeals, a component of persuasive communication (Rogers, 1975, 1983). Ifinedo (2012) asserts that the PMT is a crucial theory that explains an individual's intention to participate in cybersecurity defence. It is utilised in research on cybersecurity issues and emphasises the development of defensive behaviours against personal health threats (Johnston & Warkentin, 2010; Boss et al., 2015). PMT has also been applied to examine how employees view cybersecurity threats and develop ways to counter these threats (Vance et al., 2012). Employee experience of action is a significant factor in PMT and its implementation because it is a preceding constructor of the model. Rogers (1975) produced the PMT by including three different stimulus variables: the likelihood of the threats occurring, the severity of possible harm, and the effectiveness of the suggested response. The cognitive mediational process is based on perceived efficacy, security threats, and susceptibility. This process involves measuring possible harm, the efficacy of a response, and the probability of occurrence. Perceptions influence the protecting motive, which is equivalent to behavioural (Rogers, 1983). Self-efficacy is the knowledge that someone can successfully conduct a recommended action. Bandura (1982) proposed that self-efficacy can be increased through indirect experiences, such as observing how others accomplish a task. A human's sense of self-efficacy is affected by their understanding of persuasive information. Rogers (1983) expanded on Bandura's self-efficacy theory (Bandura,

1982) by investigating its integration within PMT. Maddux and Rogers (1983) state that self-efficacy has a significant impact on behaviour.

When reflecting on using PMT in cybersecurity, threat appraisal involves assessing the susceptibility to cyber attacks and the significance of these attacks. This assessment provides methods for employees to evaluate their abilities and capacity to prevent future losses from threats (Woon et al., 2005). It also addresses how employees might assess the impact of cybercrimes. An information systems security threat could involve a hacker's actions within a bank's credit card system. A coping assessment includes emotional response and belief in one's ability to handle the situation. Confidence significantly helps in avoiding cyber attacks. Employees can employ cybersecurity training to prevent extensive damage to a company during an attack. They can assess the severity of the threat and decide whether they should wait for expert help or get involved in the avoidance process (Herath & Rao, 2009). Employee empowerment, training, and experience are vital to preventing cyber attacks. Trained employees can identify possible assaults and recognise vulnerabilities that attackers may exploit to carry out their crimes (Vance et al., 2012). Employees who know about cybersecurity are less vulnerable to cyber attacks. The PMT has been utilised in information systems security research to establish relationships among protective behaviour, well-being, and computer security concerns. Several studies have elucidated the security practices in different information security applications in an institutional setting (e.g., Burns et al., 2017; Zhen et al., 2020; Burns et al., 2019; Menard et al., 2018; Ogbanufe & Pavur, 2022).

The second theory is BBT, which states that emotions influence human behaviour (Fredrickson, 2004). According to this theory, positive emotions enhance behaviours and thoughts. Thus, positive emotions increase individuals' ability to evaluate several factors and respond appropriately to different situations, thereby facilitating adaptive responses to the surroundings. The broadening creates the conditions for distributing the resources required to raise overall welfare. Positive emotions not only reflect present well-being but also increase future well-being. They facilitate the manifestation of thoughts and behaviours, whereas negative emotions restrict the ability to deal with challenges and difficulties (Fredrickson, 2001). According to the theory, resilient persons can engage in positive coping strategies more frequently, resulting in positive emotions (Tugade et al., 2004). Individuals who have successfully managed to feel confident and assured that they can successfully confront future difficulties. The occurrence of positive emotions results in the expansion of coping resources, increasing overall well-being and facilitating the acquisition of future information. Psychological resilience improves over time (Reschly et al., 2008). In addition, it could enhance cognitive processes while engaging in activity that promotes positive emotions and

can respond to the negative consequences of emotions. Positive emotions are also indicative of the use of flexible coping methods (Fredrickson & Joiner, 2002). The BBT covers three perspectives: the broadening role, the narrowing role, and the building role. The following sections will explore these topics.

The Broadening Role: Positive emotions strengthen individuals' capacity to see and comprehend external stimuli, such as broadening their attention span and improving their cognitive processing capabilities. It allows an individual to expand their range of thoughts and activities. A wider range of attention can also improve cognitive variation, leading to a rise in the number of distinct (Amabile et al., 2005). Fredrickson (2004) suggests that broadening individuals' comprehension of a particular problem can facilitate their ability to resolve innovative challenges. Hence, as employees utilise and engage with an organisation's information systems more frequently, they are compelled to actively safeguard their organisation's sensitive data (Boss et al., 2009; Posey et al., 2013; Hsu et al., 2015; Zhen et al., 2020; Burns et al., 2019). Positive emotions can be valuable for information security (InfoSec) as they enhance cognitive agility and expand information processing capabilities (Fredrickson, 2004; Amabile et al., 2005). In addition, positive emotions affect the range of thoughts and actions that can be used when challenged with a behavioural provocation at any particular moment. According to Baskerville et al., (2014), employees need to feel positive to take measures against quickly changing hazards. The BBT asserts that positive emotions improve thoughts and behaviours related to security, helping to bridge the gap between knowledge and action.

The Narrowing Role: Fredrickson and Branigan (2005) assert that negative emotions tend to limit the scope of thoughts. Ashby et al., (1999) argue that positive and negative emotions have distinct effects on cognition and behaviour. For example, distrust and trust are separate entities rather than differing extremes on a range (e.g., Moody et al., 2014; Lowry et al., 2015). Moreover, negative emotions have a vital influence on adaptive behaviour because they produce a narrowing of focus. They provoke particular behaviours in reaction to necessary changes (Fredrickson & Branigan, 2005). For instance, negative emotions like anxiety and fear may motivate during threats to well-being, creating a suitable preparedness for an exact achievement (Bagozzi et al., 1999). Therefore, as anticipated by the theory, the movement brought on through worry reduces the thought-action options available to those feeling negative emotions (Fredrickson, 2001).

The Building Role: Optimistic emotions contribute to the balanced development of

psychological resources such as resilience, optimism, and creativity (Fredrickson, 2001). Therefore, positive emotions, such as hope, well-being, optimism, and happiness are all worthy attributes connected with the positive psychology paradigm (Seligman & Csikszentmihaly, 2000). According to Fredrickson and Joiner (2002), emotional experiences continuously increase long-term psychological resources, forming an "upward spiral".

After this introduction to the model and overview of the theories, the following sections present thirteen hypotheses based on these theories.

3.3 Negative Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy

Cybersecurity-related risks evoke negative emotions, mainly regarding an individual's life goals. For instance, individuals may experience negative emotions when they encounter obstacles that hinder their progress towards attaining their objectives (Kemper & Lazarus, 1990). Baumeister et al. (2001) assert that negative emotions impact relationships and can be used to forecast people's behaviour. Ayoko et al. (2012) and Moons et al. (2010) state that anger, fear, and regret are the most studied negative emotions. These negative emotions impact employees' behaviour and overall workplace productivity. Previous cybersecurity research has focused on the negative emotions experienced during a cybersecurity breach. Further study is needed to determine the effect of negative emotions on an employee's motivation for protection. For instance, the majority of researchers have associated cybersecurity attacks with negative emotions such as anger, insecurity, anxiety, and sadness. Bada and Nurse (2019) found that cybersecurity attacks have resulted in psychological distress, including emotional trauma and depression. Singling out individuals due to a breach of trust has also resulted in feelings of anger, a preference for safety, a lack of interest, and anxiety. Individuals' immediate psychological reactions to cybercrime can evoke various negative emotions, such as frustration, distress, insecurity, fear, sadness, anxiety, disappointment, and anger. These emotions may have long-term effects on individuals (Beaudry & Pinsonneault, 2010; Canetti et al., 2017; Budimir et al., 2021; Liang et al., 2019).

This research goes beyond the negative reactions of employees who have experienced cybersecurity risks to emphasise the effect of adaptive negative emotions in terms of motivating employees to protect themselves. For example, feelings of anger may alter an individual's protective behaviour. The previous research on organisational behaviour examined employees' emotions in their workplace and how these may affect their behaviour. Various employee reactions and types of behaviour might stem from emotional responses (Carmichael & Piquero, 2004; Weiss & Russell, 1996). Research by Bagozzi and Pieters

(1998) on goal-directed behaviour supports the narrative that high levels of negative emotions influence people's behaviour. Beaudry and Pinsonneault (2010) state that people's primary and secondary appraisals are influenced by their responses to personal and professional significance, with regard to activities that are related to IT use. These primary and secondary assessments manifest as negative emotions in an employee's behaviour, such as worry, frustration, and wrath (Beaudry & Pinsonneault, 2010; Burns et al., 2019; Gulenko, 2014). Technology often causes powerful and negative emotions in individuals. Negative emotions like irritation, fear, and rage can impact employees' lives, thus affecting their productivity, well-being, learning experience, and social interactions. Pervez (2010) indicates that emotions impact employee performance, emphasising that businesses must cultivate people with a heightened ability to regulate their emotions in order to enhance firm productivity. Employees who encounter IT threats are likely to experience negative emotions, especially when they lack control or self-efficacy over their emotions or the consequences of these events. Negative emotions harm individuals' capacity to acquire and retain information, resulting in subpar performance (Izard, 2002). Employees who experience negative emotions often engage in conflicts and revenge, which have dysfunctional effects on their performance and information technology-related behaviour (Beaudry & Pinsonneault, 2010). Employees who experience negative emotions engage in detrimental types of behaviour, including the misuse of work computers, improper password usage, and a lack of awareness regarding information security safeguards (Burns et al., 2019; Xu, et al., 2020; Kim et al., 2016; Gulenko, 2014). Additionally, information security-related conflicts may give rise to negative emotions, like employee fatigue, that impact their actions. Renaud et al. (2021) argued that dealing with cybersecurity incidents may produce negative emotions, specifically when employees fall victim to cyber attacks that influence their behaviour. Additionally, negative emotions impact employees' IS behaviour, as evident in the context of ethical behaviour (Chu & So, 2020).

A growing body of literature is starting to draw attention to the important role of negative emotions in influencing behaviour, especially in the context of security. Zhen et al. (2022) explored the effect of negative emotions on employees' intention to violate information security policies, conducting a survey with 318 employees from organisations in China. The researchers conducted a correlational analysis of negative emotions and violating the policies. In addition, they investigated the impact of psychological ownership, organisational support, and working engagement on mitigating negative emotions. The study explored the mediation between psychological ownership and work engagement. The authors employed the terms 'fury', 'discomfort' and 'discouragement' to describe negative emotions. Zhen et al.'s (2022) findings indicated that employees are more likely to violate information security policies when they experience negative emotions, which might be mitigated by promoting a perception

among employees of organisational support and positive workplace engagement. The employees' engagement level and ownership of their tasks impacted the relationship between negative emotions and the perception that the organisation provides support. Gulenko (2014) investigated the impact of positive and negative emotions on security behaviour within the field of information system security, focusing on sadness, guilt, and interest. The study involved 22 participants and found that individuals experiencing positive emotions selected passphrases containing more words than those experiencing negative emotions. Another study by Chen et al. (2022b) investigated the impact of stress on information security challenges and adherence to information security policies, mainly focusing on the role of emotional mediation. The researchers examine the correlation between stress and the challenges of information security and compliance with information security compliance regulations. Moreover, the research investigated how positive and negative emotions can mediate the links between elements of this nature. They argued that the positive emotional range included pride, inspiration, attentiveness, and excitement, while negative emotions encompassed hostility, fear, upset, uneasiness, distress, and jitters. The study involved 217 employees from three organisations in China. It was found that positive emotions mediated the relationship between stress arising from information security challenges and compliance with information security regulations. This finding suggests that the stress caused by challenging information security situations only leads to compliance with the information security compliance regulations when it triggers positive emotions. Negative emotions did not impact employees' compliance with the information security regulations. Farshadkhah et al. (2021) examined the effect of the onlooker and their influence on affective responses to mitigating information security crimes. The researchers investigated and explored the impact of observations disclosed by bystanders on non-malicious insider behaviour regarding violating the security policy. The research was based on a correlation analysis between individuals' perceptions and emotional reactions. An experimental approach was employed, and the sample size was 690 individuals. The research findings suggest that individuals likely to engage in violations may experience negative emotions, like guilt and shame. However, the results indicate no significant differences between onlooker perceptions, the emotive response shame, and the desire to contradict the information security policies. Beaudry and Pinsonneault (2010) investigated the role of emotions within IT use. Their research was based on a correlation analysis between IT use and emotions, emphasising the emotion encountered during the early stages of IT application implementation. The study focused on emotions arising from four distinct phenomena (deterrence, loss, accomplishment, and challenge). The research collected data from 249 participants to investigate the relationship between emotions and IT utilisation. The participants' emotions were assessed in terms of their feelings of anxiety, happiness, anger, and excitement. IT utilisation was not linked directly to feelings of

anger but was related to social support utilisation, which is connected to IT utilisation. The study identified a negative correlation between computer usage and anxiety, both indirectly and directly, due to detachment psychology. Xu et al. (2020) examined the emotions of individuals and their impact on the consequences and perceptions of activities related to deviant behaviour regarding computer usage in the workplace. The research identified a correlation between feelings of anger and employees' inclination to participate in deviant behaviour related to computer usage. The perception of informal consequences impacted the relationship between these two phenomena. Moreover, the employees with perceptions of both official and informal punishments were found to be less likely to engage in deviant behaviour linked to computer usage. Ogbanufe and Pavur (2022) investigated how the impact of anticipated regret and individual motivation might encourage employees to engage in protective behaviour. The study also sought to determine the circumstances in which fear may evoke a protective response and to examine which elements contributed to inappropriate reactions in the context of identity theft. Based on a sample of 138 employees, the study found that negative emotions, such as fear arising from job insecurity, shame and fatigue, may make employees less vigilant in terms of maintaining information security.

According to Singhvi et al. (2018), negative emotions significantly impact employees' motivation to protect themselves from risks and cyber threats. Also, they argue that factors such as organisational support, awareness and training can play an essential role in determining employees' motivation to engage positively with cybersecurity. Rather than relying solely on managing employees' negative emotions, companies must address the source of these emotions to improve their employees' awareness and motivation (Fadhlurahman, 2024). In addition, another study emphasised the importance of self-efficacy in determining behaviour, suggesting that it may not be impacted significantly by negative emotions (Sleiman & Sayah, 2018). Instead, situational factors and individual differences may affect the impact of emotions on the perceived capabilities of employees. This highlights the need for updated cybersecurity programs and training that may go beyond addressing the employees' emotional responses to developing practical skills and knowledge to improve their protection and motivation behaviour (Thapa, 2023). Moreover, the impact of negative emotions on employees' cybersecurity behaviour is not limited to the actions of individuals but also extends to the organisation's overall compliance and adherence to policies. Chen et al. (2022) found that the challenges arising from information security stress can impact employees' compliance with information security policies by mediating their emotions, which indicates that emotions are significant in shaping behaviour compliance.

Given the conflicting evidence, it remains unclear whether negative emotions enhance or hinder protection motivation behaviour. To address this gap and respond to **RQ1** (How do negative and positive emotions influence employees' cybersecurity motivation behaviours and self-efficacy?), this study hypothesises:

H₁: Negative emotions promote negative protection motivation behaviour among employees.

H₂: Negative emotions promote a negative effect on employees' self-efficacy.

By empirically testing the first hypothesis, this study contributes to the body of knowledge in several ways. First, it explores the role of negative emotions in cybersecurity behaviour by assessing whether they act as motivators or deterrents. Second, it extends the application of the PMT by integrating emotional factors into cybersecurity motivation. Furthermore, the second hypothesis contributes to bridging the gap between negative emotions and self-efficacy in cybersecurity behaviour. It provides empirical evidence on whether negative emotions reduce employees' ability to engage in protective measures. Additionally, it offers insights for training programmes aimed at enhancing cybersecurity self-efficacy in work environments.

3.4 Positive Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy

Research has shown that positive emotions influence employees' attitudes towards engagement with protective activities. Positive emotions, such as determination, attentiveness, activeness, and alertness, can motivate employees to engage in protective behaviour and thus help to safeguard their organisation against cybersecurity threats. These emotions empower the employees to respond to and effectively counter such threats. Gulenko (2014) suggested that employees' positive emotions might be proactively influenced to address the cybersecurity issues associated with lacking cybersecurity awareness. Since emotions significantly affect employees' information technology-related actions, organisations should align their cybersecurity awareness strategies with their employees' values and emotions, thus enhancing awareness across the organisation (Beaudry & Pinsonneault, 2010).

A lack of research exists on how positive emotions influence employees' protection motivation behaviour regarding cybersecurity (Zhen et al., 2020; Burns et al., 2017; Gulenko, 2014; Burns et al., 2019). A growing body of research has investigated employee compliance with violation of cybersecurity standards, but few studies have focused on the internal skills and emotional

factors that enable individuals to protect organisational communication assets (Siponen & Vance, 2010; Farshadkhah et al., 2021). Positive emotions can motivate personnel to protect their information technology-related assets from external and internal threats (Zhen et al., 2020). Further efforts should be made to clarify how employees' positive emotions may encourage them to make more significant efforts to protect IT resources against cybersecurity threats. Considering the significant influence of positive emotions on employees' responses and their conduct and knowledge about cybersecurity, it is recommended that businesses inspire their employees by evoking positive emotions in them that will incentivise them to engage in protective practices.

Positive emotions significantly impact the behaviour of employees in the context of cyber and information security. Zhen et al. (2020) found that positive emotions positively influenced individuals' behaviour towards information security. Moreover, positive leadership emotions may impact work behaviour (Qin & Liu, 2019). He et al. (2020) found that the security experience of the employees, their beliefs and perceptions, positive emotions, and the training their organisations offered significantly affected the perceived severity of employees' information security, indicating the positive effects of training on cybersecurity behaviour. Many researchers have explored the mediating role of the effects of cybersecurity behaviour. For instance, Chen et al. (2022b) revealed an emotional-based mediation effect, specifically fatigue, related to information security due to the impact of information security-related conflict on behaviour, indicating that a complex relationship of emotions shapes employees' cybersecurity behaviour. Moreover, Conrad et al. (2022) offered guidelines to support positive habit formation regarding workplace cybersecurity, reflecting the employees' subjective experience and promoting a positive occupational culture that improves the activities designed to promote cybersecurity among employees. Additionally, an ethical climate appears to exert a positive impact, with ethical values and culture positively affecting employees' cybersecurity behaviour. Chen et al. (2022b) argued that a positive emotional presence can mediate the relationship between information security-related stress challenges and compliance with information security standards. The authors endorse the utilisation of positive psychology within the management context and call for an investigation into the approach's applicability to addressing stress-complex issues within organisational information security. Gulenko (2014) states that individuals experiencing positive emotions were observed to select passphrases containing more words than those experiencing negative emotions. The study revealed that, when positive emotions are experienced, individuals are more inclined to use novel techniques when creating passwords. Burns et al. (2019) investigated the effect of the emotions experienced by insiders on the level of preventive measures undertaken within the domain of organisational information systems. The research adopted a broad perspective to

examine how insiders' emotions impacted information asset protection. The study characterised negative emotions as encompassing worry, avoidance, and grief, while positive emotions were defined as interest and happiness. It was found that individuals' emotions affected their behaviour patterns differently. Bandura (1986), Schwarzer and Renner (2000), and Luthans et al. (2006) discussed the mechanisms of coping, intention implementation, and emotion regulation as factors that impact individuals' ability to cope with negative emotions and engage in protection motivation behaviour. They proposed that positive emotions, such as those related to PsyCap, can act as a cybersecurity behaviour motivator, further emphasising the importance of self-efficacy in driving motivation and behaviour. The extent to which positive emotions influence cybersecurity motivation remains underexplored. To address this gap and respond to **RQ1**, this study hypothesises:

H₃: Positive emotions promote positive protection motivation behaviour among employees.

H₄: Positive emotions promote a positive effect on employees' self-efficacy.

The third hypothesis contributes to existing research in several ways. It expands the BBT and PMT into cybersecurity behaviour, providing evidence on whether positive emotions drive protective behaviours. Furthermore, it offers practical implications for designing cybersecurity training programmes that leverage positive emotions. Additionally, the fourth hypothesis contributes to the literature by demonstrating how positive emotions strengthen cybersecurity self-efficacy. It also addresses gaps in the understanding of the influence of positive emotions on workplace security practices and provides actionable insights for fostering confidence in cybersecurity compliance.

3.5 Self-Efficacy and Employees' Cybersecurity Protection Motivation Behaviours

Self-efficacy means a person's confidence in their ability to take action and successfully overcome obstacles (Bandura, 2004; Compeau & Higgins, 1995; Brooks et al., 2019). Several studies have shown that self-efficacy directly impacts decision making, leading to specific actions (Bandura, 2012). As a result, it further affects individuals' personal goals and overall performance of their designated assignments (Bolkan et al., 2021). Further studies have established that people's experiences significantly impact their future self-efficacy (Khorakian & Sharifirad, 2019; Baral & Arachchilage, 2019). Likewise, organisations can facilitate the development of various individual characteristics that positively affect the self-efficacy of the respective individual. Any personal efforts to improve individuals' goals, performance, and decision making can be aligned to augment their self-efficacy. There are various types of efficacy, such as response and task self-efficacy. These are prone to being influenced by

emotions, thus contributing to behaviour that motivates protection. Response self-efficacy is a belief that personal behaviour contributes to risk reduction (Meijers et al., 2019). Based on the reviewed literature, it has been suggested that self-efficacy positively influences employees' motivation to participate in protective behaviour (Gross, 1998; Compeau & Higgins, 1995; Rhee et al., 2009; Parshetty, 2019; Herath & Rao, 2009; Kryshko et al., 2023; Burns et al., 2019; Zhen et al., 2020; Chen et al., 2022). Parshetty (2019) demonstrated that a positive relationship exists between motivation and self-efficacy to engage in protective behaviour in other areas (such as health promotion and theft prevention) and cybersecurity. Additionally, Kryshko et al. (2023) and Gross (1998) found that individuals who possess high levels of self-efficacy are more likely to maintain and adopt healthy behaviour, and are able to tackle challenging tasks, unlike those with low levels of self-efficacy, who prefer to execute simple tasks (Compeau & Higgins, 1995; Rhee et al., 2009).

Similarly, cybersecurity knowledge and experience impact individuals' overall response efficacy (Li et al., 2019). Factors such as low income, upbringing, and poor mental health may harm an individual's self-efficacy (Bingöl, 2018), but it may be improved by enhancing their physical and emotional well-being (Bandura, 2012). Moreover, multiple studies have indicated that one's emotions, whether negative or positive, impact one's assessment of one's self-efficacy (e.g., Beaudry & Pinsonneault, 2010). Negative emotions, such as worry and anger, might restrict a person's mentality, thereby affecting their ability to absorb and retain information (Gulenko, 2014). Mallinckrodt and Wei (2005) suggest that individuals who experience severe anxiety should contemplate participating in self-efficacy enhancement exercises. Likewise, research has established that individuals who display both attachment avoidance and anxiety tend to display a self-efficacy deficit. In addition, employees who experience negative emotions require greater self-efficacy. Conversely, positive emotions trigger cognitive enthusiasm, leading to proactive thinking that enhances self-efficacy (Zhen et al., 2020). Beaudry and Pinsonneault (2010) found that positive emotions enhanced learning and facilitated the acquisition of new skills and knowledge, particularly in relation to information systems. Regarding the PMT, the risk factors in an employee's work environment impact their reaction to the individual elements. This reaction might be either favourable or unfavourable. Employees' response to these risk variables is influenced by their knowledge of the threats and their belief in their ability to handle them (LaRose et al., 2008; Ma, 2022). Employees must thoroughly comprehend their cybersecurity obligations and be aware of the proactive measures to implement when confronted with security issues. Self-efficacy is crucial for employees to successfully adapt to and embrace new types of protective behaviour that will enhance their self-efficacy.

To examine this relationship and address **RQ2** (How does self-efficacy affect the relationship between negative and positive emotions and cybersecurity protective motivation behaviours?) this study hypothesises:

H₅: Self-efficacy promotes a positive protection motivation behaviour among employees.

H₆: Self-efficacy intervenes in negative emotions and employees' protection motivation behaviours.

H₇: Self-efficacy intervenes the positive emotions and employees' protection motivation behaviours.

These hypotheses contribute to the body of knowledge by extending the role of self-efficacy in cybersecurity protection. For example, it might confirm that cybersecurity training should focus on emotional factors to build self-efficacy and offers guidance on interventions aimed at increasing employee self-efficacy in cybersecurity practices.

3.6 Employees Cybersecurity Awareness

Cybersecurity awareness refers to the comprehension of the rules and procedures implemented to improve one's understanding of cyber vulnerabilities, hazards, and incidents resulting from intentional and unintentional actions (Berkman et al., 2018). Moreover, Shaw et al. (2009) argued that cybersecurity awareness refers to educating internet users about the importance of engaging in safe cybersecurity behaviour and defining their roles and actions related to information security control. This can be used to safeguard the organisation's data and network, which is considered the collective duty of all organisation members, therefore all employees should be informed of the necessity and procedures for safeguarding these assets (Kim, 2017). In addition, the author believed that, by participating in cybersecurity awareness programmes, employees can improve their decision making by utilising evidence-based practice to counter potential cybersecurity threats that could impact the reputation of the organisation's data and networks. Through such programmes, employees can be shown sample cybersecurity attacks and threats, like compromised phishing links that attempt to steal the organisation's crucial information through social engineering, and then led through the preventive strategies that will help them identify and avoid these phishing links. Once recognised, the employees can respond to these threats appropriately by reporting them to the cybersecurity law enforcement personnel.

Cybersecurity awareness is essential to ensure that employees are aware of the cyber threats and attacks within cyberspace that may negatively impact an organisation and its employees.

Cybersecurity programs are created to ensure the safety of internet users and the security of the information systems they access on computer networks (Balhara et al., 2018). Most of the differences experienced in cyberspace have been linked to various functional design changes and transitions. In this regard, most universities, colleges, and private companies offer tailor-made cybersecurity awareness programmes to increase their employees' awareness of cybercrime (Dodge et al., 2007). However, Shaw et al. (2009) proved that a strong cybersecurity awareness is required in order to achieve cybersecurity alertness. Recently, the focus on cybersecurity has shifted towards individual cybersecurity awareness. For instance, McCormac et al. (2017) gathered data from 1,048 employees in Australia from which they identified an association between information awareness, job-related stress, and flexibility; employees' awareness of cyber threats and attacks correlated with their ability to cope with their job-related stress and enhance their awareness of cybersecurity hazards. Large organisations have improved their employees' cybersecurity awareness by increasing the related budgetary resources and enforcing policies focused on improving this awareness (Hadlington, 2018). However, a significant concern regarding cybersecurity awareness is the nature of the cybersecurity knowledge provided to individuals. It does not promote the protection of employees' cyber activity, which is crucial for reducing cybersecurity risks and hazards (Puhakainen & Siponen, 2010).

Several studies have underlined how different factors, such as organisational support, awareness, training programmes, communication and knowledge, can impact individuals' responses to cybersecurity threats. Sulaiman et al. (2022) emphasised the role of cybersecurity awareness in shaping individuals' perceptions and cyber risk responses, while Song et al. (2024) emphasised the impact of organisational support on employees' cybersecurity behaviour. Hanus and Wu (2016) and Venard (2021) explored how communication, knowledge, and training can impact employees' cybersecurity behaviour and emotional responses. Hijji and Alam (2022) and Lee and Chua (2023) identified a relationship between emotional responses, perceived effectiveness, knowledge, awareness, and protection behaviour against cyber threats, suggesting that informed individuals would be less likely to engage in risky behaviour. Baltuttis et al. (2023) consider ways to enhance individuals' awareness and knowledge of cybersecurity behaviour. They suggested that persons with significant security knowledge are more likely to demonstrate security efficacy when implementing security measures. Most internet users have been noted to lack adequate understanding of what they should do versus what they should not do (Albrechtsen, 2007). Some variations in individuals' levels of cybersecurity knowledge can be attributed to a lack of knowledge about possible cyber threats and how to avoid them, insufficient time for

maintaining efficient cybersecurity behaviour, and the need for proper knowledge on evading specific cybersecurity threats.

Cybersecurity awareness has been associated with regulating employees' emotions and enhancing their self-efficacy. Several studies have demonstrated that a strong understanding of cybersecurity can improve employees' mood and belief in their ability to handle cybersecurity issues (Zhen et al., 2020). Employees with an understanding of cybersecurity, who demonstrate a positive disposition towards IT usage, show a higher level of cybersecurity awareness than their colleagues who lack appropriate expertise in the field of cybersecurity (Dinev & Hu, 2007; Parsons et al., 2014).

Regarding negative emotions, this study proposes that employees with a higher degree of cybersecurity awareness will weaken the relationship between negative emotions and employees' protection motivation behaviour compared to those with a lower level of awareness. Moreover, it has been proposed that employees with a higher level of cybersecurity awareness will weaken the relationship between negative emotions and employees' self-efficacy compared to those with a lower level of awareness. However, regarding the positive emotions, it proposes that employees with a higher level of cybersecurity awareness will strengthen the relationship between positive emotions and employees' protection motivation behaviour compared to those with a lower level of awareness. Nevertheless, it proposes that employees with a higher level of cybersecurity awareness will strengthen the relationship between positive emotions and employees' self-efficacy compared to those with a lower level of awareness. Finally, it proposes that employees with a higher level of cybersecurity awareness will strengthen the relationship between self-efficacy and employees' protection motivation behaviour compared to those with a lower level of awareness. In light of the above, and to address **RQ3** (Does cybersecurity awareness have a positive influence on employees' cybersecurity motivation behaviours?), this study hypothesises:

H₈: Cybersecurity awareness has a positive effect on protection motivation behaviour among employees

H₉: Cybersecurity awareness moderates the direct relationship between negative emotions and employees' protection motivation behaviour.

H₁₀: Cybersecurity awareness moderates the relationship between negative emotions and self-efficacy.

H₁₁: Cybersecurity awareness moderates the direct relationship between positive emotions

and employees' protection motivation behaviour.

H₁₂: Cybersecurity awareness moderates the relationship between positive emotions and self-efficacy.

H₁₃: Cybersecurity awareness moderates the relationship between self-efficacy and employees' protection motivation behaviour.

These hypotheses contribute to the existing body of knowledge by exploring the extent to which cybersecurity awareness directly influences protective behaviours. The research will provide empirical evidence for the moderating role of cybersecurity awareness in the emotional and cognitive factors of cybersecurity behaviour. Moreover, it will offer insights for organisations seeking to enhance employees' security behaviour through awareness initiatives.

3.7 Differences in Employees' Cybersecurity Protection Motivation Behaviour

The role of gender in shaping cybersecurity behaviours is significant. Anwar et al. (2017) indicate that women show less secure behaviours than men, highlighting the necessity of gender-sensitive information security programmes. Furthermore, gender has been found to mediate the relationship between psychosocial characteristics and self-reported cybersecurity behaviours, suggesting that men and women may respond differently to the same security risks (Anwar et al., 2017). Additionally, research on avoiding technological threats has revealed that different genders have distinct cybersecurity-related motives and behaviours, further reinforcing the need for gender-sensitive cybersecurity training (Gillam & Waite, 2021).

Another important aspect that impacts cybersecurity behaviours is age. Perceived threat severity and familiarity with cyber risks are two areas where age influences cybersecurity behaviour (Fatokun et al., 2019). The general cybersecurity behaviours of older users may differ from those of younger users due to differences in risk perception and response efficacy. According to Lee and Chua, (2023), older people are less aware of cybersecurity, making it harder for them to be safe when using the internet. Younger people, regardless of gender, are more likely to take proactive cybersecurity measures than older adults, according to research that identified statistically significant differences in cybersecurity behaviours based on age and gender (Shah & Agarwal, 2020). This shows the importance of targeting cybersecurity awareness and education programs to specific demographics based on their unique needs and vulnerabilities.

Furthermore, it is unreasonable to ignore the impact of education on cybersecurity behaviours. More highly educated persons may be better able to handle cybersecurity issues, as elements like knowledge of cyber risks and perceived severity are significantly impacted by the level of education (Fatokun et al., 2019). Knowledge of cybersecurity and implementing preventative measures also positively correlate with educational level. For example, individuals with a college degree have been reported to be better able to identify phishing efforts, comprehend the importance of frequent program upgrades, and execute vital password methodologies (Bulgurcu et al., 2010). Obtaining specialised education in IT or cybersecurity significantly improves individuals' capacity to safeguard themselves and their organisations from cyber risks. However, instructional programmes aimed at lower levels of schooling are equally vital. Educational programmes that include cybersecurity training can increase security compliance and proactively mitigate threats (Arachchilage & Love, 2014). Nevertheless, even among those with advanced education, continuing learning is crucial because of the constantly changing characteristics of cyber threats.

Employment position influences an individual's engagement with cybersecurity practices. Staff members in technical positions, such as IT administrators or cybersecurity analysts, usually understand cyber threats and are responsible for establishing and upholding security protocols. They are more inclined to adhere strictly to security measures and advocate the implementation of best practices inside the organisation (Soomro et al., 2016). However, non-technical staff may only possess limited knowledge of cybersecurity threats and the significance of adhering to security protocols. Their actions may inadvertently contribute to security breaches, such as succumbing to phishing emails, employing weak passwords, or disregarding software updates (Alshaikh et al., 2018). Insufficient knowledge highlights the necessity for inclusive cybersecurity training programmes that address all hierarchical levels inside the organisation. Managerial perspectives on cybersecurity also have a crucial impact. Effective leadership that places cybersecurity as a top priority and cultivates a culture of security consciousness increases the likelihood of employees adopting safe behaviours (Chan et al., 2005). Instead, if management fails to highlight the significance of cybersecurity, employees may view it as a diminished priority and ignore security protocols.

Having experience in cybersecurity considerably improves an individual's capacity to recognise, thwart, and counteract cyber attacks. Experienced cybersecurity professionals have superior skills in identifying trends and abnormalities that could signify security breaches. Furthermore, they can formulate extensive security policies, create resilient security architectures, and efficiently guide incident response operations (Tøndel et al., 2014). Their perspectives are critical for predicting developing risks and adjusting security protocols

accordingly. Nevertheless, the swiftly developing cyber environment requires continuing professional growth. Experienced professionals must remain updated on the most recent risks, technologies, and optimal methods by continuous education and training. Maintenance and enhancement of competence can be achieved by pursuing certifications, participating in workshops, and engaging in professional networks.

3.8 Proposed Theoretical Framework

Based on the PMT and BBT, the theoretical model is developed and illustrated in Figure 12, which shows the relationship between employees' negative and positive emotions, self-efficacy as a mediating factor, employees' cybersecurity awareness as a moderator, and employees' protection motivation behaviour (Alshammari et al., 2024).

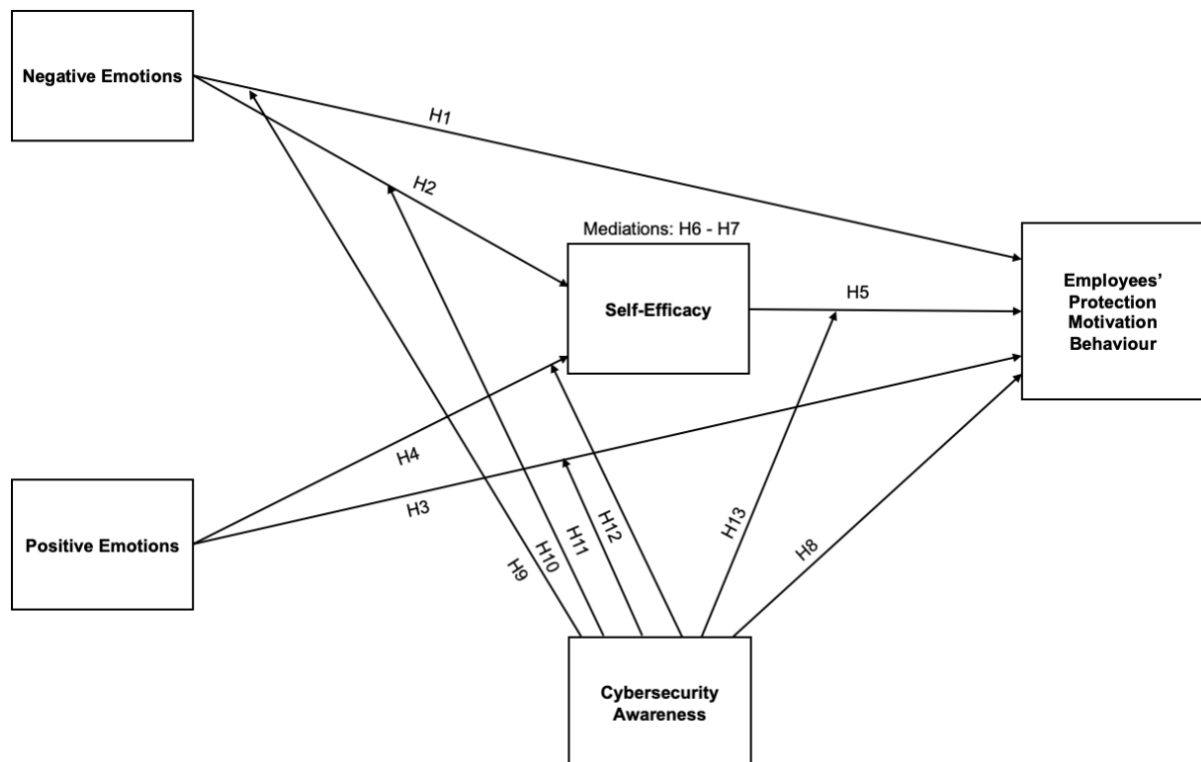


Figure 12: Proposed Theoretical Framework

3.9 Summary

The proposed theoretical model was constructed by drawing upon the existing behaviour theories, namely PMT and BBT. The research conceptual model comprises two independent variables, namely negative and positive emotions; one mediating variable, self-efficacy; one moderator variable, cybersecurity awareness; and lastly, one dependent variable, employee protection motivation behaviour. Accordingly, 13 hypotheses are formulated to explain the

relationships between the research model's constructs. Two hypotheses (**H₁** and **H₃**) were proposed between the independent variables (negative and positive emotions) and the dependent variables (employees' protection motivation behaviours). Two hypotheses (**H₂** and **H₄**) were proposed between the independent variables (negative and positive emotions) and the mediating variable (self-efficacy). One hypothesis (**H₅**) was proposed between self-efficacy and employees' protection motivation behaviours. Moreover, two hypotheses (**H₆** and **H₇**) were presented regarding the relationships between the independent and dependent variables through the mediating variable of self-efficacy. One hypothesis (**H₁₃**) was proposed in the relationship between cybersecurity awareness and employee protection motivation behaviour. Finally, five hypotheses (**H₉** – **H₁₃**) were given regarding the moderator role of cybersecurity awareness. Finally, the following chapter provides a detailed explanation of the research methodology employed to test the research hypotheses stated in this chapter.

Chapter Four: Research Methodology

4.1 Introduction

A conceptual model for the research was developed in the previous chapter based on established behavioural theories. Furthermore, the model constructs and the reasoning behind their formulation were discussed. According to Saunders et al. (2019), the research methodology sets out how researchers will gather, assess, and examine data on a particular subject to address enquiries, resolve issues, or establish facts. Accordingly, having a detailed and appropriate methodology is essential for establishing reliable data that will aid comprehension of the research subject. This chapter follows the suggested research onion model by Saunders et al. (2019). The model offers an examination and rationale for the chosen research philosophy, approach, methodological selection, research strategy, and data collection and analysis processes. The research onion is valuable because it is adaptable to various contexts and research types (Bryman & Bell, 2015).

4.2 Research Philosophy

Research philosophy relates to the procedures that enable researchers to transform their thoughts into knowledge (Saunders et al., 2019). According to Crossan (2003), a research philosophy impacts the data collection and analysis when performing studies. As such, scholars can adopt several research philosophies. This chapter presents three primary themes to elucidate the research philosophy, aiming to comprehend the ontological perspective that underlies the research assumptions. Moreover, it explores the research epistemology, the central framework for understanding the research philosophy (Al-Ababneh, 2020; Creswell, 2014; Saunders et al., 2019).

4.2.1 Ontology

Ontology explores the fundamental characteristics of existence, analysing the existence of things and the essential connections and classifications of various elements of reality (Honderich, 2005). Ontology aims to determine the fundamental aspects of the universe and offer a clarification of existence in its broadest scope (Creswell, 2014; Saunders et al., 2019). Unlike more specific sciences like biology or astronomy, ontology has a broader scope as it includes all types of existence, ranging from living beings to astronomical events (Berto & Plebani, 2015). In addition, "ontology" represents a particular theory of existence within the field instead of the broader investigation of being (Simons, 2009). It can also indicate an complicated framework or the complete set of ideas in a specific field. Creswell (2014) and Saunders et al. (2019) emphasise the implication of recognising and considering both

subjective and objective perspectives. The subjective perspective acknowledges that human variances influence reality and that these individual perspectives form societal beliefs. This implies that social entities are not separate from people. In contrast, the objective perspective maintains that an independent reality remains unaffected by human experience. This position suggests that our observations do not impact the social processes that researchers investigate (Creswell, 2014; Saunders et al., 2019). This perspective asserts that the existence of reality is not influenced by the way individuals perceive it.

4.2.2 Epistemology

Epistemology pertains to how researchers determine what qualifies as reliable knowledge and the techniques they utilise to obtain it (Saunders et al., 2019). Researchers frequently choose their epistemological method based on the precise enquiries they seek to address. Creswell (2014) and Sekaran and Bougie (2016) identified four main research paradigms: positivism, interpretivism, critical realism, and pragmatism. These frameworks influence researchers' fundamental beliefs, behaviours, and perspectives, which impact their investigations' characteristics.

4.2.2.1 Positivism

Positivism is a pragmatic approach to revealing objective reality (Saunders et al., 2019). Using this research philosophy, the scholar is an impartial analyst who dissociates from their values and works independently. The approach has been defined by Neville (2007) as a strategy for finding facts or proof of any social phenomenon that uses consistent practices such as hypothesis, measurement, and assessment. In the specific context of IS research, Niehaves and Stahl (2006) assert that it is the most prominent and widely adopted philosophy. The widespread adoption of the technique in the field is due to its potential to test hypothetic-deductive theory; it allows for the development of context and time-free generalisations. Positivist researchers can discern the facts and value judgement as most research relies on mathematical and statistical tools (Bogdan & Taylor, 1990). Altinay and Paraskevas (2009) emphasised that the research paradigm is interlinked with assumptions and quantitative research methodologies. These can range from experiments, field studies, and surveys, which contrast with qualitative techniques, implicative in interpretivism philosophies.

4.2.2.2 Interpretivism

According to Saunders et al., (2019), interpretivism was developed by combining a subjective perspective with a critique of positivism. Interpretive research theory maintains that the social world can be interpreted subjectively; as a result, the focus here is on understanding how subjects experience the social environment (Saunders et al., 2019). Unlike social

constructionism, which advances knowledge about actuality through the perspective of the daily social environment and knowledge about the phenomenon from people who have experienced it (Titchen & Hobson, 2005), interpretivism is based on the idea that the research scientist has a distinct function in studying the social world (Bryman & Bell, 2015). Thus, the researcher remains open to new knowledge and allows it to evolve. According to this research philosophy, research focuses on and relies on the researcher's interests. As previously highlighted, qualitative data methods such as observation and unstructured interviews are prominent in this approach (Saunders et al., 2019). In general, interpretivism, in contrast to positivism, requires the researcher to be receptive to new knowledge rather than confining themselves to theoretical beliefs.

4.2.2.3 Critical Realism

Critical realism, commonly called the transformative paradigm, centres on the historical context and specific requirements of a disadvantaged minority (Creswell, 2014; Sekaran & Bougie, 2016). The strategy establishes a connection between political, economic, and social actions. Researchers in this paradigm strive to advance social justice by examining and addressing the processes of power and privilege (Creswell, 2014; Sekaran & Bougie, 2016).

4.2.2.4 Pragmatism

Pragmatism asserts that no universal method can be applied to all studies. The nature of the study topics determines the philosophical approach (Saunders et al., 2019). There are two components to pragmatism: positivism and interpretivism. Strauss (2009) posits that the approach emphasises that the researcher has freedom of choice under this philosophy; they can select the appropriate procedures that meet the research purpose. Weber (2004) asserts that researchers must choose a solid research methodology that fits with the goal of their enquiry, and they can gather and synthesise information with multiple study techniques. Depending on the phenomena under investigation, any one of the study methods could yield valuable results.

4.2.3 Selected Research Philosophy

The researcher's worldview will influence the research philosophy they employ. Therefore, the researcher's assumptions will be aligned with the methodology used in the plan for the study (Saunders et al., 2019). Figure 13 describes the four paradigms in terms of their characteristics, definitions, and methodologies (Creswell, 2014; Saunders et al., 2019; Sekaran & Bougie, 2016).

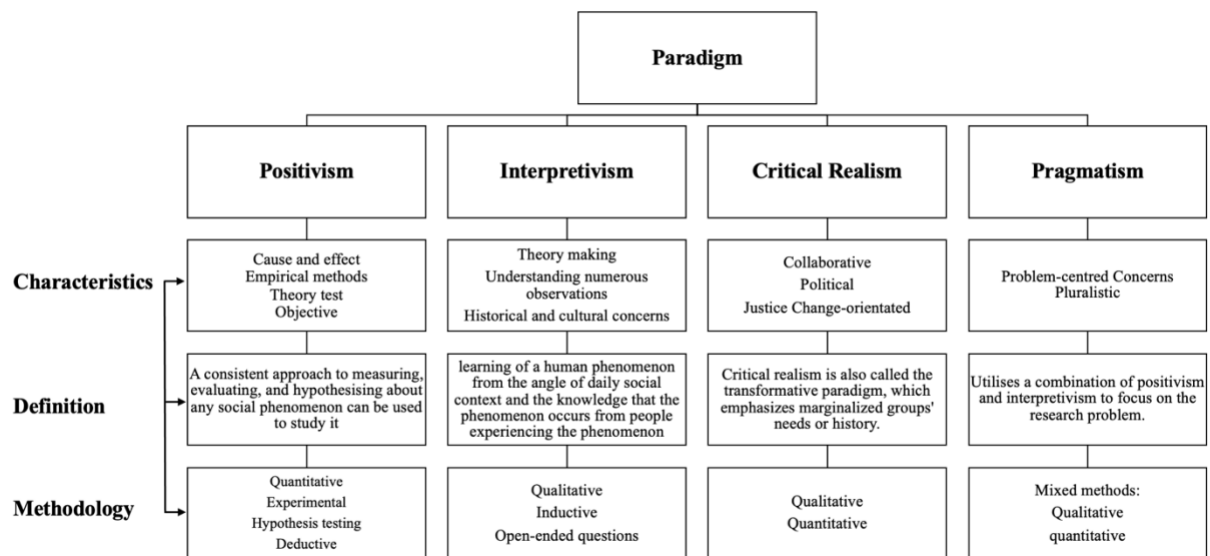


Figure 13: Research Paradigms

After considering the four paradigms and how they are different, the researcher chose to use the positivist research paradigm for the following reasons:

- I. **Quantitative measures:** Mathematical techniques and tools are used to measure and analyse relationships between variables in the quantitative approach (Creswell, 2014; Saunders et al., 2019). To fulfil the research objective, quantitative data were gathered from employees of King Abdulaziz University to provide empirical support for the suggested model and to test the formulated hypotheses. Hence, based on this standpoint, the positivist paradigm was chosen.
- II. **Deductive reasoning approach:** Emphasises that the dominating strategy for the interaction between theory and research is the positivist paradigm, which is related to the deductive theory (Creswell, 2014; Saunders et al., 2019; Trochim & Donnelly, 2001).
- III. **Cause-effect strategy:** Researchers should investigate the causes of the dependent variable since the issue under examination is affected by several elements (Sekaran & Bougie, 2016). The research problem of employees' cybersecurity protection motivation behaviour is influenced by other independent variables (negative and positive emotions). In addition, a mediation variable (self-efficacy) and a moderation variable (employees' awareness of cybersecurity) are considered. Therefore, the variables influencing employees' cybersecurity protection motivation will be tested.

- IV. **Analysis Tools:** The researcher employed advanced statistical tools to analyse the data gathered (Cohen et al., 2013). The SPSS and PLS-SEM statistical programs were selected to examine the research's theoretical model.
- V. **Previous studies:** Based on the extant literature, it has been noted that this particular approach has been employed in previous studies (e.g. Burns et al., 2017; D'Arcy & Teh, 2019; Chen et al., 2022; Beaudry & Pinsonneault, 2010; Burns et al., 2019; L. Chen et al., 2022; Farshadkhah et al., 2021; Gulenko, 2014; Liang et al., 2019; Menard et al., 2018; Ogbanufe & Pavur, 2022; Xu et al., 2020; Zhen et al., 2022, 2020). As a result, this research adopts a positivistic approach, testing hypothesised relationships against conceptual models.

4.3 Research Approach

In terms of research approaches, Saunders et al. (2019) state that there are three types: deductive, inductive, and abductive. A deductive theory is developed and then tested, while with an inductive approach, a theory is built through data collection. Abductive reasoning is the process through which one believes that their judgements or conclusions are determined by other judgements or premises, by their habit of thought (Psillos, 2011). According to Walton (2001), abduction is distinct from deduction and induction since the conclusion is a hypothesis, or best guess, based on the facts and knowledge available at the time.

4.3.1 Deductive Approach

For this study, the researcher chose the deductive approach. Deductive investigation requires the researcher to specify a particular theory, create propositions, choose measurements, and come to conclusions (Bryman, 2016). Wiles et al. (2011) believe that this approach is efficient in leveraging previous research to investigate possible relations between phenomena. The approach follows the positivist research strategy, characterised by its reliance on well-founded theories, statistical evaluation, and measurable observations (Saunders et al., 2019). However, Saunders et al. (2019) recognise that qualitative methodologies can function in deductive research. Baikie and Priest (2019) outlined a six-step approach to conducting deductive research. The process involves starting with an initial idea, refining it into a hypothesis that can be tested using existing literature, comparing the argument to previous studies, analysing statistical data to determine if they support or contradict the hypotheses, and assessing how well the findings align with the established theory. This approach progresses from central theoretical frameworks to specific empirical examinations to expand our understanding.

Based on this, the researcher starts by relating to the existing body of literature. This study began by examining existing research on the influence of employees' negative and positive emotions on their cybersecurity protection motivation behaviour. Moreover, it explores the role of self-efficacy as a mediator between emotions and protection motivation behaviour and the moderating role of cybersecurity awareness as a moderator between the relationships mentioned. In addition, the current study selected the BBT and PMT, which comprise the foundation for establishing the suggested theoretical model and formulating the research hypotheses.

4.4 Methodological Choices

Figure 14 shows the three main analysis methods: mono, mixed, and multi-method (Saunders et al., 2019). In multi-method research, qualitative and quantitative methods are combined, whereas in mono-method research, only a single quantitative or qualitative method is used. In mixed-method research, two or more quantitative and qualitative methods are used together to conduct the study (Bryman and Bell, 2015). Mixed methods differ from multi-methods primarily in the composition of their datasets as a result of combining different types of data collected through multiple methods (Flick, 2015).

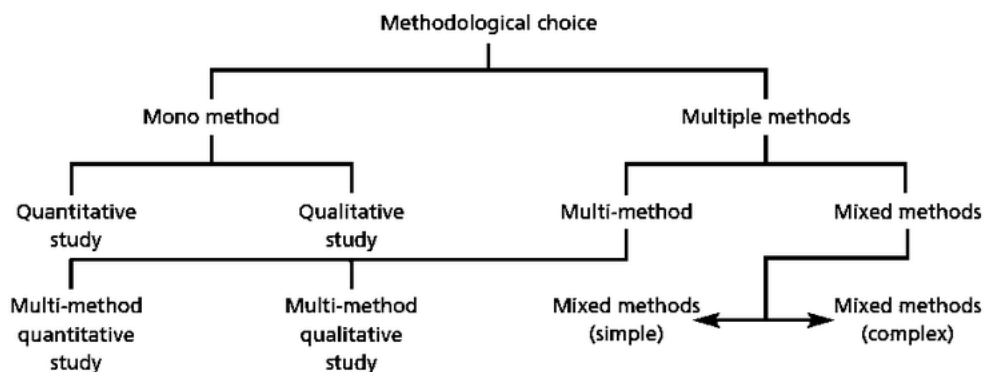


Figure 14: Methodological Choice (Saunders et al., 2019)

Research methods can be categorised into qualitative, quantitative, and combination approaches (qualitative and quantitative). Numerical data are collected quantitatively, whereas qualitative data (words, videos, images) are collected qualitatively. Quantitative methods include gathering and analysing numerical data, whereas qualitative methods involve gathering non-numerical information. However, when both quantitative and qualitative data are gathered for the same study, it is called mixed methods. As stated in this section, the researcher pursues research with a deductive approach and a positivist outlook. Most of the existing research in the research domain uses quantitative methods to advance existing

theories. According to these research conventions, this study uses a mono-method quantitative research design.

4.4.1 Quantitative Research Approach

Measuring and analysing relationships between variables is the basis of the quantitative approach (Creswell, 2014; Saunders et al., 2019). Using quantitative research methods and numerical data, the researcher establishes meanings and relationships between variables. When conducting their analysis, researchers use specific mathematical tools and techniques. In the current study, the researcher chose a quantitative methodology for several reasons:

- I. **Quantitative theory:** The BBT (Fredrickson, 2001) and PMT (Rogers, 1975; Rogers, 1983) are the core theories of this research model. In cybersecurity-related behaviour, the PMT has been applied successfully (e.g. Burns et al., 2017; Zhen et al., 2020; Burns et al., 2019; Menard et al., 2018; Ogbanufe & Pavur, 2022; Thompson et al., 2024) in studies employing a quantitative approach. In addition, the BBT has been adopted to explore the influence of emotions on individuals' behaviours (e.g., Burns et al., 2019; Zhen et al., 2020).
- II. **Positivist paradigm:** Positivist research paradigms are more appropriate for quantitative research, such as this study (Bryman & Bell, 2015; Creswell, 2014; Saunders et al., 2019). This research, which aims to objectively observe the world without the investigator influencing the research problem, requires testing hypotheses about employee protection motivation behaviour.
- III. **Research aim:** According to Creswell (2014), research that seeks to identify factors influencing outcomes should use a quantitative approach. This thesis aims to explore the influences of employees' emotions on their cybersecurity protection motivation behaviour.
- IV. **Deductive reasoning:** The BBT and PMT were used as the starting point for developing the research theoretical model and hypotheses for this research. As a result, deductive reasoning, which is associated with quantitative research, is useful in this study (Bryman, 2016; Saunders et al., 2019).

4.5 Research Strategy

The research strategy helps to formulate the research plan, encompassing the intended goals and objectives and a systematic outline of the steps to be taken (Bryman, 2016; Saunders et al., 2019). To ensure the completion of the study while balancing time and financial constraints, the research strategy must be carefully considered. A research strategy can be a survey, an experiment, a case study, a systematic literature review, or an interview. The most common

method of collecting quantitative research data is by using structured surveys. Research hypotheses are tested by gathering data from large samples (Bryman & Bell, 2015).

4.5.1 Survey Research Method

Researchers have used various methods to gather data in quantitative and qualitative studies, including interviews, surveys, experiments, case studies, etc. Research paradigms, designs, approaches, surveys, target populations, and the researcher's experience will affect the choice of the most appropriate research method (Bryman, 2016; Creswell, 2014). Data are commonly collected through survey research, one of the most popular methods. The purpose of surveys is to collect information about employees' emotions, beliefs, knowledge, and behaviour. Different forms of data collection can be used when conducting a survey, including mail, telephone, personal interviews, fax, and the internet (Fink, 2017; Saunders et al., 2019). However, with surveys, the researcher should ensure that the respondents clearly understand the underlying subject; otherwise, there is a chance of low response rates (Creswell, 2014). For the reasons outlined below, online surveys were chosen for collecting data from participants in this study:

- I. **Generalisability:** In a survey approach, the results from the sample of participants are generalised to the population from which the sample was selected (Saunders et al., 2019). Therefore, the implications of this research regarding employees' protection motivation behaviour can be applied to all employees working at King Abdulaziz University.
- II. **Cybersecurity and behaviour studies:** Questionnaires are considered the main method of data collection in cybersecurity studies investigating human behaviour (Niehaves & Stahl, 2006).
- III. **Exploring emotions:** Creswell (2014) and Saunders et al. (2019) believe that in order to explore attitudes, beliefs, experiences, and behaviours of individuals, survey research is appropriate. This research collected quantitative data about employees' emotions and behaviour related to their cybersecurity protection motivation. Likewise, based on the research model, several hypotheses were suggested in the previous chapter, and these will be analytically tested; the survey approach is necessary to achieve this.
- IV. **Large sample size:** This research collected data from employees at King Abdulaziz University in Saudi Arabia. King Abdulaziz University has 16,433 employees, of whom 8,072 are academics and 8,361 are administrators (Ministry of Education 2017). The survey method can be used to collect data from many university employees. In this study, an online questionnaire was employed to collect the data, as this was less

expensive in terms of cost and time than other tools (e.g., mail survey, interview) (Bryman, 2016).

- V. **The limited budget:** The time and financial budget for this research are limited. However, an online survey can achieve a high response rate within a short period of time without any additional expenses (Rice et al., 2017).
- VI. **Advantages of an online survey:** There is no doubt that there are disadvantages to an online survey, such as the need for an internet connection. However, despite the disadvantages, surveys also have several benefits for researchers (e.g., reducing missing data, and organising and transferring data to SPSS). Completing the survey online allowed the participants to participate from anywhere at any time that suited them (Rice et al., 2017).

4.5.2 Cross-Sectional Design

The two most often employed study designs are longitudinal and cross-sectional. Researchers can conduct longitudinal studies with the same or different participants for an extended period of time (Cohen et al., 2013). Bryman and Bell (2015) explain that a longitudinal design is rarely used because of its high financial and time costs. A cross-sectional design, on the other hand, examines the target population once within a specified period of time (Bryman, 2016). Cross-sectional studies are commonly used due to constraints such as limited funding and time (Sekaran & Bougie, 2016). Regarding this research, the data were collected through a cross-sectional design because of the time and financial constraints.

4.6 Population and Sampling

In research design vocabulary, the population refers to the complete set of persons that the researcher focuses on. In contrast, a sample is a smaller subset of study participants (Gravetter & Forzano, 2018). A sample represents a population selected based on a more significant number of people. A set of procedures should be followed to obtain a representative sample (Hair et al., 2016). These include:

- I. Identify the population of the study.
- II. Identify the sampling framework.
- III. The method of sampling should be either probability-based or non-probability-based.
- IV. Determine the size of the sample.
- V. Develop a sampling plan for the research.

4.6.1 Population

To apply the results to a population, a researcher needs to define the entire group of individuals affected by the research (Saunders et al., 2019). Moreover, Bryman (2016) described the population as all the components from which the sample will be drawn. Regarding this study, the target population was King Abdulaziz University employees in Saudi Arabia. King Abdulaziz University has 16,433 employees, of whom 8,072 are academics, and 8,361 are administrators (Ministry of Education 2017). Additionally, the researcher tried to contact other universities by email, and only King Abdulaziz responded with permission to gather the data from their employees. Thus, the target population of this study is 16,433 employees.

4.6.2 Sampling Techniques

Sample selection usually involves one of two main approaches: probability sampling or non-probability sampling (Bryman, 2016; Creswell, 2014; Gravetter & Forzano, 2018; Hair et al., 2016). Non-probability sampling is used when the investigator has no knowledge about the size of the population and has no ability to list the individuals in the population, therefore the odds of selecting a particular individual are unknown. With probability sampling, an individual's chance of being selected can be calculated. For instance, in a population of 100, each individual has a similar chance of being chosen, resulting in a choice probability of 1/100 for all individuals.

In a non-probability sampling approach, there are many possible techniques, as listed below:

1. Purposive sampling: sample elements are chosen by the researcher based on their judgement.
2. Snowball sampling: probabilistic methods are used to select the first elements in a sample that will aid in identifying the subsequent elements.
3. Quota sampling: stratified sampling is similar to convenience sampling, which selects sample elements according to a proportional basis.
4. Convenience sampling: during the research, only elements that are available to participate are selected as sample elements.

In a probability sampling approach, several techniques can be employed, as listed below:

1. In simple random sampling, probabilities of selection are equal for each unit of the population.

2. Stratified sampling: an equal number of units is sampled for each stratum (proportional), or disproportional units are sampled for each stratum (proportional units).
3. Systematic sampling: This method selects each object on the list starting at a random point in the sampling frame.
4. Cluster sampling: selection of groups rather than individuals in the population because the individuals are already clustered into pre-existing groups.

4.6.3 The Selection of a Sampling Technique

Sampling techniques should be chosen carefully to confirm the truthfulness of the findings. Several factors determine the choice, including the research's nature, the available resources, the research's aim, and the commitment of time and funds (Gravetter & Forzano, 2018; Hair et al., 2016). Therefore, comparing the sampling approaches after considering their differences, probability sampling, and simple random sampling (probabilities of selection are equal for each population unit). The sampling technique was chosen for the following reasons:

1. According to Gravetter and Forzano (2018), three conditions must be met for probability sampling: (1) it must be possible to list all the individuals and know the exact number of people in the population; (2) there must be a probability of selection for every individual in a population; and (3) it is essential that all members of a group have the same chance of selection. For this study, all the listed conditions were met, as the number of employees at King Abdulaziz University was known to be 16,433, of whom 8,072 were academics, and 8,361 were administrators. Moreover, academics and administrators at the university had the same chance to participate whatever their age, nationality or gender. All employees were invited to participate in this research through the university email.
2. Generalisability: A representative sample is usually used to ensure the generalisation of findings in a quantitative research approach. Therefore, the researcher can therefore generalise the results to the population using this sampling technique.
3. Large sample size: the total population of employees at King Abdulaziz University was large, as stated above (Ministry of Education, 2017).

4.6.4 Sampling Procedures

Simple random sampling was selected in this research. One of the basic requirements of random sampling is the ability to be selected from the population with a fair chance (Bryman & Bell, 2015; Gravetter & Forzano, 2018; Saunders et al., 2019). In addition, each selection should be independent of the others, sometimes added as a requirement. The study

population was employees at King Abdulaziz University in Saudi Arabia, which was the only university to give the researcher permission to collect data (see Appendix D), and including more than one university would have been beyond the available resources (time and cost). The university emailed all their employees requesting their participation.

4.6.5 Sample Size

Prior to initiating the data gathering phase, it is crucial to ascertain the magnitude of the target population, which involves considering multiple elements (Bryman, 2016). The research methodology should encompass various considerations, including the distinction between quantitative and qualitative approaches, the number of variables employed, the targeted population, the sample size, financial constraints, time limitations, the potential for generalisation, the precision of measurements, the application of statistical techniques, and the level of confidence in the findings (Hair et al., 2016; Saunders et al., 2019). According to Bryman and Bell (2015), a larger sample size is considered desirable for quantitative research. In this study, it was possible to determine the likely sample size to be obtained through probability sampling by using numerical formulas or by using one's own judgement (Cohen et al., 2013).

Krejcie and Morgan (1970) introduced a table for estimating sample size. Based on the information in the table, researchers can estimate the sample size either by using their own judgement to ensure that the sample accurately represents the population or by employing a mathematical method. Based on the table suggested by Krejcie and Morgan (1970), a minimum sample size of 384 with a 95% confidence level is recommended (see Table 4).

Table 4: Minimum Sample Size (Krejcie & Morgan 1970)

Population Size	Sample Size					
	Sample Table				Current Article Risk-Based Formula	
	95 % Confidence level		99 % Confidence level		Risk Probability	
	5% Error	1% Error	5% Error	1% Error	0.99	0.75
75	63	74	67	75	3	2
300	169	291	207	295	8	6
800	260	739	363	763	20	16
2,500	333	1,984	524	2,173	60	47
25,000	378	6,939	646	9,972	593	462
100,000	383	8,762	662	14,227	2,370	1,848
250,000	384	9,248	662	15,555	6,185	4,618
500,000	384	9,423	663	16,055	12,369	9,235
2,500,000	384	9,423	663	16,478	59,216	46,171

However, when performing multivariate modelling, it is crucial to adhere to specific guidelines to obtain more accurate estimations of the optimal sample size. These recommendations are

relevant in some situations, such as when dealing with a significant population, financial constraints, and limited time (Hair et al., 2016). According to Sue and Ritter (2012), when performing a study, it is essential for the total sample to be a minimum of ten times the total number of variables utilised. Hence, the most appropriate sample size for this research is 280. However, researchers must use caution when considering this approximate calculation (Hair et al., 2014). The criteria do not include the effects of elements such as size, dependability, the number of processes, or additional features that might damage the research model (Hair et al., 2012).

Determining an adequate sample size in PLS-SEM is vital due to the research model's difficulty (Hair et al., 2011). In addition, several factors should be considered when calculating the sample size in PLS-SEM (Hair et al., 2017). The first factor is the highest amount of arrows directing to a construct, followed by the selected level of significance, the desired statistical power, and the coefficient of determination (R^2). Based on the guidelines provided by Hair et al. (2014) and Cohen (1992), as shown in Table 5, this study's minimum required sample size is 137. This calculation assumes a model with four arrows directed toward a construct, a significance threshold of five per cent, a statistical power of eighty per cent, and an R^2 value below 0.10. Thus, the study meets the minimum sample size requirement.

Table 5: PLS-SEM Minimum Sample Size (Hair et al., 2014; Cohen, 1992)

Maximum No of arrows pointing at a construct	Significance Level											
	99% Minimum R2				95% Minimum R2				90% Minimum R2			
1	0.10	0.25	0.50	0.75	0.10	0.25	0.50	0.75	0.10	0.25	0.5	0.75
2	158	75	47	38	110	52	33	26	88	41	26	21
3	176	84	53	42	124	59	38	30	100	48	30	25
4	191	91	58	46	137	65	42	33	111	53	34	27
5	205	98	62	50	147	70	45	36	120	58	37	30
6	217	103	66	53	157	75	48	39	128	62	40	32
7	228	109	69	56	166	80	51	41	136	66	42	35
8	238	114	73	59	174	84	54	44	143	69	45	37
9	247	119	76	62	181	88	57	46	150	73	47	39
10	256	123	79	64	189	91	59	48	156	76	49	41

Moreover, based on the table suggested by Kock and Hadaya (2018), the minimum sample size required for this study is 137 (see Table 6). PLS-SEM investigations employ a significance threshold of five per cent, statistical power of eighty per cent, and a minimum R^2 value of 0.10 (Wong, 2013). This study managed to collect a total of 383 responses from participants, surpassing the recommended sample size specified before.

Table 6: PLS-SEM Minimum Sample Size (Kock & Hadaya, 2018)

Maximum number of arrows pointing at a construct	Minimum R^2 in the model			
	.10	.25	.50	.75
2	110	52	33	26
3	124	59	38	30
4	137	65	42	33
5	147	70	45	36
6	157	75	48	39
7	166	80	51	41
8	174	84	54	44
9	181	88	57	46
10	189	91	59	48

4.7 Instrumentation

This section offers further information regarding the online survey employed to collect participant data. This study employed a survey research approach in order to achieve its objectives and hypotheses. Surveys are one of the most common methods used by researchers to collect quantitative information. Surveys are useful when the research questions are straightforward and the respondents understand the topic; otherwise, they result in many non-responses (Creswell, 2014).

The online survey was based on a systematic methodology outlined in five stages. The first stage was reviewing the literature review to establish a foundation for the online survey. The second stage was conducting a thorough evaluation of the instrument's content and face validity by consulting with specialists. The third stage was translating the survey into Arabic by employing simple terminology and comprehensible phrasing suitable for the intended audience. The fourth stage was conducting a pilot study to guarantee precision and address any concerns with the phrasing. Finally, the dependability of the online survey items was evaluated to verify the internal coherence of the items employed. The subsequent sections provide a detailed explanation of these steps.

4.7.1 Survey Development and Measurements

The measurements of the constructs were validated, and the survey questions were based on previous studies. This study directly employed existing scales from previous studies, which included negative emotions (Beaudry & Pinsonneault, 2010; Burns et al., 2019; Zhen et al., 2022), positive emotions (Beaudry & Pinsonneault, 2010; Bhattacharjee 2001; Watson et al., 1988), self-efficacy (Compeau & Higgins, 1995; Woon & Kankanhalli, 2007; Workman et al., 2008), cybersecurity awareness (Muhirwe & White, 2016), and protection motivation behaviour (Posey et al., 2013, 2015). The online questionnaire was developed based on the

Qualtrics application systems offered by Aston University. After that, the questionnaire was distributed along with an introductory letter that mentioned the importance of the study and the voluntary participation. The online questionnaire comprised six sections: the participants' demographic profile, negative and positive emotions in cybersecurity, self-efficacy, cybersecurity awareness, and the potential influence of these elements on individuals' protection motivation behaviour in cybersecurity. This study employed Likert scales with five and seven response possibilities.

Rating scales and attitude ratings are widely employed in the social sciences (Croasmun & Ostrom, 2011). These instruments frequently employ Likert-type scales. An answer to a statement or set of assertions can be given in various ways using a Likert scale (Jamieson, 2004). However, there is disagreement among researchers as to the ideal quantity of Likert-type options (Cohen et al., 2000), Symonds (1924) claimed that a scale with seven components is the most trustworthy. If there are more than seven, it would be difficult to analyse the differences or build the instrument since the increases in dependability would be so negligible that it would not be worth the effort. In contrast, Jamieson (2004) suggested that using five scales is the most reliable. According to Matell and Jacoby (1971), the number of scale points utilised in an instrument have no bearing on its validity or reliability. In cybersecurity fields, several studies have used both five and seven Likert-type options at the same time.(e.g., Posey et al., 2015; McCormac et al., 2017), while other studies have used four- and five-point Likert-type scales (Canetti et al., 2017; Holt & Kilger, 2008).

Therefore, this study used five- and seven-point Likert-type options, following Matell and Jacoby's (1971) assertion that the validity and reliability of items are not affected by scale options. Moreover, as mentioned earlier, there is evidence that studies in cybersecurity have adopted both five- and seven-point Likert scales. Details of the adopted scales are discussed below.

4.7.1.1 Demographic Profile

The survey's demographic information section requested participants to enter details like their gender, age, level of education, and employment situation.

4.7.1.2 Negative Emotions

In exploring employees' negative emotions, this study used a seven-point, three-item Likert scale adopted from Beaudry and Pinsonneault (2010), Burns et al. (2019) and Zhen et al. (2022). In response to the statements provided, the participants indicated to what extent they

agreed or disagreed. For example, 1 = strongly disagree, 4 = neither agree nor disagree, and 7 = strongly agree.

4.7.1.3 Positive Emotions

Positive emotions were examined using a five-point nine-item Likert scale, with three items adapted from Beaudry and Pinsonneault (2010) and Bhattacharjee (2001). The scale options included happy, excited, and satisfied 'when thinking about protecting my organisation's information resources'. In addition, the researcher added six more items to the scale, adopted from Watson et al. (1988), such as 'interested in compliance with cybersecurity procedures to protect my organisation's information resources' and 'active in countering threats to protect my organisation's information resources'.

4.7.1.4 Self-efficacy

Self-efficacy was measured using a seven-point Likert scale consisting of five items (Compeau & Higgins, 1995; Woon & Kankanhalli, 2007; Workman et al., 2008). There are several scale options, such as: 'I have the skills necessary to protect myself from cybersecurity violations', etc.

4.7.1.5 Cybersecurity Awareness

Cybersecurity awareness was measured using a five-point eight-item Likert scale adapted from Muhirwe and White (2016). In the scale, participants indicated how much they agreed or disagreed with statements such as 'I am aware of the requirements for computer use policies at my workplace' and 'I am aware of the expectations of the computer use policies at my workplace', etc.

4.7.1.6 Protection Motivation Behaviour

Protective motivation behaviour was measured using a five-point three-item Likert scale, adapted from Posey et al. (2013, 2015). The participants were asked to rate how strongly they agreed or disagreed with the statements given to them, from '1 = Strongly Agree' to '5 = Strongly Disagree'. The scale statements included: 'I actively attempted to protect my organisation's information resources.' etc.

4.7.1.7 Construct summary

Table 7 shows the research constructs with item codes, statements, and sources.

Table 7: Constructs Summary

Constructs	Item Code	Statements	Source
Negative Emotions	NE1	I feel discouraged in protecting my organisation's information resources from security threats.	(Beaudry & Pinsonneault, 2010; Burns et al., 2019; Zhen et al., 2022)
	NE2	I feel uneasy in protecting my organisation's information resources from security threats.	
	NE3	I feel angry in protecting my organisation's information resources from security threats.	
Positive Emotions	PE1	I feel happy when thinking about protecting my organisation's information resources.	(Beaudry & Pinsonneault, 2010; Bhattacharjee, 2001; Watson et al., 1988)
	PE2	I feel excited when thinking about protecting my organisation's information resources.	
	PE3	I feel satisfied when thinking about protecting my organisation's information resources.	
	PE4	I feel interested in compliance with cybersecurity procedures to protect my organisation's information resources.	
	PE5	I feel strong in countering and avoiding any threats to protect my organisation's information resources.	
	PE6	I feel active in countering threats to protect my organisation's information resources.	
	PE7	I feel determined to counter any threats to protect my organisation's information resources.	
	PE8	I feel alert about any threats to protect my organisation's information resources.	
	PE9	I feel proud to avoid any threats to protect my organisation's information resources.	
Self-efficacy	SE1	I have the necessary skills to protect myself from cybersecurity violations	(Compeau & Higgins, 1995; Woon & Kankanhalli, 2007; Workman et al., 2008).
	SE2	I have the expertise to implement preventative measures to stop people from getting my confidential information	
	SE3	I have the skills to implement preventative measures to stop people from damaging my work computer	
	SE4	I believe that it is within my control to protect myself from cybersecurity violations	
	SE5	I can enable security measures on my work computer but only when I have manuals for reference	
	CSA1	I am aware of the requirements for computer use policies at my workplace	
	CSA2	I am aware of the expectations of the computer use policies at my workplace.	

Cybersecurity Awareness	CSA3	I am aware of the impact that a virus and other malicious software can have on my computer system	(Muhirwe & White 2016).
	CSA4	I am aware that virus protection software can identify and remove viruses	
	CSA5	I am aware that virus protection software requires frequent updates	
	CSA6	I am aware that I should keep my passwords secure	
	CSA7	I am aware of the impact of responding to phishing emails (e.g. unsolicited emails asking for your bank information)	
	CSA8	I am aware that encryption can prevent unauthorised access to confidential information of the vulnerabilities associated with sharing devices such as files and drives	
Protection motivation behaviours	PMB1	I actively attempted to protect my organisation's information resources.	(Posey et al., 2013, 2015).
	PMB2	I tried to safeguard my organisation's information resources from security threats.	
	PMB3	I purposefully defended my organisation from information security threats to its resources.	

4.7.2 Translation

This study was conducted at King Abdulaziz University in Saudi Arabia. The questionnaire was in two languages, 'English' and 'Arabic', as Arabic is the native language of Saudi Arabia. It is better for the participants to fill in questionnaires in their native language, and the questions should be written in a clear and understandable manner (Dörnyei & Taguchi, 2009; Sekaran & Bougie, 2016). In this regard, an Arabic translation of the questionnaire was provided so that the participants could choose the language that they wanted to complete the questionnaire in. The reason behind using two languages (English and Arabic) is that many employees from different nationalities work at the university. It was essential to ensure the respondents' comprehension of the survey items and to avoid exclusion from participation due to language problems (Ahlmark et al., 2015). Inadequate understanding of the questions can result in erroneous answers and partiality in responses (Sekaran & Bougie, 2016). Thus, it was decided to convert the questionnaire from English to Arabic.

Regarding the survey translation, Fink (2017) recommends using individuals who are fluent in the target language since this minimises the time needed to translate and review the questionnaire's content. The translators in this study were carefully chosen according to the following specifications: (1) they had to possess native proficiency in Arabic and English, along with exceptional writing abilities in both languages; and (2) they had to be well-versed in

creating questions in the Arabic language. An official translator then revised it. The survey's translators are detailed in Table 8.

Table 8: The Survey's Translators

Expert Name	Work Position	Major	Language
Dr Meshari Alali	Assistant Professor, Hail University	English Literature and Linguistics	Arabic English
Dr Fawaz Naif	Assistant Professor, Hail University	Education	
Mohammed Alhymizi	Lecturer, AlJouf University	Business	
Dr Taha Al-Edressi	Official Translator	All subjects	

After the experts had been chosen, the questionnaire was translated from English to Arabic (see Appendix A and B). The experts carried out the translation task separately. Finally, the official translator (Dr Taha Al-Edressi) compared and revised the translation of the survey. Following the initial testing and translation of the questionnaire by specialists, it was necessary to assess the generated questionnaire with participants who represented the population of the study. Thus, a pilot study was carried out.

4.7.3 Pilot Study Results

Prior to the main study, researchers can conduct a pilot study to help identify actual and perceived problems that need addressing. A pilot study is often used to ensure that the questionnaire items are logically phrased and to eliminate errors in wording (Sekaran & Bougie, 2016). It assesses the methods, techniques, interviews, and questionnaires and their functions in specific contexts. According to scholars, pilot studies in research require a small number of typical participants (Bryman, 2016), and they are essential because no one is present to clarify any ambiguities during an online survey (Bryman & Bell, 2015).

An online questionnaire was used for this pilot study so the participants could receive feedback soon after their responses were collected, and clarify any questions they were uncertain about. The pilot study involved a sample of 80 employees from King Abdulaziz University in Saudi Arabia, who were given questionnaires. However, the researcher received only 64 completed surveys. The participants were allowed to enquire about the survey via email after the researcher explained the study's aims and objectives. The construct reliability was assessed using SPSS version 28 following the completion of data collection. According to Field (2013), reliability confirms that the construct has the internal ability and consistency to produce the same findings under similar situations. The calculation is based on average reliability coefficients from splitting a test into two half-tests (Gliem & Gliem, 2003). A reliability higher

than or equal to 0.7 is regarded as acceptable (Sekaran & Bougie, 2016), while 0.8 is considered great (Bryman, 2016).

Table 9 presents the key details for each variable in the pilot study, including the sample size, the number of indicators, Cronbach's alpha, and the mean and standard deviation values. Furthermore, it provides the statistical analysis for all the variables. The evaluation of reliability for each variable utilising Cronbach's alpha is also included. The value for negative emotions, measured by three indicators, is .785. The coefficient for positive emotions, as measured by nine questions, is .949. The self-efficacy value, comprising five indications, is .900. The cybersecurity awareness value, consisting of eight questions, is .902. The value for protective motivation conduct, consisting of three signs, is .952.

Table 9: Pilot Study Construct Reliability

Constructs	N	Number of Indicators	Cronbach's Alpha
Negative emotions	64	3	.785
Positive emotions	64	9	.949
Self-efficacy	64	5	.900
Cybersecurity awareness	64	8	.902
Protection motivation behaviour	64	3	.952

4.8 Data Collection

Researchers must consider the research strategy, tactics, and research question when selecting evidence or data to use for their research (Swartz et al., 2005). Thus, this section discusses the data collection procedures and ethics.

4.8.1 Ethical Considerations

It is essential to consider ethical considerations throughout all phases of data collection in any research project (Bryman, 2016). This research followed the regulations of Aston University, and the online questionnaire was developed based on the Qualtrics application offered by Aston University. Online survey participants were provided with consent forms and participant information sheets. Participants were also informed of the research project's purpose by the researcher. The researcher formally notified the participants that their involvement in the study was completely optional, and they retained the option to withdraw at any point by closing their browser. It was communicated that any data obtained up until the point of withdrawal would not be retained or saved. The participants were told what participation involved, and that the questionnaire would take between 10 and 15 minutes to complete. They were informed that

the study data would be anonymised and that their identifying information, such as their names and emails, would not be collected and would not be possible to locate.

Additionally, the participants were informed that the data collected was for educational purposes and subject to publication. It was explained to them that their participation did not imply a loss of their legal rights. Finally, they were told that research ethical approval had been granted by the Aston University Business School Research Ethics Committee (see Appendix C). and that a formal approval letter had been received from King Abdulaziz University regarding data collection (see Appendix D).

4.8.2 Data Collection Procedures

The researcher reached the target participants with the help of King Abdulaziz University's Deanship of Scientific Research (see Appendix E). The researcher sent a formal letter to the university asking them to distribute the survey to its employees as the researcher had earlier formal approval to conduct the research at the university. As a result, King Abdulaziz University sent emails to the targeted group, administrators and academic employees (see Appendix C). The target employees received a link to the survey through their email and were asked to participate. Data collection for this study occurred over 16 weeks, starting in April 2023 and ending in July 2023.

4.9 Data Analysis

After further analysis of the survey findings, the data were loaded into SPSS. Bryman (2016) asserts that SPSS is an essential statistical method that researchers utilise to provide superior statistical analyses, which produce reliable analysis results and are able to define the correlations and differences among the study variables. The data analysis was conducted in two distinct phases. The data were first imported into SPSS software version 28 for preliminary analysis. This analysis examined the data for any missing data, outliers, unengaged responses, data normality, and common method bias, and descriptive statistics were calculated. During the second phase of the investigation, the proposed model (as described in Chapter 3) was tested. The analysis was performed using the SmartPLS 4 software package, a widely used tool for information on security research (Addae et al., 2019; Al Zaidi, 2017; Chen et al., 2022; Farshadkhah et al., 2021; Hsu et al., 2015; J. Kim et al., 2016; Lu, 2018; Menard et al., 2018; Ogbanufe & Pavur, 2022; Posey et al., 2015; Siponen & Vance, 2010; Thangavelu et al., 2021; Xu et al., 2020; Yoo et al., 2018). The following section provides a concise overview of the methods used for data preparation and the reasons for using structural equation modelling (SEM).

4.9.1 Data Preparation Process for Analysis

This section describes the procedures followed to ensure that the data used in the analysis were accurate and reliable. The process entailed examining the data for missing data, outliers, unengaged responses, data normality, and common method bias, as suggested by Hair et al. (2022). In the context of data analysis, missing data represent the lack of a value for a given variable in an individual observation within a dataset (Hair et al., 2014). Sekaran and Bougie (2016) recognised that when participants fail to answer a question in a questionnaire, it results in missing data. If there is any missing data, it can reduce the amount of data available for research, perhaps leading to inaccurate findings (Hair et al., 2014). As a result, the online survey questions were mandatory, meaning that the participants could not submit their responses without answering all the questions. The submitted replies were therefore complete, with no missing data. Moreover, the dataset was tested for outliers, referring to a participant or observation whose values deviated significantly from those of other respondents. Outliers can arise when a single variable in a univariate study develops an extreme value (Hoyle, 2012). Two types of outliers were tested for in the data: univariate and multivariate. Median Absolute Deviation (MAD) was employed to identify outliers with extreme values in a single variable (Hoyle 2012), and Mahalanobis distance was used to detect outliers with extreme values across multiple variables (Hampel, 1974). Unengaged responses was another test conducted. This refers to suspicious response patterns in which respondents consistently provide the same answer to most or all of the questions (Ibrahim et al., 2015). Mey (2016) suggested that a case should be discarded if the answer pattern is deemed suspicious, as denoted by a value 0. A normality test was also conducted; normality describes data distribution about a particular measurement variable and how much it conforms to a normal (Field, 2013). Skewness and kurtosis values that are between ± 2 are regarded as acceptable (Field, 2013; Gravetter & Forzano, 2018; Trochim & Donnelly, 2006). West et al. (1995) state that skewness levels greater than ± 2 and kurtosis values higher than 7 indicate significant non-normality. Therefore, this study adopted the suggested values above to test the normality. Common method bias was also tested for, employing two methods. This bias can arise from the data collection method rather than from the underlying relationships between variables. Harman's single-factor test suggested by Podsakoff et al. (2003) was used as an initial approach, needing to fall below the 50% threshold. The Variance Inflation Factor (VIF) in PLS-SEM suggested by Kock (2017) was also utilised, with the values of VIFs required to be below 3.3, indicating that the research is not influenced by common method bias (Kock, 2015).

4.9.2 Structural Equation Modelling (SEM)

SEM is commonly employed to examine many statistical associations concurrently by showing the connections and confirming the accuracy of the models (Dash & Paul, 2021). SEM has been utilised to overcome some of the first-generation's drawbacks as a second-generation technology. The association between many factors can be explained using multivariate SEM (Hair et al., 2021). Multiple indicators may be used to quantify unobserved variables, and when analysing the data, the measurement error must be considered (Hair et al., 2021). Due to its use with various multivariate data, it is one of the most critical advancements in quantitative research. Using SEM, the predictive power of reasoning pathways and the identification, analysis, evaluation, and evaluation of linear correlations between observable and unobserved variables are used to illustrate the theoretical validity (Hair et al., 2012). The use of mean causal links and linear relationships for hypothesis testing. The use of SEM procedures in the research is supported by its application in several connected enquiries. SEM can be conducted using two unique approaches: PLS-SEM and covariance-based SEM (CB-SEM). These methodologies could be applied through IBM SPSS Amos and SmartPLS for conducting CB-SEM and PLS-SEM analyses, respectively. Statistical software applications can be employed to investigate the concept of SEM. Two examples of partial least squares algorithms are SmartPLS (Ringle et al., 2015) and IBM SPSS Amos (Analysis of Moment Structures). After thoroughly evaluating every package, it was found that these two were the most accessible and often applied in IS research, although each piece of software has benefits and drawbacks. According to Sarstedt et al. (2021), PLS (variance/regression) is tested by SmartPLS, whilst Amos tests covariance (Hair et al., 2021).

The two SEM methods differ from one another. Only the common variance of the model is assessed by CB-SEM, which necessitates a good fit for the model (i.e., goodness-of-fit). As a result, it can only be used to support research based on established hypotheses. According to Fornell and Larcker (1981), iterating the process to increase the variance of internal structures is how PLS increases variance. The PLS-SEM methodology is founded upon total variance and applies to both exploratory and confirmatory investigations (Hair et al., 2021). Moreover, CB-SEM is commonly observed in the context of theory validation. PLS-SEM might be equally advantageous as multiple regression analysis in the context of exploratory research when the objective is to build a theoretical framework (Hair et al., 2014). In addition, they revealed that the efficacy of the PLS-SEM method in handling small sample numbers and intricate models, including several components. On the contrary, CB-SEM has been acknowledged as a proficient methodology for managing large sample sizes. According to Sarstedt et al. (2021), choosing the most suitable technique depends on the study's objective.

When a sizeable sample (such as $N = 250$) and an adequate number of measurements are utilised, the findings of both strategies are comparable (Hair et al., 2021). These conclusions are supported by numerous empirical studies (e.g., Nam et al., 2018). Both methods were compared and shown to yield similar outcomes in the investigations. Therefore, if appropriately applied, CB-SEM has the same significance as PLS-SEM (Dash & Paul, 2021; Hair et al., 2011).

Having a substantial sample size is a crucial justification for applying CB-SEM, while PLS-SEM is advised for usage with small sample sizes that can be regarded as minimum sample sizes. This is because PLS-SEM can generate statistical power at higher levels with smaller sample numbers than CB-SEM (Hair et al., 2021). PLS-SEM is primarily used for cases involving small sample sizes, non-normal data distributions, and complex research models with more than six components. For these reasons, the PLS-SEM methodology was adopted for this study.

4.10 Summary

In summary, this chapter outlined the research methods applied in the study, which followed a positivist approach and employed quantitative measures to gather empirical data. The administration of the online survey was described. The chapter also covered identifying the target population, calculating an appropriate sample size, and the rationale for the chosen sampling technique. It described the processes of creating and translating the questionnaire, and two pre-testing phases. Additionally, the chapter examined the application of the PLS-SEM method for data analysis, using SmartPLS 4. The next chapter presents the study findings and the results of the data analysis.

Chapter Five: Research Findings

5.1 Introduction

In the prior chapter, the researcher explained and justified the methods used in the current study. This chapter presents the data and the analysis of these data, collected from employees at King Abdulaziz University in Saudi Arabia. Moreover, the data were subjected to analysis after their extraction from the Qualtrics Survey System, and converted into SPSS (SAV) format. In the data preparation, SPSS was used to encode data and assign identification numbers. In addition, for the initial analysis of the data, this study follows the suggestion of Hair et al. (2022), conducting tests to compute the response rate, missing data, outliers, unengaged responses, normality, and common method bias.

Descriptive analysis of the data was conducted, and the results are presented in this chapter.

5.2 Data Preparation

Data preparation is an essential and crucial stage in the data analysis process. It entails converting raw data into a refined and practical shape. Data preparation is crucial for improving the quality and dependability of later analysis and modelling endeavours. Therefore, examining and cleaning the gathered data are vital to guarantee accuracy of the responses (Sue & Ritter, 2012). While it is not always essential to carry out corrective steps, the assessment process is considered a significant tool for ensuring that the results of the univariate and multivariate analysis are reliable (Hair et al., 2014). Hair et al. (2022) stated that it is crucial to examine the underlying reasons for any errors in the data collected, such as strange response patterns, respondents who are not engaged, missing data, outliers, and the data distribution. Therefore, SPSS was used to examine those primary data issues.

As a first step, this section evaluates the response rate to the survey, missing data, outliers (univariate and multivariate), unengaged responses, data distribution (normality), and common method bias. Moreover, the demographic profiles of the employees are presented, detailing their gender, age, educational level, workplace position, and years of experience.

5.2.1 Response Rate

The primary data gathering for the present research was carried out over the course of sixteen weeks, beginning in April 2023 and ending in July 2023. This study's demographic of interest comprised employees working at King Abdulaziz University. King Abdulaziz University has 16,433 employees, of whom 8,072 are academics and 8,361 are administrators. Moreover,

academics and administrators at the university had a chance to participate, whatever their age, nationality or gender. With the cooperation of King Abdulaziz University, all employees were invited to participate in this research through the university email. A total of 383 replies were received. After an initial assessment to detect missing data, outliers, deviations from normality, and unengaged responses, the full data set of 383 responses was deemed suitable for inclusion in the subsequent data analysis. It can be inferred that the study attained the necessary minimum sample size, as indicated in the previous chapter.

5.2.2 Missing Data

As described in Section 4.9.1, all the survey questions were mandatory, and the participants had to answer them all in order to submit the survey. As a result, there were no missing data in the submitted responses.

5.2.3 Outliers

5.2.3.1 Univariate

According to Hair et al. (2016), an outlier is a respondent (observation) whose values are considerably different from those of other respondents. According to Sekaran and Bougie (2016), unreasonable responses are frequently outliers. Hair et al. (2016) found that statistical testing can be biased in the presence of outliers, which can affect the data validity. Outliers must be identified and dealt with correctly as a result. Outliers can be divided into two categories, according to Hoyle (2012): univariate outliers, and multivariate outliers. When a single variable in a univariate analysis has an excessive value, outliers can develop (Hoyle, 2012).

As a univariate identification method, Median Absolute Deviation (MAD) was applied to find outliers according to the suggestion of (Hampel, 1974). According to Hair et al. (2014), univariate detection locates distinctive observations by examining all the metric variables. Three threshold values are frequently employed in univariate statistics to identify outlying values (± 2 or ± 2.5). According to Leys et al. (2013) and Miller (1991), a threshold value of ± 2.5 is recommended, which is considered to be sufficiently conservative. The present study employed a univariate detection method to identify a total of 23 cases that were deemed potential outliers, as they exceeded the threshold of ± 2.5 on numerous items. According to Hair et al. (2014), a choice must be made on the retention or removal of outliers in the dataset after they have been identified as being present in the dataset. A comparison was made between the item's mean value and its 5% trimmed mean value in this study. The purpose of this comparison was to determine whether or not the outliers had an effect on the remaining analysis. Pallant (2020) states that a significant discrepancy between a variable's mean and

a 5% trimmed mean demonstrates the outlier's influence. Table 10 show the item means and trimmed means; there were no significant differences between them.

Table 10: Univariate Outliers

No.	Constructs	Item Code	Mean	5% Trimmed Mean
1	Negative emotions	NE1	2.72	2.59
		NE2	3.06	2.95
		NE3	2.71	2.58
2	Positive emotions	PE1	4.23	4.31
		PE2	4.18	4.25
		PE3	4.21	4.28
		PE4	4.23	4.30
		PE5	4.07	4.15
		PE6	4.04	4.11
		PE7	4.07	4.14
		PE8	4.22	4.28
		PE9	4.27	4.34
3	Self-efficacy	SE1	5.07	5.19
		SE2	5.28	5.40
		SE3	5.16	5.28
		SE4	5.34	5.45
		SE5	5.50	5.64
4	Cybersecurity awareness	CSA1	3.85	3.93
		CSA2	3.75	3.81
		CSA3	4.12	4.21
		CSA4	4.17	4.26
		CSA5	4.33	4.42
		CSA6	4.52	4.62
		CSA7	4.38	4.48
		CSA8	4.17	4.26
5	Protection motivation behaviours	PMB1	4.17	4.26
		PMB2	4.15	4.24
		PMB3	4.14	4.23

5.2.3.2 Multivariate

Multivariate outliers are cases where more than one variable has abnormally high values (Hoyle, 2012; Tabachnick et al., 2013). According to the suggestion of Hair et al., (2014), Hoyle (2012), and Tabachnick et al. (2013), Mahalanobis distance (D^2) can be a beneficial method for detecting multivariate outliers. McLachlan (1999) describes D^2 as the separation between a specific case and the mean of an independent variable. When D^2/df is greater than 3 or 4, with a p-value less than .001, (Hair et al., 2014), this indicates a significant outlier in multivariate analysis for extensive data ($N > 80$). df denotes the study's total number of independent variables, four. Table 11 shows that only five cases were likely be classified as multivariate outliers. The threshold has been exceeded in every case between -4.973 and 2.619.

Table 11: Multivariate Outliers

ID	D ²	p-Value	d/f
5	35.49802	p<.001	-4.9738
77	27.11977	p<.001	-4.38396
1	26.15129	p<.001	-3.97305
50	20.86312	p<.001	-3.31637
78	19.75165	p<.001	2.61968

However, for the following reasons, removing the outliers was not considered. First, there was inadequate proof that these outliers were not among the study's intended participants because the organisation had only emailed the survey to its staff members. This is supported by Hoyle (2012), Tabachnick et al. (2013) and Hair et al. (2014), who state that outliers should not be eliminated unless there is convincing proof that they do not belong to the study population. Second, Hair et al. (2010) state that it is possible that the multivariate analysis may be improved by removing outliers, but this would limit the results' generalisability. Therefore, outliers should not be removed in order to maintain generalisability to the entire study population, if there is inadequate evidence that they are not part of the study population (Hair et al., 2010). Finally, Hoyle (2012) stated that a small number of outliers within a sizeable sample should not cause concerns. Additionally, it is common for a large sample to include a few outliers (Parke, 2012), but these outliers should not have a big impact on the results.

5.2.4 Unengaged Responses

The term "unengaged responses" describes suspicious response patterns in which respondents give a single response to all or nearly all of the questions (Ibrahim et al., 2015). The idea of a line can be denoted as straight-lining (Hair et al., 2017). Diagonal lines have been identified as an additional type of responding response that raises concerns, as noted by Hair et al. (2017). It is assumed that a suspicious response pattern means that the respondent is not engaging actively with the survey.

To detect straight-lining patterns, the standard deviation was calculated for each case, following the methods used by several studies in the domain of information systems (e.g. Barbour et al., 2021; Gotthardt & Mezhuyev, 2022; Kuriakose & Robbins, 2016). According to Mey (2016), the case should be eliminated if the answer pattern is suspicious, which is indicated by a value of 0. After calculating the standard deviation, this study found that the participants in the survey were fully engaged throughout, and the respondents provided different responses to each question. Thus, all answers were included in the data analysis.

5.2.5 Normality

The concept of normality refers to the manner in which data are distributed with respect to a certain metric variable and the level to which they reflect a normal distribution (Field, 2013). The test of normality is a preliminary assessment conducted to ascertain the suitability of the collected data for statistical examination. Hair et al. (2014) stated that in essence, the presence of non-normally distributed data has the potential to influence the accuracy and reliability of multivariate data analysis.

Hair et al. (2022, 2014) suggested testing the skewness and kurtosis of the data distribution. Therefore, the metrics of kurtosis and skewness were utilised to evaluate the distribution of the data. Additionally, the SPSS programme was used to analyse the data for this study. Skewness is a statistical metric used to evaluate the extent of symmetry or asymmetry in a data distribution, indicating whether it is uniformly infrequent or shows a tendency towards elongation. Kurtosis evaluates the degree to which the distribution of data deviates from an average or narrower shape in the centre, specifically measuring the level of peakiness showed by the data. Hair et al. (2016) provide criteria for the examination of the data distribution, with kurtosis and skewness values over ± 1 being indicative of non-normality. Alternative research contends that skewness and kurtosis values that fall within the range of ± 2 are considered to be acceptable (Field, 2013; Gravetter & Forzano, 2018; Trochim & Donnelly, 2006). According to West et al. (1995), skewness levels exceeding ± 2 and kurtosis values surpassing 7 are indicative of significant non-normality. Initially, the demographic data and constructs were tested for skewness and kurtosis, then all the components of the constructs were assessed.

Based on the data presented in Table 12, it can be seen that the bulk of the demographic variables have kurtosis and skewness values that are within the range of ± 2 . Based on this range, it appears that the data relevant to these demographic factors follow a normal distribution. All of the skewness values for the five different constructs were found to fall within the range of ± 2 . However, in relation to the kurtosis findings, it was determined that one particular construct (CSA) did not fall inside the range of ± 2 .

Table 12: Demographic and Construct Normality

	Variables	Skewness		Kurtosis	
		Statistic	Std. Error	Statistic	Std. Error
Demographic Variables	Gender	.549	.125	-1.708	.249
	Age	.867	.125	.541	.249
	Educational level	.021	.125	-1.318	.249
	Work position	-.238	.125	-1.954	.249
	Years of experience	-1.008	.125	.026	.249
Constructs	NE	.744	.125	-.382	.249
	PE	-.736	.125	1.261	.249
	SE	-.717	.125	.015	.249
	CSA	-1.280	.125	3.589	.249
	PMB	-1.031	.125	1.287	.249

Table 13: Item Normality

Indicators	Skewness		Kurtosis	
	Statistic	Std. Error	Statistic	Std. Error
NE1	.832	.125	-.425	.249
NE2	.635	.125	-.823	.249
NE3	.910	.125	-.214	.249
PE1	-1.260	.125	2.418	.249
PE2	-1.040	.125	1.384	.249
PE3	-1.142	.125	1.975	.249
PE4	-1.206	.125	2.026	.249
PE5	-.935	.125	.717	.249
PE6	-.776	.125	.515	.249
PE7	-.748	.125	.067	.249
PE8	-.901	.125	.755	.249
PE9	-1.038	.125	.870	.249
SE1	-.884	.125	.120	.249
SE2	-1.080	.125	.584	.249
SE3	-.858	.125	.079	.249
SE4	-.857	.125	.086	.249
SE5	-1.123	.125	.628	.249
CSA1	-.938	.125	.477	.249
CSA2	-.785	.125	.070	.249
CSA3	-1.178	.125	1.435	.249
CSA4	-1.237	.125	2.027	.249
CSA5	-1.605	.125	3.581	.249
CSA6	-2.087	.125	5.653	.249
CSA7	-1.631	.125	3.222	.249
CSA8	-1.124	.125	1.199	.249
PMB1	-1.116	.125	1.450	.249
PMB2	-1.140	.125	1.473	.249
PMB3	-1.159	.125	1.450	.249

Therefore, it is possible to draw the conclusion that the skewness and kurtosis continue to remain within the scope suggested by West et al. (1995), To be more specific, the authors

recommend that statistically significant deviations from normality are indicated by skewness values that exceed ± 2 and kurtosis values that exceed 7. In addition, this research adopted PLS-SEM, and one of its characteristics is that the data are not necessarily normally distributed (Hair et al., 2022).

Furthermore, Hair et al. (2014) argue that sample size has an effect on the normally distributed nature of the data. Likewise, a sample size of fewer than 200 could affect the data distribution's normality. However, the investigation into data distribution did not reveal any problems with extreme non-normal distribution. As a result, it was decided to keep all of the construct elements since there were no particularly severe implications of non-normality for the dispersed data.

5.2.6 Common Method Bias

According to Malhotra et al. (2006), the primary method of data collecting in the domains of information systems, psychology, and organisational studies is self-reported surveys. This is the case the majority of the time. The use of a self-reported approach for data collection may be susceptible to frequent method bias (Anderson & Agarwal, 2010). Therefore, carrying out an investigation into the existence of prevalent technique bias was an essential part of this research.

Two methods for measuring common method variance were employed to measure the potential presence of common method bias. Regarding the first method, Podsakoff et al. (2003) suggested using Harman's single-factor test as the initial approach. The outcome indicated that the initial component accounts for merely 37.1% of the variation, which falls below the 50% threshold. This implies that there is no significant risk of significant bias. The second technique was proposed by Kock (2017) using the Variance Inflation Factor (VIF). In the PLS-SEM, common method bias refers to a phenomenon that arises from the measuring method employed in a study rather than from the underlying network of causal relationships among the latent variables in the study (Kock, 2015). For instance, the instructions given at the beginning of a questionnaire can impact the responses of several participants in a similar manner, resulting in the indicators displaying a certain level of shared variation. Another potential factor contributing to common method bias is the subconscious tendency to provide socially desirable responses while answering questionnaire questions, resulting in the indicators sharing a certain degree of shared variance (Kock, 2015).

To test common method bias, this research adopted the VIF suggested by Kock (2015). The author further stated that if the VIF is greater than 3.3, this is believed to be a sign of abnormal

collinearity. If VIFs are lower than 3.3, it can be concluded that the research model is not affected by common method bias Kock (2015). The researcher tested the common method bias in SmartPLS, using Collinearity Statistics – the inner model list was calculated for the constructs used in the research. Table 14 shows that all the constructs met the acceptable criterion as they did not exceed 3.3.

Table 14: VIF

Paths	VIF
CSA -> PMB	1.808
NE -> PMB	1.116
NE -> SE	1.075
PE -> PMB	1.776
PE -> SE	1.078
SE -> PMB	2.051

5.3 Demographic Profile

Huysamen (1990) states that descriptive statistics can consolidate, summarise, and present data systematically and accurately. Data were gathered via the online survey about the respondents' demographics. The respondents' profiles, which include details on gender, age, educational level, work position, and years of experience, demonstrate the diversity of the workforce participating in this survey.

5.3.1 Gender

All respondents were instructed to indicate their gender by selecting from a nominal scale, with the options of (1) male or (2) female. As shown in Table 15 and Figure 15, male employees were found to be in the majority, accounting for 63.2% of the total employees, whereas female employees made up 36.8%.

Table 15: Gender of Respondents

Gender	Number (n)	Percentage
Male	242	63.2%
Female	141	36.8%
Total	383	100

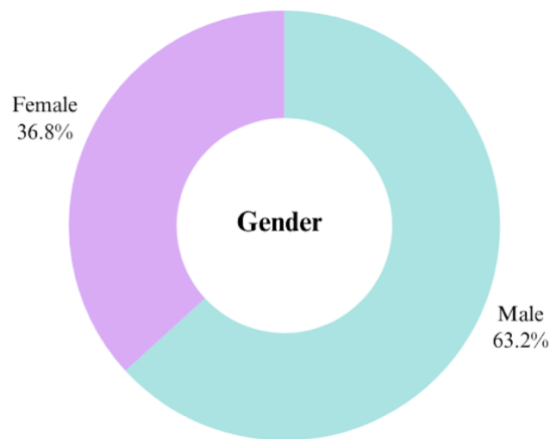


Figure 15: Gender Distribution

5.3.2 Age

The measurement of age in this study employed a nominal scale, with the age variable categorised into five distinct groups: 18 to 29, 30 to 39, 40 to 49, 50 to 59, and 60 and above. The participants were instructed to select their age category. The data presented in Table 16 and Figure 16 reveal that most participants fell within the age range of 30 to 39 years, accounting for 53% of the total respondents. The second highest percentage of responders, at 19.6%, were 40 to 49 years old. The other age distributions of the survey respondents are as follows: 18 to 29-year-olds account for 14.4% of the total, 50 to 59-year-olds account for 9.7%, and those aged 60 and beyond account for 3.4%.

Table 16: Age of Respondents

Age	Number (n)	Percentage
18 to 29	55	14.4%
30 to 39	203	53%
40 to 49	75	19.6%
50 to 59	37	9.7%
60 and over	13	3.4%
Total	383	100

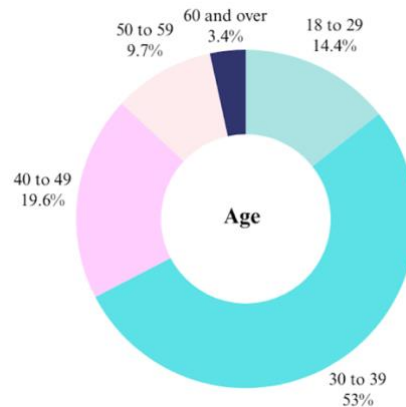


Figure 16: Age Distribution

5.3.3 Employees' Educational Level

The measurement of education level was conducted using an ordinal scale, wherein employees were required to indicate their educational attainment by selecting one of the following options: (1) high school, (2) bachelor's degree, (3) diploma, (4) master's degree, (5) doctorate in philosophy, or (6) other. The respondents' educational levels are analysed and presented in Table 17 and Figure 17. The results found that (5.2%) of the respondents had a high school; (37.1%) had a bachelor, (4.7 %) had a Diploma, (31.0 %) had a master, (19.3 %) had a Doctor of Philosophy, and finally, 1.8 % of the respondents indicate other.

Table 17: Educational Level of Respondents

Education level	Number (n)	Percentage
High school	20	5.2%
Bachelor	142	37.1%
Diploma	18	4.7%
Master	122	31.9%
Doctor of Philosophy	74	19.3
Other	7	1.8%
Total	383	100%

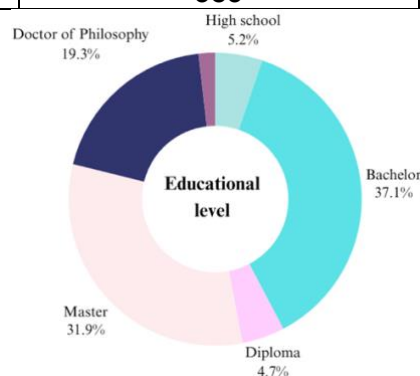


Figure 17: Educational Level Distribution

5.3.4 Employees' Work Position

Based on the employees' responses, Table 18 and Figure 18 present the frequency and percentages of employees who worked in either an academic or administrative role at the university. A total of 169 employees, accounting for 44.1% of the respondents, were classified as academic, whilst 214 employees, representing 55.9% of the respondents, were categorised as administrative.

Table 18: Work Position of Respondents

Work Position	Number (n)	Percentage
Academic	169	44.1%
Administrative	214	55.9%
Total	383	100.0

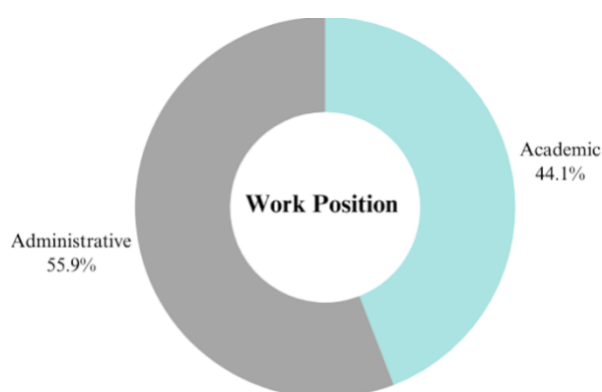


Figure 18: Work Position Distribution

5.3.5 Employees' Years of Experience

The measurement of employees' years of experience was conducted using a nominal scale. The employees were provided with the options of selecting either (1) less than one year or (2) one to three years. Option (3) represents a time frame of less than 3-5 years, option (4) corresponds to a duration of 5-10 years, and option (5) denotes a period above 10 years. Table 19 and Figure 19 shows that 24 (6.3%) of the employees had < 1-year of work experience, 35 (9.1%) had 1-3 years of experience, 48 (12.5%) had 3-5 years of experience, 117 (30.5%) had 5-10 to 5 years of experience, and finally, 159 (41.5%) of them have more than 10 years of experience.

Table 19: Years of Experience of Respondents

Years of Experiences	Number (n)	Percentage
< 1 year	24	6.3%
1-3 years	35	9.1%
3-5 years	48	12.5%

5-10 years	117	30.5%
More than 10 years	159	41.5%
Total	383	100

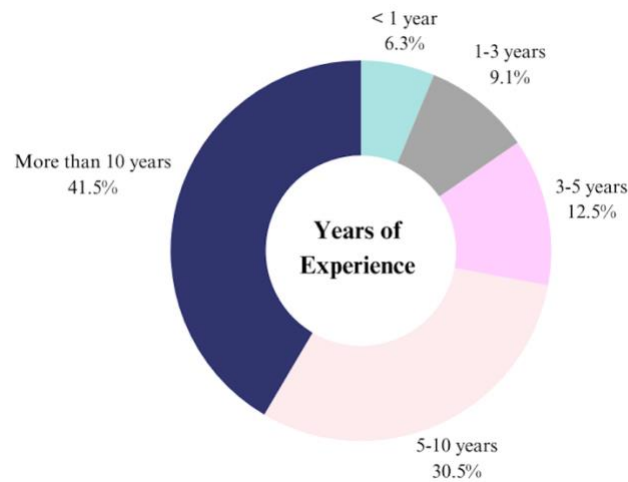


Figure 19: Years of Experience Distribution

5.4 Descriptive Statistics of the Constructs

The construct of the descriptive statistics is used to comprehend data in a quantitative manner. The standard deviation and mean are used in this research to define its constructs. Table 20 presents a descriptive analysis of the construct code, number of respondents, indicators of each construct, the highest and lowest values, as well as the standard deviation and mean of each construct. The means range from 2.8294 to 5.2700. The mean for negative emotions (2.8294) is closer to 3 ("Somewhat disagree") than it is to 7 ("Strongly agree"). The findings demonstrate that employees are likely to disagree somewhat that negative emotions affect their protection motivation behaviour. The mean for positive emotions is 4.1688, which indicates that they are closer to 7 "Strongly agree" than to 1 "Strongly disagree", which suggests that employees believed that positive emotions had a positive effect on their protection motivation. The mean for self-efficacy (5.2700) is closer to 7 ("Strongly agree") than it is to 1 ("Strongly disagree"), which indicates that the employees felt that they were capable in their protection motivation. The mean for employee cybersecurity awareness (4.1622) is closer to 5 than 1, thus indicating that the employees believed that they had a high level of cybersecurity awareness. Finally, the mean for protection motivation behaviour (4.1575) is also closer to 5 than it is to 1, which indicates that the employees felt that they engaged in protection motivation behaviour. The standard deviations ranged from .65377 to 1.59202. Therefore, all indicators continue to have low standard deviation (SD) values.

Table 20: Descriptive Statistics

	Constructs Code	N Statistic	Indicators	Minimum	Maximum	Mean	Std. Deviation
1	NE	383	3	1	7	2.8294	1.59202
2	PE	383	9	1	5	4.1688	.65398
3	SE	383	5	1	7	5.2700	1.25807
4	CSA	383	8	1	5	4.1622	.63577
5	PMB	383	3	1	5	4.1575	.79474

5.5 Model Evaluation

In the previous section, the statistical program SPSS was employed to carry out several initial assessments. These analyses comprised descriptive analysis of the response rate, data preparation, the demographic profiles of the participants, and the research constructs. This section looks at the methodology utilised, which includes analysis and justification for the adoption of the PLS-SEM method for performing the analysis and then evaluating the model.

The data were taken from SPSS and saved in a .csv file format. They were imported into SmartPLS software version 4 so that additional analysis and model testing could be carried out. Researchers have proposed a process for utilising PLS-SEM for model testing (Fornell et al., 2018; Hair et al., 2022; Henseler et al., 2016; Ali et al., 2018). The process involves two separate phases: the evaluation of the measurement model and the evaluation of the structural model. The subsequent sections of this section illustrate the execution techniques to evaluate the fitness of the model to the data.

5.5.1 Measurement Model

Hair et al. (2014) and Henseler and Sarstedt (2013) stated that the measurement model is a framework encompassing the relationships across variables and related indicators. Indicators are used to measure constructions, and the measurement model refers to the manner in which we use these indicators. The utilisation of SEM allows researchers to employ multiple indicators to measure a single variable, thereby improving the precision of the measurement (Hair et al., 2022). On account of this, the dependability and validity of the indicators that are employed in the analysis of numerous variables are crucial. Additionally, it is assumed that the assessment of the measurement model needs to satisfy the essential principles of validity and reliability. When this occurs, the assessment of the structural model that will take place in the subsequent stage is rendered meaningless (Hair et al., 2012).

Hair et al. (2022) and Fornell et al. (2018) offered suggestions for the evaluation and evidence of the measurement model. Several important characteristics are included in the principles discussed in this research. These characteristics include convergent validity, discriminant

validity, concept reliability, and indicator reliability. Table 21 summarises the criteria employed within the context of PLS-SEM to assess the measurement framework utilised in the current study.

Table 21: Measurement Model Criteria

Criteria	Test	Values	Source
Indicator reliability	loadings	Loadings/A value of 0.7 or higher	(Chin, 1998; Hulland, 1999)
Internal consistency	Cronbach's alpha (CA)	A value of 0.7 or higher	(Cronbach, 1951)
Construct reliability	Composite reliability (CR)	A value of 0.7 or higher	(Hair et al., 2022)
	Confidence intervals	95% bootstrap confidence interval	(Hair et al., 2019)
Convergent validity	AVE	A value of 0.5 or higher	(Fornell & Larcker, 1981)
Discriminant validity	Cross-loadings	The correlations between the observed variables and other variables.	(Chin, 1998).
	Fornell-Larcker Criterion	Calculating AVE and comparing it to between the correlation's constructs.	(Fornell & Larcker, 1981)
	HTMT	A value of 0.90 or less	(Henseler et al., 2015)
	Bootstrapping	HTMT should exclude the value of 1.0.	(Hair et al., 2016)

The subsequent subsections show the outcomes of assessments to determine the research reliability and validity in accordance with the specified standards and recommendations.

5.5.1.1 Indicator Reliability

Indicator reliability is calculated using the outer-loading terms. According to Snyder (2019), when outer loading is high, there is a high degree of similarity. The outer loading is a variable that ranges from zero to one. A more significant rate, closer to one, implies a higher reliability (Torlak et al., 2021). According to the suggestions from researchers (Chin, 1998; Hulland, 1999), it is advisable to make sure that each outer-loading indicator can surpass 0.7 to attain the reliability of the indicator. Utilising the PLS algorithm with the iteration of 1000, the findings in Table 22 show that most of the indicators in the outer loading meet the acceptability criteria except items (CSA 1, CSA2, and CSA4). These fell short of the threshold suggested, and were therefore removed from the analysis.

Table 22: Measurement Model Assessment Results

Constructs	Items	Loadings > 0.7	Cronbach's alpha > 0.7	Composite reliability > 0.7	Average variance extracted > 0.5
CSA	CSA3	0.779	0.848	0.850	0.622
	CSA5	0.766			
	CSA6	0.788			
	CSA7	0.840			
	CSA8	0.766			
NE	NE1	0.912	0.868	0.917	0.787
	NE2	0.846			
	NE3	0.902			
PE	PE1	0.791	0.913	0.928	0.589
	PE2	0.799			
	PE3	0.791			
	PE4	0.751			
	PE5	0.734			
	PE6	0.775			
	PE7	0.791			
	PE8	0.701			
	PE9	0.767			
PMB	PMB1	0.891	0.896	0.935	0.827
	PMB2	0.927			
	PMB3	0.910			
SE	SE1	0.855	0.854	0.891	0.637
	SE2	0.851			
	SE3	0.859			
	SE4	0.713			
	SE5	0.695			

5.5.1.2 Construct Reliability

Ensuring the measurement model's reliability is critical in any research because if the constructs are unreliable, then the final research outcomes will not be achieved when the data are analysed (Hwang et al., 2021). Reliability consistently provides the same results when used for similar scenarios or cases (Field 2013). In the context of social science, researchers have used internal consistency to measure the variables' reliability using the method of CA (Ali et al., 2018). CA can sometimes make items more reliable than they could be (Bairagi & Munot, 2019). Thus, researchers are suggested to report CR and CA to gain a clear and accurate picture of construct reliability (Hair et al., 2022). In situations where the numbers are ignored, the dependability scores can range from zero to one, with greater values closer to one representing more excellent reliability. Different researchers set different standards. Some

state that 0.6 and 0.7 are acceptable, and according to some, 0.8 is acceptable (Hair et al., 2022). In the context of an exploratory study, it has been suggested by Ali et al. (2018) that values ranging from 0.6 to 0.7 for CA and CR are deemed adequate. Table 22 presents the results of the reliability test for this study. The CA ratings range between 0.848 and 0.913, and the CR values sit between 0.850 and 0.935. The findings demonstrate that the measuring model that was provided possesses a high degree of reliability.

5.5.1.3 Convergent Validity

Convergent validity is a crucial concept in research and it is used to validate measurement tools and assess the strength of connections among the constructs (Russo & Stol, 2021). In addition, it refers to the degree to which two or more processes may be predicted to be related in a theoretical sense. The empirical findings demonstrate a positive relationship between them (Babii, 2020). Construct validity is validated by convergent validity, which investigates whether or not distinct measures of the same variables or constructs come together as estimated and offer evidence of construct validity. Fornell and Larcker (1981) stated that convergent validity is accomplished when each indicator's outer loading is above 0.7 and AVE is 0.5 or above for each construct.

Convergent validity is one essential aspect that assists researchers in establishing measurement instruments' precision and accuracy. When multiple measures of the same construct yield the same results, it increases the researchers' confidence that they are measuring what they were intended to measure (Devi, 2017). Conversely, if measures do not converge as expected, it indicates problems with the measurement tools of the conceptualisation construct (Deng et al., 2018). If the AVE is equal to or greater than 0.5, this suggests that approximately fifty per cent of the inconsistency in the measurement variables can be justified through the variables being measured (Fornell & Larcker, 1981; Makransky & Petersen, 2019). Table 22 illustrates the values of AVE.

5.5.1.4 Discriminant Validity

Discriminant validity implies to the extent to which a particular indicator or idea is distinguishable from several other variables contained within the model and successfully captures the specific characteristics of the parameter that is being targeted (Sarstedt & Cheah, 2019). According to Latan et al. (2017), each variable must show a correlation with its respective indicator rather than with other construct variables. In testing the discriminant validity, the researcher could apply three necessary tests, namely cross-loadings, Fornell-Larcker, and finally, HTMT Ratio (Avkiran & Ringle, 2018; Chua, 2022)

5.5.1.4.1 Cross-Loading

Cross-loading is the concept commonly encountered in confirmatory factor analysis (CFA) and SEM. It involves a scenario where the observed variable or indicator demonstrates significant factor loadings on many latent variable constructs or factors in the measurement model (Chua, 2022). The presence of cross-loading can create difficulties in ensuring the distinctiveness and compatibility of the measurement model, as it suggests that the indicator cannot be a pure reflection of a single variable (Sarstedt & Cheah, 2019). Hair et al. (2023) provide the guideline that the cross-loading value is acceptable if it lies between 0.5 and 0.7. However, items/constructs with a cross-loading value <0.5 are eliminated because they cannot contribute to AVE and CR or composite reliability. Sarstedt and Cheah (2019) stated that independent subjectivity can help to minimise multi-collinearity among the latent constructs when a variable's AVE is greater than the correlation of a latent variable with another construct. Table 23 below demonstrates that each indicator's value meets the suggested thresholds.

Table 23: Cross-Loadings

	CSA	NE	PE	PMB	SE
CSA3	0.779	-0.227	0.389	0.511	0.520
CSA5	0.766	-0.270	0.358	0.407	0.408
CSA6	0.788	-0.226	0.396	0.423	0.401
CSA7	0.840	-0.239	0.380	0.447	0.375
CSA8	0.766	-0.183	0.404	0.477	0.447
NE1	-0.298	0.912	-0.133	-0.178	-0.153
NE2	-0.154	0.846	-0.059	-0.066	-0.135
NE3	-0.280	0.902	-0.157	-0.185	-0.139
PE1	0.347	-0.047	0.791	0.434	0.378
PE2	0.403	-0.049	0.799	0.464	0.400
PE3	0.389	-0.148	0.791	0.445	0.368
PE4	0.361	-0.156	0.751	0.411	0.366
PE5	0.336	-0.087	0.734	0.319	0.365
PE6	0.396	-0.169	0.775	0.435	0.410
PE7	0.361	-0.072	0.791	0.372	0.403
PE8	0.422	-0.125	0.701	0.420	0.440
PE9	0.354	-0.114	0.767	0.416	0.349
PMB1	0.487	-0.169	0.460	0.891	0.486
PMB2	0.570	-0.167	0.518	0.927	0.522
PMB3	0.519	-0.136	0.497	0.910	0.477
SE1	0.435	-0.150	0.403	0.462	0.855
SE2	0.493	-0.138	0.451	0.421	0.851
SE3	0.404	-0.131	0.397	0.460	0.859
SE4	0.368	-0.050	0.349	0.421	0.713
SE5	0.496	-0.169	0.414	0.406	0.695

5.5.1.4.2 Fornell-Larcker Criterion

The Fornell-Larcker criterion is a widely used method for SEM and CFA to assess the research construct discriminant validity (Lê Cao & Welham, 2021). By measuring the AVE square root, the Fornell-Larcker test is utilised to control the variance of each item (Fornell & Larcker, 1981; Wong, 2019). This testing method provides a statistical test to determine whether the extracted variance from factors or latent constructs in the model is more significant than the construct-shared variances (Hair et al., 2023). Latan et al. (2017) state that the principle of discriminant validity helps to determine whether or not various construct measures are sufficiently dissimilar. Table 24 demonstrates that the AVE values exceed the correlation coefficient between the components, suggesting that discriminant validity is satisfactory (Fornell & Larcker, 1981).

Table 24: Fornell-Larcker Criterion

	CSA	NE	PE	PMB	SE
CSA	0.788				
NE	-0.289	0.887			
PE	0.490	-0.140	0.767		
PMB	0.579	-0.173	0.542	0.910	
SE	0.551	-0.161	0.505	0.545	0.798

5.5.1.4.3 Heterotrait-Monotrait (HTMT) Ratio

Another method to test the validity is HTMT. According to Deng et al. (2018), the HTMT ratio is a statistical test used to assess the relationship between variables. Deng et al. (2018) defined threshold values of HTMT as less than 1, representing the variable's discriminant validity as close to 1. Researchers may not agree universally on the specific value of the threshold for the HTMT ratio; a common guideline is that the ratio should be below 0.85 or 0.90 for the discriminant validity of solid evidence (Hwang et al., 2021; Crespo et al., 2019; Henseler et al., 2015). The average correlation between different variables should be less than 85% to 90% of the average correlation between similar variables/constructs. Table 25 shows that each construct's value is less than 0.9. Hence, the test shows that the constructs defined are discriminately valid and there is no multi-collinearity between the variables.

Table 25: HTMT

	CSA	NE	PE	PMB	SE
CSA					
NE	0.322				
PE	0.553	0.152			
PMB	0.658	0.182	0.595		
SE	0.644	0.185	0.572	0.624	

This section tested and discussed the validity and reliability of the model, including CA and CR. The next section assesses the research model.

5.5.2 Structural Model Assessment

It is usual practice to refer to the "structural model" as the "inner model" when discussing the linkages between variables. Its evaluation involves the examination of links among variables or constructs within the model (Torlak et al., 2021). The evaluation and reporting of structural models should follow specific guidelines and principles, including the examination of collinearity, path coefficients, R^2 (Coefficient of Determination), effect size (f^2), and the use of a cross-validated predictive ability test (CVPAT) (Hair et al., 2022; Hair et al., 2011; Kock, 2017; Chin, 1998; Cohen, 1988; Liengard et al., 2021; Avkiran & Ringle, 2018). Moreover, researchers on PLS-SEM have identified that most researchers report the criteria mentioned above for the structural model examination (Latan et al., 2017). Table 26 illustrates the guidelines used widely by researchers to test structural models.

Table 26: Structural Model Assessment

Criteria	Standards	Source
Collinearity	• Tolerance > 2 • VIF < 5	(Hair et al., 2022; Hair et al., 2011).
Path coefficients	• p-value < 0.05 • One-tailed • Bootstrapping with 10,000 sub-samples	(Hair et al., 2022; Kock, 2017).
Coefficient of Determination – R^2	• Weak effect if $0 < R^2 < 0.9$ • Moderate effect if $0 < R^2 < 0.33$ • High effect if $0 < R^2 < 0.67$	(Chin, 1998).
Effect Size - f^2	• 0.02 small • 0.15 moderate • 0.35 large	(Cohen, 1988)
Predictive relevance	• Cross-Validated Predictive Ability Test (CVPAT) • < 0	(Liengard et al., 2021)

5.5.2.1 Collinearity

Collinearity in any research arises when two constructs are highly correlated, producing issues related to interpretation (Kock, 2017). According to Kock and Hadaya (2018), the VIF is used to assess collinearity and is calculated by taking the reciprocal of the tolerance value. The tolerance value represents the variance attributed to the independent variables. A VIF value higher than 5 reveals an extreme degree of collinearity (Hair et al., 2022, 2011). Table 27 shows the VIF values for this study's independent variables/constructs and shows that collinearity is not an issue.

Table 27: Collinearity

	CSA	NE	PE	PMB	SE
CSA				1.808	
NE				1.116	1.075
PE				1.776	1.078
PMB					
SE				2.051	

5.5.2.2 Path Coefficients

In research, the path coefficient refers to the estimated relationships among the constructs of a model (Chua, 2022). This aids in establishing the correlation between the construct articulated and specified by the hypothesis (Wong, 2019). Various tests are conducted in order to ascertain the relationship between variables. Topor (2016) defines the route coefficient as a quantitative measure that can vary between 1 and -1. A value of 1 signifies a strong positive correlation, whereas a value of 0 implies a weaker correlation or no correlation at all, and a value of -1 signifies a significant negative relationship. When allocating the path of PLS, it is essential for researchers to include the path coefficient value, as well as the p-value, t-value, and level of significance (Torlak et al., 2021). According to Civelek (2018), PLS-SEM is commonly employed in research studies to analyse and provide several statistical measures. These measures include path coefficients, significance levels, p-values, and t-values, which are crucial when assessing the structural model. The aforementioned values would be recorded in the path analysis.

In SmartPLS 4, the first step is to run the PLS algorithm that generates a path coefficient to show relationships, either positive or negative. The second step is bootstrapping, which provides the p-value, t-value, and significance level to determine constructed relationships. SmartPLS 4 was employed to evaluate the research hypotheses and determine the path coefficients. Moreover, bootstrapping was used with 10000 sub-samples—this is a method of informal statistical analysis that involves the extraction of numerous sub-samples from the

initial data sample (Hair et al., 2022; Kock, 2017). Subsequently, models are reviewed and analysed for each of these sub-samples (Basias & Pollalis, 2018). For hypothesis testing, one-tailed testing was performed in the context of hypothesis acceptance; it is considered appropriate to accept a hypothesis when the significance level (p-value) is below 0.05 and the t-value is above 1.96. Table 28 defines the hypotheses' directions.

Table 28: Results of Path Analysis

H#	Path direction	Path meaning
H ₁	NE -> PMB	The relationship between negative emotions and protection motivation behaviour.
H ₂	NE -> SE	The relationship between negative emotions and self-efficacy
H ₃	PE -> PMB	The relationship between positive emotions and protection motivation behaviour.
H ₄	PE -> SE	The relationship between positive emotions and self-efficacy
H ₅	SE-> PMB	The relationship between self-efficacy and protection motivation behaviour.
H ₆	NE -> SE -> PMB	Self-efficacy intervenes in negative emotions and employees' protection motivation behaviours.
H ₇	PE -> SE -> PMB	Self-efficacy intervenes the positive emotions and employees' protection motivation behaviours..
H ₈	CSA-> PMB	The relationship between cybersecurity awareness and protection motivation behaviour
H ₉	CSA x NE -> PMB	Cybersecurity awareness moderates the direct relationship between negative emotions and protection motivation behaviours.
H ₁₀	CSA x NE -> SE	Cybersecurity awareness moderates the relationship between negative emotions and self-efficacy.
H ₁₁	CSA x PE -> PMB	Cybersecurity awareness moderates the direct relationship between positive emotions and protection motivation behaviours.
H ₁₂	CSA x PE -> SE	Cybersecurity awareness moderates the relationship between positive emotions and self-efficacy.
H ₁₃	CSA x SE -> PMB	Cybersecurity awareness moderates the relationship between Self-efficacy and protection motivation behaviours.

Based on the analysis results, Table 29 and Figure 20 show the overall hypotheses relationships tested in the model. Eight out of 13 hypotheses were supported, and five were rejected. The accepted hypotheses are H₃, H₄, H₅, H₇, H₈, H₁₀, H₁₁, and H₁₂. The rejected hypotheses are H₁, H₂, H₆, H₉, and H₁₀.

Table 29: Hypotheses' Results

H#	Paths	Original sample	Sample mean	Standard deviation	T statistics	P-values
H ₁	NE -> PMB	-0.007	-0.011	0.040	0.184	0.854
H ₂	NE -> SE	-0.009	-0.012	0.042	0.209	0.835
H ₃	PE ->PMB	0.266***	0.267	0.054	4.885	0.000
H ₄	PE -> SE	0.545***	0.544	0.040	13.542	0.000
H ₅	SE-> PMB	0.232***	0.233	0.052	4.454	0.000
H ₆	NE -> SE -> PMB	-0.002	-0.002	0.010	0.204	0.839
H ₇	PE -> SE -> PMB	0.127***	0.127	0.030	4.239	0.000
H ₈	CSA-> PMB	0.322***	0.322	0.068	4.767	0.000
H ₉	CSA x NE -> PMB	-0.016	-0.019	0.047	0.337	0.736
H ₁₀	CSA x NE -> SE	0.029	0.028	0.047	0.611	0.542
H ₁₁	CSA x PE -> PMB	0.180*	0.168	0.087	2.080	0.038
H ₁₂	CSA x PE -> SE	0.776*	0.720	0.328	2.366	0.018
H ₁₃	CSA x SE -> PMB	-0.204*	-0.198	0.080	2.539	0.011

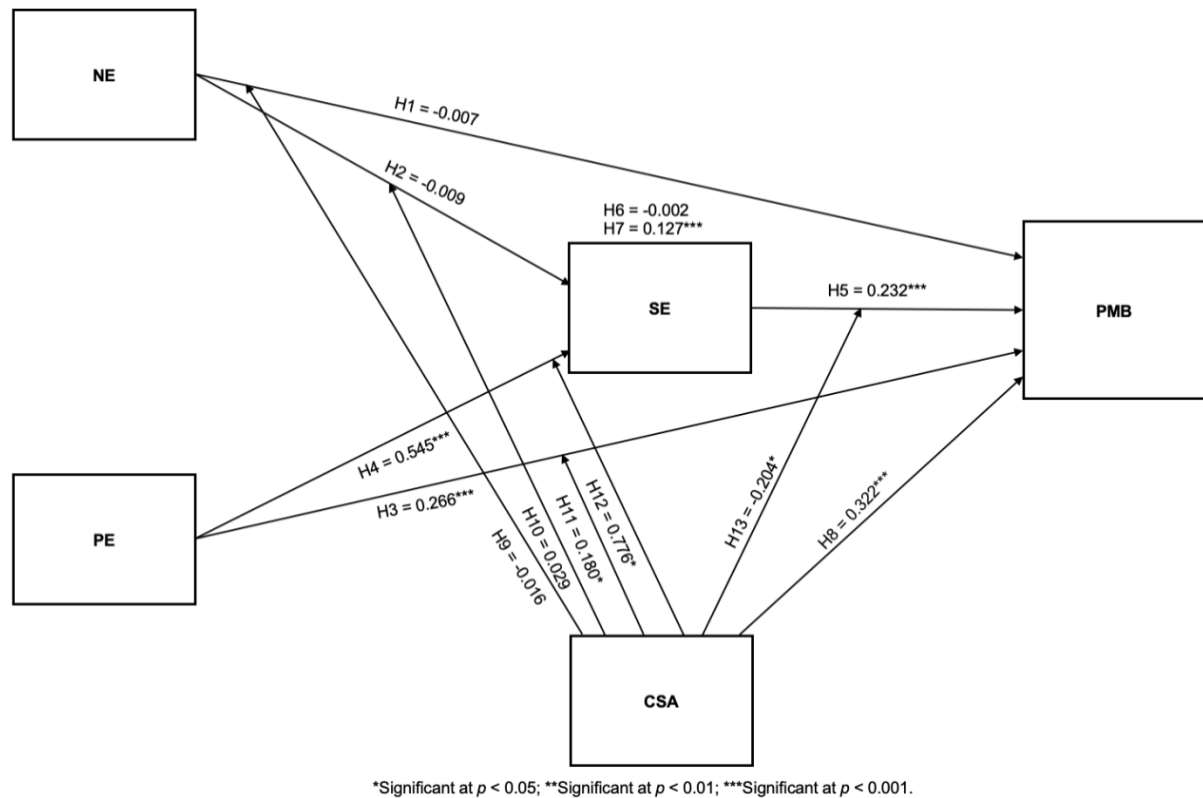


Figure 20: Theoretical Framework Results

Figure 20 represents the model of the results interpreted above. **H₁**, which hypothesises that negative emotions promote negative protection motivation behaviour among employees, was rejected (β -value = -0.007 and p -value = 0.845). **H₂**, which hypothesises that negative emotions have a negative effect on employees' self-efficacy, was also rejected (β -value = -

0.009 and p-value = 0.835). **H₃**, which hypothesises that positive emotions promote a positive protection motivation behaviour among employees, was accepted (β -value = 0.266*** and p-value = 0.000). Hypothesis **H₄**, which states that positive emotions have a beneficial effect on employees' self-efficacy, was also accepted (β -value = 0.545*** and p-value = 0.000). **H₅**, which hypothesises that self-efficacy promotes a positive protection motivation behaviour among employees, was accepted (β -value = 0.232*** and p-value = 0.000), and finally, **H₈**, which hypothesises that cybersecurity awareness has a positive effect on employee protection motivation behaviour, was accepted (β -value = 0.332*** and p-value = 0.000).

5.5.2.3 Mediation

The mediation model is employed to explain the mechanisms by which a predictor variable is linked to an outcome indicator (Baron & Kenny, 1986; Frazier et al., 2004). Moreover, the mediator variable is an indicator that enables a causal association between both the independent and the dependent variables. It reveals the correlation between the reliant variable and the independent variable (Hair et al., 2022). Mediation modelling is beneficial in cybersecurity and information security research because it assesses complex relational patterns across factors, hence presenting valued perceptions of complex psychological effects. According to the PMT, this research shows that self-efficacy mediates the relationship between negative and positive emotions and employees' cybersecurity protection motivation behaviour. Therefore, the researcher employed the suggestion of Hair et al. (2022), that in SmartPLS, the outcomes of the PLS-SEM algorithm and the bootstrap technique encompass the direct effect, total indirect effect, particular indirect effects, and overall effect. Thus, the SmartPLS results reports provide the necessary outputs for a mediator analysis.

A mediation analysis was performed to assess the mediating role of self-efficacy in the relationship between negative and positive emotions and employees' protection motivation behaviour. The results in Table 30 reveal an insignificant indirect effect of negative emotions on protection motivation behaviour (**H₆**: β = -0.002, t = 0.204, p = 0.839). The total impact of negative emotions on protection motivation behaviour was insignificant (β = -0.009, t = 0.232, p = 0.817); with the inclusion of the mediator, the effect of negative emotions on protection motivation behaviour was still insignificant (β = -0.007, t = 0.184, p = 0.854). This shows that self-efficacy insignificantly mediates the relationship between negative emotions and protection motivation behaviour. Hence, **H₆** was rejected.

Moreover, the results revealed a significant indirect effect of positive emotions on protection motivation behaviour (**H₇**: β = 0.127***, t = 4.239, p < .001). The total impact of positive emotions on protection motivation behaviour was significant (β = 0.393, t = 7.117, p < .001),

and with the inclusion of the mediator the effect of positive emotions on protection motivation behaviour was still significant ($\beta = 0.266^{***}$, $t = 4.885$, $p < .001$). This shows that self-efficacy partially mediates the relationship between positive emotions and protection motivation behaviour. Hence, **H₇** was supported.

Table 30: Mediation Effects

H#	Path	Total Effect	T	P	Direct Effect	T	P	Path	Indirect Effects	T	P
H ₆	NE - PMB	-0.009	0.232	0.817	-0.007	0.184	0.854	NE - SE - PMB	-0.002	0.204	0.839
H ₇	PE - PMB	0.393	7.117	0.000	0.266	4.885	0.000	PE - SE - PMB	0.127	4.239	0.000

Note. T: T-value, P: p-value, NE: negative emotions, PE: positive emotions, PMB: protection motivation behaviour

5.5.2.4 Moderation Effects

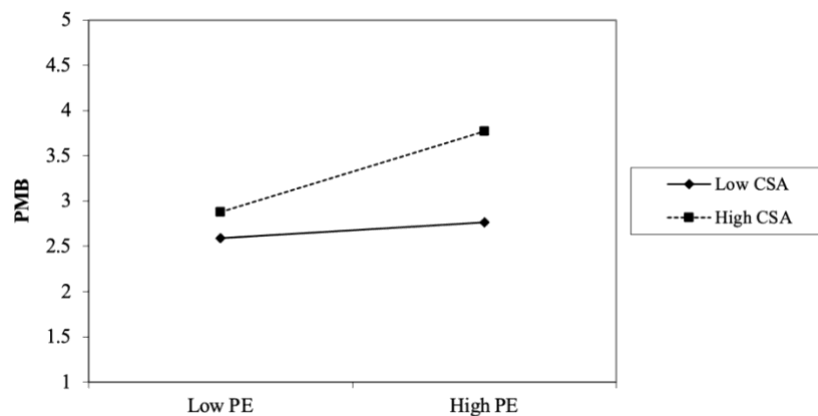
Moderation appears when the relationship between two concepts is not predictable but instead depends on the values of a third variable called a moderator variable (Baron & Kenny, 1986). A moderating variable is a factor that modifies the relationship between the independent and dependent variables (Sarstedt et al., 2021). Organisations recognise the importance of employees' cybersecurity awareness as it plays a significant role in protecting the organisation's assets. Thus, the moderation analysis was performed to evaluate the moderating role of cybersecurity awareness in the direct relationship between negative emotions, positive emotions and protection motivation behaviour; in the relationship between negative emotions, positive emotions and self-efficacy; and finally, in the relationship between self-efficacy and protection motivation behaviour.

The results in Table 31 reveal the insignificant moderating role of cybersecurity awareness in the relationship between negative emotions and protection motivation behaviour and self-efficacy (**H₉**: β -value = -0.016, t = 0.337, and p -value = 0.736). Moreover, cybersecurity awareness does not moderate the relationship between negative emotions and self-efficacy (**H₁₀**: β -value = 0.029, t = 0.611, and p -value = 0.542). However, cybersecurity awareness significantly moderates the direct relationship between positive emotions and protection motivation behaviour (**H₁₁**: β -value = 0.180, t = 2.080, and p -value = 0.038), and it also plays a significant moderating role in the relationship between positive emotions and employees' self-efficacy (**H₁₂**: β -value = 0.776, t = 2.366, and p -value = 0.018). Finally, cybersecurity awareness significantly and negatively moderates the relationship between self-efficacy and protection motivation behaviour (**H₁₃**: β -value = -0.204, t = 2.539, and p -value = 0.011).

Table 31: Moderation Effects

H#	Paths	Original sample	Sample mean	Standard deviation	T statistics	P-values
H ₉	CSA x NE -> PMB	-0.016	-0.019	0.047	0.337	0.736
H ₁₀	CSA x NE -> SE	0.029	0.028	0.047	0.611	0.542
H ₁₁	CSA x PE -> PMB	0.180*	0.168	0.087	2.080	0.038
H ₁₂	CSA x PE -> SE	0.776*	0.720	0.328	2.366	0.018
H ₁₃	CSA x SE -> PMB	-0.204*	-0.198	0.080	2.539	0.011

In the following analysis, the researcher performed a slope test in order to investigate the moderating effect of cybersecurity awareness. According to Figure 21, cybersecurity awareness positively influences the relationship between positive emotions and protection motivation behaviour (H₁₁). The figure demonstrates the relationship between positive emotions and protection motivation behaviour at two levels of cybersecurity awareness, specifically high and low. The steeper slope of the solid line indicates that for employees with high cybersecurity awareness, as positive emotions increase, protection motivation behaviour increases more than for employees with low cybersecurity awareness (represented by the flatter dashed line). Since the slope of the line for high cybersecurity awareness is steeper, this indicates that when employees have high cybersecurity awareness, their positive emotions have a more positive influence on protection motivation behaviour.

**Figure 21:** H₁₁ Slope Test Results

The results for H₁₂ (see Figure 22) show that cybersecurity awareness plays a significant moderating role in the relationship between positive emotions and employees' self-efficacy. The steeper slope of the solid line implies that for employees with high cybersecurity awareness, as positive emotions increase, self-efficacy increases more than for employees with low cybersecurity awareness. Since the slope of the line for high cybersecurity awareness

is steeper, this indicates that when employees have high cybersecurity awareness, their positive emotions have a more positive influence on their self-efficacy.

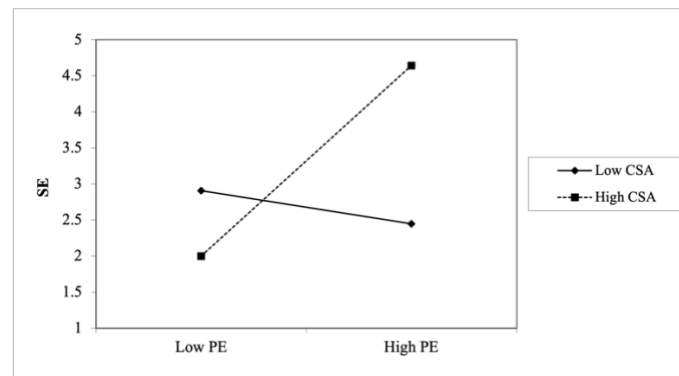


Figure 22: H₁₂ Slope Test Results

Finally, this study proposed that cybersecurity awareness positively moderates the relationship between self-efficacy and protection motivation behaviour. However, Figure 23 (H₁₃) shows that cybersecurity awareness moderates the relationship between self-efficacy and protection motivation behaviour in a negative way. According to the figure, the steeper slope of the dashed line (representing low cybersecurity awareness) suggests that for employees with low cybersecurity awareness, as self-efficacy increases, protection motivation behaviour increases more than for employees with high cybersecurity awareness (represented by the flatter solid line). The negative beta value (-0.204) and the steeper slope for the low cybersecurity awareness line in the figure suggest a negative moderation. Therefore, the positive effect of self-efficacy on protection motivation behaviour is weaker for employees with high cybersecurity awareness than for those with low cybersecurity awareness. In other words, as self-efficacy increases, protection motivation behaviour increases more for those with low cybersecurity awareness compared to those with high cybersecurity awareness.

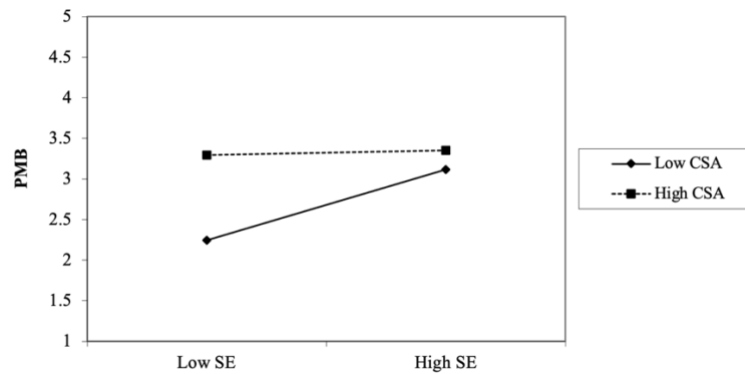


Figure 23: H₁₃ Slope Test Results

5.5.2.5 Coefficient of Determination (R^2 value)

The coefficient of determination refers to the statistical metric that precisely measures the amount of difference in the determined construct and can be described by the independent construct. The R^2 statistic is a measure of statistical significance employed to evaluate the degree of appropriateness of the model's fit. It addresses the degree to which the independent variable accounts for changes in the dependent variable within the model context. In simple terms, R^2 measures how well the model accounts for the observed data variability (Crespo et al., 2019). Therefore, it can be used to evaluate the adequacy of the model in capturing the strength of the relationship between data outcomes and predictors. Ringle et al. (2012) conducted an analysis in the field of information systems that utilised PLS-SEM. Their findings indicated that out of 109 models, R^2 was recorded in 105. R^2 quotes range from zero to one, with zero indicating a low level of explained variation and one indicating a high level of justified variance. In marketing studies, R^2 values of 0.25 are considered low, while 0.50 is moderate and 0.75 is high (Hair et al., 2011). However, Chin (1998) proposed that R^2 values of 0.19 are low, 0.33 is moderate, and 0.67 can be classified as high. In this research, the R^2 value for the PMB is 0.44, while for the SE it is 0.45, describing a moderate effect, as illustrated in Table 32.

Table 32: R-Square

	R-square	R-square adjusted
PMB	0.457	0.447
SE	0.462	0.455

5.5.2.6 Effect Size - f^2

The f^2 is an additional criterion employed in PL_SEM to measure the structural model. This evaluates the extent to which the utilisation of predictors enhances the amount of divergence

accounted for through the internal variable. The effect size refers to the alteration in the R^2 assessment after a particular external factor is excluded (Hair et al., 2014). This alteration is used to assess the significant influence of the excluded factor on the internal factor being studied (p. 201). f^2 quantifies the impact on R^2 when a predictor is removed from the model. Cohen (1988) provides criteria for the value of the effect size: 0.02 is small, 0.15 is a moderate effect, and 0.35 is a large effect. The effect increases proportionally with the number's magnitude. Based on the guideline above, the magnitude of the influence is determined by employing SmartPLS 4 for the calculation. Table 33 shows the effect size of f^2 on R^2 . The findings show that the effect size of CSA on PMB is 0.106, the effect size of NE on PMB is 0.00, the effect size of NE on SE is 0.00, the effect size of PE on PMB is 0.073, the effect size of PE on SE is 0.512; and finally, the effect size of SE on PMB is 0.049.

Table 33: Effect Size

Paths	f-square
CSA -> PMB	0.106
NE -> PMB	0.000
NE -> SE	0.000
PE -> PMB	0.073
PE -> SE	0.512
SE -> PMB	0.049

5.5.2.7 Predictive Relevance

Cross-validity redundancy is the validation research concept that assesses how well new measures can correlate with measures established for the same variable (Ali et al., 2018). It evaluates whether new measures and any incremental validity exist beyond what the measures explain (Ringle et al., 2020). Cross-validity redundancy assists researchers in determining whether the instruments can provide new perceptions or merely replicate information captured by measures already established (Torlak et al., 2021). In the literature, three techniques are recommended to assess the predictive ability of models, which are: blindfolding (Geisser, 1974; Stone, 1974), PLSpredict (Shmueli et al., 2019), and CVPAT (Liengaard et al., 2021). The differences between blindfolding, PLSpredict, and CVPAT in PLS-SEM are crucial for understanding the predictive performance assessment in PLS-SEM. Blindfolding, denoted by cross-validated redundancy (Q^2), is used to evaluate the predictive validity in PLS (Chin, 2010; Hair et al., 2019). It is beneficial for understanding the significance of the structural paths in predicting the endogenous constructs in the model. Shmueli et al. (2019) introduced the PLSpredict procedure, which translates k-fold cross-validation, a well-known procedure from predictive analytics, into a PLS-SEM framework. The improved prediction accuracy of PLS-SEM can be assessed by contrasting the reduced values of the Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) metrics with those of the

Linear Regression Model (LM) (Hair, 2020; Liengard et al., 2021). Shmueli et al. (2019) found that when evaluating the PLS-SEM indicator in the LM, the former demonstrates minor values of RMSE and MAE. This indicates that the model shows a moderate degree of predictive efficacy. According to Shmueli et al. (2019), the model's predictive capability can be assessed as low, medium, or high. As a model's prediction quality increases, its ability to forecast changes in other variables also improves.

The newest method was introduced by Liengard et al. (2021), and this method introduced the CVPAT, based on the PLSpredict procedure proposed by Shmueli et al. (2019). According to Liengard et al. (2021), CVPAT and PLSpredict are two different methods used to assess the prediction accuracy of PLS-SEM results. The CVPAT is a tool used for comparing prediction-oriented models in the PLS-SEM comparison (Liengard et al., 2021; Chin et al., 2020; Hair, 2020; Sharma et al., 2022). Sharma et al. (2022) expanded the use of the CVPAT to assess the model's ability to predict. CVPAT uses an out-of-sample forecast technique to calculate the forecasting accuracy of the model error, determining the average loss value. In the evaluation of prediction-based models, the average loss amount is measured in relation to the typical loss value obtained by using indicator averages (IA) as a basic benchmark, and the average loss value obtained by using an LM forecast as a more conservative benchmark. The general loss of PLS-SEM must be below the mean loss of the comparisons, as evidenced by a negative variance in the average loss values. The CVPAT assesses if the mean loss of PLS-SEM is significantly lower than that of the comparisons. Therefore, in order to showcase the model's improved ability to anticipate outcomes compared to other prediction benchmarks, the difference among the mean loss amounts should be significantly negative.

This research shows a negative average loss value difference in CVPAT outcomes, comparing PLS-SEM with IA and PLS-SEM with LM, as shown in Table 34. PLS-SEM shows a lower average loss than the IA and LM prediction standards. Furthermore, given that the p-value is less than 0.05, we can infer that the predictive skills of PLS-SEM are significantly superior to those of the two benchmark predictions. Therefore, the CVPAT results confirm that the model of the research has a solid ability to predict, compared to the prediction benchmark (Hair et al., 2022).

Table 34: CVPAT

PLS-SEM vs. Indicator average (IA)			
	Average loss difference	t-value	p-value
PMB	-0.230	6.617	0.000
SE	-0.670	7.188	0.000
Overall	-0.505	8.063	0.000
PLS-SEM vs. Linear model (LM)			

	Average loss difference	t-value	p-value
PMB	-0.042	2.263	0.024
SE	-0.031	0.449	0.654
Overall	-0.035	0.778	0.437

5.5.2.8 M Goodness-of-Fit (GoF)

Hair et al. (2022) stated that GoF pertains to the level at which a model accurately aligns with the observed empirical data. The aim of using GoF is to assess the statistical model fit, an SEM, to the data observed. These indices provide information on how well the predictions of the model can match the actual data and assist researchers in determining whether the model would be a good fit for the data (Ali et al., 2018). Hair et al. (2016) and Kock (2017) acknowledge that it is essential to consider the combination of these indicators and that researchers should not rely on single measures to assess the model goodness and fit. PLS-SEM was developed for predictive purposes without the inclusion of GoF indices (Sarstedt et al., 2021). CB-SEM users heavily depend on the criteria established by the GoF approach, in contrast to PLS-SEM users (Ringle et al., 2020). Nevertheless, CB-SEM aims to reduce the parameters of the covariance matrix to justify the research model. Researchers have advised using the model's predictive power instead of GoF guidelines (Ringle et al., 2020; Sarstedt et al., 2021). This may explain why most PLS-SEM investigations have not used GoF indices (Ringle et al., 2020). Henseler et al. (2017) assert that SRMR is the sole indicator used for validating PLS-SEM models, representing the total of squared differences between the association structure implied by the model and the observed association of the structure. The SmartPLS 4, the metrics used to evaluate and assess the model fit, are given in Table 35 below.

Table 35: GoF

Fit Index	Saturated Model	Estimated Model
SRMR	0.051	0.058
d_{ULS}	1.070	1.371
d_G	0.428	0.436
Chi-square	951.743	941.727
NFI	0.855	0.856

The next section will assess the correlations between variations in employees' protection motivation behaviour and their demographic characteristics.

5.5.3 Assessing Employees' Differences in Cybersecurity Protection Motivation Behaviour

Following the completion of the examination of the link between the model variables for the dataset in question, the subsequent stage entails determining the level to which employee differences constructs have control over the model. The same guidelines are used to

determine the measurement and structural model to assess employee differences. To evaluate a model regarding employee differences in protection motivation behaviours, criteria were set earlier in the measurement model and the structural model assessment sections (Sections 6.2 and 6.3). The defined requirements for the measurement model are as follows: the loadings must be larger than or equivalent to 0.7, the CA and CR must be larger than or equivalent to 0.7, the AVE must be larger than or equivalent to 0.5, the p-value should be less than or equivalent to 0.05, and the t-value must be more than 1.96.

5.5.3.1 Gender

Gender is evaluated using a categorical scale, and for this variable, there is therefore no need to refine the data set (Sarstedt & Cheah, 2019). Regarding gender differences, the researcher adhered to Foth's (2016) approach, and categorised the entire sample into two groups: males and females. SmartPLS 4 was utilised to run separate models. The data indicate that there were 242 male participants and 141 female respondents among the employee sample. Each group achieved the minimal criteria suggested by Cohen (1992), Hair et al. (2022), and Kock and Hadaya (2018) of a significance level of 5%, a minimum R^2 value of 0.25, and a total sample size of 65.

After completing these examinations, the researcher evaluated the measurement and structural models. Table 36 describes the measurement model assessment for the gender variable results using 1,000 iterations based on the PLS algorithm. Moreover, the table presents data on the CA and CR of each construct, indicating that all constructs surpass the cut-off point, thereby demonstrating suitable dependability. In addition, it should be noted that values of AVE exceeding 0.5 indicate sufficient evidence of convergent validity for each concept.

Table 36: Gender Measurement Model Assessment Results

Indicators	Males				Females			
	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5
CSA3	0.719	0.766	0.775	0.517	0.767	0.844	0.889	0.616
CSA5	0.749				0.812			
CSA6	0.800				0.789			
CSA7	0.631				0.818			
CSA8	0.686				0.736			
NE1	0.914	0.856	0.920	0.909	0.908	0.875	0.922	0.798
NE2	0.824				0.862			
NE3	0.891				0.909			
PE1	0.794	0.909	0.911	0.925	0.783	0.911	0.927	0.586

PE2	0.802				0.786			
PE3	0.810				0.765			
PE4	0.739				0.728			
PE5	0.729				0.725			
PE6	0.759				0.791			
PE7	0.777				0.834			
PE8	0.671				0.697			
PE9	0.762				0.774			
PMB1	0.876	0.855	0.889	0.929	0.896	0.890	0.932	0.820
PMB2	0.925				0.913			
PMB3	0.904				0.907			
SE1	0.848	0.846	0.853	0.982	0.841	0.853	0.896	0.634
SE2	0.843				0.850			
SE3	0.863				0.841			
SE4	0.709				0.736			
SE5	0.671				0.700			

The values for the Fornell-Larcker Criterion are shown in Table 37. The findings are displayed along a diagonal line, which indicates a stronger correlation between the constructs compared to their correlations with other constructs. By engaging in this practice, the measurement model's evaluation becomes an evaluation conducted on a population subset.

Table 37: Gender Fornell-Larcker Criterion

Males					
	CSA	NE	PE	PMB	SE
CSA	0.719				
NE	-0.265	0.877			
PE	0.450	-0.147	0.761		
PMB	0.605	-0.169	0.524	0.902	
SE	0.618	-0.144	0.497	0.542	0.791
Females					
	CSA	NE	PE	PMB	SE
CSA	0.785				
NE	-0.283	0.893			
PE	0.515	-0.116	0.766		
PMB	0.567	-0.164	0.562	0.906	
SE	0.567	-0.170	0.516	0.556	0.796

Table 38 presents the hypotheses results by gender using the technique of bootstrapping with 10,000 samples, as suggested by Hair et al. (2022) and Kock (2017).

Table 38: Hypotheses Results by Gender

H#	Paths	Males		Females		Main Result	
		β	Adj. R^2	β	Adj. R^2	β	Adj. R^2
H ₁	NE -> PMB	-0.007	0.451	-0.015	0.454	-0.007	0.447
H ₂	NE -> SE	0.013	0.446	-0.032	0.447	-0.009	0.455
H ₃	PE ->PMB	0.260***	0.451	0.277***	0.454	0.266***	0.447
H ₄	PE -> SE	0.551***	0.446	0.562***	0.447	0.545***	0.455
H ₅	SE-> PMB	0.183**	0.451	0.292***	0.454	0.232***	0.447
H ₆	NE -> SE -> PMB	0.002	0.451	-0.009	0.454	-0.002	0.447
H ₇	PE -> SE -> PMB	0.101**	0.451	0.164***	0.454	0.127***	0.447
H ₈	CSA -> PMB	0.370***	0.451	0.279***	0.451	0.322***	0.447
H ₉	CSA x NE -> PMB	0.010	0.451	-0.067	0.454	-0.016	0.447
H ₁₀	CSA x NE -> SE	0.047	0.446	0.048	0.447	0.029	0.455
H ₁₁	CSA x PE -> PMB	0.146	0.451	0.266*	0.454	0.180*	0.447
H ₁₂	CSA x PE -> SE	0.804*	0.446	0.911*	0.447	0.776*	0.455
H ₁₃	CSA x SE -> PMB	0.017**	0.451	-0.984**	0.454	-0.204*	0.447

For H₃, both males ($\beta = 0.260^{***}$) and females ($\beta = 0.277^{***}$) show a significant positive relationship, with the main model result also being significant ($\beta = 0.266^{***}$). Similarly, for H₄, both males ($\beta = 0.551^{***}$) and females ($\beta = 0.562^{***}$) show a significant positive relationship, with the main model result also being significant ($\beta = 0.545^{***}$). For H₅, the relationship is significant for both males ($\beta = 0.183^{**}$) and females ($\beta = 0.292^{***}$), with the main model result showing a significant positive relationship ($\beta = 0.232^{***}$). H₇ shows significant positive relationships for both males ($\beta = 0.101^{**}$) and females ($\beta = 0.164^{***}$), with the main model result β also being significant ($\beta = 0.127^{***}$). H₈ reveals significant positive relationships for both males ($\beta = 0.370^{***}$) and females ($\beta = 0.279^{***}$), with the main model result also being significant ($\beta = 0.322^{***}$).

H₁₁ is significant for females ($\beta = 0.266^*$), with the main model result β showing a significant positive relationship ($\beta = 0.180^*$). H₁₂ reveals significant positive relationships for both males ($\beta = 0.804^*$) and females ($\beta = 0.911^{***}$), with the main model result β also being significant ($\beta = 0.776^{***}$). H₁₃ shows a significant positive relationship for males ($\beta = 0.017^{**}$) but a significant negative relationship for females ($\beta = -0.984^{**}$), with the main model result also indicating a significant negative relationship ($\beta = -0.204^{**}$). There are significant differences between males' and females' paths.

5.5.3.2 Age

Age is examined using a categorical scale, and for this variable, there is therefore no need to refine the data set (Sarstedt & Cheah, 2019). Using the median-split method, this study categorised participants into two age groups: younger (18 to 39 years old) and older (40 years

and above). Following the implementation of the median-split processes with a median value of 2, there were 258 employees in the group of younger employees (below 39 years old) and 125 people in the group of older employees (above 40 years old). Each group surpassed the minimal sample size (42) suggested by Cohen (1992), Hair et al. (2022) and Kock and Hadaya (2018). Therefore, the researcher continued to evaluate the structural and measurement models. Table 39 presents the measurement model assessment for the age variable results using 1,000 iterations based on the PLS algorithm. In addition, the table presents data on the CA and CR values for each construct, indicating that they are above the designated threshold, thereby demonstrating the dependability of the constructs. In addition, it can be inferred that constructs have sufficient convergent validity when AVE values exceed 0.5.

Table 39: Age Measurement Model Assessment Results

Indicators	Younger Employees				Older Employees			
	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5
CSA3	0.776	0.915	0.937	0.937	0.828	0.839	0.886	0.608
CSA5	0.764				0.795			
CSA6	0.780				0.898			
CSA7	0.830				0.914			
CSA8	0.747				0.883			
NE1	0.913	0.843	0.902	0.902	0.903	0.872 0.915	0.919	0.792
NE2	0.845				0.839			
NE3	0.910				0.861			
PE1	0.798	0.892	0.912	0.912	0.720	0.890	0.929	0.595
PE2	0.797				0.823			
PE3	0.797				0.727			
PE4	0.764				0.612			
PE5	0.732				0.746			
PE6	0.771				0.804			
PE7	0.805				0.665			
PE8	0.697				0.720			
PE9	0.773				0.759			
PMB1	0.884	0.928	0.954	0.954	0.939		0.932	0.820
PMB2	0.925				0.941			
PMB3	0.908				0.925			
SE1	0.848	0.865	0.904	0.904	0.914	0.852	0.895	0.633
SE2	0.853				0.839			
SE3	0.856				0.869			
SE4	0.706				0.765			
SE5	0.699				0.631			

The values for the Fornell-Larcker Criterion are shown in Table 40. The findings are displayed along a diagonal line, which indicates a stronger correlation between the constructs compared to their correlations with other constructs. Engaging in this process evaluates the measurement model on a subset of the population.

Table 40: Age Fornell-Larcker Criterion

Younger Employees					
	CSA	NE	PE	PMB	SE
CSA	0.780				
NE	-0.283	0.890			
PE	0.475	-0.140	0.771		
PMB	0.566	-0.176	0.516	0.906	
SE	0.512	-0.140	0.487	0.519	0.796
Older Employees					
	CSA	NE	PE	PMB	SE
CSA	0.865				
NE	-0.326	0.868			
PE	0.577	-0.129	0.733		
PMB	0.641	-0.142	0.712	0.935	
SE	0.825	-0.304	0.620	0.691	0.810

Table 41 presents the hypotheses' results by age using the technique of bootstrapping with 10,000 samples, as suggested by Hair et al. (2022) and Kock (2017).

Table 41: Hypotheses Results by Age Group

H#	Paths	Younger employees		Older employees		Main Result	
		β	Adj. R^2	β	Adj. R^2	β	Adj. R^2
H ₁	NE -> PMB	-0.017	0.566	0.058	0.424	-0.007	0.447
H ₂	NE -> SE	0.017	0.456	-0.319*	0.473	-0.009	0.455
H ₃	PE -> PMB	0.239***	0.566	0.509**	0.424	0.266***	0.447
H ₄	PE -> SE	0.545***	0.456	0.601***	0.473	0.545***	0.455
H ₅	SE -> PMB	0.228**	0.566	0.262	0.424	0.232***	0.447
H ₆	NE -> SE -> PMB	-0.004	0.566	-0.084	0.424	-0.002	0.447
H ₇	PE -> SE -> PMB	0.124***	0.566	0.158	0.424	0.127***	0.447
H ₈	CSA -> PMB	0.337***	0.566	0.144	0.424	0.322***	0.447
H ₉	CSA x NE -> PMB	-0.028	0.566	0.080	0.424	-0.016	0.447
H ₁₀	CSA x NE -> SE	0.017	0.456	0.297	0.473	0.029	0.455
H ₁₁	CSA x PE -> PMB	0.201*	0.566	-0.399	0.424	0.180*	0.447
H ₁₂	CSA x PE -> SE	0.880*	0.456	-0.950	0.473	0.776*	0.455
H ₁₃	CSA x SE -> PMB	-0.017	0.566	0.411	0.424	-0.204*	0.447

For H₃, younger employees ($\beta = 0.239***$) and older employees ($\beta = 0.509**$) show a significant positive relationship, with the main model result also being significant ($\beta = 0.266***$).

Similarly, for **H₄**, both younger ($\beta = 0.545^{***}$) and older employees ($\beta = 0.601^{***}$) show a significant positive relationship, with the main model result also being significant ($\beta = 0.545^{***}$). For **H₅**, the relationship is significant for younger employees ($\beta = 0.228^{**}$) but not for older employees ($\beta = 0.262$), with the main model result showing a significant positive relationship ($\beta = 0.232^{***}$). For **H₇** there is a significant positive relationships for younger employees ($\beta = 0.124^{***}$) but not for older employees ($\beta = 0.158$), with the main model result also being significant ($\beta = 0.127^{***}$). For **H₈**, the relationship is significant for younger employees ($\beta = 0.337^{***}$) but not for older employees ($\beta = 0.144$), with the main model result showing a significant positive relationship ($\beta = 0.322^{***}$). **H₁₁** is significant for younger employees ($\beta = 0.201^*$), with the main model result β showing a significant positive relationship ($\beta = 0.180^*$). **H₁₂** shows significant positive relationships for younger employees ($\beta = 0.880^*$), with the main model result β also being significant ($\beta = 0.776^{***}$). However, there are differences between younger and older employees. **H₂** shows a significant negative relationship for older employees ($\beta = -0.319^*$) but not for younger employees ($\beta = 0.017$). **H₁₁** is significant only for younger employees ($\beta = 0.201^*$), not for older employees ($\beta = -0.399$). **H₁₂** reveals a significant positive relationship for younger employees ($\beta = 0.880^*$), while older employees show a non-significant negative relationship ($\beta = -0.950$). **H₁₃** reveals no significant relationship between younger employees ($\beta = -0.017$) and older employees ($\beta = 0.411$). The main model result reflects an overall significant negative relationship ($\beta = -0.204^*$), indicating a complex interaction effect across the age groups.

5.5.3.3 Employees' Educational Level

Employees' educational levels are measured using a categorical or nominal scale, and for this variable, there is therefore no need to refine the data set (Sarstedt & Cheah, 2019). This study categorised participants into two groups, High School to Bachelor's and Master's and PhD, using the median-split method. Following the implementation of the median-split processes, there were 180 employees in the High School/Diploma/Bachelor group and 203 employees in the Master's/PhD/Other group. Each group surpassed the minimal sample size (65) suggested by Cohen (1992), Hair et al. (2022), and Kock and Hadaya (2018). Table 42 presents the measurement model assessment for employees' educational level variable results using 1,000 iterations based on the PLS Algorithm. In addition, the table presents data on the CA and CR of each construct, indicating that they are above the designated threshold, hence demonstrating the strong consistency of the variables. Moreover, it can be inferred that constructs show satisfactory convergent validity when their AVE values exceed 0.5.

Table 42: Educational Level Measurement Model Assessment Results

Indicators	High School – Diploma – Bachelor				Master's – PhD – Other			
	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5
CSA3	0.800	0.843	0.888	0.615	0.760	0.855	0.896	0.635
CSA5	0.713				0.823			
CSA6	0.844				0.732			
CSA7	0.851				0.838			
CSA8	0.767				0.763			
NE1	0.939	0.857	0.912	0.777	0.902	0.875	0.904	0.760
NE2	0.778				0.848			
NE3	0.891				0.893			
PE1	0.822	0.898	0.916	0.549	0.755	0.926	0.938	0.629
PE2	0.823				0.770			
PE3	0.853				0.740			
PE4	0.823				0.688			
PE5	0.799				0.663			
PE6	0.776				0.770			
PE7	0.810				0.759			
PE8	0.674				0.737			
PE9	0.746				0.783			
PMB1	0.858	0.906	0.941	0.842	0.914	0.877	0.925	0.803
PMB2	0.929				0.924			
PMB3	0.901				0.914			
SE1	0.849	0.849	0.894	0.630	0.857	0.854	0.896	0.635
SE2	0.860				0.839			
SE3	0.840				0.869			
SE4	0.676				0.733			
SE5	0.743				0.649			

Table 43 shows the values for the Fornell-Larcker Criterion. The findings are displayed along a diagonal line, which indicates a stronger correlation between the constructs compared to correlations with other constructs. By engaging in this practice, the evaluation of the measurement model becomes an evaluation conducted on a subset of the population.

Table 43: Educational Level Fornell-Larcker Criterion

High School – Diploma - Bachelor					
	CSA	NE	PE	PMB	SE
CSA	0.797				
NE	-0.193	0.872			
PE	0.511	-0.017	0.793		
PMB	0.658	-0.112	0.563	0.896	
SE	0.639	-0.095	0.537	0.555	0.797
Master's – PhD - Other					
	CSA	NE	PE	PMB	SE
CSA	0.784				
NE	-0.423	0.881			
PE	0.478	-0.325	0.741		
PMB	0.523	-0.300	0.518	0.918	
SE	0.478	-0.271	0.469	0.521	0.794

Table 44 presents the hypotheses' results for the employees' educational level using the technique of bootstrapping with 10,000 samples, as suggested by Hair et al. (2022) and Kock (2017).

Table 44: Hypotheses Results by Educational Level

H#	Paths	High School – Diploma – Bachelor		Master's – PhD – Other		Main Result	
		β	Adj. R^2	β	Adj. R^2	β	Adj. R^2
H ₁	NE -> PMB	-0.018	0.386	-0.027	0.501	-0.007	0.447
H ₂	NE -> SE	0.009	0.408	-0.090	0.519	-0.009	0.455
H ₃	PE -> PMB	0.295***	0.386	0.249**	0.501	0.266***	0.447
H ₄	PE -> SE	0.602***	0.408	0.446***	0.519	0.545***	0.455
H ₅	SE -> PMB	0.105	0.386	0.274***	0.501	0.232***	0.447
H ₆	NE -> SE -> PMB	0.001	0.386	-0.025	0.501	-0.002	0.447
H ₇	PE -> SE -> PMB	0.063	0.386	0.122***	0.501	0.127***	0.447
H ₈	CSA -> PMB	0.461***	0.386	0.262**	0.501	0.322***	0.447
H ₉	CSA x NE -> PMB	-0.073	0.386	0.018	0.501	-0.016	0.447
H ₁₀	CSA x NE -> SE	0.071	0.408	-0.068	0.519	0.029	0.455
H ₁₁	CSA x PE -> PMB	0.135	0.386	-0.045	0.501	0.180*	0.447
H ₁₂	CSA x PE -> SE	0.736*	0.408	-0.750	0.519	0.776*	0.455
H ₁₃	CSA x SE -> PMB	-0.158	0.386	0.054	0.501	-0.204*	0.447

For H₃, the High School/Diploma/Bachelor group ($\beta = 0.295***$) and the Master's/PhD/Other group ($\beta = 0.249**$) show a significant positive relationship, with the main model result β also being significant ($\beta = 0.266***$). Similarly, for H₄, both the High School/Diploma/Bachelor group ($\beta = 0.602***$) and the Master's/PhD/Other group ($\beta = 0.446***$) show a significant positive relationship, with the main model result β also being significant ($\beta = 0.545***$). For H₅, the relationship is significant for the Master's/PhD/Other group ($\beta = 0.274***$) but not for the High School/Diploma/Bachelor group ($\beta = 0.105$). The Master's/PhD/Other group aligns with the

main model result, showing a significant positive relationship ($\beta = 0.232^{***}$). For H_7 , there is a significant positive relationship for the Master's/PhD/Other group ($\beta = 0.122^{***}$), while for the High School/Diploma/Bachelor group ($\beta = 0.063$) the relationship was found to be insignificant. The Master's/PhD/Other group aligns with the main model result, which is also significant ($\beta = 0.127^{***}$). For H_8 , both the High School/Diploma/Bachelor ($\beta = 0.461^{***}$) and Master's/PhD/Other group ($\beta = 0.262^{**}$) show a significant positive relationship, with the main model result β also being significant ($\beta = 0.322^{***}$).

H_{11} is not significant for either group ($\beta = 0.135$ for the High School/Diploma/Bachelor group and $\beta = 0.056$ for the Master's/PhD/Other group, but the main model result β shows a significant positive relationship ($\beta = 0.180^*$). For H_{12} there were significant positive relationships for the High School/Diploma/Bachelor group ($\beta = 0.736^*$) but not for the Master's/PhD/Other group ($\beta = -0.750$). The High School/Diploma/Bachelor group aligns with the main model result, which was significant ($\beta = 0.776^{***}$). For H_{13} , there was no significant relationship for either the High School/Diploma/Bachelor group ($\beta = -0.158$) or the Master's/PhD/Other group ($\beta = 0.054$), resulting in a significant negative main model result ($\beta = -0.204^*$).

5.5.3.4 Employees' Work Position

Employees' work position is measured using a categorical scale, and therefore, for this variable, there is no need to refine the data set (Sarstedt & Cheah, 2019). The sample comprised 169 academic and 214 administrative respondents. Each group in this study achieved the minimal sample size (65) suggested by Cohen (1992), Hair et al. (2022), and Kock and Hadaya (2018). After completing these examinations, the researcher evaluated the measurement and structural models. Table 45 describes the measurement model assessment for employees' work position variable results using 1,000 iterations based on the PLS algorithm. Additionally, the table presents data on the CA and CR of each construct, indicating that all constructs surpass the cut-off point and demonstrate strong dependability. In addition, it should be noted that values of AVE exceeding 0.5 indicate satisfactory levels of convergent validity for each construct.

Table 45: Work Position Measurement Model Assessment Results

Indicators	Administrative				Academic			
	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5
CSA3	0.769	0.853	0.895	0.630	0.778	0.850	0.893	0.625
CSA5	0.779				0.767			
CSA6	0.775				0.797			
CSA7	0.835				0.851			
CSA8	0.792				0.771			
NE1	0.917	0.866	0.915	0.783	0.833	0.888	0.930	0.815
NE2	0.876				0.905			
NE3	0.914				0.802			
PE1	0.783	0.915	0.930	0.597	0.801	0.916	0.931	0.598
PE2	0.798				0.808			
PE3	0.786				0.757			
PE4	0.750				0.760			
PE5	0.734				0.774			
PE6	0.785				0.789			
PE7	0.820				0.694			
PE8	0.725				0.763			
PE9	0.776				0.882			
PMB1	0.896	0.888	0.931	0.818	0.925	0.907	0.942	0.844
PMB2	0.937				0.906			
PMB3	0.922				0.848			
SE1	0.872	0.854	0.896	0.635	0.846	0.865	0.904	0.654
SE2	0.870				0.866			
SE3	0.859				0.708			
SE4	0.730				0.702			
SE5	0.694				0.778			

Table 46 shows the values for the Fornell-Larcker Criterion. The findings are displayed along a diagonal line, indicating a stronger correlation between the constructs compared to their correlations with other constructs. By engaging in this practice, the evaluation of the measurement model becomes an evaluation focused on samples.

Table 46: Work Position Fornell-Larcker Criterion

Administrative					
	CSA	NE	PE	PMB	SE
CSA	0.793				
NE	-0.276	0.885			
PE	0.498	-0.141	0.773		
PMB	0.591	-0.145	0.548	0.904	
SE	0.563	-0.143	0.512	0.548	0.797
Academic					
	CSA	NE	PE	PMB	SE
CSA	0.790				
NE	-0.389	0.903			
PE	0.481	-0.206	0.774		
PMB	0.609	-0.238	0.549	0.919	
SE	0.533	0.224	0.532	0.560	0.164

Table 47 presents the hypotheses' results for the employee's work position using the technique of bootstrapping with 10,000 samples, as suggested by Hair et al. (2022) and Kock (2017).

Table 47: Hypotheses Results by Work Position

H#	Paths	Administrative		Academic		Main Result	
		β	Adj. R^2	β	Adj. R^2	β	Adj. R^2
H₁	NE -> PMB	0.020	0.459	0.012	0.479	-0.007	0.447
H₂	NE -> SE	-0.021	0.480	0.011	0.459	-0.009	0.455
H₃	PE ->PMB	0.241***	0.459	0.253***	0.479	0.266***	0.447
H₄	PE -> SE	0.547***	0.480	0.583***	0.459	0.545***	0.455
H₅	SE-> PMB	0.186	0.459	0.221***	0.479	0.232***	0.447
H₆	NE -> SE -> PMB	-0.004	0.459	0.002	0.479	-0.002	0.447
H₇	PE -> SE -> PMB	0.102**	0.459	0.129**	0.479	0.127***	0.447
H₈	CSA -> PMB	0.392***	0.459	0.347***	0.479	0.322***	0.447
H₉	CSA x NE -> PMB	-0.069	0.459	-0.020	0.479	-0.016	0.447
H₁₀	CSA x NE -> SE	0.015	0.480	0.033	0.459	0.029	0.455
H₁₁	CSA x PE -> PMB	0.010	0.459	0.006	0.479	0.180*	0.447
H₁₂	CSA x PE -> SE	0.324***	0.480	0.403***	0.459	0.776*	0.455
H₁₃	CSA x SE -> PMB	-0.098	0.459	0.019	0.479	-0.204*	0.447

For **H₃**, both the administrative ($\beta = 0.241^{***}$) and academic ($\beta = 0.253^{***}$) groups show a significant positive relationship, with the main model result also being significant ($\beta = 0.266^{***}$). Similarly, for **H₄**, both administrative ($\beta = 0.547^{***}$) and academic ($\beta = 0.583^{***}$) groups show a significant positive relationship, with the main model result also being significant ($\beta = 0.545^{***}$). For **H₅**, the relationship is significant for academics ($\beta = 0.221^{***}$), but not for

administrative staff ($\beta = 0.186$), and academics align with the main model result, which shows a significant positive relationship ($\beta = 0.232^{***}$). For **H₇**, the results show significant positive relationships for both the administrative ($\beta = 0.102^{**}$) and academic ($\beta = 0.129^{***}$) groups, with the main model result also being significant ($\beta = 0.127^{***}$). For **H₈**, both the administrative ($\beta = 0.392^{***}$) and academic ($\beta = 0.347^{***}$) groups show a significant positive relationship, with the main model result also being significant ($\beta = 0.322^{***}$). However, the result for **H₁₁** is not significant for either group ($\beta = 0.010$ for administrative staff and 0.306 for academics), but the main model result shows a significant positive relationship ($\beta = 0.180^*$). For **H₁₂** there are significant positive relationships for both administrative ($\beta = 0.324^{***}$) and academic staff ($\beta = 0.403^{***}$), with the main model result also being significant ($\beta = 0.776^{***}$). The results for **H₁₃** reveal no significant relationship for either the administrative ($\beta = -0.098$) or academic staff ($\beta = 0.019$), while the main model result is significant ($\beta = -0.204^*$).

5.5.3.5 Employees' Years of Experience

Employees' years of experience are assessed using a categorical or nominal scale. To ensure accuracy and reliability, it is necessary to enhance the dataset for this particular variable (Hair et al., 2014). Using the median-split method, this study categorised participants' experiences into two groups: less than 10 years and more than 10 years (Hair et al., 2014). The results of this process showed that 224 participants have less than 10 years of experience, and 159 employees have more than 10 years of experience. In addition, this study achieved the minimum sample size (42) proposed by Cohen (1992), Hair et al. (2022), and Kock and Hadaya (2018). Table 48 describes the measurement model assessment for employees' years of experience variable results using 1,000 iterations based on the PLS algorithm. In addition, the table presents data on the CA and CR values for each construct, indicating that all constructs surpass the designated cut-off point, thereby demonstrating the dependability of the constructs. In addition, it can be inferred that constructs possess satisfactory convergent validity when their AVE values exceed 0.5.

Table 48: Years of Experience Measurement Model Assessment Results

Indicators	10 or Less Years' Experience				10+ Years Experiences			
	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5	Loadings > 0.7	CA > 0.7	CR > 0.7	AVE > 0.5
CSA3	0.769	0.840	0.887	0.611	0.734	0.851	0.894	0.630
CSA5	0.729				0.681			
CSA6	0.797				0.879			
CSA7	0.848				0.855			
CSA8	0.760				0.803			
NE1	0.889	0.848	0.906	0.763	0.862	0.835	0.896	0.743
NE2	0.842				0.824			
NE3	0.890				0.898			
PE1	0.793	0.909	0.925	0.578	0.821	0.916	0.930	0.599
PE2	0.778				0.800			
PE3	0.765				0.814			
PE4	0.767				0.788			
PE5	0.720				0.798			
PE6	0.770				0.723			
PE7	0.785				0.777			
PE8	0.708				0.683			
PE9	0.752				0.748			
PMB1	0.863	0.872	0.921	0.795	0.765	0.817	0.890	0.731
PMB2	0.923				0.913			
PMB3	0.888				0.880			
SE1	0.828	0.828	0.881	0.599	0.805	0.831	0.881	0.599
SE2	0.856				0.843			
SE3	0.826				0.800			
SE4	0.685				0.704			
SE5	0.651				0.706			

The values for the Fornell-Larcker Criterion are shown in Table 49. The findings are displayed along a diagonal line, which indicates a stronger correlation between the constructs compared to correlations with other constructs. By engaging in this practice, the evaluation of the measurement model becomes an evaluation conducted on samples.

Table 49: Years of Experience Fornell-Larcker Criterion

10 or Less Years' Experience					
	CSA	NE	PE	PMB	SE
CSA	0.782				
NE	-0.291	0.874			
PE	0.497	-0.150	0.760		
PMB	0.609	-0.226	0.523	0.892	
SE	0.561	-0.164	0.558	0.547	0.774

10+ Years Experiences					
	CSA	NE	PE	PMB	SE
CSA	0.794				
NE	-0.297	0.862			
PE	0.609	-0.071	0.774		
PMB	0.671	-0.215	0.592	0.855	
SE	0.624	-0.125	0.631	0.562	0.774

Table 50 presents the hypotheses' results for the employee's years of experience using the technique of bootstrapping with 10,000 samples, as suggested by Hair et al. (2022) and Kock (2017).

Table 50: Hypotheses Results by Years of Experience

H#	Paths	10/Less Years		10+ Years		Main Result	
		β	Adj. R^2	β	Adj. R^2	β	Adj. R^2
H ₁	NE -> PMB	-0.038	0.448	0.025	0.489	-0.007	0.447
H ₂	NE -> SE	0.032	0.518	-0.033	0.605	-0.009	0.455
H ₃	PE ->PMB	0.235**	0.448	0.284***	0.489	0.266***	0.447
H ₄	PE -> SE	0.578***	0.518	0.499***	0.605	0.545***	0.455
H ₅	SE-> PMB	0.190**	0.448	0.252***	0.489	0.232***	0.447
H ₆	NE -> SE -> PMB	0.006	0.448	-0.008	0.489	-0.002	0.447
H ₇	PE -> SE -> PMB	0.110**	0.448	0.126***	0.489	0.127***	0.447
H ₈	CSA -> PMB	0.341***	0.448	0.292***	0.489	0.322***	0.447
H ₉	CSA x NE -> PMB	0.059	0.448	-0.045	0.489	-0.016	0.447
H ₁₀	CSA x NE -> SE	0.099	0.518	-0.036	0.605	0.029	0.455
H ₁₁	CSA x PE -> PMB	0.049	0.448	0.040	0.489	0.180*	0.447
H ₁₂	CSA x PE -> SE	0.943*	0.518	0.986*	0.605	0.776*	0.455
H ₁₃	CSA x SE -> PMB	-0.066	0.448	-0.040	0.489	-0.204*	0.447

For H₃, both employees with 10 or fewer years of experience ($\beta = 0.235^{**}$) and those with more than 10 years of experience ($\beta = 0.284^{***}$) show a significant positive relationship, with the main model result also being significant ($\beta = 0.266^{***}$). Similarly, for H₄, employees with 10 or fewer years of experience ($\beta = 0.578^{***}$) and those with more than 10 years of experience ($\beta = 0.499^{***}$) show a significant positive relationship, with the main model result also being significant ($\beta = 0.545^{***}$). For H₅, the relationship is significant for both employees with 10 or fewer years ($\beta = 0.190^{**}$) and those with more than 10 years of experience ($\beta = 0.252^{***}$), with the main model result showing a significant positive relationship ($\beta = 0.232^{***}$). The results for H₇ show significant positive relationships for both employees with 10 or fewer years ($\beta = 0.110^{**}$) and those with more than 10 years of experience ($\beta = 0.126^{***}$), with the main model result also being significant ($\beta = 0.127^{***}$). For H₁₂, both employees with 10 or fewer years ($\beta = 0.341^{***}$) and those with more than 10 years of experience ($\beta = 0.292^{***}$)

show a positive significant relationship and align with the main model result, which showed a significant relationship ($\beta = 0.322^{***}$).

However, H_{11} is not significant for either those with 10 or fewer years' experience ($\beta = 0.049$) or for those with more than 10 years' experience ($\beta = 0.040$), but the main model result shows a significant positive relationship ($\beta = 0.180^*$). The results for H_{12} reveal significant positive relationships for both employees with 10 or fewer years of experience ($\beta = 0.943^*$) and those with more than 10 years of experience (0.986^*), with the main model result also being significant ($\beta = 0.776^{***}$). For H_{13} , both employees with 10 or fewer years of experience ($\beta = -0.066$) and those with more than 10 years of experience ($\beta = -0.040$) show an insignificant relationship; however, the main model result shows a significant relationship ($\beta = -0.204^*$).

5.6 Summary

The data were exported from the Qualtrics system and a preliminary examination of the exported data was performed. This chapter presents the results. Section (5.2) examines the gathered data, including response rate, data preparation, and normality. A total of 383 replies were considered appropriate for inclusion in the ensuing data analysis. The study achieved the required minimum sample size, and there were no missing data because all the employees had to answer all the questions in order to submit the survey.

Regarding outliers, based on the univariate analysis, 23 cases were identified as univariate outliers. According to Pallant (2020), when there is a notable difference between the average value of a variable and its 5% trimmed mean, it indicates the strong impact of an outlier. Therefore, a comparison was made between the definitions of "item" and "trimmed", and no significant distinctions were found between them. The identified outliers had minimal or negligible influence; five cases were identified as potential multivariate outliers based on the D^2 . The researcher retained all the responses due to insufficient evidence suggesting that these outliers were separate from the study's target participants, as the organisation had only distributed the survey by email to all its staff members. Hoyle (2012), Tabachnick et al. (2013), and Hair et al. (2014) state that outliers should not be excluded unless there is strong proof that they do not belong to the research population. Moreover, Hair et al. (2010) note that while it is likely that the multivariate analysis will be enhanced by removing outliers, this would limit its generalisability. Concerning unengaged responses, this study employed the straight-lining patterns approach to identify and exclude unresponsive answers by utilising standard deviation, drawing from prior studies in the information systems domain (e.g. Barbour et al., 2021; Gotthardt & Mezhyuev, 2022; Kuriakose & Robbins, 2016). Mey (2016) suggests that a case should be discarded if the answer pattern is deemed suspicious, as denoted by a value

of 0. Upon computing the standard deviation, this investigation determined that the participants in the survey showed complete involvement throughout, and the respondents offered distinct answers to each query. The data normality was assessed using the recommended criteria (Field, 2013; Gravetter & Forzano, 2018; Trochim & Donnelly, 2006), with values between 2 and being deemed acceptable. In addition, West et al. (1995) asserted that skewness levels greater than ± 2 and kurtosis values over 7 indicate a difference from normalcy. Thus, it was determined that all constituent parts should be retained due to the absence of significant adverse effects of non-normality on the scattered data. Moreover, this research employed PLS-SEM, and one of its characteristics is that the data does not necessarily have to be normally distributed (Hair et al., 2022). Finally, a test for common method bias was performed, and this study utilised two techniques to measure common method variation and evaluate the probable existence of common method bias. This research followed Podsakoff et al. (2003), who suggested utilising Harman's single-factor test. The result only explains 37.1% of the variation, which is lower than the 50% requirement. The second technique, VIF, was proposed by Kock (2015). According to the author, a VIF over 3.3 is considered a sign of aberrant collinearity and may show that a model is influenced by common method bias. In this investigation, all the constructs were less than a value of 3.3.

After preparing the data, the data analysis was performed (see Section 5.5.1). The section evaluated the model's measurement model. The assessment outcomes led to four variables being excluded from the CSA components due to their failure to meet the 0.5 threshold. The results of the other items demonstrated the measurement model's reliability and validity; therefore, analysis began with evaluating the structural model (see Section 5.5.2). The analysis revealed that 8 out of 13 hypotheses (**H₃**, **H₄**, **H₅**, **H₇**, **H₈**, **H₁₁**, **H₁₂**, and **H₁₃**) were accepted. The rejected hypotheses were **H₁**, **H₂**, **H₆**, **H₉**, and **H₁₀**. Finally, Section 5.5.3 reveals the results of the analysis regarding employee differences based on demographics. The analysis across different demographics, including gender, age, education level, profession, and years of experience, revealed how various factors influenced specific outcomes. Consistent significant paths, such as those hypothesised in **H₃** and **H₄**, indicate that positive emotions drive positive protection motivation behaviour and self-efficacy across all groups. The results for **H₃** across all groups suggest that when employees experience positive emotions, they are motivated and encouraged to engage actively in protective behaviour in cybersecurity. Moreover, the results for **H₄** suggest that positive emotion improves the self-efficacy of employees, indicating that employees with positive emotions are likely to engage effectively in tasks, including cybersecurity. The next chapter will discuss the results and explore their relationship with the literature review.

Chapter Six: Discussion

6.1 Introduction

The data were analysed in the last chapter using SmartPLS 4 software. This chapter provides a detailed discussion of the results. It also offers justification for the acceptance or rejection of the proposed hypotheses, interprets the findings, and aligns them with existing literature on cybersecurity protection motivation behaviour. The chapter contains two main sections. First, it discusses the direct relationship between negative and positive emotions and employees' protection motivation behaviour and their self-efficacy; the relationship between self-efficacy and employees' protection motivation behaviour; the role of self-efficacy as a mediator of the relationship between negative and positive emotions and employee's protection motivation behaviour; and the relationship between cybersecurity awareness and employees' protection motivation behaviour. It also discusses the moderating role of employees' cybersecurity awareness in the relationship between negative and positive emotions and employees' protection motivation behaviour; in the relationship between negative and positive emotions and employees' self-efficacy; and in the relationship between self-efficacy and protection motivation behaviour. Second, it describes employees' differences based on their demographic variables.

6.2 Proposed Theoretical Framework

This section will discuss the research findings presented in the previous chapter. This section answers the first, second, and third research questions. The first research question concerns whether negative and/or positive emotions directly affect employees' cybersecurity protection motivation behaviours. Moreover, the second research question concerns how self-efficacy may contribute to cybersecurity protective motivation behaviours and how it can mediate the effects of negative and positive emotions. Finally, the third research question concerns whether employees' cybersecurity awareness positively affects protection motivation behaviour and whether it moderates the direct relationship between negative and positive emotions and employees' protection motivation behaviour, the relationship between negative and positive emotions and employees' self-efficacy, and the relationship between employees' self-efficacy and protection motivation behaviour.

Figure 24 illustrates the findings of the proposed model. The results show that eight out of 13 hypotheses were significant and accepted, and five were not statically significant, and were therefore rejected. The accepted hypotheses are **H₃**, **H₄**, **H₅**, **H₇**, **H₈**, **H₁₁**, **H₁₂**, and **H₁₃**. The

rejected hypotheses are **H₁**, **H₂**, **H₆**, **H₉**, and **H₁₀**. In the following subsection, the findings of the proposed hypotheses are discussed.

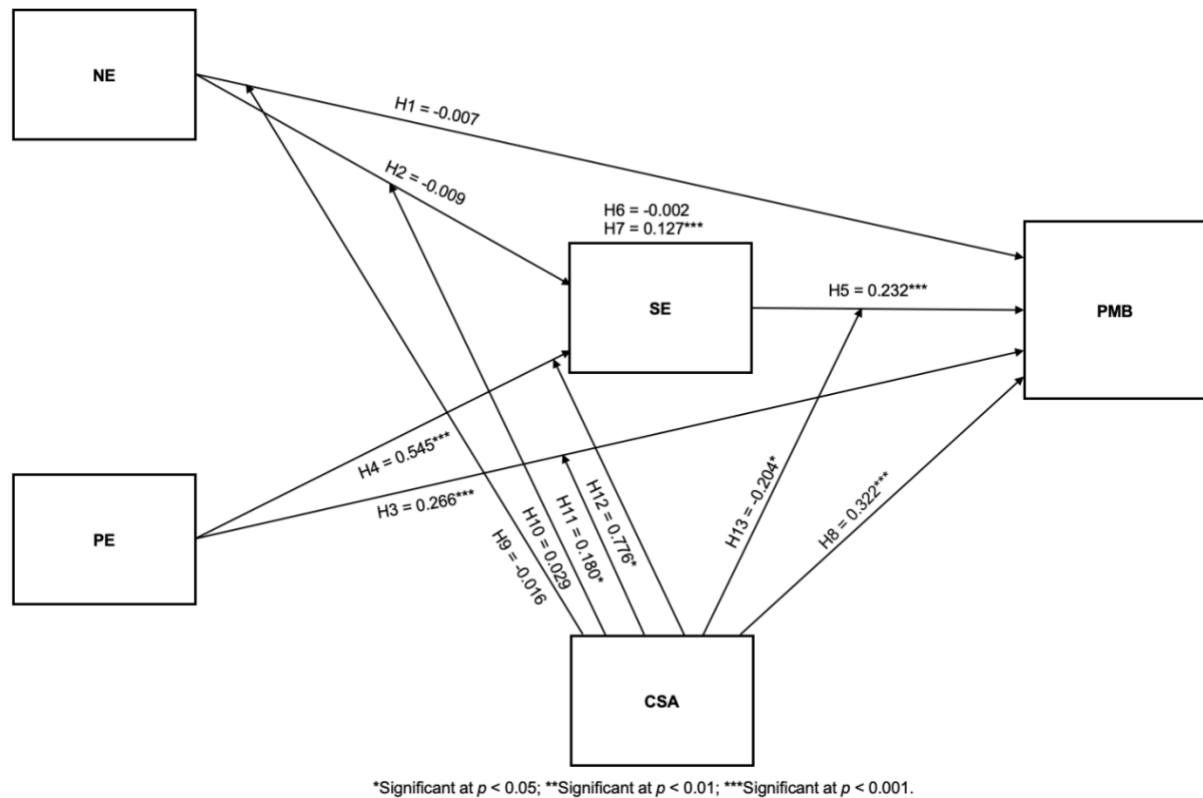


Figure 24: Proposed Theoretical Framework Findings

6.2.1 Negative Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy

This study hypothesised in the proposed model that negative emotions promote negative protection motivation behaviour among employees (**H₁**), suggesting that when employees experience negative emotions, it can lead to a decline in their motivation to engage in protective behaviours in cybersecurity. The first hypothesis was tested, looking at the differences in magnitude of the effect between groups. The p-values indicate the likelihood of obtaining such results if there is no difference among groups. The results (β -value = -0.007 and p-value = 0.845) suggest that the hypothesis is not accepted, and the high p-value indicates that there is no evidence for a null hypothesis rejection. This means that negative emotions do not significantly influence the protection motivation behaviour of the employees.

The hypothesis result differs from that of other researchers, who found that negative emotions promote a negative influence on behaviour (e.g., Zhen et al., 2022; Farshadkhah et al., 2021; Gulenko 2014). However, the result aligns with Chen et al. (2022b), who found that the stress caused by challenging information security situations only leads to compliance with ISP

regulations when it triggers positive emotions and negative emotions do not have any influence. Moreover, Zhao et al. (2018) found that the effect of employees' organisational citizenship activity was influenced by positive emotions but not by negative emotions. Negative emotions, such as fear and anxiety, are frequently seen as critical variables that drive employees to engage in protective motivational behaviours in different situations. However, this study used negative emotions such as anger, discouragement, and uneasiness to explore their influence. Therefore, in the context of employees' protection motivation behaviour in cybersecurity, the significance of these negative emotions might not be as prominent as often assumed (Conrad et al., 2022). The PMT proposes that motivation to be involved in protection behaviour is driven by the perception of a threat and the desire to prevent negative consequences (Floyd et al., 2000). Negative emotions can elicit a feeling of urgency or worry, but they may not be the main factors that drive employees' protective behaviours in cybersecurity. Negative emotions can provoke powerful reactions and may be linked to behavioural responses in cybersecurity (Conrad et al., 2022), their impact on employees' protection motivation behaviour to safeguard themselves may not be as significant as previously believed. Moreover, factors such as the efficiency of defensive measures, the use of positive reinforcement, and the factual application of cybersecurity rules seem to have a significant influence on determining employees' attitudes and actions related to cybersecurity. Negative emotions might trigger responses and reactions in employees, the data indicates that they may not influence protective motive behaviour in the context of cybersecurity. Therefore, understanding employees' emotions includes exploring cyber threats' psychological impact on employees and determining their needs for cybersecurity training programs. This may go beyond addressing the emotional response to include knowledge and practical skills to encourage protection motivation behaviour (Fadhlurahman, 2024).

Moreover, it was hypothesised that negative emotions promote a negative effect on employees' self-efficacy (H_2). In a cybersecurity context, self-efficacy encompasses employees' confidence in their capability to engage in protective behaviours and effectively protect against cyber threats. The analysis results provided the values β -value = -0.009 and p-value = 0.835, indicating that the results were statistically insignificant, leading to hypothesis rejection. The result suggests that negative emotions do not influence employees' self-efficacy in a cybersecurity context.

This result conflicts with some findings that would support the hypothesis that negative emotions negatively influence protection motivation behaviour and self-efficacy within the cybersecurity and information security. Chen et al. (2022b) and Farshadkhah et al., (2021) illustrate that negative emotions, encompassing discomfort, shame, fear and discouragement,

are linked with employees' tendency to engage in behaviours that contravene information security policies and compromise security measures. Moreover, Ogbanufe and Pavur (2022) demonstrate how motivational fear factors and anticipatory regret can impact individuals' decision making regarding the protective behaviour against identity theft threats. Additionally, Chu and So (2020) and Renaud et al. (2021) highlight how negative emotions arising from cybersecurity threats and the context of unethical behaviour can further exacerbate employees' unwillingness or inability to adhere to protocols for security. These findings highlight the detrimental influence of negative emotions on employees' attitudes and actions towards cybersecurity, thereby supporting the hypothesis.

However, several research areas that describe the relationship between self-efficacy and emotions support this finding. According to Sleiman and A Sayah (2018), self-efficacy is important for determining performance and behaviour. However, the main focus of research is on several aspects, the general idea of self-efficacy is considered a critical factor in influencing behaviour that aligns with rejecting the hypothesis. If self-efficacy is not significantly impacted by negative emotion, then it implies that other factors are influencing it. Thapa (2023) outlines the complexities of the relationship between cognitive appraisals and emotions. Negative emotion may not lead to a decline in self-efficacy; differences between individuals and situational factors can contribute to the emotional impact on self-efficacy. To address the influence of negative emotions on employees' self-efficacy, organisations should focus on interventions that promote self-efficacy regardless of emotions. This includes targeted training programmes, skill-building initiatives, developing a culture supportive of an organisation, and empowering employees to take proactive steps in cybersecurity. Understanding the distinction relationship between self-efficacy and emotion could inform effective strategies to improve employees' confidence in dealing with risks and cyber threats.

6.2.2 Positive Emotions and Employees' Cybersecurity Protection Motivation Behaviours and Self-Efficacy

This study hypothesised that positive emotions promote positive protection motivation behaviour among employees (H_3). The hypothesis's statistical results state β -value = 0.266 and p-value = 0.000, so the hypothesis is accepted and statistically significant. This result implies that positive emotion positively influences employee protection motivation behaviour, suggesting that when employees experience positive emotions, they are motivated and encouraged to engage in protective behaviour in cybersecurity actively.

In cybersecurity, employees faced with decision-making tasks related to their online behaviour may receive benefits from positive emotions that lead them to be security-conscious and make influential choices. Peters (2018) found that positive emotions can increase problem-solving and decision-making abilities. According to the BBT, positive emotion can broaden individuals' action and thought repertoire, leading to open-mindedness, increased creativity, and flexibility (Fredrickson, 2001). In cybersecurity, positive emotion contributes to proactive and optimistic viewpoints that motivate employees to adopt positive and willing behaviour. The theory also posits that positive emotions can develop personal resources such as social connection and resilience, which can further improve the ability of individuals to cope with issues, including those related to cybersecurity. According to the IA (2022), individuals experiencing positive emotions are likely to approach work creatively and enthusiastically. This approach can translate into an engaged and proactive stance towards cybersecurity measures. When employees have positive emotions, they are actively inclined to seek information on best cybersecurity practices, willing to participate in programmes for training, and voluntarily adopt preventive measures.

The results align with several studies that support the idea that positive emotion plays a key role in motivation and behaviour in several contexts, including cybersecurity and workplace areas (Zhen et al., 2020; Chen et al., 2022b; Gulenko, 2014; Qin & Liu, 2019; Peters, 2018; He et al., 2020). Zhen et al. (2020) found that positive emotions positively and significantly influence behaviour in information security. In addition, Chen et al. (2022b) found that positive emotions mediate the effect between information security stress and information security policy compliance. Gulenko (2014) found that persons who feel positive emotions tend to choose passphrases with more words than those who experience negative emotions. Moreover, positive leadership emotions impact work behaviour (Qin & Liu, 2019). He et al. (2020) described the considerable influence of employees' security experience, beliefs, and perceptions, as well as the training provided by companies, on how employees evaluate the severity of information security issues.

This study explains the crucial significance of positive emotions in employees' protection motivation behaviour, thereby establishing a potential relationship across BBT and PMT. This outcome provides an original viewpoint on PMT, which operationalised the concept of employees' protection motive behaviours, which were initially abstract, by providing precise details within cybersecurity. Therefore, to address the critical role of positive emotions in employees' protection motivation behaviour, strategies need to be implemented by organisations to cultivate positive emotions in the workplace. This includes promoting a positive culture in the organisation, recognising and rewarding employees for

accomplishments in cybersecurity, and providing resources for emotional management and well-being. In addition, the inclusion of positive psychology elements in cybersecurity training programmes can increase initiatives' effectiveness by tapping into positive emotions and motivational power. Overall, the acceptance of the third hypothesis highlights strong positive emotions and their important impact on employees' protection motivation behaviour in cybersecurity. Drawing on empirical evidence and established theories, organisations can utilise this understanding to develop interventions that promote positive emotions and improve the motivation of employees to participate actively in cybersecurity efforts.

Moreover, it was hypothesised that positive emotions positively influence employees' self-efficacy (**H₄**). With β -value = 0.545 and p-value = 0.000, the results indicate that the hypothesis is accepted and significant statistically. This implies that positive emotion improves the self-efficacy of employees, suggesting that employees with positive emotions are likely to feel capable of engaging effectively in cybersecurity tasks.

This result aligns with several studies that support the idea that positive emotions are an important and supporting influencer of self-efficacy in domains such as cybersecurity and the workplace (Zhen et al., 2020; Bandura, 1986; Schwarzer & Renner, 2000; Luthans et al., 2006). According to Bernhard (2020), self-efficacy plays a vital role in mental processes, behaviour, and motivation. Positive emotion effectively contributes to the positive feedback loop, improving an individual's belief in their capabilities and skills and impacting their performance and motivation. Maniyeva (2022) investigates the relationship between self-efficacy and PsyCap, which includes efficacy, resilience, hope, and optimism. The findings indicated a positive relationship between self-efficacy and PsyCap, emphasising the role of attitudes and positive emotions in shaping an individual's confidence and abilities. In cybersecurity, cultivating psychological resources and positive emotions increases employment. Rusbult and Agnew (2010) explored broadening and building positive emotional effects. The study highlights that positive emotion can broaden individuals' behavioural and cognitive repertoires and facilitate problem-solving and thinking (flexible) abilities. The broadening effect positively impacts self-efficacy by providing an expansive and optimistic mindset for individuals, potentially improving their belief in their ability to handle issues related to cybersecurity.

In cybersecurity, employees with self-efficacy can approach tasks with a positive mindset, leading to effective decision making and problem-solving related to security measures. Previous research supports the hypothesis that positive emotions significantly influence employee protection, motivation behaviour, and self-efficacy within the cybersecurity context.

Zhen et al. (2020) and He et al. (2020) demonstrated increased awareness of information security and positive experiences of security, as the result of training and organisational support, along with improved perceptions of the severity of information security threats and the ability to engage in protection motivation behaviour. This aligns with positive emotions promoting positive protection motivation behaviour among employees. Zhen et al. (2020) reveal that positive emotions positively influence self-efficacy as psychological capital and emotional intelligence, which can underline the positive impact of positive emotions on self-efficacy. The research body collectively highlights positive emotions' role in shaping employees' attitudes towards cybersecurity, thereby supporting the hypothesis. The acceptance of the fourth hypothesis highlights the significant influence of positive emotions on self-efficacy. Companies can develop strategies to improve employees' self-efficacy by drawing on established theories and empirical evidence. This understanding can inform targeted interventions that influence positive emotions and motivational power, contributing to a resilient and secure workforce. This finding supports the theories of BBT and PMT by demonstrating that positive emotions benefit employees. Applying this research confirms the use of positive emotions in cybersecurity and enhances the connections between aspects of PMT by integrating PMT and BBT. Moreover, this study reveals the positive emotions that influence employees' self-efficacy and behaviour in terms of protection motivation. The empirical results provide evidence supporting the arguments that expand the scope of BBT in cybersecurity.

6.2.3 Self-Efficacy and Employees' Cybersecurity Protection Motivation Behaviours

This study hypothesised that self-efficacy promotes a positive protection motivation behaviour among employees (H_5). This means that employees believe in their ability to perform specified tasks successfully or achieve a goal that promotes positive protection motivation behaviour in a cybersecurity context. The results reveal that self-efficacy significantly influences employees' protection motivation behaviour (β -value = 0.232 and p -value = 0.000). This suggests that self-efficacy influences employee protection motivation behaviour in a positive way, implying that when employees believe in their capability to protect themselves from threats, they are likely to engage in positive and proactive behaviours for protection.

The findings align with several studies that support the idea that self-efficacy is critical for shaping decision making, motivation, and behaviour cybersecurity (Gross, 1998; Compeau & Higgins, 1995; Rhee et al., 2009; Parshetty, 2019; Herath & Rao, 2009; Kryshko et al., 2023). According to Gross (1998), individuals with high levels of self-efficacy are more likely to both continue and adopt beneficial behaviours, in contrast to those with low self-efficacy (Compeau & Higgins, 1995; Rhee et al., 2009). Parshetty (2019) stated that individuals with higher self-

efficacy would likely approach challenging tasks with resilience, persistence and confidence. In cybersecurity, employees who have strong self-efficacy are proactive, actively seek best practices information, and willingly participate in training programmes to improve skills and knowledge. Herath and Rao (2009) examined the relationship between the PMT and business compliance with security policies. They found that self-efficacy and response efficacy influenced individuals' attitudes towards complying with security policies. The findings indicated a positive relationship between protection motivation and self-efficacy, supporting the idea that individuals who believe in their ability to protect themselves are motivated to take action for prevention. Kryshko et al. (2023) examined self-efficacy's impact on health-related behaviours. While not directly linked to cybersecurity, the study identifies that individuals with high self-efficacy were likely to maintain and adopt behaviours to promote health. This supports the notion in broader terms that self-efficacy is a powerful motivation predictor.

The acceptance of the hypothesis is consistent with the research on applying the PMT. The PMT suggests that individuals are likely to engage in protective behaviours if they can perceive a threat, believe the suggested actions are practical and have confidence in their ability to take action. In cybersecurity, self-efficacy becomes a critical factor that impacts individuals' motivation to adopt and maintain proactive protection measures. Overall, the hypothesis acceptance emphasises the significance of self-efficacy in promoting positive protection motivation behaviour among individuals. By drawing on established psychology theories and empirical evidence, organisations can implement strategies to improve employees' self-efficacy. This understanding can inform targeted interventions that empower employees to take proactive steps to protect themselves against threats, contributing to a security-conscious and resilient workforce.

Regarding self-efficacy, this research also hypothesised that self-efficacy intervenes in the relationship between negative emotions and employees' protection motivation behaviours (H_6). It implies that people with higher levels of self-efficacy are more likely to manage and lessen the negative effects of emotions on their protection motivation behaviour. The obtained results are not statistically significant, as the β -value = -0.002 and the p-value = 0.839, leading to the hypothesis's rejection. This implies that, in the case of cybersecurity, self-efficacy might not have a significant intervening effect on the association between employees' protection motivation behaviour and negative emotions. The research on the relationship between negative emotions, self-efficacy, and protective motivation behaviour is still limited, therefore perceptions from particular fields could be beneficial for interpreting the results. Folkman and Lazarus (1988) highlight the function of coping strategies in mitigating the effect of stimuli on psychological consequences. Negative emotions can be considered stressors in

cybersecurity, and self-efficacy might be a coping strategy. However, the lack of statistical significance in the current study suggests that the relationship would need to be stronger to prove the hypothesised mediation.

Furthermore, the idea of implementation intentions, which involve making precise plans regarding when, where, and how to act in a particular situation, has been studied by Gollwitzer and Kinney (1989). An increase in self-efficacy can help people to successfully implement intentions to overcome negative emotions and be involved in protection motivation behaviours. However, the lack of statistical evidence in the current study makes the importance of self-efficacy unclear. The emotion regulation theory might explain the rejection of the sixth hypothesis. Gross (1998) implies that people with strong emotional regulation skills are more likely to be better at controlling and reducing the effects of negative emotions. Self-efficacy and emotional regulation are two distinct terms, but they have some things in common as they are both linked to a person's capacity to control their emotions. The lack of statistically proven results might suggest that emotional regulation plays a vital role in mediating the relationship between negative emotions and protective motivation behaviour, rather than self-efficacy alone.

Organisations must consider multidimensional treatments to deal with the role of self-efficacy as a mediator between negative emotions and employees' cybersecurity protection motivation behaviour. This could involve adding components of emotional control and increasing self-efficacy through focused training programmes. Maintaining an encouraging work atmosphere that addresses the psychological effects of cybersecurity risks can also help to develop a resilient and motivated staff. The rejection of the sixth hypothesis emphasises the need for a more complex study of how negative emotions, self-efficacy, and protective motivation behaviours are interlinked in cybersecurity. However, self-efficacy was not found to have a significant role in this study; more research into related psychological ideas could result in useful information on creating strategies to reduce the emotional toll that cybercrime takes on employees.

Concerning self-efficacy, the seventh hypothesis states that self-efficacy intervenes in the relationship between positive emotions and employees' protection motivation behaviours (**H₇**). The obtained results are statistically significant, with a β -value= of 0.127 and a p-value of 0.000, leading to the hypothesis's acceptance. In particular, it implies that the greater the levels of self-efficacy, the better the person will use positive emotions to increase their protective motivation behaviour involvement. The relationship between positive emotions and employees' protection motivation behaviour is significantly influenced by self-efficacy, implying

that those with greater self-efficacy levels are more likely to convert positive emotions into active and beneficial cybersecurity actions. Adopting the seventh hypothesis is proportional to the BBT and PMT, which emphasise the powerful impact of self-efficacy in regulating behaviours, particularly when positive emotions are involved. People who have self-efficacy at higher levels are more likely to see positive emotions as a sign that they can accomplish the task (Bandura, 1986). Positive emotions motivate people to accept protective behaviour in the context of cybersecurity, enabling them to do so with confidence, excitement, and faith in their ability to carry out cybersecurity precautions. The study result aligns with the existing literature (Zhen et al., 2020; Schwarzer & Renner, 2000). Schwarzer and Renner (2000) studied the relationship between health behaviours, self-efficacy, and positive effect. According to the research, higher levels of self-efficacy in people will result in higher positive emotions, and they are more likely to be involved in activities that promote health. This highlights the potential functions of self-efficacy in the relationship between positive emotions and behaviour, although not connected with cybersecurity. In addition, it has been found that self-efficacy mediates the association between protection motivation behaviour and positive emotions among employees (Zhen et al., 2020). Moreover, Fredrickson (2001) stated in the BBT that positive emotions can increase a person's repertoire of thoughts and actions. Positive emotions can make people more open to adopting new security measures, looking for more information on best developments, and readily engaging in training programmes in cybersecurity. The conversion of such positive emotions into long-lasting and successful protective motivation behaviour may be assisted by more significant levels of self-efficacy. The adoption of the seventh hypothesis is also linked to the idea of PsyCap, which involves self-efficacy as one of its main components. PsyCap has been seen to improve people's motivation, resilience, and performance (Luthans et al., 2006). In cybersecurity, those with higher levels of PsyCap might have a stronger drive to safeguard systems when experiencing positive emotions.

Therefore, organisations must create strategies that focus on developing positive emotions and self-efficacy. Training programmes can be excellent for promoting suitable cybersecurity measures, assisting skill development, and cultivating an excellent organisational atmosphere. The seventh hypothesis illustrates self-efficacy's role as a facilitator in the relationship between protection motivation behaviour and positive emotions in cybersecurity. Organisations can create initiatives to promote security-conscious staff by using positive emotions and increasing self-efficacy. This will help to maintain a resilient and active cybersecurity policy.

6.2.4 Employees' Cybersecurity Awareness

The eighth hypothesis posited that cybersecurity awareness positively influences protection motivation behaviours (H_8). The hypothesis statistical results were β -value= 0.322 and p-value = 0.000. The result shows that cybersecurity awareness has a positive effect on protection motivation behaviour. This means that employees' motivation to protect themselves from cyber threats increases as they become more aware of cybersecurity issues.

The hypothesis results align with the existing literature, which has reported that cybersecurity awareness positively affects protection motivation behaviour (Bada et al., 2014; Cram et al., 2017; Hanus & Wu, 2016; Hong et al., 2023). According to Bada et al. (2014), cybersecurity awareness programmes positively affect users' security behaviours and attitudes, resulting in more proactive and knowledgeable security practices. Similarly, Hanus and Wu (2016) found a positive relationship between cybersecurity awareness and individuals' evaluations of threats and coping strategies. This, in turn, resulted in a greater inclination to take security measures. This link emphasises the significance of awareness in influencing how individuals perceive and react to cyber threats. Moreover, Cram et al. (2017) indicated that there was a positive correlation between employees' awareness of information security and adherence to information security regulations. This highlights the importance of awareness in promoting a secure culture within organisations. Similarly, Hong et al. (2023) found that all-encompassing cybersecurity education initiatives enhance individual understanding and perspectives, and organisational ability to withstand cyber assaults. The hypothesis indicates that organisations and individuals who invest in cybersecurity awareness programmes can expect tangible benefits. These include improved security behaviours and a reduced susceptibility to cyber threats. By raising awareness and educating their workforce, organisations can build a stronger defence against the constantly changing setting of cyber threats, promoting more security-conscious employees.

Regarding the moderation effect, this study hypothesised that cybersecurity awareness moderates the direct relationship between negative emotions and employees' protection motivation behaviours (H_9). In other words, it proposes that employees with higher cybersecurity awareness will weaken the relationship between negative emotions and protection motivation behaviours compared to those with lower awareness. The results provided for the hypothesis (β -value = -0.016 and p-value = 0.736) indicate that the hypothesis was rejected. There is also no evidence in existing research that cybersecurity awareness moderates the relationship between employee negative emotions and their protection motivation behaviour. While the hypothesis is rejected, it is necessary to consider the key reasons behind the results and draw from existing literature and research. Sulaiman

et al. (2022) highlighted the importance of examining factors that impact the responses of individuals to cybersecurity threats. Cybersecurity awareness is a critical determinant of how individuals perceive and respond to cyber risks. Song et al. (2024) emphasise the organisation's support role in impacting employees' cybersecurity behaviour. The findings suggest that employees are likely to engage in protective behaviour when strong organisational support for cybersecurity is perceived. This outlines the importance of considering the broader factors of the organisation to understand and address employees' protection motivation behaviour. Additionally, research on PMT by Thornton and Turley (2020) suggested that the perceived severity of threats and the efficacy of protective measures are critical determinants of protection motivation. While cybersecurity awareness may contribute to the perceived efficacy, other factors related to threat severity and the effectiveness of available protective measures would influence protection motivation behaviour. The rejection of the hypothesis suggests that cybersecurity awareness did not significantly moderate the relationship between negative emotions and protection motivation behaviour among employees in the research context. Further research could explore a broader set of individual and organisational factors that might provide an understanding of the dynamics impacting employees' protection motivation behaviour regarding cybersecurity threats.

Moreover, the tenth hypothesis posited that cybersecurity awareness moderates the relationship between negative emotions and self-efficacy (H_{10}). This suggested that, for employees with higher cybersecurity awareness, there will be a weaker relationship between negative emotions and employees' self-efficacy compared to those with lower awareness. The results provided for the hypothesis (β -value = 0.029 and p -value = 0.542) indicate that the hypothesis was rejected. This means there is no evidence that cybersecurity awareness moderates the relationship between negative emotions and employee self-efficacy. As the hypothesis is rejected, it is crucial to explore the potential explanations for this outcome and draw from existing research.

In the literature, there is a lack of evidence for the statistical significance of cybersecurity awareness as a moderator of the relationship between negative emotions and self-efficacy under the tested conditions. According to Venard (2021), communication, importance, and training programmes can shape employees' cybersecurity behaviours. The finding indicated that individuals with higher cybersecurity awareness would be likely to adopt protection measures. One possible explanation for the non-significant result in this study is that the effectiveness of awareness programmes may vary, and other factors like training design and delivery, organisational support, and employees' cognitive information processing can impact the relationships observed. Moreover, research on cybersecurity psychology considers the

relationship between emotional and mental factors. Hanus and Wu (2016) investigated the relationship between behaviour, knowledge and emotion. The findings indicated that individuals with a higher understanding of security would be likely to experience positive emotions about security, finally impacting their protective behaviours. While research cannot explore self-efficacy, it can highlight the cognitive factors that are interconnected in nature, emotional experience, and cybersecurity behaviour. The rejection of the hypothesis also prompts a close examination of cybersecurity awareness components related to self-efficacy. While general awareness contributes to individuals' understanding of cyber threats, the context emphasises developing self-efficacy within awareness programs would be critical. Organisations must refine cybersecurity programmes to take into account the influence of negative emotions on self-efficacy and include elements that improve self-efficacy regarding negative emotions. This includes training targeted at coping approaches, developing resilience, and providing resources for employees to manage and prevent the emotional impact of cybersecurity threats. The rejection of the hypothesis suggests that cybersecurity awareness cannot significantly moderate the relation between negative emotions and self-efficacy within the research scope. Organisations can investigate specific awareness programme components and their impact on the emotional aspects and cognitive factors of cybersecurity behaviour, providing valuable understandings for designing effective interventions.

The eleventh hypothesis suggests that cybersecurity awareness moderates the direct relationship between positive emotions and employees' protection motivation behaviours (H_{11}). This implies that, for employees with higher cybersecurity awareness, there will be a stronger relationship between positive emotions and employees' protection motivation behaviours, compared to those with lower awareness. The hypothesis statistical results (β -value = 0.180 and p -value = 0.038) indicate that the hypothesis is accepted and statistically significant. The results suggest that, when employees have high cybersecurity awareness, their positive emotions positively influence protection motivation behaviour.

While research on how cybersecurity awareness moderates the relationship between positive emotions and employees' cybersecurity protection motivation behaviour is currently limited, knowledge from specific domains can help to understand the findings. Lee and Chua (2023) demonstrated cybersecurity awareness's impact on individual protection behaviour. They found that individuals with high awareness were more likely to adopt security measures than those with low awareness. The research does not just explore awareness as a mediator of the association between positive emotions and protection motivation behaviour, but it also lays the groundwork to understand the impact of awareness on cybersecurity actions. Positive

emotions can contribute to an optimistic perception of the effectiveness of proactive measures. Cybersecurity awareness can increase this effect by providing individuals with the skills, knowledge, and understanding required to translate positive emotions into tangible protection motivation behaviour. Moreover, research on the role of positive emotions in decision making can support awareness of the fact that emotions impact behaviour. Positive emotions may motivate individuals to take risks, but heightened awareness can prevent this by guiding positive emotions towards constructive protection motivation behaviour. The results of the hypothesis indicated the importance of considering individuals' emotions and awareness levels while designing interventions to increase employees' protection motivation behaviour in cybersecurity. Thus, organisations should prioritise cybersecurity awareness programmes that inform employees about cyber threats and guide them on how to translate positive emotions into effective protection actions. These programmes can include real-life scenarios, simulations, and practical guidance on implementing cybersecurity best practices.

The twelfth hypothesis posited that cybersecurity awareness moderates the relationship between positive emotions and employees self-efficacy (H_{12}). In other words, it proposed that, for employees with higher cybersecurity awareness, there will be a stronger relationship between positive emotions and their self-efficacy compared to those with lower awareness. The hypothesis's statistical results (β -value = 0.776 and p -value = 0.018) indicate that the hypothesis is accepted and statistically significant. This means that when employees have high cybersecurity awareness, their positive emotions positively influence their self-efficacy.

The hypothesis aligns with existing research on the relationship between emotion and self-efficacy, and its impact on behaviour. For example, Zhen et al. (2020) found that having an awareness of security can strengthen the positive impact of positive emotions. Baltutis et al. (2023) studied how to enhance individuals' awareness and knowledge of cybersecurity behaviour. They suggest that persons with security knowledge are more likely to demonstrate security efficacy when implementing security measures. Moreover, positive emotion's role in decision making supports the idea that cybersecurity awareness can moderate the influence of positive emotions on self-efficacy. Lee and Chua (2023) stated that positive emotions lead to risk-taking behaviour, but this effect is attenuated when employees are aware of and informed of the risks. Positive emotions may impact individuals' beliefs in their ability to protect themselves, but heightened awareness can increase this effect by providing employees with knowledge and understanding essential to strengthen their self-efficacy. The hypothesis results highlight the importance of cybersecurity awareness training that promotes employee confidence and their ability to protect against threats. This training enables individuals to learn about risks and empowers them with the knowledge and skills they need to identify and

prevent them. However, organisations need to prioritise training programmes focusing on self-efficacy development in the face of positive emotions. These can guide the practice of cybersecurity in real life and create opportunities for employees to develop essential skills.

The thirteenth hypothesis posited that cybersecurity awareness moderates the relationship between self-efficacy and employees' protection motivation behaviours (H_{13}). The hypothesis statistical results state the β -value= -0.204 and p-value= 0.011. The result shows that cybersecurity awareness moderates the relationship between self-efficacy and protection motivation behaviour in a negative way. This indicates that as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours decreases.

The result differs from that of Zhen et al. (2020), who found that higher degrees of information security awareness in employees have a more beneficial influence on their protection behaviour when combined with self-efficacy, compared to individuals with lower levels of information security awareness. According to Li et al. (2019), individuals with a high level of security knowledge can show self-efficacy in adopting security measures. The result for this hypothesis can be attributed to various factors. Firstly, employees with a strong understanding of cybersecurity may become overly confident, resulting in complacency and reduced vigilance (Ainia and Lutfi, 2019). Moreover, Witte (1992) explains that when employees believe that their level of knowledge is enough to keep them safe, the influence of self-efficacy on their safety-related actions may decrease. Secondly, disparity may exist between awareness and practical implementation. Bada et al. (2014) indicate that increasing cybersecurity awareness might not automatically lead to changes in behaviour. Employees may have knowledge of cybersecurity threats, but they often struggle to convert this awareness into effective self-efficacy or protective behaviours. This aligns with the findings published by Parsons et al. (2014), which emphasise the discrepancy between knowledge and behaviour in cybersecurity. Thirdly, a higher level of cybersecurity awareness might lead to increased complexity or the misinterpretation of risks. Bravo-Lillo et al. (2010) suggest that abundant information and intricacy can overpower users, resulting in poorer security choices. Herath and Rao (2009) indicate that employees who feel overwhelmed may have less desire to depend on their self-efficacy to engage in protective behaviours. Finally, a higher level of cybersecurity knowledge can lead to an illusory sense of security when employees mistakenly believe that being aware of potential threats is enough. Vishwanath et al. (2011) have shown that individuals who feel more knowledgeable tend to engage in riskier behaviours because they overestimate their ability to defend themselves. One's belief influences this decrease in desire to participate in protective behaviours in one's capacity to do those behaviours effectively (Rogers, 1975).

Therefore, further investigation into these factors would be necessary to fully understand the underlying reasons for this unexpected result.

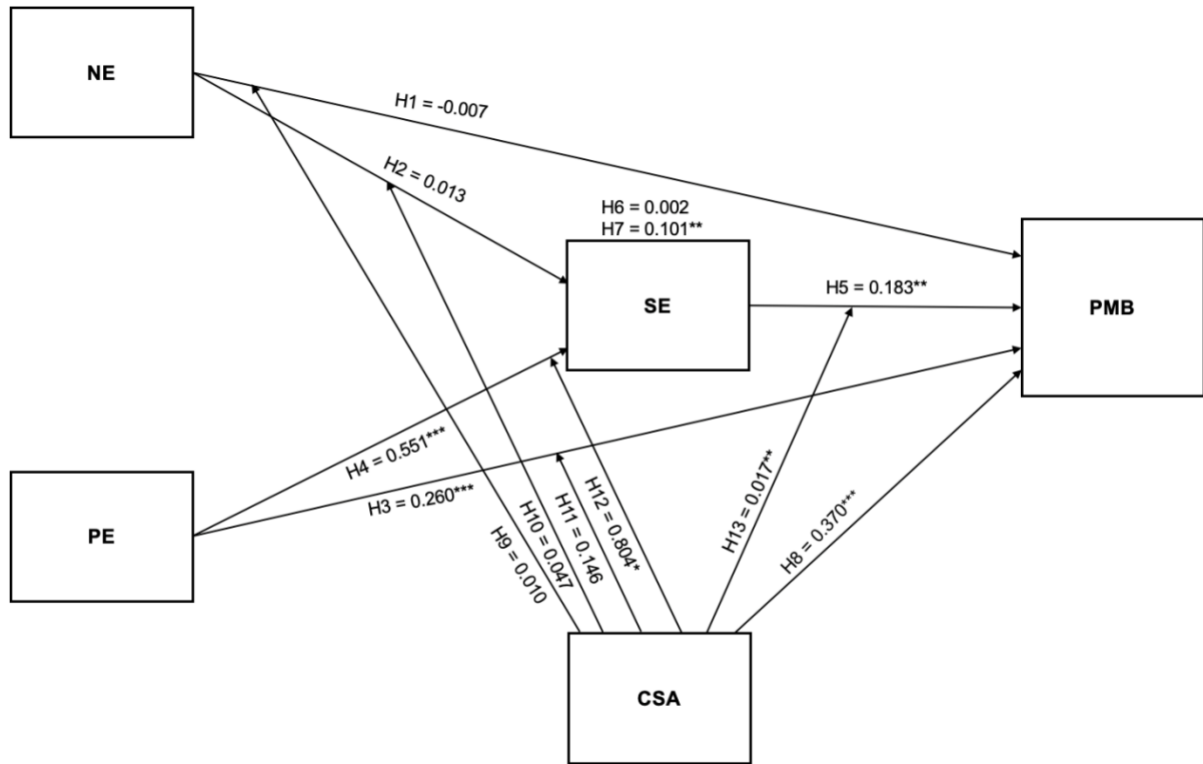
The outcomes of this study have reflective implications for organisations seeking to improve their employees' cybersecurity attitude through awareness training and educational initiatives. While promoting cybersecurity awareness among employees is vital for creating a culture of security and resilience, it is equally important to identify the potential boundaries of interventions that rely solely on awareness. Likewise, the results emphasise the requirement for cybersecurity training and an education strategy that focus on increasing awareness. Finally, this study enhances our comprehension of the intricate dynamics that drive employee behaviour in cybersecurity. By acknowledging the influence of cybersecurity awareness on the relationship between self-efficacy and protection motivation behaviour among employees, organisations can improve their strategies for building a culture of security awareness and resilience. The implications of the results will be discussed in detail in Chapter 7.

6.3 Assessing Employees' Differences in Cybersecurity Protection Motivation Behaviour

In this research, the fourth question concerns the differences between employees in terms of the effects of negative and positive emotions, self-efficacy, and cybersecurity awareness on their protection motivation, according to their demographic characteristics of gender, age, level of education, work position, and years of experience. Understanding employee differences can lead to a greater understanding of the decision-making process when selecting among different employee groups. Comprehending this information makes it possible to develop specific strategies for each employee group, enhancing the likelihood of their engagement in protective motivational behaviour. The following subsections will discuss these findings in detail.

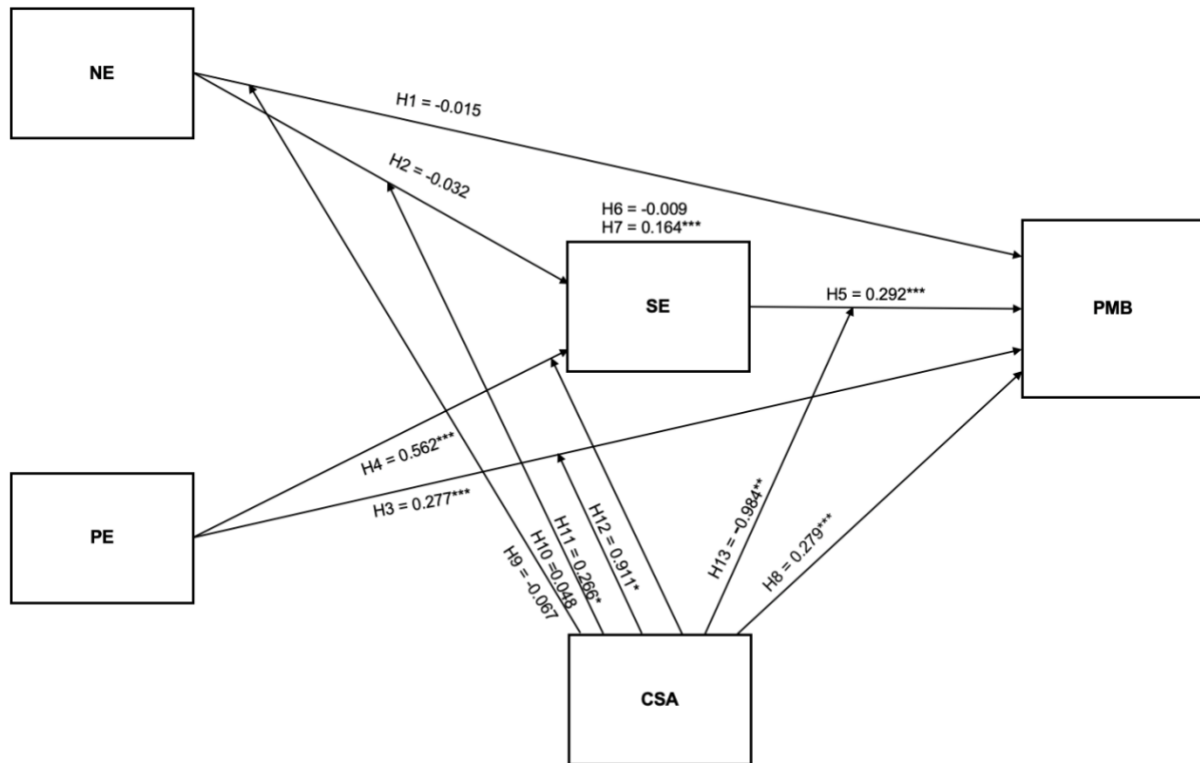
6.3.1 Gender

This subsection compares the differences between male and female employees. The data indicate that there were 242 male participants and 141 female participants in the survey. Figures 25 and 26 illustrate the hypotheses model results for males and females. The figures show the results of the tested pathway, looking at the effects of negative emotion, positive emotion, and self-efficacy on protection motivation behaviour for males and females, as well as the original model result. The model also considers the moderation effects of these variables with cybersecurity awareness. The statistically significant results show some differences between males and females. Female employees were found to have more statistically significant relationships in the model.



Note: *Significant at $p < 0.05$; **Significant at $p < 0.01$; ***Significant at $p < 0.001$.

Figure 25: Model Findings for Male Employees



Note: *Significant at $p < 0.05$; **Significant at $p < 0.01$; ***Significant at $p < 0.001$.

Figure 26: Model Findings for Female Employees

With regard to **H₃**, positive emotion had a significant positive effect on protection motivation behaviour for both males and females. The effect is more significant for females ($\beta = 0.277^{***}$) than males ($\beta = 0.260^{***}$). Bagozzi and Moore (1994) and Floyd et al. (2000) indicate that positive emotions might increase the sense of optimism and empowerment, enhancing employees' motivation to be involved in actions that protect their well-being. The influence of positive emotions on protective behaviour may vary according to gender, and this variation may be affected by social and psychological factors such as emotional expressiveness and coping methods. These factors are more commonly observed among females (Grossman & Wood, 1993).

With reference to **H₄**, positive emotion had a significant positive influence on self-efficacy for both males and females. However, the effect is more significant for females $\beta (= 0.562^{***})$ than males ($\beta = 0.551^{***}$). According to Fredrickson (2001), positive emotions can enhance self-efficacy by promoting a positive self-esteem and increasing the ability to handle stress. According to Else-Quest et al. (2012), differences in the impact of positive emotions on self-efficacy between genders might be related to socialisation processes that promote emotional comparison and the cultivation of confidence in females.

With regard to **H₅**, self-efficacy had a significant positive effect on protection motivation behaviour for both males and females, with a more significant influence for females ($\beta = 0.292^{***}$) than males ($\beta = 0.183^{**}$). Increased levels of self-efficacy improve the chances of taking activities that protect well-being, indicating a strong belief in one's capability to handle threats effectively (Maddux & Rogers, 1983). Societal expectations and roles that prioritise self-confidence and agency in females may influence the gender disparity in how self-efficacy affects behaviour (Luszczynska & Schwarzer, 2015). By acknowledging the importance of self-efficacy in promoting protective behaviours and comprehending the intricate gender dynamics involved, interventions can be customised to increase individuals' confidence in their capacity to reduce risks and effectively address threats. Enabling both males and females to cultivate and sustain strong self-confidence might enhance their ability to take proactive and resilient measures to safeguard against cybersecurity threats and other potential hazards.

The results for **H₇** show that self-efficacy positively intervenes in the relationship between positive emotions and protection motivation behaviour among males and females. However, the effect is more significant for females ($\beta = 0.164^{***}$) than for males ($\beta = 0.101^{**}$). Self-efficacy is crucial for converting positive emotions into actions that protect oneself. For females this influence is more evident, highlighting the significance of strengthening self-beliefs to encourage proactive reactions to risks (Schwarzer & Fuchs, 1996).

The results for **H₈** show that cybersecurity awareness has a positive influence on protection motivation behaviour for both male and female employees. The influence is stronger for male employees ($\beta = 0.370^{***}$), suggesting that as their understanding of cybersecurity matters deepens, their drive to safeguard themselves against cyber attacks significantly intensifies. The influence is less evident for females but there is a positive impact ($\beta = 0.279^{***}$). This is consistent with the overarching model, which indicates a significant and statistically significant positive correlation ($\beta = 0.322^{***}$). Both male and female employees engage in more protection motivation behaviour as their cybersecurity understanding and awareness grows.

For **H₁₁**, the results show that cybersecurity awareness has a significant positive moderation effect on the relationship between positive emotion and protection motivation behaviour for females ($\beta = 0.266^*$). This effect is more significant for females than it is for males. The female's results for **H₁₁** align with those for the original model ($\beta = 0.180^*$). This means that there is no evidence that cybersecurity awareness moderates the relationship between positive emotions and protection motivation behaviour among male employees. Increasing knowledge about cybersecurity threats can increase the beneficial impact of emotions on behaviour, by enabling individuals, particularly females, to proactively safeguard themselves (Luszczynska & Schwarzer, 2015).

Regarding **H₁₂**, the results show that cybersecurity awareness has a significant positive moderation effect on the relationship between positive emotion and self-efficacy. This effect is more significant for females ($\beta = 0.911^{***}$) than for males ($\beta = 0.804^*$). According to Schwarzer and Fuchs (1996), females can use positive emotions and self-efficacy to increase their capability to address cybersecurity threats by promoting awareness about such threats.

With reference to **H₁₃**, the results show that cybersecurity awareness has a significant moderation effect on the relationship between self-efficacy and protection motivation behaviour. This effect is negative for females ($\beta = -0.984^{**}$) but positive for males ($\beta = 0.017^{**}$). In females, this means that as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours decreases. In males, however, as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours increases. In other words, as females learn about cybersecurity threats and challenges, their belief in their capabilities is less likely to result in engaging in preventative behaviour. Nevertheless, as male employees gain awareness of cybersecurity concerns, their self-efficacy increases their motivation to engage

in protective behaviours. The greater their awareness about cybersecurity, the more their trust in their abilities (self-efficacy) leads them to engage in preventive behaviours.

This study's results offer significant understandings and emphasise the critical significance of considering differences by gender in the influence of emotions, self-efficacy, and cybersecurity awareness on employees' protection motivation behaviour. The findings demonstrate differences, indicating that positive emotions and self-efficacy have a more significant beneficial influence on protection motivation behaviour in females than in males. The moderation effect of cybersecurity awareness on the relationships with positive emotions and self-efficacy is more pronounced for females than for males, highlighting the importance of gender-specific approaches in cybersecurity awareness training. This result differs from that by Anwar et al. (2017), who found that females show less secure behaviours than men, highlighting the necessity of gender-sensitive information security programmes.

6.3.2 Age

The age group was divided into two groups, younger and older employees, using the median-split method. As a result, there are 258 employees in the younger employees group (below 39 years old) and 125 people in the older employees group (above 40 years old). Figure 27 shows the results of the model testing for younger employees, whereas Figure 28 shows the results for older employees. The statistically significant results show some differences between younger and older employees. It was found that the relationships under study were more statistically significant for younger employees. This suggests that younger employees might be more influenced by factors like emotions and self-efficacy in their cybersecurity protection motivation behaviour.

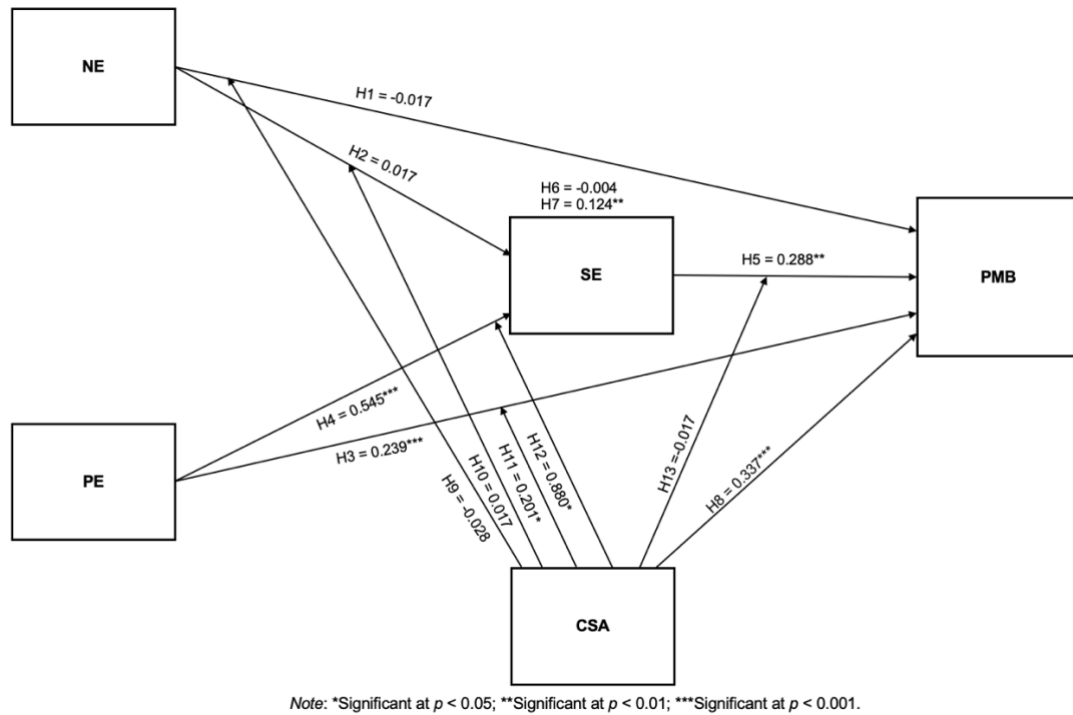


Figure 27: Model Findings for Younger Employees

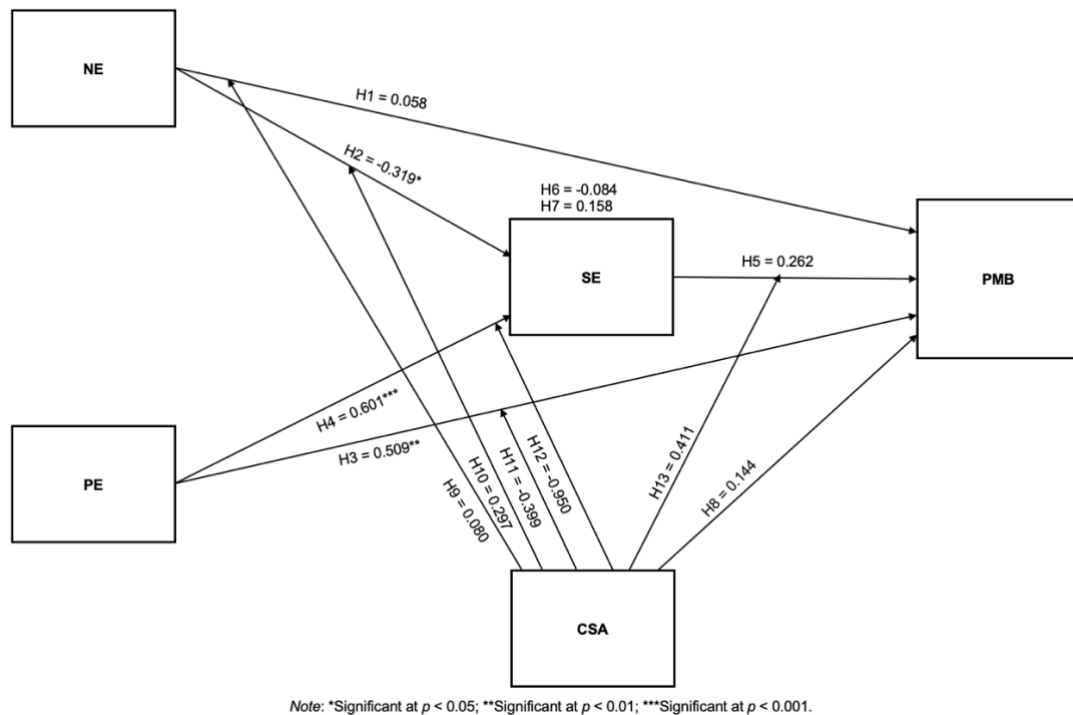


Figure 28: Model Findings for Older Employees

Regarding H_2 , it was found that negative emotions promote a negative effect on employees' self-efficacy. The effect is significant for older employees ($\beta = -0.319^*$) but not for younger employees ($\beta = 0.017$). This means that there is evidence that negative emotions negatively affect older employees' self-efficacy. This indicates the importance of adding emotions to

cybersecurity training programmes. Czaja and Sharit (1998) stated that older people might be experiencing anxiety and stress in relation to technology, which can reduce their self-efficacy in dealing with cybersecurity risks. Therefore, customised interventions that target emotional support can potentially enhance the self-efficacy of older employees in cybersecurity practices.

Regarding **H₃**, it was found that positive emotion has a significant positive effect on protection motivation behaviour for younger and older people. However, the effect is more significant for older ($\beta = 0.509^{**}$) than for younger people ($\beta = 0.239^{***}$). The valuable influence of positive emotions on employees' protective motive behaviour highlights the significance of emotional well-being in promoting cybersecurity involvement among individuals of all age groups. Younger employees demonstrate a stronger reaction to positive emotions, suggesting the necessity of emotional reinforcement to encourage them to embrace preventative cybersecurity practices (Fredrickson, 2001). Organisations can utilise this understanding by implementing measures to promote positive emotions among employees to increase their motivation to engage in cybersecurity activities.

Similarly, the results for **H₄** demonstrate that positive emotion has a significant positive influence on self-efficacy for younger and older people. However, the effect is more significant for older ($\beta = 0.601^{***}$) than for younger people ($\beta = 0.545^{***}$). Therefore, it is clear that both generations may benefit from a positive and enthusiastic outlook on cybersecurity, which can encourage them to take precautions and face threats confidently. The finding that positive emotions enhance self-efficacy highlights the significance of emotional support in promoting the confidence to address cybersecurity threats among employees of all age groups. Younger employees may depend more on emotional support to strengthen their belief in their abilities (Bandura et al., 1999). Organisations might adopt programmes to promote positive emotional experiences and empower staff to cultivate the self-efficacy necessary for effective cybersecurity operations.

H₅ shows that self-efficacy has a significant positive effect on protection motivation behaviour, but only for younger employees ($\beta = 0.228^{**}$). Therefore, no evidence exists that self-efficacy promotes a positive protection motivation behaviour among older employees as the relationship is insignificant ($\beta = 0.262$). The relationship between self-efficacy and protection motive behaviour among younger employees emphasises the importance of cultivating self-assurance in dealing with cybersecurity threats to encourage proactive measures. The result indicates that the confidence of younger employees in their capacity to manage cybersecurity threats is an essential factor driving their participation in preventative actions. Organisations

should prioritise the improvement of self-efficacy among younger employees by implementing specialised training programmes that promote the adoption of proactive cybersecurity measures.

The results for **H₇** show that self-efficacy positively intervenes in the relationship between positive emotions and protection motivation behaviour among younger employees ($\beta = 0.124^{***}$). However, no evidence exists that self-efficacy positively intervenes in the relationship between positive emotions and protection motivation behaviour among older employees, as the relationship is insignificant ($\beta = 0.158$). The significance of emotional well-being in enhancing self-confidence to promote protective activities is highlighted by the mediating role of self-efficacy between positive emotions and protection motivation behaviour in younger employees. The result implies that cultivating positive emotions might increase self-efficacy and stimulate younger employees to participate actively in cybersecurity procedures (Czaja & Sharit, 1998). Organisations can create interventions that enhance positive emotional experiences, strengthen self-efficacy, and increase protective behaviour among younger employees.

The results for **H₈** show that cybersecurity awareness has a positive effect on protection motivation behaviour among younger employees. This effect is significant for younger $\beta = 0.337^{***}$) but not for older employees ($\beta = 0.144$), with the original model result showing a significant positive relationship ($\beta = 0.322^{***}$). The findings suggest that younger employees with a higher level of cybersecurity awareness are more likely to engage in protection motivation behaviour. This is supported by a strong positive effect ($\beta = 0.337^{***}$). As younger employees acquire more information about cybersecurity challenges, their inclination to safeguard themselves from cyber risks significantly intensifies. However, for older employees, cybersecurity awareness does not significantly affect their protective motivation behaviour. When examining all employees, a significant positive correlation remains between cybersecurity awareness and protection motivation behaviour ($\beta = 0.322^{***}$). The overall importance of this finding indicates that younger employees play a major role in the positive impact of cybersecurity awareness on protective motivation behaviour.

Regarding **H₁₁**, the results show that cybersecurity awareness has a significant positive moderation effect on the relationship between positive emotion and protection motivation behaviour for the younger employees ($\beta = 0.201^*$). This effect is more significant for younger employees than for older employees ($\beta = -0.399$). The effect for the younger group for **H₁₁** aligns with the original model as the effect is significant ($\beta = 0.180^*$). There is no evidence to suggest that cybersecurity awareness moderates the relationship between positive emotions

and protection motivation behaviour among older employees. These results emphasise the importance of awareness in promoting cybersecurity engagement. According to Venkatesh et al. (2003), younger employees gain more significant advantages from awareness programmes that improve their comprehension of cybersecurity concerns. Organisations can utilise cybersecurity awareness programmes to enhance the beneficial impact of emotions and inspire younger employees to embrace protective cybersecurity behaviours.

Regarding H_{12} , the results show that cybersecurity awareness has a significant positive moderation effect on the relationship between positive emotion and self-efficacy among younger employees ($\beta = 0.880^*$) but not for older employees ($\beta = -0.950$). The result for the younger employees aligns with the original result ($\beta = 0.776^{***}$). There is no evidence that cybersecurity awareness moderates the relationship between positive emotions and protection motivation behaviour among older employees, but the result suggests the important role of cybersecurity awareness in improving the relationship between younger employees' positive emotions and self-efficacy. According to Fredrickson (2001), awareness about hazards can increase the influence of positive emotions on people's self-efficacy. Therefore, organisations can leverage cybersecurity awareness to increase the relationship between positive emotions and self-efficacy, allowing younger employees to contribute actively to cybersecurity measures.

The results for H_{13} show that cybersecurity awareness has a statistically insignificant moderating effect on the relationship between self-efficacy and protection motivation behaviours for both younger ($\beta = -0.017$) and older employees ($\beta = 0.411$). The original model result reflects an overall significant negative relationship ($\beta = -0.204^*$), indicating a complex interaction effect across the age groups. Thus there is no evidence to suggest that cybersecurity awareness moderates the relationship between self-efficacy and protection motivation behaviour among younger and older employees. The finding differs from the original results, which indicate that as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours decreases. The result indicates the complex nature of the factors that impact cybersecurity practices and highlights the need for complete explanations that combine awareness with enhancements in emotional well-being and self-efficacy (Venkatesh et al., 2003). Thus, organisations might use complete approaches that combine cybersecurity expertise with interventions to increase emotional well-being and self-efficacy. This approach will encourage employees of all age groups to adopt cybersecurity practices.

These discussions offer a deeper understanding of the relationships between emotions, self-efficacy, and cybersecurity awareness and how they shape protective motivation behaviour among employees of different age groups. The study results align with the existing literature that states that younger people are more likely to take proactive cybersecurity measures than older adults (Lee & Chua, 2023; Shah & Agarwal, 2020). Organisations can utilise these observations to customise cybersecurity training programmes and assist with initiatives that target the distinct emotional and cognitive requirements of employees in various age ranges.

6.3.3 Employees' Educational Level

This study categorised participants into two groups, High School/Diploma/Bachelor and Master's/PhD/Other, using the median-split method. Thus, there are 180 employees in the High School/Diploma/Bachelor group and 203 employees in the Master's/PhD/Other group. Figure 29 shows the results of the hypothesis testing regarding employees with High School/Diploma/Bachelor qualifications, whereas Figure 30 shows the results for employees with Master's/PhD/Other qualifications. The results show some differences between employees' educational levels. Employees with Master's/PhD/Other qualifications were found to have more significant relationships in the model. This suggests that employees with Master's/PhD/Other qualifications might be more influenced by factors like emotions and self-efficacy in their cybersecurity protection motivation behaviour.

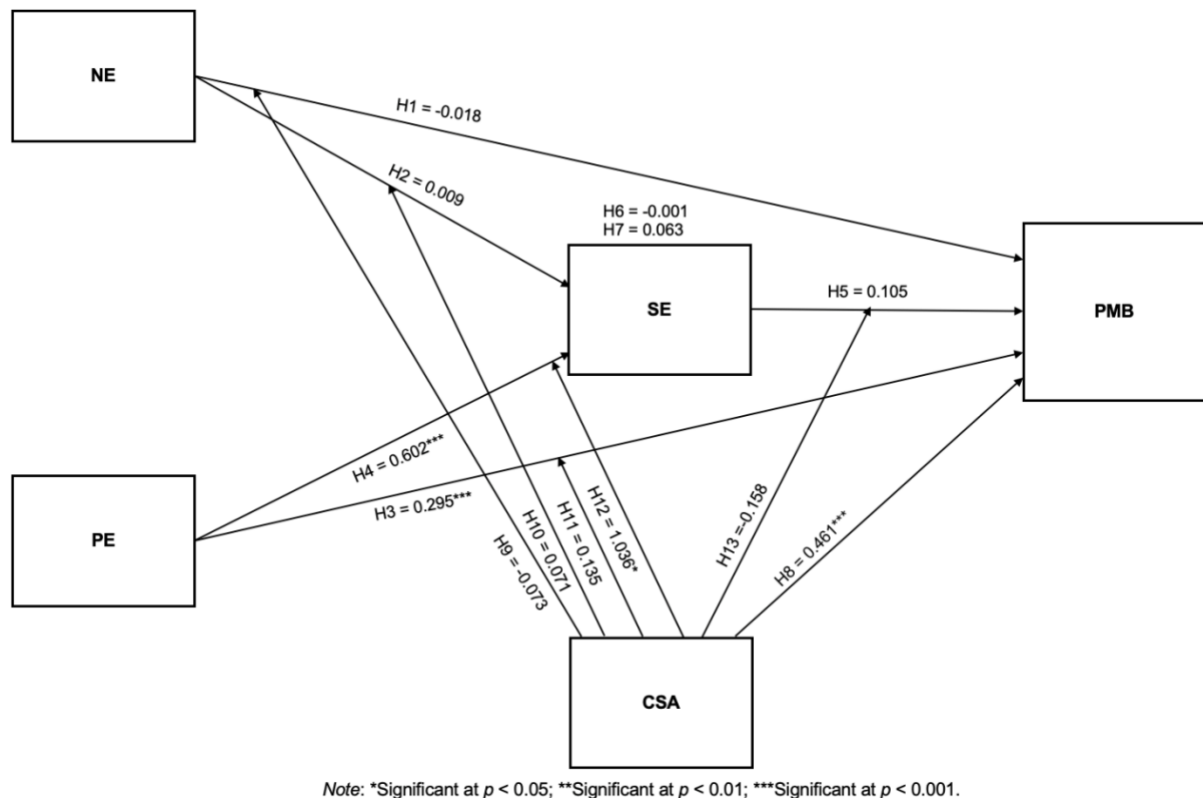


Figure 29: Model Findings for Employees with High School/Diploma/Bachelor Qualifications

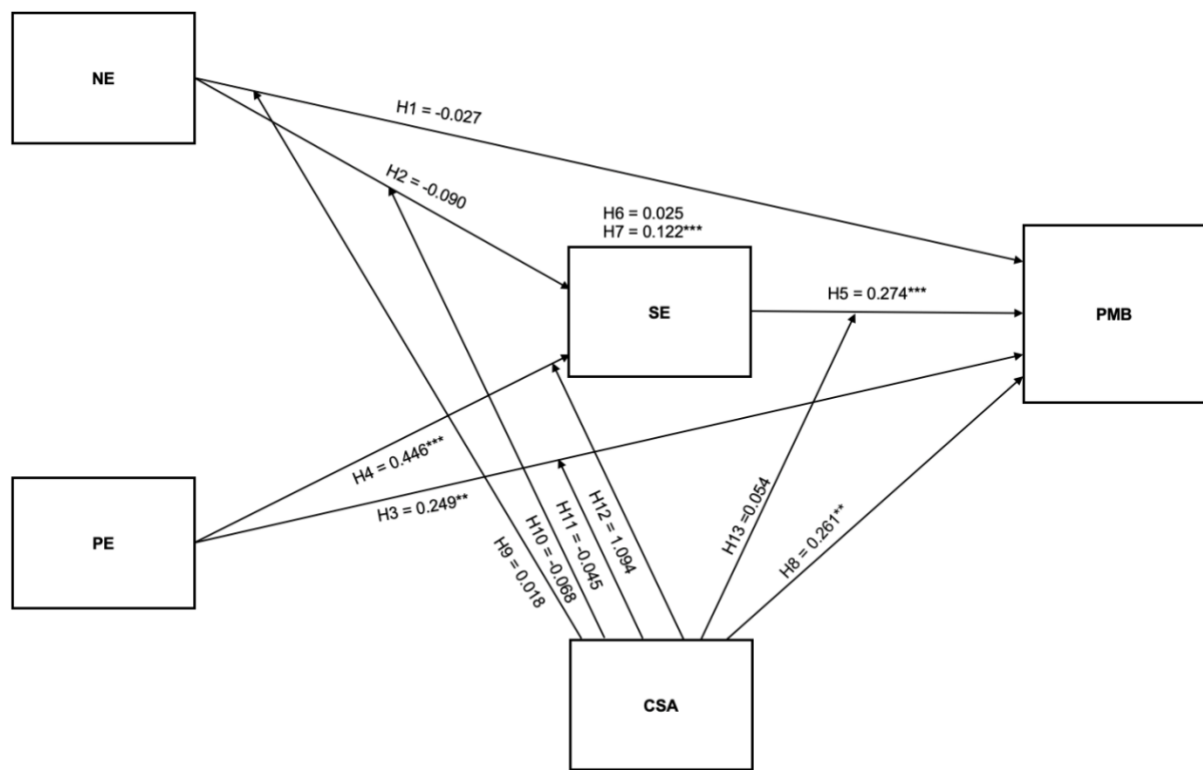


Figure 30: Model Findings for Employees with Master's/PhD/Other Qualifications

The results for **H₃** demonstrate that positive emotion has a significant positive effect on protection motivation behaviour for employees with High School/Diploma/Bachelor qualifications ($\beta = 0.295^{***}$) and Master's/PhD/Other qualifications. ($\beta = 0.249^{**}$). These results align with the original results ($\beta = 0.266^{***}$), although the significance is greater for employees with High School/Diploma/Bachelor qualifications. The findings are consistent with literature indicating that positive emotions enhance employees' motivation to engage in protective behaviours. According to the BBT, positive emotions can cause employees to think and act differently, enhancing their motivation to engage in protective behaviours. The marginal benefit perceived among employees with High School/Diploma/Bachelor qualifications might be recognised as the immediate and practical implications of positive emotions in their daily responsibilities. This implies that positive emotions can have a more direct influence on behaviour in less complex job positions.

The results for **H₄** show that positive emotion has a significant positive effect on self-efficacy for employees with High School/Diploma/Bachelor qualifications ($\beta = 0.602^{***}$) and Master's/PhD/Other qualifications ($\beta = 0.446^{***}$). These results align with the original results ($\beta = 0.545^{***}$) that positive emotions positively affect self-efficacy, although the effect is more significant for employees with High School/Diploma/Bachelor qualifications. Employees with

High School/Diploma/Bachelor qualifications may experience a larger increase in self-efficacy because of positive emotions. They might rely more on emotions to navigate job tasks than employees with Master's/PhD/Other qualifications, who may rely more on their advanced skills and knowledge.

The results for **H₅** show that self-efficacy only has a significant positive effect on protection motivation behaviour for employees with Master's/PhD/Other qualifications ($\beta = 0.274^{***}$), echoing the original results ($\beta = 0.232^{***}$). However, there is no evidence that self-efficacy promotes positive protection motivation behaviour among employees with High School/Diploma/Bachelor qualifications, as the relationship is insignificant ($\beta = 0.105$). This finding suggests that self-efficacy is a more critical determinant of protection motivation behaviour for employees with Master's/PhD/Other qualifications. This aligns with existing literature indicating that individuals with higher education levels can better translate self-efficacy into protective behaviours because of their advanced knowledge and skills (Compeau & Higgins, 1995). For employees with High School/Diploma/Bachelor qualifications, other factors besides self-efficacy might need to be focused on to enhance protection and motivation behaviour.

The results for **H₇** show that self-efficacy positively intervenes in the relationship between positive emotions and protection motivation behaviour for employees with Master's/PhD/Other qualifications ($\beta = 0.122^{***}$), which aligns with the original results ($\beta = 0.127^{***}$). However, there is no evidence to indicate that self-efficacy positively intervenes in the relationship between positive emotions and protection motivation behaviour for employees with High School/Diploma/Bachelor qualifications, as the relationship is insignificant ($\beta = 0.063$). This result indicates evidence for the PMT, which posits that self-efficacy is crucial for mediating the relationship between emotions and behaviour. Therefore, self-efficacy plays a significant role in how positive emotions can lead to performance-based motivation for employees with Master's/PhD/Other qualifications. The other group of employees might require distinct mediations to effectively enhance their emotional and cognitive resources.

The results for **H₈** show that cybersecurity awareness has a positive effect on protection motivation behaviour among employees of all educational levels. The findings suggest that having a strong understanding of cybersecurity greatly increases the likelihood of employees engaging in protective behaviours, regardless of their level of education. The impact is significant ($\beta = 0.461^{***}$) for employees who have a High School/Diploma/Bachelor qualification. This suggests that as these employees gain more information about cybersecurity challenges, their drive to safeguard themselves against cyber threats improves significantly. Likewise, there is

a notable positive impact ($\beta = 0.262^{**}$) for employees who possess Master's/PhD/Other educational credentials, but it is lower than for the previous group. This is consistent with the entire model, demonstrating a significant and statistically significant positive correlation ($\beta = 0.322^{***}$). Thus, as employees' awareness of cybersecurity develops, individuals with any level of education demonstrate an enhanced inclination towards protection motivation behaviour.

The results of H_{11} were found to be insignificant for all educational levels, which means that there is no evidence that cybersecurity awareness moderates the relationship between positive emotions and protection motivation behaviour. These results are different from the original results, which indicate that the impact of positive emotion on protective motivation behaviour is significant among employees of all levels of education ($\beta = 0.180^*$). This suggests that while cybersecurity awareness is essential, its interaction with emotional factors might not significantly influence protection motivation behaviour across different educational levels. The original assumption that higher awareness would enhance the impact of positive emotions on protection motivation behaviour may not hold, indicating the need for more complex, integrated approaches to improve cybersecurity behaviours (Pahnila et al., 2007).

The results for H_{12} show that cybersecurity has a significant positive moderation effect on the relationship between positive emotion and self-efficacy among employees with High School/Diploma/Bachelor qualifications ($\beta = 1.036^*$), which aligns with the original results ($\beta = 0.776^{***}$). However, this effect was insignificant for employees with Master's/PhD/Other qualifications ($\beta = 1.094$). This indicates that enhancing cybersecurity awareness could significantly increase positive emotions' impact on self-efficacy, but mainly for employees with High School/Diploma/Bachelor qualifications.

The results for H_{13} revealed an insignificant effect for employees of all educational levels, which means there is no evidence that cybersecurity awareness moderates the relationship between self-efficacy and protection motivation behaviour based on employees' educational level. These results are different from the original results ($\beta = -0.204^*$), which indicate that as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours decreases.

The findings highlight significant details of the impact of emotions, self-efficacy, and cybersecurity awareness on protection motivation behaviour among employees based on their levels of education. Employees with Master's/PhD/Other qualifications have more significant relationships in the model, which aligns with existing literature demonstrating that higher-

educated persons may be better able to handle cybersecurity issues (Bulgurcu et al., 2010; Fatokun et al., 2019). These findings suggest the significance of customising interventions to the employees' requirements and several educational levels to improve cybersecurity behaviours effectively. Further investigation is essential to investigate these dynamics and include additional demographic variables to develop a more thorough understanding of the factors that might motivate employees to engage in protective behaviours.

6.3.3 Employees' Work Position

The data show that there were 169 academic and 214 administrative respondents among the employees. The findings of the hypotheses testing for administrative employees are displayed in Figure 31, while the results for academic employees are displayed in Figure 32. The significant results indicate some notable distinctions between academic and administrative employees. It was found that the relationships were more statistically significant for the academic employees. This indicates that academic employees may be more susceptible to being influenced by emotions and self-efficacy regarding the motivational behaviour required for cybersecurity protection.

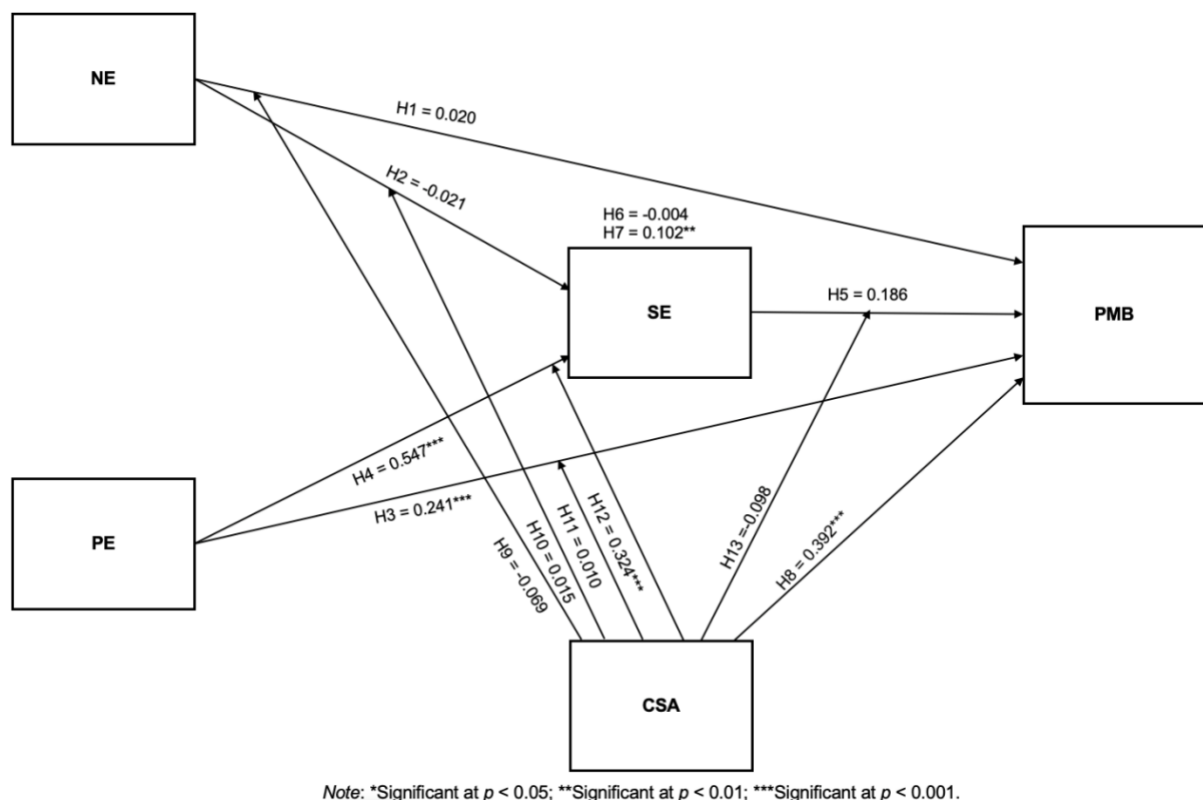


Figure 31: Model Findings for Administrative Employees

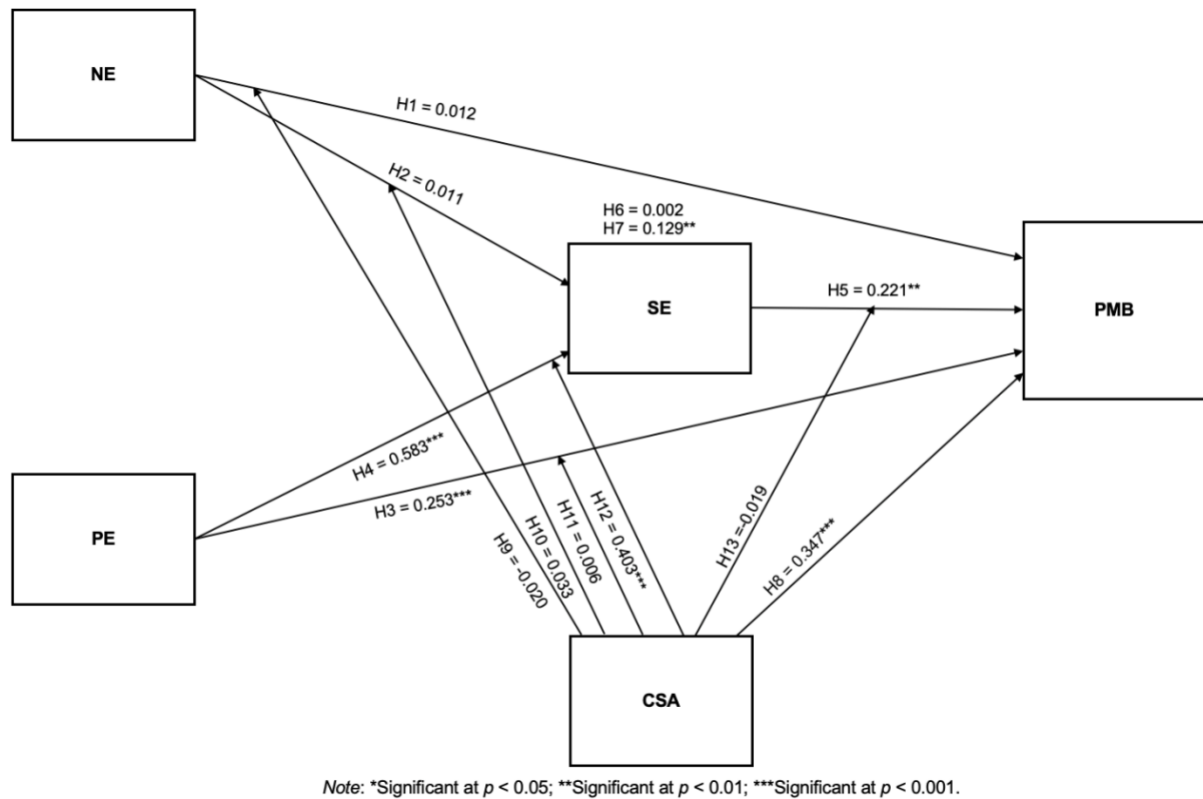


Figure 32: Model Findings for Academic Employees

The results for **H₃** demonstrate that positive emotion has a significant positive effect on protection motivation behaviour for both administrative and academic staff, although the effect is more significant for academic staff ($\beta = 0.253^{***}$) than for administrative employees ($\beta = 0.241^{***}$). This result aligns with the original result ($\beta = 0.266^{***}$). The influence of positive emotion on protection motive behaviour for administrative and academic employees is consistent with the PMT. This suggests that positive emotions improve one's belief in one's ability to achieve goals, increasing one's drive to participate in behaviours that safeguard one's well-being (Floyd et al., 2000). Moreover, the BBT suggests that positive emotions enhance cognitive and behavioural capabilities, particularly in roles that demand higher levels of cognitive involvement, such as academia (Fredrickson, 2001).

The results for **H₄** demonstrate that positive emotion has a significant positive influence on self-efficacy for both administrative and academic personnel. The effect is more significant for academic employees ($\beta = 0.583^{***}$) than for administrative staff ($\beta = 0.547^{***}$). This result aligns with the original result ($\beta = 0.545^{***}$). Therefore, positive emotion has a beneficial influence on both groups' self-efficacy, which aligns with the self-efficacy theory—this posits that positive emotions increase individuals' confidence in their capacity to carry out behaviours required to achieve particular outcomes (Bandura, 1977). This may be because the academic

job is more independent and intellectually demanding. This allows for a better utilisation of positive emotions to enhance self-efficacy.

The results for **H₅** show that self-efficacy has a significant positive effect on protection motivation behaviour, but only for academic employees ($\beta = 0.221^{***}$). This latter result aligns with the original model ($\beta = 0.232^{***}$). However, there is no evidence that self-efficacy promotes a positive protection motivation behaviour among administrative employees, as the relationship is insignificant ($\beta = 0.186$). This difference might be due to the contrasting job characteristics and the level of autonomy in the two positions. Academic employees are regularly required to independently handle their cybersecurity practices, making self-efficacy a vital element. Administrative employees might place more emphasis on organisational policies and less on individual self-efficacy. Ifinedo (2012) emphasises the importance of self-efficacy in driving proactive security behaviours, especially in occupations that include independent action and decision making, such as academic positions.

The results for **H₇** show that self-efficacy positively mediates the relationship between positive emotions and protection motivation behaviour for both academic and administrative employees, which aligns with the original model. The effect is more significant for academic ($\beta = 0.129^{***}$) than administrative personnel ($\beta = 0.102^{**}$). This aligns with the original result ($\beta = 0.127^{***}$). The mediating role of self-efficacy suggests that improving employees' self-assurance in their ability to engage in protective behaviours is vital for converting positive emotions into tangible protective behaviour. The impact is mainly evident in academic environments, which rely more on personal advantage and self-regulation. Pahnla et al. (2007) stated that self-efficacy is crucial for changing motivational features into actions in positions that require personal responsibility and proactivity.

The result for **H₈** shows that cybersecurity awareness has a positive effect on protection motivation behaviour among academic and administrative staff. The findings suggest that both groups of employees improve their protection motivation behaviour when they strongly understand cybersecurity. The influence on administrative employees is significant ($\beta = 0.392^{***}$), suggesting that as their understanding of cybersecurity matters improves, their inclination to safeguard themselves against cyber risks increases significantly. Similarly, academic employees also experience a positive influence ($\beta = 0.347^{***}$), but on a lesser scale than the administrative group. This is consistent with the overall model, which indicates a strong positive correlation ($\beta = 0.322^{***}$).

The findings related to **H₁₁** were insignificant for both academic and administrative employees, which means there is no evidence that cybersecurity awareness moderates the relationship between positive emotions and employees' protection motivation behaviours. This indicates that the central purpose of cybersecurity awareness may lay in developing self-efficacy rather than directly influencing protective behaviours once self-efficacy has been achieved. This result differs from the original result ($\beta = 0.180^*$).

The findings related to **H₁₂** show that cybersecurity awareness has a significant positive moderation effect on the relationship between positive emotion and self-efficacy. This effect is more significant for academic ($\beta = 0.403^{***}$) than administrative staff ($\beta = 0.324^{***}$). The overall result aligns with the original model ($\beta = 0.776^{***}$). This suggests the need to be more aware of cybersecurity in order to improve the valuable impacts of emotions on self-efficacy. The relationship is more beneficial for academic employees, most likely because of the nature of their roles, which require higher levels of self-directed learning and information application. The significant impact of moderation on academic employees suggests that modified awareness programmes could significantly enhance their self-efficacy.

Regarding **H₁₃**, the findings revealed insignificant relationships for both academic and administrative employees, which means there is no evidence that cybersecurity awareness moderates the relationship between self-efficacy and protection motivation behaviour among academic and administrative employees. These results differ from the original results ($\beta = -0.204^*$), which indicates that as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours decreases.

The results provide valuable understanding of the problematic relationship between psychological characteristics and cybersecurity behaviour among academic and administrative employees. The more statistically significant links in the model for academic employees indicate a potentially higher vulnerability to factors such as emotions and self-efficacy influencing their cybersecurity protective behaviours. However, the lack of evidence demonstrating specific relationships amongst administrative employees calls into doubt the suitability of motivating frameworks in various organisational settings. Moreover, the differences between the present findings and the initial results emphasise the ever-changing nature of cybersecurity behaviours and the requirement for continuous research to improve our understanding and approaches for supporting efficient cybersecurity practices within organisations.

6.3.4 Employees' Years of Experience

Using the median-split method, this study categorised employees' years of experience into two groups: less than 10 years and more than 10 years. With this split, 224 employees had less than 10 years of experience, and 159 employees had more than 10 years of experience. Figure 33 shows the results of the hypothesis testing regarding employees with 10 or fewer years of experience, whereas Figure 34 shows the results for employees with 10+ years of experience. The statistically significant results show little difference between the results based on employees' years of experience. Both groups' paths were found to have the same statistically significant relationships in the model. However, slightly stronger relationships were observed for employees with 10+ years of experience.

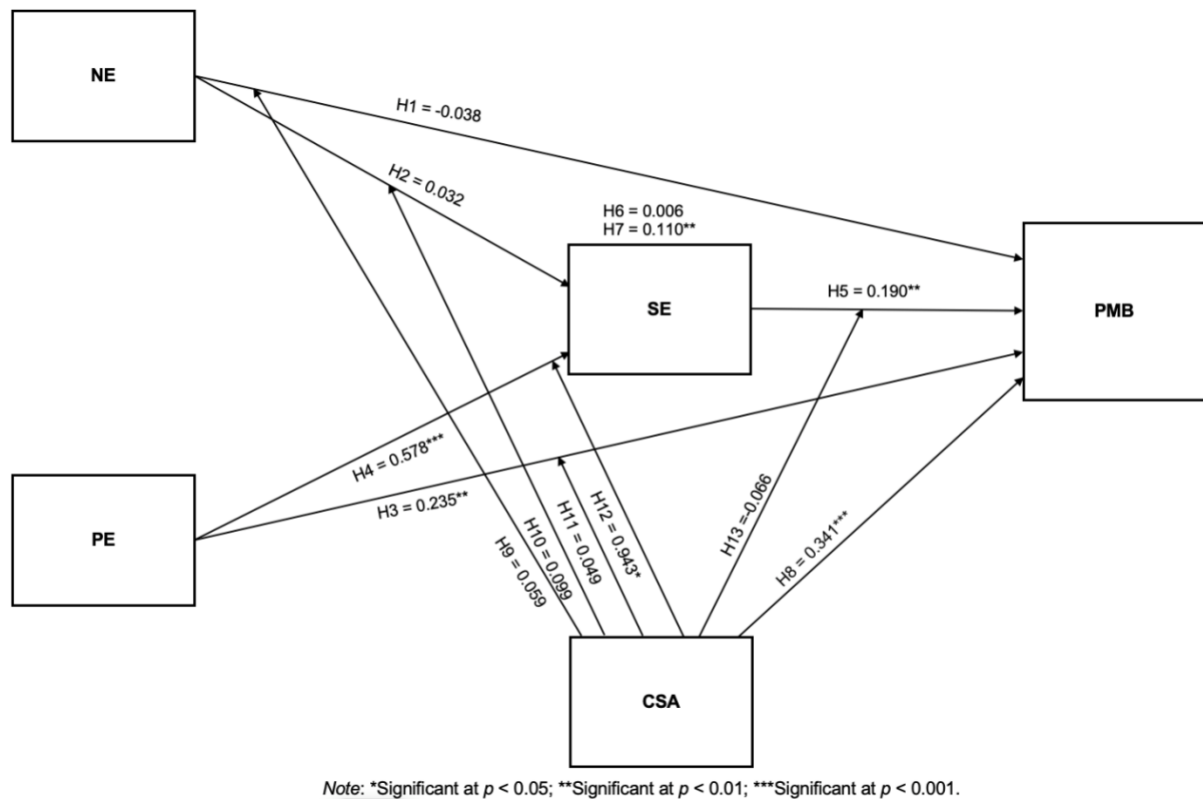
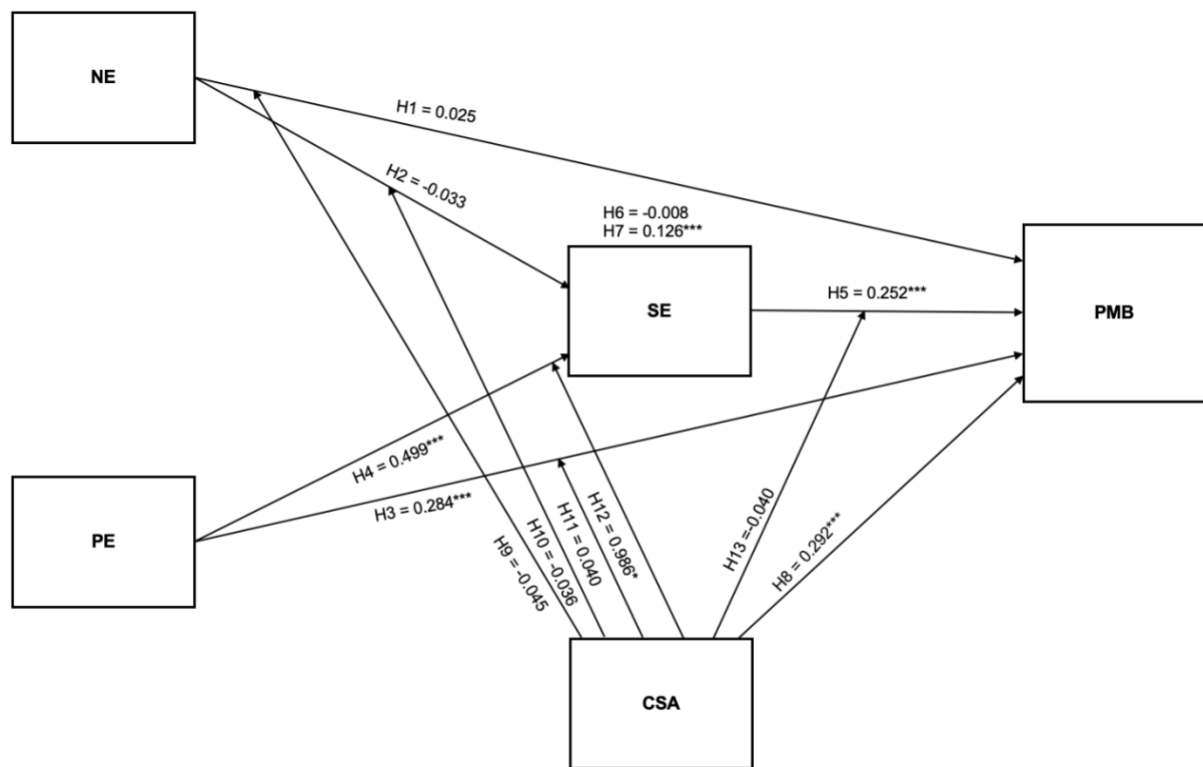


Figure 33: Model Findings for Employees with Less than 10 Years of Experience



Note: *Significant at $p < 0.05$; **Significant at $p < 0.01$; ***Significant at $p < 0.001$.

Figure 34: Model Findings for Employees with More than 10 Years of Experience

The results for **H₃** demonstrate that positive emotion has a significant positive effect on protection motivation behaviour for employees with 10 or fewer and 10+ years of experience. However, the effect is more significant for employees with 10+ years of experience ($\beta = 0.284^{***}$) than for those with 10 or fewer years of experience ($\beta = 0.235^{**}$). This result aligns with the original result ($\beta = 0.266^{***}$). Therefore, employees with more experience are more adept at utilising positive emotions because they better understand organisational processes and security protocols. Additionally, they are more likely to have encountered security concerns. The BBT states that positive emotions increase an individual's awareness and promote new, diverse, and adventurous ideas and activities (Fredrickson, 2001). Employees with 10+ years of experience are more likely to convert their improved cognitive abilities into preventive actions.

The results for **H₄** demonstrate that positive emotion has a significant positive influence on self-efficacy for employees with 10 or fewer and 10+ years of experience. However, the effect is more significant for employees with 10 or fewer years of experience ($\beta = 0.578^{***}$) than for those with 10+ years of experience ($\beta = 0.499^{***}$). The significant positive effect aligns with the original result ($\beta = 0.545^{***}$). This could be attributed to the fact that less-experienced employees are in a developmental phase of their professional journey, during which positive

emotions play an essential role in raising confidence and self-assurance. Bandura et al. (1999) highlight the influence of positive emotions on enhancing self-efficacy, as they help them to overcome initial obstacles and uncertainties in their roles.

Regarding **H₅**, the results show that self-efficacy has a significant positive effect on protection motivation behaviour for both employees with 10 or fewer and 10+ years of experience, with a more significant influence for employees with 10+ years of experience ($\beta = 0.252^{***}$) than for employees with 10 or fewer years of experience ($\beta = 0.190^{**}$). This result aligns with the original result ($\beta = 0.232^{***}$). Therefore, employees with more experience can better interpret their belief in their abilities into concrete protective actions since they are knowledgeable about procedures and possible threats. Rogers (1983) stated that individuals with higher levels of self-efficacy are more likely to engage in actions that promote their protection. The increased effect on employees with 10+ years of experience can be attributed to their deep understanding of organisational risks and their confidence in handling them.

The results for **H₇** show that self-efficacy positively mediates the relationship between positive emotions and protection motivation behaviour among employees, regardless of their years of experience. However, the effect is more significant for employees with 10+ years of experience ($\beta = 0.126^{***}$) than for those with 10 or fewer years of experience ($\beta = 0.110^{**}$). This mediation result aligns with the original result ($\beta = 0.127^{***}$). Researchers of organisational behaviour have studied the significant role of self-efficacy as a mediator. Stajkovic and Luthans (1998) highlight the significance of self-efficacy in linking positive psychological capital with performance. Therefore, employees with more years of experience are more likely to possess a higher level of self-efficacy due to their accumulated knowledge and confidence.

Regarding **H₈**, the results show that cybersecurity awareness has a positive effect on protection motivation behaviour among all employees, whatever their level of experience. The findings suggest that employees' protective motivation behaviour is greatly improved by cybersecurity awareness, regardless of their level of work experience. The impact is significant ($\beta = 0.341^{***}$) for employees who have worked for 10 years or less. This suggests that as these employees gain more understanding of cybersecurity matters, their need to safeguard themselves from cyber risks significantly intensifies. Likewise, there is a statistically significant positive impact ($\beta = 0.292^{***}$) for employees with more than 10 years of experience, although it is less significant than for the group with less experience. This is consistent with the overall model, which indicates a strong positive relationship ($\beta = 0.322^{***}$). Thus, as employees' awareness of cybersecurity develops, individuals with different degrees of work experience have an enhanced inclination towards protection motivation behaviour.

The results for **H₁₁** found an insignificant effect for all employees regardless of their years of experience. There is therefore no evidence that cybersecurity awareness moderates the direct relationship between positive emotions and employees' protection motivation behaviours. This indicates that the central purpose of cybersecurity awareness may lay in developing self-efficacy rather than directly influencing protective behaviours once self-efficacy has been achieved. This result differs from the original result ($\beta = 0.180^*$), which indicated that cybersecurity awareness moderates the direct relationship between positive emotions and employees' protection motivation behaviours.

The results for **H₁₂** show that cybersecurity awareness has a significant positive moderation effect on the relationship between positive emotion and self-efficacy. This effect is more significant for employees with 10+ years of experience ($\beta = 0.986^*$) than for employees with 10 or fewer years of experience ($\beta = 0.943^*$). The moderation result aligns with the original result ($\beta = 0.776^{***}$). This highlights the necessity of improving cybersecurity awareness to improve the valuable effects of positive emotions on self-efficacy.

The results for **H₁₃** showed an insignificant effect for all employees, regardless of their years of experience. This means that there is no evidence that cybersecurity awareness moderates the relationship between self-efficacy and protection motivation behaviour among employees. These results differ from the original results ($\beta = -0.204^*$), which indicate that as cybersecurity awareness increases, the strength of the relationship between self-efficacy and protection motivation behaviours decreases.

The findings show that there are similarities in the influences between psychological characteristics and cybersecurity behaviour among employees with varying levels of experience, but there are also significant distinctions. Employees with more than 10 years of experience are impacted more, suggesting a possible cumulative effect of the term on cybersecurity views. These refined distinctions have consequences for the measures taken by organisations to protect their cybersecurity. Customised interventions may be necessary to satisfy the various needs of employees with differing degrees of expertise. Training programmes could be personalised to enhance self-efficacy and positive emotions for less-experienced employees, emphasising higher cybersecurity knowledge for more skilled employees. Moreover, the difference between these and the original results emphasises the need to research specific contexts and continually evaluate and improve strategies in response to changing dynamics within organisations and employee demographics.

6.4 Summary

This chapter presented the findings related to answering the research questions. The chapter comprised two sections. The first section discussed the answers to the first, second, and third research questions, which examine the direct relationship between negative and positive emotions and employees' protection motivation behaviour and self-efficacy. It also discussed the relationship between self-efficacy and employees' protection motivation behaviour and the mediating role of self-efficacy in the relationship between negative and positive emotions and employees' protection motivation behaviour. It clarified the relationship between cybersecurity awareness and protection motivation behaviour among employees, as well as the relationship between cybersecurity awareness and protection motivation behaviour. In addition, the results were discussed regarding the moderating role of employees' cybersecurity awareness in the relationship between negative and positive emotions and employees' protection motivation behaviour; the relationship between negative and positive emotions and employees' self-efficacy; and the relationship between self-efficacy and protection motivation behaviour. This first section presented an analysis of the results obtained from testing the 13 hypotheses, and compared these to the extant literature. Providing explanations for the acceptance and rejection of the direct links in the structural model clarified the influence of the independent, mediation, and moderation factors on the dependent variable. The second section discussed employee differences by their demographic characteristics.

The next chapter represents the conclusion of this study. It begins with discussing how the research questions, aims, and objectives have been answered and addressed. It examines the research conducted and highlights the main findings and their consequences. It discusses the contributions made by this research, both in terms of theories and methodology. It acknowledges any limitations encountered. Finally, it provides guidance for future research endeavours.

Chapter Seven: Conclusion

7.1 Introduction

This chapter offers a summary of the research's main findings. It starts by addressing the research questions, aim, and objectives, followed by an exploration of the practical implications. The chapter further offers the research's practical implications and discusses the contributions to theories and methodology. In addition, limitations are listed, followed by future research.

7.2 Addressing Research Questions, Aim and Objectives

This thesis explores the influences of employees' emotions on their cybersecurity protection motivation behaviour. The research questions, aim and objectives have been accomplished, which include:

1. Review the existing literature to provide evidence that supports the identified gap. Conduct a broad investigation of the existing literature on the influence of emotions on cybersecurity protection motivation behaviour. The investigation will have a wide scope, including the literature on emotions and the behavioural motivation for cybersecurity protection.

In Chapter 2, the literature review identified the role of emotions in influencing employees' cybersecurity protection motivation behaviour in organisations. This was achieved by conducting a systematic literature review published by Alshammari et al. (2023) to identify the existing research gap. This review formed the foundation for understanding how emotions influence employees' motivation to engage in cybersecurity protective behaviours and their self-efficacy.

2. Develop a proposed theoretical framework that includes the influence of negative and positive emotions on employees' cybersecurity protection motivation behaviour and self-efficacy; the role of self-efficacy as a mediating variable; and the influence of cybersecurity awareness on employees' cybersecurity protection motivation behaviour; cybersecurity awareness as a moderator variable in the relationship between negative and positive emotions and employees' protection motivation behaviour, in the relationship between negative and positive emotions and employees' self-efficacy, and in the relationship between self-efficacy and protection motivation behaviour.

In Chapter 3, based on the systematic literature review findings, this study established a model and developed hypotheses based on two popular theories: BBT and PMT (Alshammari et al., 2024). These theories helped to explore the influence of negative and positive emotions on employees' cybersecurity protection motivation behaviour and self-efficacy. Moreover, self-efficacy was identified as a mediator between negative and positive emotions and employees' cybersecurity protection motivation behaviour. Furthermore, cybersecurity awareness was recognised as a moderator variable in the relationship between negative and positive emotions and employees' protection motivation behaviour, between negative and positive emotions and employees' self-efficacy, and between self-efficacy and protection motivation behaviour.

3. To identify an appropriate measurement scale for negative and positive emotions, self-efficacy, cybersecurity awareness, and cybersecurity protection motivation behaviour.

In Chapter 4, to accomplish the goal of identifying suitable measurement scales for analysing negative and positive emotions, self-efficacy, cybersecurity awareness, and cybersecurity protection motivation behaviour, the researcher carried out extensive literature research and assessed multiple existing scales. The priority was selecting scales with high validity, reliability, and relevance. The scales undertook evaluation and pilot testing with a sample population of 64 employees from King Abdulaziz University to verify their appropriateness. After considering the feedback and testing the results, the researcher improved the scales and incorporated them into the framework for gathering and analysing data. This process established a solid basis for precisely evaluating the influence of employees' emotions on their motivation to defend cybersecurity.

4. Conduct empirical testing to confirm and identify whether negative and/or positive emotions affect employees' cybersecurity motivation behaviours and self-efficacy. This validation enables the researcher to address the first study question (**RQ1**).

In Chapter 5, the findings showed that negative emotions did not influence employee protection motivation behaviour as the relationship was insignificant. Moreover, the influence of negative emotions on self-efficacy was insignificant. There was therefore no evidence that negative emotions affected employees' protection motivation behaviour or self-efficacy. However, positive emotions had a significant positive effect on employees' protection and motivation behaviour. Additionally, positive emotions had a significant positive influence on

employees' self-efficacy. This finding suggests that positive emotions benefit employees who engage in protective behaviour in cybersecurity. Moreover, it suggests that positive emotions enhance employees' self-efficacy, indicating that people who experience positive emotions are more likely to possess the necessary skills to effectively engage in tasks such as cybersecurity.

5. Conduct empirical testing to explore how self-efficacy may contribute to cybersecurity protective motivation behaviours by mediating the effects of negative and positive emotions. This answers the second research question (**RQ2**).

In Chapter 5, the results reveal that self-efficacy significantly affects employees' protection motivation behaviour. However, self-efficacy does not significantly mediate the relationship between negative emotions and employees' protection motivation behaviours. However, self-efficacy significantly mediated the relationship between positive emotions and employees' protection motivation behaviours. This means that higher levels of self-efficacy lead to more effective utilisation of positive emotions, resulting in increased motivation and engagement in protective behaviours.

6. Conduct empirical testing to examine the relationship between cybersecurity awareness and employees' cybersecurity protection motivation behaviour and how cybersecurity awareness could moderate the relationship between negative and positive emotions and employees' protection motivation behaviour, the relationship between negative and positive emotions and employees' self-efficacy, and the relationship between self-efficacy and protection motivation behaviour. This will answer the third research question. This answers the third research question (**RQ3**).

In Chapter 5, the results show that cybersecurity awareness positively affects employees' motivation to protect their cybersecurity. Regarding the moderation effect of cybersecurity awareness, it was found that it did not moderate the relationship between negative emotions and employees' protection motivation behaviour and self-efficacy. However, cybersecurity awareness positively and significantly moderated the relationship between positive emotions and employees' protection motivation behaviour and self-efficacy. Finally, cybersecurity awareness significantly and negatively moderated the relationship between self-efficacy and employee protection motivation.

7. Analyse the similarities and differences in the research model among employees, considering their demographic attributes. This contrast is crucial for addressing the fourth research question (**RQ4**).

Chapter 5 presented several significant results regarding employee differences based on demographic characteristics. Female employees demonstrated more statistically significant relationships in the model than male employees. Age was an additional crucial variable, as younger employees had higher statistically significant relationships in the model. The educational level also had an influence, as these characteristics influenced employees who held Master's, PhD, or other degrees. Regarding the employees' work position, it was found that academic employees showed more significant relationships in the model. With regard to years of experience, both groups of employees displayed similar statistically significant correlations. However, the beta coefficient was higher for those with more than ten years of experience.

7.3 Research Overview and Key Findings

The research explored the influence of emotions on employees' cybersecurity protection motivation behaviour and self-efficacy. The study proposed thirteen hypotheses about the influence of negative and positive emotions on employees' cybersecurity protection motivation behaviour and self-efficacy. In addition, it examined the mediating role of self-efficacy in the relationship between emotions and employees' cybersecurity protection motivation behaviour. It also investigated the influence of cybersecurity awareness on employee's protection motivation behaviour and the moderating effect of cybersecurity awareness on the relationship between negative and positive emotions and employees' protection motivation behaviour, the relationship between negative and positive emotions and employees' self-efficacy, and the relationship between self-efficacy and protection motivation behaviour. Finally, the study examined the extent to which the influence of negative and positive emotions, self-efficacy, and cybersecurity awareness on protection motivation behaviour differed between employees based on their demographic characteristics of gender, age, level of education, work position, and years of experience.

The results for **H₁** indicated that negative emotions did not motivate employees to engage in protective behaviours. Similarly, **H₂** posited that negative emotions do not negatively influence self-efficacy. However, the results for **H₃** showed that positive emotions positively influenced protection motivation behaviour, demonstrating that the employees were motivated to engage in protection behaviour in cybersecurity. Furthermore, the findings for **H₄** revealed that positive

emotions positively influenced self-efficacy, indicating that positive emotions encouraged employees' beliefs in their ability to efficiently and effectively engage in protective tasks.

The results for **H₅** showed that self-efficacy promoted positive employee protection motivation behaviour, suggesting that employees with higher self-efficacy tended to engage in protection motivation behaviour. The findings for **H₆** revealed that self-efficacy did not mediate the relationship between negative emotions and employees' protection motivation behaviour, suggesting that self-efficacy cannot significantly mediate this relationship. However, **H₇** indicated that self-efficacy did mediate the relationship between positive emotions and employees' protection motivation behaviours, indicating that higher levels of self-efficacy enhance the positive influence of positive emotions on protection motivation behaviour.

Regarding **H₈**, the results showed that cybersecurity awareness positively influenced the relationship between protection motivation behaviours and cybersecurity awareness, suggesting that employees' cybersecurity awareness increases their motivation to engage in protection behaviour. The findings for **H₉** revealed that cybersecurity awareness did not moderate the direct relationship between negative emotions and protection motivation behaviour in cybersecurity. Moreover, the analysis for **H₁₀** showed that cybersecurity awareness did not moderate the relationship between negative emotions and self-efficacy. This means that regarding **H₉** and **H₁₀**, there is no evidence that cybersecurity awareness moderates the relationship between negative emotions and employee protection motivation or self-efficacy. However, **H₁₁** showed that cybersecurity awareness can moderate the direct relationship between positive emotions and employees' protection motivation behaviours, indicating that for employees with high cybersecurity awareness, the relationship between positive emotions and employees' protection motivation behaviours will be strong. Moreover, the analysis for **H₁₂** revealed that cybersecurity awareness moderated the relationship between positive emotions and self-efficacy, indicating that when employees had high cybersecurity awareness, their positive emotions positively influenced their self-efficacy. The findings for **H₁₃** showed that cybersecurity awareness moderated the relationship between self-efficacy and employees' protection motivation behaviours. However, cybersecurity awareness negatively moderated this relationship, suggesting that as employees become more aware of cybersecurity, the strength of the relationship between their self-belief in their ability to defend themselves and their willingness to take protective actions reduces.

Several key findings emerged regarding employee differences based on their demographic profiles. Regarding gender, the results revealed the significant effects of positive emotions on protection motivation behaviour and self-efficacy for both genders, although more for females

than males. Additionally, self-efficacy played a significant role for both genders in translating positive emotions into action; the relationship is more vital for females than males. Moreover, self-efficacy positively influences protection motivation behaviour, but more significantly for females than for males. Self-efficacy significantly mediates the relationship between positive emotions and protection motivation behaviour, with the effect being more significant for males. Cybersecurity awareness significantly affects protection motivation behaviour for both genders, but the effect is stronger for males. Moreover, cybersecurity awareness significantly moderated the relationships between positive emotions and protection motivation behaviour and self-efficacy, more significantly for females. These findings suggest that promoting a positive cybersecurity mindset is essential for employees, but focusing on building self-efficacy might be especially valuable for improving female employees' cybersecurity behaviours.

Regarding age, it was found that positive emotions positively affected both age groups, although the effect was more significant for older employees. Self-efficacy positively impacted the motivation behaviour of younger and older employees for cybersecurity protection. However, self-efficacy did not mediate the relationship between positive emotions and protection motivation behaviour among older employees. Furthermore, cybersecurity awareness significantly influenced younger employees' protection and motivation behaviour. It also moderated the relationship between positive emotions and self-efficacy, with this effect being more significant for younger employees.

Looking at the level of education, it was found that positive emotions positively influenced all participants regardless of their level of education in terms of both protection motivation behaviour and self-efficacy. For employees with Master's/PhD/Other qualifications, self-efficacy mediated the effect of positive emotions on protection behaviour. Furthermore, cybersecurity awareness significantly influenced both groups' protection and motivation behaviour. Moreover, cybersecurity awareness positively moderated the relationship between positive emotions and self-efficacy for all employees, whatever their level of education.

Regarding the employees' role at work, it was found that positive emotions positively influenced protection motivation and self-efficacy for both academics and administrative employees, with the influence being stronger on academics regarding protection motivation and self-efficacy. Self-efficacy positively influenced employees' protection motivation behaviour, but only for academic employees. However, self-efficacy mediated the relationship between positive employee protection and motivation behaviour. Furthermore, cybersecurity awareness positively influenced both employee groups' protection and motivation behaviour.

Moreover, cybersecurity awareness did not moderate the direct relationship between positive emotions and protection motivation behaviour, but it moderated the relationship between positive emotions and self-efficacy for both sets of employees.

Regarding years of experience, it was found that positive emotions positively influenced employees to take security protection motivation behaviour, and the effect was more significant for those with 10+ years of experience. The influence of positive emotions on self-efficacy was found to be significant for employees and was more significant for those with less than 10 years of experience. Self-efficacy significantly mediated the relationship between positive emotions and employee protection motivation behaviour, being more significant for those with 10+ years of experience. Furthermore, cybersecurity awareness significantly influenced employees' protection and motivation behaviour. It did not directly influence protection motivation behaviour but moderated the relationship between positive emotions and self-efficacy for both groups of employees.

Overall, the research contributes a deeper understanding of how emotions influence employees' self-efficacy and cybersecurity protection motivation behaviour. The findings also emphasise the importance of positive emotions within organisational settings to improve protection motivation behaviour and self-efficacy in cybersecurity efforts. The research emphasises the role of self-efficacy in promoting protection motivation behaviour and outlines the importance of promoting positive emotions and self-efficacy within organisations to improve cybersecurity practices. The mediating effect of self-efficacy on the relationship between protection motivation behaviour and negative emotions was insignificant. This indicates that organisations must consider multidimensional strategies, including regulating emotions to support employees in their cybersecurity efforts.

Cybersecurity is a significant concern for organisations worldwide in today's digitally growing era. Self-efficacy and cybersecurity awareness can influence employees' protection and motivation behaviour. The hypotheses and statistical analyses explored in this research can provide insights into the complex relationship between protection motivation behaviour, self-efficacy, awareness, and emotions, highlighting the importance of cybersecurity awareness programmes in promoting a resilient and security-conscious workforce.

7.4 Research Contributions and Practical Implications

This research enhances theoretical understanding and provides decision makers with practical recommendations on the influence of emotions on employees' motivation to engage in cybersecurity protection within higher education institutions.

7.4.1 Contribution to Theories

This study enhances both the BBT and PMT, offering significant implications for future researchers. Future studies may utilise the proposed framework to explore the influence of emotions on employees' cybersecurity protection motivation behaviour within the higher education sector across different contexts. The proposed model explores the influence of emotions on employees' self-efficacy and protection motivation behaviour in cybersecurity. This model also explores how self-efficacy may contribute to cybersecurity protective motivation behaviours by mediating the effects of negative and positive emotions. Moreover, this model also considers the moderating influence of cybersecurity awareness on the relationship between negative and positive emotions and employees' protection motivation behaviour, negative and positive emotions and employees' self-efficacy, and between self-efficacy and protection motivation behaviour. Hence, the proposed model could be used by future researchers to investigate how emotions, both negative and positive, and self-efficacy interact with cybersecurity awareness in various disciplines.

In addition, this study contributes to confirming previous contradictory findings. It also adds new knowledge by empirically establishing relationships related to the influence of emotions on cybersecurity protection motivation behaviour. This contributes to establishing a potential connection between BBT and PMT. This study further enhances the field of BBT and PMT by demonstrating the mediating function of self-efficacy in the relationship between positive emotions and protection-motivated behaviours. The findings on the role of self-efficacy in mediating the relationship between positive emotions and employees' cybersecurity protection motivation behaviour confirms the use of positive emotions in cybersecurity. It enhances the connections between PMT elements by merging PMT and BBT. Moreover, this study validates the significance of cybersecurity awareness in moderating the relationships between employees' negative and positive emotions and protection motivation behaviour as well as self-efficacy. Additionally, it validates the importance of cybersecurity awareness in moderating the relationships between employees' self-efficacy and protection motivation behaviours. This demonstrates that combining emotions with awareness can influence cybersecurity behaviour. Such insights call for an expanded BBT and PMT view, where awareness and emotional valence are interactive factors instead of isolated determinants. These results complement existing studies on cybersecurity by highlighting the importance of cybersecurity awareness. Therefore, this study extends the work of previous researchers by exploring the moderating effect of cybersecurity awareness. Thus, this study advances the theories by extending both BBT and PMT.

This thesis provides significant theoretical insights into the field of cybersecurity protection motivation behaviour by exploring the influence of employee demographic factors (gender, age, education level, job position, and years of experience) on negative and positive emotions, self-efficacy, cybersecurity awareness, and cybersecurity protection motivation behaviour. By including a wide range of demographic characteristics, this study expands upon previous research, contributing to the relevance of PMT and BBT theories by introducing demographic sensitivity. Understanding demographic differences is crucial for building effective and inclusive cybersecurity policies and training programmes in Saudi Arabia, where efforts like Vision 2030 prioritise the integration of advanced cyberinfrastructure. The findings of this research can assist educational decision makers and business policymakers in designing their cybersecurity plans to more effectively target the distinct requirements and vulnerabilities of various demographic groups. For example, implementing customised policies could improve the level of confidence in cybersecurity among older employees or leverage the flexibility and technological expertise of younger employees. Thus, this study has expanded upon the research conducted by earlier scholars by quantifying the differences among employees according to the demographic characteristics of gender, age, educational level, work position, and years of work experience.

Finally, this thesis makes a significant methodological contribution by developing and validating a novel survey instrument. This study utilised survey items sourced from multiple disciplines and adapted them to align with the specific cultural context of Saudi Arabia. Furthermore, this research expands the body of knowledge by incorporating six additional positive emotion items into the scale: interested, strong, active, determined, alert, and proud. The survey underwent multiple validation processes, including face validity with four academic experts, a pilot study involving 64 employees, and a full-scale study with 383 employees. The survey items demonstrated satisfactory levels of indicator reliability, construct reliability, convergent validity, and discriminant validity. Additionally, the instrument was translated into Arabic, the primary language of the target population. As a result, two versions of the instrument exist, one in Arabic and one in English, allowing for broader applicability in future research (see Appendices A and B). Thus, future studies can replicate and validate the survey across diverse cultural contexts.

7.4.2 Practical Implications

The research findings offer several practical implications to organisations seeking to improve their cybersecurity practices by enhancing employees' behaviours. By understanding the role of emotions, self-efficacy, and cybersecurity awareness, organisations can create practical approaches to promote and adopt protective behaviours among employees.

The finding that negative emotions have no significant influence on employees' protection motivation behaviour or self-efficacy reveals important implications for organisational management and the approach to employee well-being. This implies that negative emotions may not directly undermine an employee's motivation to participate in protective actions or their confidence in their ability to carry out activities effectively related to cybersecurity. This suggests that employees may be resilient enough to fulfil their professional responsibilities while experiencing negative emotions. Organisations can enhance and reinforce this resilience by offering resources such as mental health assistance, stress management courses, and resilience training. These activities can assist employees in efficiently managing negative emotions and prevent them from affecting their work performance.

Moreover, the finding that negative emotions do not significantly influence self-efficacy or protection motivation suggests that factors like organisational culture, support systems, and job satisfaction play a more crucial role. This emphasises the importance of an approach to employee well-being beyond managing negative emotions. Therefore, organisations must invest in creating a supportive work environment that encourages transparent communication and mutual assistance among employees. Such a culture can effectively mitigate the potential disruptive effects of negative emotions on job productivity. Moreover, this understanding could help organisations avoid placing excessive importance on overpowering negative emotions while neglecting to address underlying issues such as job dissatisfaction or interpersonal conflict. Instead, creating a conducive environment that promotes the healthy expression and control of various emotions may be more advantageous. This method supports emotional well-being and sustains consistent levels of motivation and effectiveness among employees, which are essential for achieving organisational objectives, particularly in vital areas such as cybersecurity.

The research findings indicate that positive emotions significantly and positively influence employees' protection, motivation behaviour, and self-efficacy. These findings have crucial practical implications for how organisations are managed and the culture they promote. The research indicates a relationship between positive emotions and protective motivation behaviour. This implies that employees with positive emotions are more inclined to take proactive measures to ensure cybersecurity. Therefore, promoting a positive work environment could increase employees' motivation to comply with cybersecurity regulations and practices. Organisations might consider strategies that promote positive emotional experiences in the workplace, such as team-building events, wellness programmes, and efforts to achieve a healthy work–life balance. According to research, implementing these

strategies can enhance morale and increase motivation to engage in cybersecurity protective behaviours. Moreover, acknowledging and rewarding secure behaviours might strengthen the positive emotions linked to these activities, thereby establishing a cycle of positive emotions and motivated cybersecurity behaviour. Furthermore, the influence of positive emotions on self-efficacy highlights the significance of psychological well-being in empowering employees. Employees with a sense of capability and confidence are more motivated to participate in cybersecurity protective activities effectively. Thus, the implementation of positive interventions in the workplace can directly enhance employees' perceptions and involvement in organisational security, thereby increasing their self-efficacy. Training programmes that provide clear, achievable goals and positive feedback can help build this confidence. These findings should prompt organisations to include emotional well-being in their cybersecurity plans. This will improve employees' security level and contribute to a more involved workforce that can recover quickly from challenges. Implementing policies that promote positive emotions, and self-efficacy is crucial for creating an environment where employees are motivated and capable of actively contributing to cybersecurity initiatives.

The results of this study show that employees with a high level of self-efficacy are proactively engaged in cybersecurity behaviours. The research supports the assertion that individuals are likely to engage in protection behaviour if they believe in the suggested actions' effectiveness and their ability to make such decisions or perform the actions. Furthermore, self-efficacy serves as a mediator between negative and positive emotions and employees' motivation to engage in protective behaviour. This study has found that self-efficacy does not mediate the effect of employee's negative emotions on their protection motivation behaviour. However, self-efficacy has been found to mediate positive emotions and their effect on protection motivation behaviour. These findings have significant value for organisations. The relationship between self-efficacy and protection motivation behaviour emphasises the importance of self-efficacy in the workplace. These findings indicate that organisations could gain advantages by implementing strategies that enhance employees' confidence in their skills to handle cybersecurity risks, especially in situations that require cautious or protective behaviour, such as health and safety procedures or cybersecurity protections. Furthermore, self-efficacy is a mediator between positive emotions and protection motivation behaviour, suggesting that creating a positive emotional environment can indirectly promote protective actions by increasing self-efficacy. This highlights the significance of promoting a positive workplace culture and implies that efforts to improve employee morale and well-being may raise their motivation to comply with protective standards and practices. Finally, organisations should consider training programmes that address the technical aspects of safety and security and emphasise the development of confidence and resilience. These programmes may consist of

resilience training, workshops on coping skills, and regular feedback sessions to advance employees' self-efficacy in handling protective tasks properly. Furthermore, a conducive environment that promotes positive emotional encounters could reinforce this safeguarding drive. This may entail acknowledging employee accomplishments, offering assistance during difficulties, and creating a cooperative and inclusive work environment.

This research identified that cybersecurity awareness positively affects employees' protection motivation behaviour, which has important implications for organisational policy and strategy. Understanding the significance of awareness in cybersecurity implies that organisations should prioritise inclusive cybersecurity education and training programmes. Organisations can improve security by ensuring that employees are well-informed on potential risks and the most effective methods for reducing these threats. These programmes would provide employees with essential knowledge and enhance their motivation to engage in behaviours safeguarding their personal and organisational digital assets.

In addition, it was found that cybersecurity awareness moderates the relationships between positive emotions, self-efficacy, and protective motivation behaviour, leading to an additional level of strategic consideration. This suggests that the influence of positive emotions and self-efficacy on promoting protective behaviours might be increased or decreased depending on the level of awareness of cybersecurity. Hence, organisations should plan to include emotional intelligence training into cybersecurity education. Improving employees' capacity to control their emotions effectively could significantly enhance the effectiveness of cybersecurity awareness, thereby increasing their motivation and effectiveness in implementing secure practices. Moreover, organisations can adopt regular and updated training sessions to address the most recent cybersecurity risks and defence measures. Creating a conducive atmosphere that promotes continuous learning and emotional assistance might further strengthen the preventive actions motivated by increased cybersecurity awareness. Implementing policies that promote clear communication on cybersecurity issues and facilitate knowledge exchange among employees could further enhance this influence. This inclusive strategy supports an organisation's protection against cyber threats and promotes a workplace culture that appreciates and applies emotional understanding to improve security.

This study provides significant understanding for enhancing cybersecurity practices by considering five demographics: gender, age, education level, work position, and years of experience. In terms of gender, organisations should emphasise the development of women's self-efficacy while also promoting favourable views about cybersecurity. Delivering cybersecurity awareness training to females may necessitate employing distinct strategies to

prevent damage to the relationship between self-efficacy and proactive behaviour. Age is also considered an essential factor and could promote positive cybersecurity attitudes across all age groups. To enhance the positive influence of emotions on younger employees, it is necessary to highlight the significance of self-efficacy and awareness. Also, regarding employee education level, organisations can create specialised training programmes for highly educated employees that emphasise converting positive emotions into tangible behaviours. Cybersecurity awareness training can enhance the relationship between positive emotions and self-efficacy for individuals with lower levels of education. Moreover, the organisation could implement techniques to improve self-efficacy while promoting positive mindsets for academic employees. Finally, the organisation could emphasise the development of self-efficacy for employees with various levels of experience but for distinct purposes based on employees' years of experience. Employees with less expertise can enhance the beneficial influences of their emotions through self-efficacy.

Overall, the research's statistically significant findings emphasise the roles of positive emotions, cybersecurity awareness, and self-efficacy in shaping protection motivation behaviour. Positive emotions act as a foundational construct, influencing both self-efficacy and cybersecurity awareness, which, in turn, drive protection motivation. The model presented in Figure 35 highlights the accepted hypotheses based on their statistical significance, showing the relationships between the constructs.

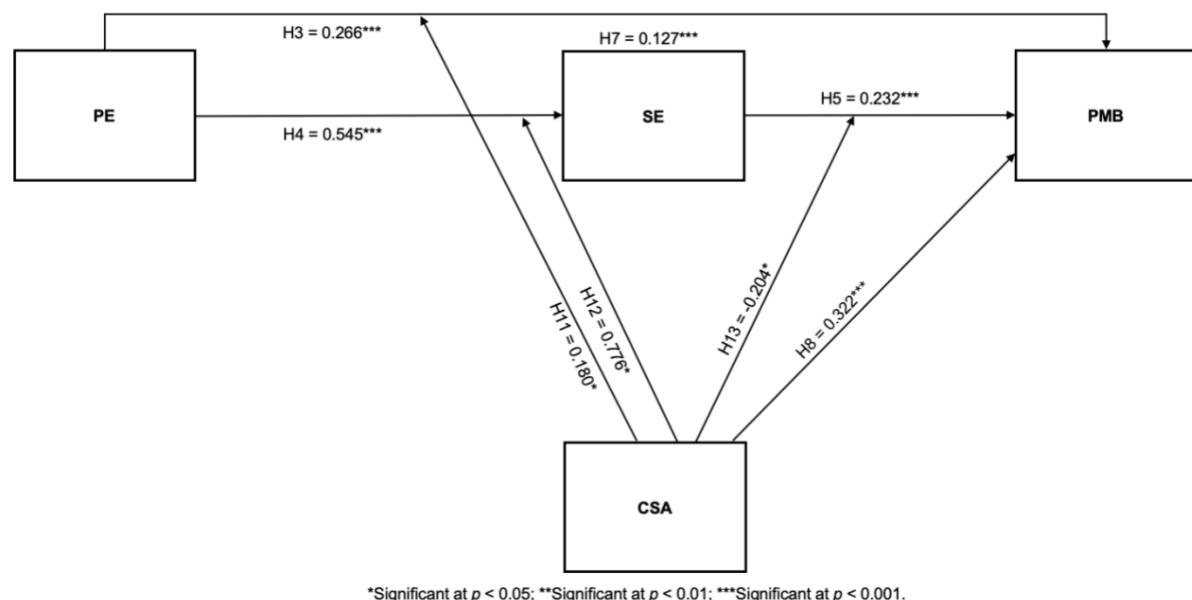


Figure 35: Significance of the Model Findings

Figure 35 shows significant paths with their respective coefficients and significance levels. The results indicate several significant positive effects. Positive emotions positively influence

employees' cybersecurity protection motivation behaviour (**H₃**). Moreover, positive emotions positively influence self-efficacy (**H₄**). Additionally, self-efficacy positively influences employees' protection motivation behaviour (**H₅**). The analysis also found that self-efficacy mediates the relationship between positive emotions and employees' protection motivation behaviour (**H₇**). The findings also indicate that cybersecurity awareness positively influences employees' protection motivation behaviour (**H₈**). Furthermore, cybersecurity awareness positively moderates the relationships between positive emotions and employees' protection motivation behaviour (**H₁₁**) and between positive emotions and self-efficacy (**H₁₂**). However, cybersecurity awareness negatively moderates the relationship between self-efficacy and employees' protection motivation behaviour (**H₁₃**). This suggests that while cybersecurity awareness is crucial for promotion protection motivation behaviour, it may introduce challenges that weaken employees' self-efficacy. As a results, these findings have significant implications for cybersecurity training and interventions. By promoting positive emotions and enhancing self-efficacy, organisations can improve cybersecurity awareness and encourage proactive protection behaviours among employees.

7.5 Research Limitations

While the research contributed to understanding the role of emotions in shaping protection motivation behaviour, self-efficacy, and cybersecurity awareness, it has limitations:

- One of the primary limitations is the sample's diversity and the generalisability of the results. The research findings are based on a sample from a specific population at King Abdulaziz University in Saudi Arabia that may not adequately represent all employees. Factors like organisation type, location, age, and size can influence cybersecurity behaviour and attitudes. Therefore, the results only apply partially to some groups of employees in an organisation.
- Self-reported data reliance can introduce biases such as recall and desirability bias. Participants may over-report positive or under-report negative behaviours, leading to skewed results. In addition, explorations of negative and positive emotions, self-efficacy, cybersecurity awareness, and self-reported protection motivation behaviour may not accurately reflect actual behaviours.
- The study employed validated scales to explore negative and positive emotions, self-efficacy, cybersecurity awareness, and protection motivation behaviour. However, the tools' comprehensiveness and sensitivity would still be limited. The emotions, self-efficacy, cybersecurity awareness, and protection motivation behaviour constructs are

multifaceted and complex, and the tools used may only partially capture some relevant dimensions.

- The research acknowledges external factors, such as incidents of cybersecurity or recent changes in organisations' policies, which can influence participants' responses. However, controlling for these variables would be challenging. These factors can introduce data variability, which needs to be accounted for in the analysis.
- The organisation's context, including communication practices, support systems and culture, is crucial for shaping cybersecurity behaviour. While the research considers these aspects, others may need to account for their impact in their organisation.
- The research integrates two theories, BBT and PMT, but some relevant models and theories may need to be considered. Cybersecurity behaviours are impacted by a wide range of environmental, social, and cognitive factors, and including extra perspectives from different theories could provide a more detailed understanding.

The research increases understanding of the relationship between self-efficacy, emotions, cybersecurity awareness, and protection motivation behaviour. It is essential to consider the above limitations when interpreting the results. Addressing these limitations in future research could assist with developing a strong understanding of cybersecurity behaviour in organisations. Therefore, the next section will offer future research suggestions based on these limitations.

7.6 Future Research

Recognising the limitations mentioned in the previous section is critical when interpreting the findings and guiding future research. This research offers several recommendations for future research. First, future research should aim to include diverse samples to improve the findings' generalisability. Second, including objective measures, such as tracking actual cybersecurity practices or using assessments of third parties, could mitigate biases. Third, future research must consider developing or refining instruments for measurement to reflect constructs accurately. It should explore exact models of emotion and consider emotions' temporal dynamics in impacting cybersecurity behaviour. Fourth, more detailed qualitative research can provide insights into how specific factors interact with cybersecurity awareness and positive and negative emotions to influence protection motivation behaviour. Fifth, future research should integrate theoretical frameworks in a broader range to capture cybersecurity behaviour complexities. Theories from sociology, psychology, and organisational behaviour can provide

extra perspectives and assist in determining new factors that impact cybersecurity practices. For example, the social cognitive and planned behaviour theory can provide valuable perceptions into how social influence and processes impact cybersecurity behaviours. Sixth, this study relies on one-tailed tests in statistical analysis. While these tests help establish directional relationships between variables, future research could explore the application of two-tailed tests to capture a broader range of possible effects. This approach would allow for a more comprehensive analysis of how psychological factors influence cybersecurity behaviour and provide deeper insights into how organisations can refine security policies. Finally, this research assessed several demographic factors, including gender, age, educational level, work position, and years of experience. Future studies could further explore how additional demographic variables, such as employees' specialisation, influence their protection motivation behaviour.

7.7 Conclusion

The research contributed to exploring the influence of negative and positive emotions on employees' cybersecurity protection motivation behaviour and self-efficacy. Moreover, self-efficacy was identified as a mediator between negative and positive emotions and employees' cybersecurity protection motivation behaviour. Furthermore, cybersecurity awareness was recognised as a moderator variable between negative and positive emotions on employees' protection motivation behaviour, negative and positive emotions on employees' self-efficacy, and between self-efficacy and protection motivation behaviour. Despite some hypothesis rejection, the research findings highlight the relationship between factors and emphasise the importance of personalised and intervention. They were improving cybersecurity awareness programs, promoting a supportive culture of organisation addressing cybersecurity emotional aspects, and significantly improving security practices.

Additionally, objective behavioural tracking and courier interventions can provide a practical and accurate approach to cybersecurity training. The suggestion and future research directed in the study aim to guide organisations in developing well cybersecurity strategies and contribute to a broader knowledge body on cybersecurity behaviours. By addressing the limitations identified and exploring new research avenues, future research can further refine the understanding and support the development of effective interventions to improve organisational cybersecurity.

References

- Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. In *User Modeling and User-Adapted Interaction* (Vol. 29, Issue 3). Springer Netherlands. <https://doi.org/10.1007/s11257-019-09236-5>
- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), 1–15. <https://doi.org/10.1093/cybsec/tyy006>
- Ahlmark, N., Algren, M. H., Holmberg, T., Norredam, M. L., Nielsen, S. S., Blom, A. B., Bo, A., & Juel, K. (2015). Survey nonresponse among ethnic minorities in a national health survey—a mixed-method study of participation, barriers, and potentials. *Ethnicity & Health*, 20(6), 611–632.
- Ainia, N. S. N., & Lutfi, L. (2019). The influence of risk perception, risk tolerance, overconfidence, and loss aversion towards investment decision making. *Journal of Economics, Business, & Accountancy Ventura*, 21(3), 401–413.
- Aksan, N., Goldsmith, H. H., Essex, M. J., & Vandell, D. L. (2013). Communicative functions of emotions in sibling relationships. *Journal of Communications Research*, 5(1), 87–110.
- Al-Ababneh, M. (2020). Linking ontology, epistemology and research methodology. *Science & Philosophy*, 8(1), 75–91.
- Al-Muhtadi, J., Saleem, K., Al-Rabiaah, S., Imran, M., Gawanmeh, A., & Rodrigues, J. J. P. C. (2021). A lightweight cyber security framework with context-awareness for pervasive computing environments. *Sustainable Cities and Society*, 66, 102610.
- AL-Nuaimi, M. N. (2022). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. *Global Knowledge, Memory and Communication*.
- Al Zaidi, M. M. (2017). Cyber security behavioural intentions for trade secret protection. *PQDT - UK & Ireland*.
http://proxy.libraries.smu.edu/login?url=https://search.proquest.com/docview/2204769118?accountid=6667%0Ahttps://smu.primo.exlibrisgroup.com/discovery/openurl?institution=01SMU_INST&vid=01SMU_INST:01SMU&?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mt
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security*, 26(4), 276–289. <https://doi.org/10.1016/j.cose.2006.11.004>
- Alfalah, A. A. (2023). The role of Internet security awareness as a moderating variable on cyber security perception: Learning management system as a case study. *International Journal of Advanced and Applied Sciences*, 10(4), 136–144.
<https://doi.org/10.21833/ijaas.2023.04.017>

- Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. *Sensors*, 21(20), 6901.
- Alharbi, T. (2022). Developing cost-effective cybersecurity management system for academic institutions in Saudi Arabia. *J. Eng. Appl. Sci*, 9, 57.
- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, 5(2), 23.
- Alharthi, S., ALHARTHI, A., & ALHARTHI, M. (2019). Sustainable Development Goals in the Kingdom of Saudi Arabia's 2030 Vision. *WIT Transactions on Ecology and the Environment*, 238, 455–467.
- Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach. *Cogent Education*, 10(2). <https://doi.org/10.1080/2331186X.2023.2265227>
- Ali, F., Rasoolimanesh, S. M., Sarstedt, M., Ringle, C. M., & Ryu, K. (2018). An assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. *International Journal of Contemporary Hospitality Management*, 30(1), 514–538.
- Almaliki, A. A., & Safari, S. (2023). *EMPLOYEES AWARENESS OF CYBER SECURITY IN SAUDI UNIVERSITIES : A PAPER*. 14(05), 26–36.
- Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science*, 7, e703.
- Almrezeq, N., Alserhani, F., & Humayun, M. (2021). Exploratory study to measure awareness of cybercrime in Saudi Arabia. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10), 2992–2999.
- Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 154–158.
- Alotibi, G. (2024). A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks. *Engineering, Technology and Applied Science Research*, 14(2), 13787–13795. <https://doi.org/10.48084/etasr.7123>
- Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589.
- AlRuthia, Y., Alsenaidy, M. A., Alrabiah, H. K., AlMuhaisen, A., & Alshehri, M. (2018). The status of licensed pharmacy workforce in Saudi Arabia: a 2030 economic vision perspective. *Human Resources for Health*, 16, 1–8.
- Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate

- current security education training and awareness programs in organisations. *Computers & Security*, 100, 102090.
- Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). *An exploratory study of current information security training and awareness practices in organizations*.
- Alshammari, A., Benson, V., & Batista, L. (2024). The Influences of Employees' Emotions on their Cyber Security Protection Motivation Behaviour: A Theoretical Framework. *26th International Conference on Enterprise Information Systems*.
- Alshammari, A., Benson, V., & Benson, V. (2023). *Emotional Cost of Cyber Crime and Cybersecurity Protection Motivation Behaviour : A Systematic Literature Review*. *Emotional Cost of Cyber Crime and Cybersecurity Protection Motivation Behaviour : A Systematic Literature Review*. <https://aisel.aisnet.org/pacis2023/133>
- Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research*, 6(12).
- Altinay, L., & Paraskevas, A. (2009). *Planning research in hospitality & tourism*. Routledge.
- Amabile, T. M., Barsade, S. G., Mueller, J. S., & Staw, B. M. (2005). Affect and creativity at work. *Administrative Science Quarterly*, 50(3), 367-403.
- Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, 34(4), 1082–1112.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 613–643.
- Angraini, Alias, R. A., & Okfalisa. (2020). A model of information security policy compliance for public universities: A conceptual model. *Emerging Trends in Intelligent Computing and Informatics: Data Science, Intelligent Information Systems and Smart Computing* 4, 810–818.
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443.
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312.
- Arnold, M. B. (1960). *Emotion and personality*. Columbia University Press.
- Ashby, F. G., Isen, A. M., & Turken, A. U. (1999). A neuropsychological theory of positive affect and its influence on cognition. *Psychological Review*, 106(3), 529–550. <https://doi.org/10.1037/0033-295X.106.3.529>
- Averill, J. R. (1980). A constructivist view of emotion. In *Theories of emotion* (pp. 305–339). Elsevier.

- Averill, J. R. (1983). Studies on anger and aggression: Implications for theories of emotion. *American Psychologist*, 38(11), 1145.
- Avkiran, N. K., & Ringle, C. M. (2018). *Partial least squares structural equation modeling: Recent advances in banking and finance* (Vol. 239). Springer.
- Ayoko, O. B., Konrad, A. M., & Boyle, M. V. (2012). Online work: Managing conflict and emotions for performance in virtual teams. *European Management Journal*, 30(2), 156–174. <https://doi.org/10.1016/j.emj.2011.10.001>
- Babii, A. (2020). Important aspects of the experimental research methodology. *Вісник Тернопільського Національного Технічного Університету*, 97(1), 77–87.
- Bada, M., & Nurse, J. R. C. (2019). The Social and Psychological Impact of Cyber-Attacks. In *Emerging cyber threats and cognitive vulnerabilities*. Academic Press. (pp. 73–92). <https://doi.org/10.1002/j.2161-1920.1985.tb00808.x>
- Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, July, 38.
- Bagozzi, R. P., Gopinath, M., & Prashanth U. Nyer. (1999). The Role of Emotions in Marketing. *Journal of Academic Marketing Science*, 27(2), 184–206.
- Bagozzi, R. P., & Moore, D. J. (1994). Public service advertisements: Emotions and empathy guide prosocial behavior. *Journal of Marketing*, 58(1), 56–70.
- Bagozzi, R. P., & Pieters, R. (1998). Goal-directed Emotions. *Cognition and Emotion*, 12(1), 1–26. <https://doi.org/10.1080/026999398379754>
- Baikie, N., & Priest, J. (2019). *Designing social research: the logic of anticipation*. Cambridge: Polity Press.
- Bairagi, V., & Munot, M. V. (2019). *Research methodology: A practical and scientific approach*. CRC Press.
- Balabel, A., & Alwetaishi, M. (2021). Towards sustainable residential buildings in Saudi Arabia According to the conceptual framework of “Mostadam” rating system and vision 2030. *Sustainability*, 13(2), 793.
- Balhara, Y. P. S., Harshwardhan, M., Kumar, R., & Singh, S. (2018). Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness programme. *Asian Journal of Psychiatry*, 34, 38–42. <https://doi.org/10.1016/j.ajp.2018.04.010>
- Baltutis, D., Teubner, T., & Adam, M. (2023). The New Reality at Work: An Employee Typology of Cybersecurity Behavior. *Available at SSRN 4547047*.
- Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support. *Communications of the Association for Information Systems*, 37(1), 8.

- Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, 37(2), 122–147. <https://doi.org/10.1037/0003-066X.37.2.122>
- Bandura, A. (1986). Social foundations of thought and action. *Englewood Cliffs, NJ*, 1986(23–28), 2.
- Bandura, A. (2004). Health promotion by social cognitive means. *Health Education and Behavior*, 31(2), 143–164. <https://doi.org/10.1177/1090198104263660>
- Bandura, A. (2012). On the functional properties of perceived self-efficacy revisited. *Journal of Management*, 38(1), 9–44. <https://doi.org/10.1177/0149206311410606>
- Bandura, A., Freeman, W. H., & Lightsey, R. (1999). *Self-efficacy: The exercise of control*. springer.
- Baral, G., & Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour. *Proceedings - 2019 Cybersecurity and Cyberforensics Conference, CCC 2019*, Ccc, 102–110. <https://doi.org/10.1109/CCC.2019.000-1>
- Barbour, N., Menon, N., & Mannering, F. (2021). A statistical assessment of work-from-home participation during different stages of the COVID-19 pandemic. *Transportation Research Interdisciplinary Perspectives*, 11, 100441.
- Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51(6), 1173.
- Barrett, L. F. (2006). Solving the emotion paradox: Categorization and the experience of emotion. *Personality and Social Psychology Review*, 10(1), 20–46.
- Barrett, L. F. (2017). The theory of constructed emotion: an active inference account of interoception and categorization. *Social Cognitive and Affective Neuroscience*, 12(1), 1–23.
- Basias, N., & Pollalis, Y. (2018). Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. *Review of Integrative Business and Economics Research*, 7, 91–105.
- Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, 51(1), 138–151. <https://doi.org/10.1016/j.im.2013.11.004>
- Baumeister, R. F., Bratslavsky, E., Finkenauer, C., & Vohs, K. D. (2001). Bad Is Stronger Than Good. *Review of General Psychology*, 5(4), 323–370. <https://doi.org/10.1037/1089-2680.5.4.323>
- Beaudry and Pinsonneault. (2010). *The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use*¹. 34(4), 689–710.
- Beedie, C., Terry, P., & Lane, A. (2005). Distinctions between emotion and mood. *Cognition*

& *Emotion*, 19(6), 847–878.

Benson, V. (2017). The state of global cyber security: Highlights and key findings. *Learning Tree*.

Benson, Vladlena., Saridakis, G., & Mohammed, A.-M. (2020). Understanding the Relationship between Cybercrime and Human Behavior through Criminological Theories and Social Networking Sites. *Encyclopedia of Criminal Activities and the Deep*, 1990, 1–10.

Benson, Vladlena, & McAlaney, J. (2019). *Cyber influence and cognitive threats*. Academic Press.

Benson, Vladlena, Saridakis, G., Benson, V., Ezingear, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, 102, 320–330. <https://doi.org/10.1016/j.techfore.2015.08.012>

Beris, O., Beaument, A., & Sasse, M. A. (2015). Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. *ACM International Conference Proceeding Series*, 08-11-Sept, 73–84. <https://doi.org/10.1145/2841113.2841119>

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508–526. <https://doi.org/10.1016/j.jaccpubpol.2018.10.003>

Bernhard, F. (2020). On the emotions that spark innovative and entrepreneurial behaviors in employees. In *Innovation Management* (pp. 182–188). Edward Elgar Publishing.

Berto, F., & Plebani, M. (2015). *Ontology and metaontology: A contemporary guide*. Bloomsbury Publishing.

Bhattacharjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, 351–370.

Bilal Khan., Alghathbar., K. S., Nabi., S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26), 10862–10868. <https://doi.org/10.5897/ajbm11.067>

Bingöl, T. Y. (2018). Determining the predictors of self-efficacy and cyber bullying. *International Journal of Higher Education*, 7(2), 138–143. <https://doi.org/10.5430/ijhe.v7n2p138>

Bogdan, R., & Taylor, S. J. (1990). Looking at the bright side: A positive approach to qualitative policy and evaluation research. *Qualitative Sociology*, 13(2), 183–192.

Bolanio, J. B., Paredes, R. K., & Il, R. E. (2021). Network security policy for higher education institutions based on ISO standards. *Network Security Policy for Higher Education*

Institutions Based on ISO Standards (March 28, 2021). Mediterranean Journal of Basic and Applied Sciences (MJBAS).

- Bolkan, S., Pedersen, W. C., Stormes, K. N., & Manke, B. (2021). Predicting 4-Year Graduation: Using Social Cognitive Career Theory to Model the Impact of Prescriptive Advising, Unit Load, and Students' Self-Efficacy. *Journal of College Student Retention: Research, Theory and Practice*, 22(4), 655–675.
<https://doi.org/10.1177/1521025118783485>
- Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, 86, 350–357.
- Borod, J. C. (2000). *The neuropsychology of emotion*. Oxford University Press.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems*, 39(4), 837–864. <https://doi.org/10.25300/MISQ/2015/39.4.5>
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151–164.
<https://doi.org/10.1057/ejis.2009.8>
- Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, 127, 107082.
<https://doi.org/10.1016/j.chb.2021.107082>
- Braun, V., & Clarke, V. (2012). *Thematic analysis*. American Psychological Association.
- Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2010). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2), 18–26.
- Brooks, A. T., Krumlauf, M., Beck, K. H., Fryer, C. S., Yang, L., Ramchandani, V. A., & Wallen, G. R. (2019). A Mixed Methods Examination of Sleep Throughout the Alcohol Recovery Process Grounded in the Social Cognitive Theory: The Role of Self-Efficacy and Craving. *Health Education and Behavior*, 46(1), 126–136.
<https://doi.org/10.1177/1090198118757820>
- Bryman, A. (2016). *Social research methods*. Oxford university press.
- Bryman, A., & Bell, E. (2015). *Business research methods* (4th ed.). Oxford university press.
- Budimir, S., Fontaine, J. R. J., & Roesch, E. B. (2021). Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 612–616. <https://doi.org/10.1089/cyber.2020.0525>
- Bulgurcu, Burc, Cavusoglu, H., & Benbasat, I. (2010). Information security policy

- compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 523–548.
- Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190–209.
<https://doi.org/10.1016/j.chb.2016.11.018>
- Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, 30(4), 1228–1247.
<https://doi.org/10.1287/isre.2019.0860>
- Callen-naviglia, J., Bank, P. N. C., & James, J. (2018). Fintech, Regtech and the Importance of Cybersecurity. *Issues In Information Systems*, 19(3), 220–225.
https://doi.org/10.48009/3_iis_2018_220-225
- Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., & Cohen, H. (2017). How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks. *Cyberpsychology, Behavior, and Social Networking*, 20(2), 72–77.
<https://doi.org/10.1089/cyber.2016.0338>
- Cannon, W. B. (1927). The James-Lange theory of emotions: A critical examination and an alternative theory. *The American Journal of Psychology*, 39(1/4), 106–124.
- Carmichael, S., & Piquero, A. R. (2004). Sanctions, Perceived Anger, and Criminal Offending. *Journal of Quantitative Criminology*, 20(4), 371–393.
- Carver, C. S., & Harmon-Jones, E. (2009). Anger is an approach-related affect: evidence and implications. *Psychological Bulletin*, 135(2), 183.
- Carver, C. S., & Scheier, M. F. (1990). Origins and functions of positive and negative affect: a control-process view. *Psychological Review*, 97(1), 19.
- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, 1(3), 18–41.
- Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. *Computers & Security*, 97, 101959.
- Chapman, J., Chinnaswamy, A., & Garcia-Perez, A. (2018). The severity of cyber attacks on education and research institutions: a function of their security posture. *Proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited*, 111–119.
- Chen, H., Liu, M., & Lyu, T. (2022). Understanding employees' information security-related stress and policy compliance intention: the roles of information security fatigue and psychological capital. *Information and Computer Security*, 30(5), 751–770.

<https://doi.org/10.1108/ICS-03-2022-0047>

Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022). The Impact of Challenge Information Security Stress on Information Security Policy Compliance: The Mediating Roles of Emotions. *Psychology Research and Behavior Management*, 15, 1177–1191.

<https://doi.org/10.2147/PRBM.S359277>

Chin, W., Cheah, J. H., Liu, Y., Ting, H., Lim, X. J., & Cham, T. H. (2020). Demystifying the role of causal-predictive modeling using partial least squares structural equation modeling in information systems research. *Industrial Management and Data Systems*, 120(12), 2161–2209. <https://doi.org/10.1108/IMDS-10-2019-0529>

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295–336.

Chin, W. W. (2010). How to write up and report PLS analyses. In *Handbook of partial least squares: Concepts, methods and applications* (pp. 655–690). Springer.

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers and Security*, 97, 101931. <https://doi.org/10.1016/j.cose.2020.101931>

Christianson, S.-Å. (1992). Emotional stress and eyewitness memory: a critical review. *Psychological Bulletin*, 112(2), 284.

Chrousos, G. P., Loriaux, D. L., & Gold, P. W. (2013). *Mechanisms of physical and emotional stress* (Vol. 245). Springer Science & Business Media.

Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability*, 12(8), 3163.

Chua, Y. P. (2022). *A step-by-step guide PLS-SEM data analysis using SmartPLS 4*. Researchtree Education.

CITC. (2024). *Saudi Internet 2024*. 2024.

<https://www.cst.gov.sa/en/indicators/saudiinternet/internt-saudi-2021.pdf>

Civelek, M. E. (2018). *Essentials of structural equation modeling*. Lulu. com.

Clore, G. C. (1994). *Why emotions are felt*. In P. Ekman & R. J. Davidson (Eds.), *The nature of emotion: Fundamental questions* (pp. 103-111). New York: Oxford University Press.

Clore, G. L., & Palmer, J. (2009). Affective guidance of intelligent agents: How emotion controls cognition. *Cognitive Systems Research*, 10(1), 21–30.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Academic press.

Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, 112(July), 155–159.

<http://www2.psych.ubc.ca/~schaller/528Readings/Cohen1992.pdf>

Cohen, L., Manion, L., & Morrison, K. (2000). *Research methods in education* (5" ed.) London. England: RoutledgeFalmer.

- Cohen, Louis, Manion, L., & Morrison, K. (2013). *Research methods in education* (7th ed.). Oxford, UK: Routledge.
- Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly: Management Information Systems*, 23(2), 145–158. <https://doi.org/10.2307/249749>
- Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly: Management Information Systems*, 19(2), 189–210. <https://doi.org/10.2307/249688>
- Conrad, C. D., Aziz, J. R., Henneberry, J. M., & Newman, A. J. (2022). Do emotions influence safe browsing? Toward an electroencephalography marker of affective responses to cybersecurity notifications. *Frontiers in Neuroscience*, 16, 922960.
- Cosmides, L., & Tooby, J. (2000). Evolutionary psychology and the emotions. *Handbook of Emotions*, 2(2), 91–115.
- Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26, 605–641.
- Crespo, L. R. Á., Ojeda, J. L. M., Salas, L. S., & Gómez, X. S. G. (2019). Consolidate the responsibility value from the Research Methodology and Statistics subject. *EduMeCentro*, 11(3), 131–144.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
- Croasmun, J. T., & Ostrom, L. (2011). Using likert-type scales in the social sciences. *Journal of Adult Education*, 40(1), 19–22.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297–334.
- Crossan, F. (2003). Research philosophy: towards an understanding. *Nurse Researcher (through 2013)*, 11(1), 46.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, 32(June), 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>
- Czaja, S. J., & Sharit, J. (1998). Age differences in attitudes toward computers. *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, 53(5), P329–P340.
- D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), 285–318. <https://doi.org/10.2753/MIS0742-1222310210>

- D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, 50(10), 113–117.
- D'Arcy, J., & Hovav, A. (2009). An integrative framework for the study of information security management Research. In *Handbook of Research on Information Security and Assurance* (pp. 55–67). IGI Global.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98.
- D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information and Management*, 56(7), 103151. <https://doi.org/10.1016/j.im.2019.02.006>
- Damasio, A. (1994). *Descartes' error: emotion, reason, and the human brain penguin*. New York: Penguin. Paola Iannello-Michela Balconi-Alessandro Antonietti.
- Darwin, C. (1872). *The expression of the emotions in man and animals*. New York, USA.
- Dash, G., & Paul, J. (2021). CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, 173(June), 121092. <https://doi.org/10.1016/j.techfore.2021.121092>
- DataReportal. (2023). *DIGITAL AROUND THE WORLD*. <https://datareportal.com/global-digital-overview>
- Davidson, R. J., Sherer, K. R., & Goldsmith, H. H. (2009). *Handbook of affective sciences*. Oxford University Press.
- Davitz, J. R. (2013). *The language of emotion*. Academic Press.
- Deng, L., Yang, M., & Marcoulides, K. M. (2018). Structural equation modeling with many variables: A systematic review of issues and developments. *Frontiers in Psychology*, 9, 580.
- Devi, P. S. (2017). *Research methodology: A handbook for beginners*. Notion Press.
- Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), 386–408. <https://doi.org/10.17705/1jais.00133>
- Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security*, 26(1), 73–80. <https://doi.org/10.1016/j.cose.2006.10.009>
- Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056.
- Dörnyei, Z., & Taguchi, T. (2009). Questionnaires in second language research: Construction, administration, and processing: Second edition. In *Questionnaires in Second Language Research: Construction, Administration, and Processing: Second*

Edition. <https://doi.org/10.4324/9780203864739>

- Ekman, P. (1992). An argument for basic emotions. *Cognition & Emotion*, 6(3–4), 169–200.
- Elliot, A. J., & Thrash, T. M. (2002). Approach-avoidance motivation in personality: approach and avoidance temperaments and goals. *Journal of Personality and Social Psychology*, 82(5), 804.
- Else-Quest, N. M., Higgins, A., Allison, C., & Morton, L. C. (2012). Gender differences in self-conscious emotional experience: a meta-analysis. *Psychological Bulletin*, 138(5), 947.
- Essa, S., & Harvey, B. (2022). Education for sustainable development in Saudi Arabia: A critical discourse analysis of media and government policy documents. *Interdisciplinary Journal of Environmental and Science Education*, 18(2), e2266.
- European Union Agency for Cybersecurity (ENISA). (2016). *ENISA threat taxonomy*. Retrieved from <https://www.enisa.europa.eu>
- European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape 2023*. Retrieved from <https://www.enisa.europa.eu>
- European Union Agency for Cybersecurity (ENISA). (2024). *Threat landscape*. Retrieved from <https://www.enisa.europa.eu>
- Fadhurahman, A. S. (2024). Enhancing Employee Performance: The Impact of Quality of Work Life, Organizational Citizenship Behavior, and Work Motivation. *Academia Open*, 9(2), 10–21070.
- Faqihi, Y. A. A., & Al-Ababneh, A. F. A. (2022). A Proposed Strategy for Promoting Entrepreneurship Education and Attitude to Entrepreneurial University in Light of Saudi Vision 2030. *European Journal of Social Sciences Studies*, 7(3).
- Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers and Security*, 100, 102082. <https://doi.org/10.1016/j.cose.2020.102082>
- Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. *Journal of Physics: Conference Series*, 1339(1), 12098.
- Field, A. (2013). *Discovering statistics using SPSS*. In Sage (Vol. 2nd, Issue Third Edition).
- Fink, A. (2017). *How to conduct surveys: A step-by-step guide* (6th ed.). Sage Publications.
- Fink, A. (2019). *Conducting research literature reviews: From the internet to paper*. Sage publications.
- Flick, U. (2015). *Introducing research methodology: A beginner's guide to doing a research project*. Sage.
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on

- protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407–429.
- Folkman, S., & Lazarus, R. S. (1988). Coping as a mediator of emotion. *Journal of Personality and Social Psychology*, 54(3), 466.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.
- Fornell, C., Larcker, D. F., Henseler, J., Ringle, C. M., Sarstedt, M., Hair Jr, J. F. J., Hair Jr, J. F. J., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Bairagi, V., Munot, M. V., Basias, N., Pollalis, Y., Babii, A., Civelek, M. E., Avkiran, N. K., Ringle, C. M., Chin, W. W., ... Dordeska, M. (2018). An assessment of the use of partial least squares structural equation modeling (PLS-SEM) in hospitality research. *International Journal of Contemporary Hospitality Management*, 28(1), 514–538.
<https://doi.org/10.4337/9781788976374.00007>
- Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, 25(2), 91–109.
- Frazier, P. A., Tix, A. P., & Barron, K. E. (2004). Testing moderator and mediator effects in counseling psychology research. *Journal of Counseling Psychology*, 51(1), 115.
- Fredrickson, B. (2001). The Role of Positive Emotions in Positive Psychology. *The American Psychologist*, 56, 218–226. <https://doi.org/10.1037//0003-066X.56.3.218>
- Fredrickson, B L. (1998). *What good are positive emotions? Review of General Psychology*, 2 (3), 300-319.
- Fredrickson, Barbara L. (2004). The broaden-and-build theory of positive emotions. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 359(1449), 1367–1377. <https://doi.org/10.1098/rstb.2004.1512>
- Fredrickson, Barbara L., & Branigan, C. (2005). Positive emotions broaden the scope of attention and thought-action repertoires. *Cognition and Emotion*, 19(3), 313–332.
<https://doi.org/10.1080/02699930441000238>
- Fredrickson, Barbara L., & Joiner, T. (2002). Positive emotions trigger upward spirals toward emotional well-being. *Psychological Science*, 13(2), 172–175.
<https://doi.org/10.1111/1467-9280.00431>
- Fredrickson, Barbara L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. *American Psychologist*, 56(3), 218.
- Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, 45(5), 521–536.
<https://doi.org/10.1109/TSE.2017.2782813>
- Frijda, N. H. (1986). *The emotions*. Cambridge University Press.

- Frijda, N. H. (1994). *Emotions are functional, most of the time*.
- Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud and Security*, 2020(12), 6–12.
[https://doi.org/10.1016/S1361-3723\(20\)30127-5](https://doi.org/10.1016/S1361-3723(20)30127-5)
- Gallaher, M. P., Link, A. N., & Rowe, B. (2008). *Cyber security: Economic strategies and public policy alternatives*. Edward Elgar Publishing.
- Garba, A. A., Jeribi, F., Al-Shourbaji, I., Alhameed, M., Reegu, F., & Alim, S. (2021). An Approach to Weigh Cybersecurity Awareness Questions in Academic Institutions Based on Principle Component Analysis: A Case Study of Saudi Arabia. *Int. J. Sci. Technol. Res*, 10, 319–326.
- Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika*, 61(1), 101–107.
- General Authority for Statistics. (2022). *Population Summary Report*.
<https://www.stats.gov.sa/en>
- Gerić, S., & Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and Organizational Sciences*, 31(1), 51–61.
- Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*.
- Gillam, A. R., & Waite, A. M. (2021). Gender differences in predictors of technology threat avoidance. *Information & Computer Security*, 29(3), 393–412.
- Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales*.
- Goh, R. (2003). *Information Security: The Importance of the Human Element*. Singapore: Preston University.
- Gollwitzer, P. M., & Kinney, R. F. (1989). Effects of deliberative and implemental mind-sets on illusion of control. *Journal of Personality and Social Psychology*, 56(4), 531.
- Gotthardt, M., & Mezhyuev, V. (2022). Measuring the Success of Recommender Systems: A PLS-SEM Approach. *IEEE Access*, 10, 30610–30623.
- Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, 111(7).
- Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, 181, 59–66.
- Gravetter, F. J., & Forzano, L.-A. B. (2018). *Research methods for the behavioral sciences*. Cengage learning.
- Gross, J. J. (1998). Antecedent-and response-focused emotion regulation: divergent consequences for experience, expression, and physiology. *Journal of Personality and Social Psychology*, 74(1), 224.

- Gross, J. J. (2015). Emotion regulation: Current status and future prospects. *Psychological Inquiry*, 26(1), 1–26.
- Gross, J. J., & Thompson, R. A. (2007). Emotion regulation: conceptual foundations. JJ Gross (Ed.), *Handbook of emotion regulation*. New York: *The Guilford Press*, 3, 25.
- Grossman, M., & Wood, W. (1993). Sex differences in intensity of emotional experience: a social role interpretation. *Journal of Personality and Social Psychology*, 65(5), 1010.
- Gulenko, I. (2014). Improving passwords: influence of emotions on security behaviour. *Information Management & Computer Security*, 22(2), 167–178.
<https://doi.org/10.1108/imcs-09-2013-0068>
- Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: the NIST handbook* (Vol. 800, Issue 12). Diane Publishing.
- Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology*, 12(1), 262–274. <https://doi.org/10.5281/zenodo.495776>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks. Sage, 165.
- Hair, Joe F, Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152.
- Hair, Joe F, Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, 40, 414–433.
- Hair, Joseph.F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE Publications, Incorporated.
- Hair, Joseph F, Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate data analysis: A global perspective* (Vol. 7). Upper Saddle River, NJ: Pearson.
- Hair, Joseph F, Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2014). Pearson new international edition. *Multivariate Data Analysis, Seventh Edition*. Pearson Education Limited Harlow, Essex.
- Hair, Joseph F, Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24.
- Hair Jr, J., Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage publications.
- Hair Jr, J., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. *European Business Review*, 26(2), 106–121.

- Hair Jr, J.F., Wolfinbarger, M., Money, A. H., Samouel, P., & Page, M. J. (2016). Essentials of business research methods. *Essentials of Business Research Methods*, 1–507.
<https://doi.org/10.4324/9780429203374>
- Hair Jr, Joe F. (2020). Next-generation prediction metrics for composite-based PLS-SEM. *Industrial Management & Data Systems*, 121(1), 5–11.
- Hair Jr, Joseph F, Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2023). *Advanced issues in partial least squares structural equation modeling*. saGe publications.
- Hair Jr, Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, 26(2), 106–121.
- Ham, J. Van Der. (2021). Toward a Better Understanding of “Cybersecurity.” *Digital Threats: Research and Practice*, 2(3), 3–5. <https://doi.org/10.1145/3442445>
- Hampel, F. R. (1974). The influence curve and its role in robust estimation. *Journal of the American Statistical Association*, 69(346), 383–393.
- Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66, 52–65.
- Hanus, B., & Wu, Y. “Andy.” (2016). Impact of users’ security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2–16.
- Harré, R. (1986). The social construction of emotions. (*No Title*).
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4, 1–13.
- Haußinger, F. (2015). *Studies on Employees’ Information Security Awareness*. 200.
- He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees’ intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21(2), 203–213.
- Henseler, J, Hubona, G., & Ray, P. A. (2017). *Partial least squares path modeling: Updated guidelines*. Springer International Publishing.
- Henseler, Jörg, Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems*, 116(1), 2–20.
- Henseler, Jörg, Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 115–135.
- Henseler, Jörg, & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path

- modeling. *Computational Statistics*, 28, 565–580.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Hertenstein, M. J., Verkamp, J. M., Kerestes, A. M., & Holmes, R. M. (2006). The communicative functions of touch in humans, nonhuman primates, and rats: a review and synthesis of the empirical research. *Genetic, Social, and General Psychology Monographs*, 132(1), 5–94.
- Hess, U. (2001). The communication of emotion. In *Emotions, qualia, and consciousness* (pp. 397–409). World Scientific.
- Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) framework for remote working employees. *Sensors*, 22(22), 8663.
- Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, 564–569.
- Hina, S., & Dominic, D. D. (2017). Need for information security policies compliance: A perspective in Higher Education Institutions. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6.
- Holt, T. J., & Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. *Proceedings - WOMBAT Workshop on Information Security Threats Data Collection and Sharing, WISTDCS 2008*, 67–78. <https://doi.org/10.1109/WISTDCS.2008.9>
- Honderich, T. (2005). *The Oxford companion to philosophy*. OUP Oxford.
- Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies*, 28(1), 439–470.
- Hosseini, S., Turhan, B., & Gunarathna, D. (2017). A systematic literature review and meta-analysis on cross project defect prediction. *IEEE Transactions on Software Engineering*, 45(2), 111–147.
- Hoyle, R. H. (2012). *Handbook of structural equation modeling*. Guilford press.
- Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 26(2), 282–300.
- Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3).
- Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A

- review of four recent studies. *Strategic Management Journal*, 20(2), 195–204.
- Huysamen, G. K. (1990). *Introductory statistics and research design for the behavioural sciences*. Bloemfontein: van Schaik.
- Hwang, H., Cho, G., Jung, K., Falk, C. F., Flake, J. K., Jin, M. J., & Lee, S. H. (2021). An approach to structural equation modeling with both factors and components: Integrated generalized structured component analysis. *Psychological Methods*, 26(3), 273.
- I. M. Y. Woon., Tan., W., & R. T. Low. (2005). *A PROTECTION MOTIVATION THEORY APPROACH TO HOME WIRELESS SECURITY*. 5, 186–204.
- IA, I. H. (2022). The Impact of Organizational Behavior, Trust, Commitment and Job Motivation on Academic Staff and Employees. *Psychology & Psychological Research International Journal*, 7(4), 1–7. <https://doi.org/10.23880/pprij-16000313>
- IBM, S. (2023). *Cost of a Data Breach Report*.
- Ibrahim, N., Wong, K. W., & Shiratuddin, M. F. (2015). Persuasive impact of online media: investigating the influence of visual persuasion. *2015 Asia Pacific Conference on Multimedia and Broadcasting*, 1–7.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Imran, M., Arif, T., & Shoab, M. (2018). A statistical and theoretical analysis of cyberthreats and its impact on industries. *International Journal of Scientific Research in Computer Science Applications and Management Studies*, 7(5), 1–7.
- ISO/IEC 17799:2005. (2005). Code of practice for information security management. *British Standard Institution*.
- Izard, C. (1991). The psychology of emotions. New York, NY US. *Plenum Press*. Jost, JJ, & Banaji, MR (1994). *The Role of Stereotyping in System-Justification and the Production of False Consciousness*. *British Journal of Social Psychology*, 33, 1–27.
- Izard, C. E. (1971). *The face of emotion*.
- Izard, C. E. (2002). Translating emotion theory and research into preventive interventions. *Psychological Bulletin*, 128(5), 796–824. <https://doi.org/10.1037/0033-2909.128.5.796>
- Izard, C. E. (2007). Basic emotions, natural kinds, emotion schemas, and a new paradigm. *Perspectives on Psychological Science*, 2(3), 260–280.
- Jamieson, S. (2004). Likert scales: How to (ab) use them? *Medical Education*, 38(12), 1217–1218.
- Johnson-Laird, P. N., & Oatley, K. (1989). The language of emotions: An analysis of a semantic field. *Cognition and Emotion*, 3(2), 81–123.
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly: Management Information Systems*, 34(SPEC).

- ISSUE 3), 549–566. <https://doi.org/10.2307/25750691>
- Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, 25(3), 231–251.
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). *AN ENHANCED FEAR APPEAL RHETORICAL FRAMEWORK: LEVERAGING THREATS TO THE HUMAN ASSET THROUGH SANCTIONING RHETORIC*. 39(1), 113–134.
- Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489–496. <https://doi.org/10.1016/j.procs.2014.05.452>
- Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, 67, 267–279.
- Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, 43–48.
- Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61, 46–58.
- Keltner, D., & Haidt, J. (1999). Social functions of emotions at four levels of analysis. *Cognition & Emotion*, 13(5), 505–521.
- Keltner, D., & Haidt, J. (2001). *Social functions of emotions*.
- Kemper, T. D., & Lazarus, R. S. (1990). Emotion and Adaptation. *Contemporary Sociology*, 21(4), 522. <https://doi.org/10.2307/2075902>
- Kensinger, E. A., & Schacter, D. L. (2008). Memory and emotion. *Handbook of Emotions*, 3, 601–617.
- Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, 29(1), 4–23.
- Khorakian, A., & Sharifirad, M. S. (2019). Integrating Implicit Leadership Theories, Leader–Member Exchange, Self-Efficacy, and Attachment Theory to Predict Job Performance. *Psychological Reports*, 122(3), 1117–1144. <https://doi.org/10.1177/0033294118773400>
- Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security*. Jones & Bartlett Publishers.
- Kim, J., Park, E. H., & Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information and Management*, 53(1), 91–108. <https://doi.org/10.1016/j.im.2015.09.003>
- Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing Management*, 48(4), 16–19. <https://doi.org/10.1097/01.NUMA.0000514066.30572.f3>
- Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature

- reviews in software engineering. *Technical Report, Ver. 2.3 EBSE Technical Report. EBSE*.
- Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of E-Collaboration*, 11(4), 1–10.
<https://doi.org/10.4018/ijec.2015100101>
- Kock, N. (2017). Common method bias: a full collinearity assessment method for PLS-SEM. *Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and Applications*, 245–257.
- Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, 28(1), 227–261.
- Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607–610.
- Kryshko, O., Fleischer, J., Grunschel, C., & Leutner, D. (2023). University Students' Self-Efficacy for Motivational Regulation, Use of Motivational Regulation Strategies, and Satisfaction With Academic Studies: Exploring Between-Person and Within-Person Associations. *Journal of Educational Psychology*, 115(4), 571–588.
<https://doi.org/10.1037/edu0000785.supp>
- Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. In *Journal of Management Information Systems* (Vol. 25, Issue 2). <https://doi.org/10.2753/MIS0742-1222250210>
- Kuriakose, N., & Robbins, M. (2016). Don't get duped: Fraud through duplication in public opinion surveys. *Statistical Journal of the IAOS*, 32(3), 283–291.
- Kushwah, S., Dhir, A., Sagar, M., & Gupta, B. (2019). Determinants of organic food consumption. A systematic literature review on motives and barriers. *Appetite*, 143, 104402.
- Kyobe, M. (2010). Towards a framework to guide compliance with IS Security policies and Regulations in a university. *2010 Information Security for South Africa*, 1–6.
- Kyva, V. (2022). Analysis of factors affecting cyber security of a higher military educational institution. *Cybersecurity: Education, Science, Technique*, 3(15), 53–70.
- Lankton, N. K., Stivason, C., & Gurung, A. (2019). Information protection behaviors: morality and organizational criticality. *Information & Computer Security*, 27(3), 468–488.
- LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3), 71–76.
<https://doi.org/10.1145/1325555.1325569>
- Latan, H., Noonan, R., & Matthews, L. (2017). Partial least squares path modeling. *Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and*

Applications.

- Lazarus, R. S. (1991). *Emotion and adaptation*. Oxford University Press.
- Lê Cao, K.-A., & Welham, Z. M. (2021). *Multivariate data integration using R: methods and applications with the mixOmics package*. CRC Press.
- LeDoux, J. (2012). Rethinking the emotional brain. *Neuron*, 73(4), 653–676.
- LeDoux, J. E. (1989). Cognitive-emotional interactions in the brain. *Cognition & Emotion*, 3(4), 267–289.
- Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, 00111287231180093.
- Levenson, R. W. (2014). The autonomic nervous system and emotion. *Emotion Review*, 6(2), 100–112.
- Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9.
- Leys, C., Ley, C., Klein, O., Bernard, P., & Licata, L. (2013). Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median. *Journal of Experimental Social Psychology*, 49(4), 764–766.
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45(February 2018), 13–24.
<https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. (2019). What users do besides problem-focused coping when facing it security threats: An emotion-focused coping perspective. *MIS Quarterly: Management Information Systems*, 43(2), 373–394.
<https://doi.org/10.25300/MISQ/2019/14360>
<https://doi.org/10.25300/MISQ/2019/14360>
- Liengaard, B. D., Sharma, P. N., Hult, G. T. M., Jensen, M. B., Sarstedt, M., Hair, J. F., & Ringle, C. M. (2021). Prediction: coveted, yet forsaken? Introducing a cross-validated predictive ability test in partial least squares path modeling. *Decision Sciences*, 52(2), 362–392.
- Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3–4), 215–228.
- Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, 25(5), 433–463.
<https://doi.org/10.1111/isj.12043>

- Lowry, P. B., Schuetzler, R. M., Giboney, J. S., & Gregory, T. A. (2015). Is Trust Always Better than Distrust? The Potential Value of Distrust in Newer Virtual Teams Engaged in Short-Term Decision-Making. *Group Decision and Negotiation*, 24(4), 723–752. <https://doi.org/10.1007/s10726-014-9410-x>
- Lu, Y. (2018). Cybersecurity Research: A Review of Current Research Topics. *Journal of Industrial Integration and Management*, 03(04), 1850014. <https://doi.org/10.1142/s2424862218500148>
- Luszczynska, A., & Schwarzer, R. (2015). Social cognitive theory. *Fac Health Sci Publ*, 2015, 225–251.
- Luthans, F., Youssef, C. M., & Avolio, B. J. (2006). *Psychological capital: Developing the human competitive edge*. Oxford university press.
- Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing and Management*, 59(1), 102744. <https://doi.org/10.1016/j.ipm.2021.102744>
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. [https://doi.org/10.1016/0022-1031\(83\)90023-9](https://doi.org/10.1016/0022-1031(83)90023-9)
- Majeed, M. T., & Ayub, T. (2018). Information and communication technology (ICT) and economic growth nexus: A comparative global analysis. *Pakistan Journal of Commerce and Social Sciences (PJCSS)*, 12(2), 443–476.
- Makransky, G., & Petersen, G. B. (2019). Investigating the process of learning with desktop virtual reality: A structural equation modeling approach. *Computers & Education*, 134, 15–30.
- Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, 52(12), 1865–1883.
- Mallinckrodt, B., & Wei, M. (2005). Attachment, social competencies, social support, and psychological distress. *Journal of Counseling Psychology*, 52(3), 358–367. <https://doi.org/10.1037/0022-0167.52.3.358>
- Mamun, M. R. Al, Prybutok, V. R., Peak, D. A., Torres, R., & Pavur, R. J. (2023). The role of emotional attachment in IPA continuance intention: an emotional attachment model. *Information Technology and People*, 36(2), 867–894. <https://doi.org/10.1108/ITP-09-2020-0643>
- Maniyeva, R. M. (2022). the Impact of Emotions on Cadet'S Training Motivation. *Habitus*, 42, 69–73. <https://doi.org/10.32782/2663-5208.2022.42.11>
- Masmali, H. H., & Miah, S. J. (2022). Emergent Insight of the Cyber Security Management for Saudi Arabian Universities: A Content Analysis. *Proceedings of Seventh*

- International Congress on Information and Communication Technology: ICICT 2022, London, Volume 2*, 153–171.
- Matell, M. S., & Jacoby, J. (1971). Is there an optimal number of alternatives for Likert scale items? Study I: Reliability and validity. *Educational and Psychological Measurement*, 31(3), 657–674.
- McAlaney, J., Benson, V., & Frumkin, L. A. (2018). Psychological and Behavioral Examinations in Cyber Security. In *Psychological and Behavioral Examinations in Cyber Security*. <https://doi.org/10.4018/978-1-5225-4053-3>
- McAlaney, J., Hills, P. J., & Cole, T. (2024). *Forensic Perspectives on Cybercrime: Human Behaviour and Cybersecurity*. Taylor & Francis.
- McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security*, 26(3), 277–289. <https://doi.org/10.1108/ICS-03-2018-0032>
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.065>
- McLachlan, G. J. (1999). Mahalanobis distance. *Resonance*, 4(6), 20–26.
- Meijers, M. H. C., Remmelswaal, P., & Wonneberger, A. (2019). Using Visual Impact Metaphors to Stimulate Environmentally Friendly Behavior: The Roles of Response Efficacy and Evaluative Persuasion Knowledge. *Environmental Communication*, 13(8), 995–1008. <https://doi.org/10.1080/17524032.2018.1544160>
- Melnyk, S. A., Speier-Pero, C., & Connors, E. (2019). Blockchain is vastly overrated; supply chain cyber security is vastly underrated. *Supply Chain Management Review*.
- Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security*, 75, 147–166. <https://doi.org/10.1016/j.cose.2018.01.020>
- Mesquita, B., & Frijda, N. H. (1992). Cultural variations in emotions: a review. *Psychological Bulletin*, 112(2), 179.
- Mey, M. T. (2016). The value relevance of straight-lining lease expenses. *International Business & Economics Research Journal (IBER)*, 15(6), 301–314.
- Mihalinec, I., Stevanovic, R., & Skala, K. (2008). Emotion recognition and its aesthetic interpretation. *2008 50th International Symposium ELMAR*, 2, 491–494.
- Miller, J. (1991). Reaction time analysis with outlier exclusion: Bias varies with sample size. *The Quarterly Journal of Experimental Psychology Section A*, 43(4), 907–912.
- Ministry of Education. (2017). Higher Education Statistics. In *Ministry of Education*.
- Miroslav, B. (2017). The risk assessment of information system security . *Ukrainian Scientific Journal of Information Security*, 23(2). <https://www.openaire.eu/search?q=&Search=>

- Mitchell, B., & Alfuraih, A. (2018). The Kingdom of Saudi Arabia: Achieving the aspirations of the National Transformation Program 2020 and Saudi vision 2030 through education. *Journal of Education and Development*, 2(3), 36.
- Mohamad, M., Afthanorhan, A., Awang, Z., & Mohammad, M. (2019). Comparison between CB-SEM and PLS-SEM: Testing and confirming the maqasid syariah quality of life measurement model. *The Journal of Social Sciences Research*, 5(3), 608–614.
- Mohammed, M., & Bamasoud, D. M. (2022). The Impact of Enhancing Awareness of Cybersecurity on Universities Students: A Survey Paper. *Journal of Theoretical and Applied Information Technology*, 100(15).
- Moody, G. D., Galletta, D. F., & Lowry, P. B. (2014). When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. *Electronic Commerce Research and Applications*, 13(4), 266–282.
<https://doi.org/10.1016/j.elerap.2014.05.001>
- Moody, G. D., Siponen, M., & Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems*, 42(1), 285–311. <https://doi.org/10.25300/MISQ/2018/13853>
- Moons, W. G., Eisenberger, N. I., & Taylor, S. E. (2010). Anger and fear responses to stress have different biological profiles. *Brain, Behavior, and Immunity*, 24(2), 215–219.
<https://doi.org/10.1016/j.bbi.2009.08.009>
- Moore, A. P., Hanley, M., & Mundie, D. (2011). A pattern for increased monitoring for intellectual property theft by departing insiders. *Proceedings of the 18th Conference on Pattern Languages of Programs*, 1–10.
- Muhirwe, J., & White, N. (2016). Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users. *Issues In Information Systems*, 17(li), 183–192.
https://doi.org/10.48009/2_iis_2016_183-192
- Mulligan, K., & Scherer, K. R. (2012). Toward a working definition of emotion. *Emotion Review*, 4(4), 345–357.
- Nadia, Y. (2017). Changes required in Saudi universities curriculum to meet the demands of 2030 Vision. *International Journal of Economics and Finance*, 9(9), 111.
- Nam, S., Kim, D., & Jin, C. (2018). A comparison analysis among structural equation modeling (AMOS, LISREL and PLS) using the same data. *Journal of the Korea Institute of Information and Communication Engineering*, 22(7), 978–984.
- Naqvi, N., Shiv, B., & Bechara, A. (2006). The role of emotion in decision making: A cognitive neuroscience perspective. *Current Directions in Psychological Science*, 15(5), 260–264.
- National Institute of Standards and Technology (NIST). (2012). *Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1)*. Retrieved from

<https://nvlpubs.nist.gov>

- National Institute of Standards and Technology (NIST). (2020). *Cybersecurity framework version 1.1*. Retrieved from <https://www.nist.gov>
- NCA. (2020). *Cybersecurity Quarterly Bulletin, Q4 2020*.
https://nca.gov.sa/files/qb2020q4_en.pdf
- Neville, C. 2007. (2007). *Effective Learning Service: Introduction to Research and Research Methods*. University of Bradford School of Management. UK.
- NICCS. (2022). *Vocabulary Explore Terms : A Glossary of Common Cybersecurity Words and Phrases Letter : A*. 1–35.
- Nicho, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, 26(1), 10–38.
- Niehaves, B., & Stahl, C. (2006). *Criticality , epistemology and behaviour vs . Design – information systems research across different sets of paradigms*.
- Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12* (Vol. 1).
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf>
- Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, 26(1), 1–20. <https://doi.org/10.1057/s41303-016-0025-y>
- Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, 13(1), 49–72.
- Oatley, K., & Johnson-Laird, P. N. (1987). Towards a cognitive theory of emotions. *Cognition and Emotion*, 1(1), 29–50.
- Oatley, K., Keltner, D., & Jenkins, J. M. (1996). *Understanding emotions*. Blackwell publishing.
- Ogbanufe, O., & Pavur, R. (2022). Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management*, 62(August 2021). <https://doi.org/10.1016/j.ijinfomgt.2021.102432>
- Ouassini, A., Boynton, K., Romaniuk, S., & Manjikan, M. (2021). The silicon valley of the Middle East: cybersecurity, Saudi Arabia, and the path to vision 2030. *Routledge Companion to Global Cyber-Security Strategy*. Oxon: Routledge.
- Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 156b-156b.
- Pallant, J. (2020). *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. McGraw-hill education (UK).
- Panksepp, J. (1988). Brain emotional circuits and psychopathologies. In *Emotions and*

- psychopathology* (pp. 37–76). Springer.
- Papez, J. W. (1937). A proposed mechanism of emotion. *Archives of Neurology & Psychiatry*, 38(4), 725–743.
- Parke, C. S. (2012). *Essential first steps to data analysis: Scenario-based examples using SPSS*. Sage Publications.
- Parrott, W. G. (2001). *Emotions in social psychology: Essential readings*. psychology press.
- Parshetty, S. (2019). Employee Motivation and Their Impact on Employee Performance in Banking Sector in Hyderabad Karnataka Region. *International Journal of Trend in Scientific Research and Development*, 3(4), 390–393.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176.
- Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals*. National Institute of Standards and Technology.
- Pearson, S. (2013). *Privacy, security and trust in cloud computing*. Springer.
- Pervez, M. A. (2010). Impact of emotions on employee's job performance: An evidence from organizations of Pakistan. *OIDA International Journal of Sustainable Development*, 1(5), 11–16.
- Pessoa, L. (2009). How do emotion and motivation direct executive control? *Trends in Cognitive Sciences*, 13(4), 160–166.
- Peters, M. M. M. S. (2018). Insights from rodent food protection behaviors. *Learning and Motivation*, 61, 52–62.
- Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, 11(4), 489–510.
- Plutchik, R. (2001). The nature of emotions: Human emotions have deep evolutionary roots, a fact that may explain their complexity and provide tools for clinical practice. *American Scientist*, 89(4), 344–350.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.
- Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 30(6–7), 486–497.
- Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations' protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems*, 26(6), 585–604.

- Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179–214.
- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly: Management Information Systems*, 37(4), 1189–1210.
<https://doi.org/10.25300/MISQ/2013/37.4.09>
- Power, M. J. (2006). The structure of emotion: An empirical comparison of six models. *Cognition and Emotion*, 20(5), 694–713. <https://doi.org/10.1080/02699930500367925>
- Psillos, S. (2011). An explorer upon untrodden ground: Peirce on abduction. In *Handbook of the History of Logic* (Vol. 10, pp. 117–151). Elsevier.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, 34(4), 757–778. <https://doi.org/10.2307/25750704>
- Qin, P., & Liu, Y. (2019). The empirical research of the influence of leadership positive emotion on counterproductive work behavior. *Psychology*, 10(6), 877–902.
- Rahman, R., & Al-Borie, H. M. (2021). Strengthening the Saudi Arabian healthcare system: role of vision 2030. *International Journal of Healthcare Management*, 14(4), 1483–1491.
- Rahman, R., & Qattan, A. (2021). Vision 2030 and sustainable development: state capacity to revitalize the healthcare system in Saudi Arabia. *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, 58, 0046958020984682.
- Renaud, K., Zimmermann, V., Schürmann, T., & Böhm, C. (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1). <https://doi.org/10.1057/s41599-021-00746-5>
- Reschly, A. L., Huebner, E. S., Appleton, J. J., & A. (2008). Engagement as flourishing: The contribution of positive emotions and coping to adolescents' engagement at school and with learning. *Journal of Adolescence*, 45(5), 419–431. <https://doi.org/10.1002/pits>
- Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, 28(8), 816–826. <https://doi.org/10.1016/j.cose.2009.05.008>
- Rice, S., Winter, S. R., Doherty, S., & Milner, M. (2017). Advantages and Disadvantages of Using Internet-Based Survey Methods in Aviation-Related Research. *Journal of Aviation Technology and Engineering*, 7(1), 58–65. <https://doi.org/10.7771/2159-6670.1160>
- Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023). The influence of organizational values on employee attitude and information security behavior: the mediating role of

- psychological capital. *Information and Computer Security*, 31(2), 172–198.
<https://doi.org/10.1108/ICS-10-2022-0156>
- Ringle, C. M., Sarstedt, M., Mitchell, R., & Gudergan, S. P. (2020). Partial least squares structural equation modeling in HRM research. *The International Journal of Human Resource Management*, 31(12), 1617–1643.
- Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS-SEM in "MIS Quarterly". *MIS Quarterly*, iii–xiv.
- Ringle, C. M., Wende, S., & Becker, J.-M. (2015). *SmartPLS 3. Bönningstedt: SmartPLS*.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.
<https://doi.org/10.1080/00223980.1975.9915803>
- Rogers W., R. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In *Social Psychophysiology: A Sourcebook* (pp. 153–177).
- Rojas, A., Vexo, F., Thalmann, D., Raouzaïou, A., Karpouzis, K., & Kollias, S. (2006). Emotional body expression parameters in virtual human ontology. *1st International Workshop on Shapes and Semantics*, 63–70.
- Rosch, E., Mervis, C. B., Gray, W. D., Johnson, D. M., & Boyes-Braem, P. (1976). Basic objects in natural categories. *Cognitive Psychology*, 8(3), 382–439.
- Rozin, P., Haidt, J., McCauley, C. R., Lewis, M., & Haviland-Jones, J. M. (2008). Handbook of emotions. In *Disgust*. (pp. 757–776). The Guilford Press.
- Rusbult, C. E., & Agnew, C. R. (2010). *Prosocial motivation and behavior in close relationships*.
- Russell, J. A. (1980). A circumplex model of affect. *Journal of Personality and Social Psychology*, 39(6), 1161.
- Russo, D., & Stol, K. J. (2021). PLS-SEM for software engineering research: An introduction and survey. *ACM Computing Surveys*, 54(4). <https://doi.org/10.1145/3447580>
- Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability (Switzerland)*, 15(12). <https://doi.org/10.3390/su15129426>
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, 53, 65–78. <https://doi.org/10.1016/j.cose.2015.05.012>
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70–82.
- Salem, M. A., & Sobaih, A. E. E. (2023). A Quadruple “E” Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education

- Students in Saudi Arabia amid COVID-19 Pandemic. *Electronics*, 12(10), 2268.
- Sandberg, J. (2015). *Human element of corporate espionage risk management: literature review on assessment and control of outsider and insider threats*.
- Sapolsky, R. M. (2004). *Why zebras don't get ulcers: The acclaimed guide to stress, stress-related diseases, and coping*. Holt paperbacks.
- Sarstedt, M., & Cheah, J.-H. (2019). *Partial least squares structural equation modeling using SmartPLS: a software review*. Springer.
- Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In *Handbook of market research* (pp. 587–632). Springer.
- Saunders et al. (2019). Research Methods for Business Students. In *Pearson* (8th ed., Issue 1). Financial Times Prentice Hall, Harlow.
[https://eclass.teicrete.gr/modules/document/file.php/DLH105/Research Methods for Business Students%2C 5th Edition.pdf](https://eclass.teicrete.gr/modules/document/file.php/DLH105/Research%20Methods%20for%20Business%20Students%2C%205th%20Edition.pdf)
- Scherer, K. R., Schorr, A., & Johnstone, T. (2001). *Appraisal processes in emotion: Theory, methods, research*. Oxford University Press.
- Schlomer, G. L., Bauman, S., & Card, N. A. (2010). Best practices for missing data management in counseling psychology. *Journal of Counseling Psychology*, 57(1), 1.
- Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). *Scientific knowledge of the human side of information security as a basis for sustainable trainings in organizational practices*.
- Schwarzer, R., & Fuchs, R. (1996). Self-efficacy and health behaviours. *Predicting Health Behavior: Research and Practice with Social Cognition Models*, 163(196), 9781315800820–10.
- Schwarzer, R., & Renner, B. (2000). Social-cognitive predictors of health behavior: action self-efficacy and coping self-efficacy. *Health Psychology*, 19(5), 487.
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.
- Seligman, M. E. ., & Csikszentmihaly, M. (2000). Positive Psychology An Introduction by Martin Seligman and Mihaly Csikzentmihalyi. In *American Psychologist Asociation* (Vol. 55, Issue 1, pp. 5–14).
- Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314–341.
- Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security*, 28(2), 293–318.
- Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviors among Employees. *International Journal of Academic Research in Business and Social Sciences*, 9(6), 560–571.
<https://doi.org/10.6007/ijarbss/v9-i6/5972>

- Sharabi, W. A. N. (2023). The Cybersecurity Practice in Saudi Universities to Protect the Intellectual Rights of Faculty Members' Publications. *International Journal of Instruction*, 16(4), 173–188. <https://doi.org/10.29333/iji.2023.16411a>
- Shariff, A. F., & Tracy, J. L. (2011). What are emotion expressions for? *Current Directions in Psychological Science*, 20(6), 395–399.
- Sharma, P. N., Liengaard, B. D., Hair, J. F., Sarstedt, M., & Ringle, C. M. (2022). Predictive model assessment and selection in composite-based modeling using PLS-SEM: extensions and guidelines for using CVPAT. *European Journal of Marketing*, ahead-of-print.
- Shaver, P., Schwartz, J., Kirson, D., & O'Connor, C. (1987). Emotion knowledge: further exploration of a prototype approach. *Journal of Personality and Social Psychology*, 52(6), 1061.
- Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers and Education*, 52(1), 92–100. <https://doi.org/10.1016/j.compedu.2008.06.011>
- Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer*, 10(4), 16.
- Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European Journal of Marketing*, 53(11), 2322–2347.
- Shweder, R. A., Haidt, J., Horton, R., & Joseph, C. (2010). The of Cultural the Emotions Psychology. *Handbook of Emotions*.
- Simons, P. (2009). Ontology meets ontologies: philosophers as healers. *Metascience*, 18(3), 469–473.
- Singhvi, P. A. S., Dhage, N. N., & Sharma, P. P. (2018). Compensation and Its Impact on Motivation Employee" s Satisfaction and Employee" s Performance. *International Academic Journal of Organizational Behavior and Human Resource Management*, 5(02), 1–43.
- Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations1. *MIS Quarterly*, 34(3), 487–502.
- Siponen, Mikko, Mahmood, M. A., & Pahnla, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224.
- Sleiman, F., & A Sayah, S. (2018). The Impact of Employees' Motivation On Employees' Productivity. *Available at SSRN 3793840*.
- Smith, C. A., & Lazarus, R. S. (1990). Emotion and adaptation. *Handbook of Personality: Theory and Research*, 21, 609–637.

- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339.
- Snyman, D. P., Kruger, H., & Kearney, W. D. (2018). I shall, we shall, and all others will: paradoxical information security behaviour. *Information and Computer Security*, 26(3), 290–305. <https://doi.org/10.1108/ICS-03-2018-0034>
- Song, S., Gao, N., Zhang, Y., & Ma, C. (2024). BRITD: behavior rhythm insider threat detection with time awareness and user adaptation. *Cybersecurity*, 7(1), 2.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225.
- Spidalieri, F., & Kern, S. (2014). *Professionalizing Cybersecurity: A path to universal standards and status*. 401. http://www.salve.edu/sites/default/files/filesfield/documents/JPME_Cyber_Leaders.pdf.
- Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin*, 124(2), 240.
- Stallings, W. (2020). *Computer security: Principles and practice* (4th ed.). Pearson.
- Stanley, R. O., & Burrows, G. D. (2001). Varieties and functions of human emotion. *Emotions at Work: Theory, Research and Applications in Management*, 3–19.
- Stanton, J. M., Stam, K. R., Mastrangelo, P. M., & Jolton, J. A. (2006). *Human-Computer Interaction in Management Information Systems (Chapter on Behavioral Information Security: An Overview, Results, and Research Agenda)*. Saddle River, NG: ME Sharpe.
- Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, 36(2), 111–133.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441–469.
- Strauss, A. (2009). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. In *Management Learning* (Vol. 31, Issue 4). Sage. <https://doi.org/10.1177/1350507600314007>
- Strongman, K. T. (1996). *The psychology of emotion: Theories of emotion in perspective*. John Wiley & Sons.
- Sue, V. M., & Ritter, L. A. (2012). *Conducting online surveys*. Sage.
- Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, 13(9), 413.
- Swartz, E., Money, A., Williams, B., & Remenyi, D. (2005). *Doing research in business and management: an introduction to process and method*. SAGE Publications Ltd.
- Sweigart, C. (2003). *Interested in learning more ? In sti tu te , A ut ho ins Il r igh*. Security

- 401, 1–39. <https://www.giac.org/paper/gsec/3907/introduction-computer-security-incident-response/106281>
- Symonds, P. M. (1924). On the Loss of Reliability in Ratings Due to Coarseness of the Scale. *Journal of Experimental Psychology*, 7(6), 456.
- Tabachnick, B. G., Fidell, L. S., & Ullman, J. B. (2013). *Using multivariate statistics* (Vol. 6). pearson Boston, MA.
- Talib, A. M., Alomary, F. O., Alwadi, H. F., & Albusayli, R. R. (2018). Ontology-based cyber security policy implementation in Saudi Arabia. *Journal of Information Security*, 9(4), 315–333.
- Tangney, J. P., Stuewig, J., & Mashek, D. J. (2007). Moral emotions and moral behavior. *Annu. Rev. Psychol.*, 58(1), 345–372.
- Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. *Computers and Security*, 109, 102401. <https://doi.org/10.1016/j.cose.2021.102401>
- Thapa, R. (2023). The Impact of Compensation towards Employees' Performance: Employees' Motivation as the Mediating Role. *The Spectrum*, 1(1), 79–95.
- Thompson, N., McGill, T., & Narula, N. (2024). “No point worrying” – The role of threat devaluation in information security behavior. *Computers and Security*, 143(September 2023). <https://doi.org/10.1016/j.cose.2024.103897>
- Thompson, R. A. (1994). Emotion regulation: A theme in search of definition. *Monographs of the Society for Research in Child Development*, 25–52.
- Thornton, D., & Turley, F. (2020). Dynamic Difficulty Adjustment in Cybersecurity Awareness Games: Analysis of Player Behavior and the Potential of Electroencephalography. *Innovations in Cybersecurity Education*, 3–17.
- Titchen, A., & Hobson, D. (2005). *Phenomenology*. In Somekh, Bridget and Cathy Lewin (eds.) *Research Methods in the Social Science*. Sage.
- Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys (CSUR)*, 51(2), 1–27.
- Tomkins, S. S. (1984). Affect theory. *Approaches to Emotion*, 163(163–195), 31–65.
- Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42–57.
- Topor, F. S. (2016). *Handbook of research on individualism and identity in the globalized digital age*. IGI Global.
- Torlak, N. G., Demir, A., & Budur, T. (2021). Using VIKOR with structural equation modeling for constructing benchmarks in the Internet industry. *Benchmarking: An International*

- Journal*, 28(10), 2952–2976.
- Tracy, J. L., & Robins, R. W. (2004). "Putting the Self Into Self-Conscious Emotions: A Theoretical Model." *Psychological Inquiry*, 15(2), 103–125.
- Trochim, W M K, & Donnelly, J. P. (2006). *The Research Methods Knowledge Base: Atomic Dog. Cincinnati, OH.*
- Trochim, William M K, & Donnelly, J. P. (2001). *Research methods knowledge base* (Vol. 2). Atomic Dog Pub. Macmillan Publishing Company, New York.
- Tugade, M. M., Fredrickson, B. L., & Barrett, L. F. (2004). Psychological resilience and positive emotional granularity: Examining the benefits of positive emotions on coping and health. *Journal of Personality*, 72(6), 1161–1190. <https://doi.org/10.1111/j.1467-6494.2004.00294.x>
- Tyng, C. M., Amin, H. U., Saad, M. N. M., & Malik, A. S. (2017). The influences of emotion on learning and memory. *Frontiers in Psychology*, 8, 235933.
- Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39.
- Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, 15(10), 2.
- Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts. *MIS Quarterly*, 39(2), 345–366.
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, 49(3–4), 190–198. <https://doi.org/10.1016/j.im.2012.04.002>
- Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, 9(4), 1–22.
- Venard, B. (2021). Cybersecurity behavior under covid-19 influence. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–9.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.
- Verizon. (2022). *Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), 576–586.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security.

- Computers & Security*, 38, 97–102.
- Walton, D. (2001). Abductive, presumptive and plausible arguments. *Informal Logic*, 21(2).
- Walton, N., & Chinnaswamy, A. (2022). Indian Tech 2.0-Digital Platforms, Cloud, AI and Cybersecurity. *Aston India Centre for Applied Research Conference*.
- Waly, N., Tassabehji, R., & Kamala, M. (2012). *Measures for improving information security management in organisations: the impact of training and awareness programmes*.
- Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20(3), 267–284.
- Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, 17(3), 194–215.
<https://doi.org/10.17705/1jais.00424>
- Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, 27(5), 781–799.
- Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of Personality and Social Psychology*, 54(6), 1063.
- Weber, R. (2004). The rhetoric of positivism versus interpretivism. *MIS Quarterly*, 28(1).
- Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii–xxiii.
- Weiner, B. (2012). *An attributional theory of motivation and emotion*. Springer Science & Business Media.
- Weiss, H. M., & Russell, C. (1996). Affective Events Theory. In *Research in organizational behavior* (Vol. 18, pp. 1–74).
- West, S. G., Finch, J. F., & Curran, P. J. (1995). *Structural equation models with nonnormal variables: Problems and remedies*.
- Whissell, C. (2009). Using the revised dictionary of affect in language to quantify the emotional undertones of samples of natural language. *Psychological Reports*, 105(2), 509–521.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.
- Wilbanks, L. (2007). Cybersecurity: Welcome to my world. *IT Professional*, 9(2), 61–64.
- Wiles, R., Crow, G., & Pain, H. (2011). Innovation in qualitative research methods: A narrative review. *Qualitative Research*, 11(5), 587–604.
- Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly: Management Information Systems*, 37(1), 1–20.

<https://doi.org/10.25300/MISQ/2013/37.1.01>

- Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4), 329–349.
- Wong, K. K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24(1), 1–32.
- Wong, K. K.-K. (2019). *Mastering partial least squares structural equation modeling (PLS-Sem) with Smartpls in 38 Hours*. IUiverse.
- Woon, I. M. Y., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. *International Journal of Human Computer Studies*, 65(1), 29–41. <https://doi.org/10.1016/j.ijhcs.2006.08.003>
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816. <https://doi.org/10.1016/j.chb.2008.04.005>
- Xu, F., Luo, X. (Robert), & Hsu, C. (2020). Anger or fear? Effects of discrete emotions on employee's computer-related deviant behavior. *Information and Management*, 57(3), 103180. <https://doi.org/10.1016/j.im.2019.103180>
- Xu, L., Lin, H., Pan, Y., Hui, R., & Chen, J. (2008). Constructing the Affective Lexicon Ontology. *Journal of The China Society for Scientific and Technical Information*, 27(2), 180–185.
- Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, 14(4), 998–1010.
- Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, 8(2), 34–42.
- Yoo, C. W., Sanders, G. L., & Cervený, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, 108(July 2017), 107–118. <https://doi.org/10.1016/j.dss.2018.02.009>
- Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, 24(1), 34.
- Zhao, Y., Yan, L., & Keh, H. T. (2018). The effects of employee behaviours on customer participation in the service encounter: The mediating role of customer emotions. *European Journal of Marketing*, 52(5–6), 1203–1222. <https://doi.org/10.1108/EJM-10-2016-0559>
- Zhen, J., Xie, Z., & Dong, K. (2020). Positive emotions and employees' protection-motivated behaviours: A moderated mediation model. *Journal of Business Economics and Management*, 21(5), 1466–1485. <https://doi.org/10.3846/jbem.2020.13169>
- Zhen, J., Xie, Z., Dong, K., & Chen, L. (2021). Impact of negative emotions on violations of

information security policy and possible mitigations. *Behaviour and Information Technology*, 41(11), 2342–2354. <https://doi.org/10.1080/0144929X.2021.1921029>

Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169–187.

Appendix A: Questionnaire (English)



Invitation

We would like to invite you to take part in a research study forming part of a PhD project for Abdulelah Alshammari. Before you decide if you would like to participate, take time to read the following information carefully and, if you wish, discuss it with others such as your family, friends or colleagues. If there is anything that is not clear or if you would like more information before you make your decision, please ask a member of the research team, whose contact details can be found at the end of this information sheet.

What is the purpose of the study?

This research project studies the effect of employees' emotions and reputation on their cybersecurity protection motivation behaviour in Saudi Arabia's higher education. Protection motivation behaviour means your cognitive processes regarding your intention to take preventive action in the face of cybersecurity threats. This research mainly aims to establish a model for measuring the emotional and reputation effects on employees' protection motivation in cybersecurity risks. This is through investigating the direct impact of negative emotions, positive emotions, and reputation on employees' cybersecurity protection motivation behaviour. Based on its expected results, this research will provide a clear understanding of the direct effects of emotions and reputation on employees' cybersecurity protection motivation. Thus, the results will have practical implications for the appropriate and academic fields.

Why have I been invited?

You are being invited to take part in this study because:

You are:

- Working at King Abdulaziz University as an academic or an administrator.
- Using a computer to achieve your work goals.

What will happen to me if I take part?

You will be invited to participate in a survey on the Qualtrics survey software. You will be asked to answer questions regarding your demographic profile, negative and positive emotions in

cybersecurity, reputational awareness in cybersecurity, self-efficacy, cybersecurity awareness, and how these factors can influence your protection motivation behaviour in cybersecurity. Please note that there is no right or wrong answer. I would appreciate it if you could spare 10-15 minutes of your time.

Do I have to take part?

No. It is up to you to decide whether or not you wish to take part. If you do decide to participate, you will be asked to provide informed consent. Your participation in this research is voluntary, and you are free to withdraw at any time during the study by closing down the browser, without giving a reason and without my legal rights being affected. However, you cannot withdraw your participation after submitting it. This is because the research is anonymous and removing a participant from the dataset is not possible, as the researcher cannot know which answers are yours.

Will my taking part in this study be kept confidential?

Yes. A code will be attached to all the data provide to maintain anonymity. Analysis of your data will be undertaken using coded data. The data that will be collected will be safe in line with the university guidelines on data and privacy protection, and their responses will be held strictly confidential and only reported in aggregate. The data will be protected by a strong password and changed every six months, and the data will be accessed by my supervisors only and the researcher.

What are the possible benefits of taking part?

There may be no direct benefit to you as a result. However, you will play a critical role in measuring the effect of employees' emotions and reputational on their cybersecurity protection motivation behaviour in Saudi Arabia higher education. I hope that the findings of this research will be valuable to the cybersecurity research field, which your participant will consider as part of this research.

What are the possible risks and burdens of taking part?

Your participation in this research will be anonymous; no information regarding your names and emails will be collected. Moreover, participating in the research is not anticipated to cause you any disadvantages or discomfort research.

What will happen to the results of the study?

The output of this research will be used in the PhD thesis of Abdulelah Alshammari. In addition, the results of this study may be published in scientific journals and/or presented at

conferences. Please provide your email on the consent form or contact the researcher via email, if you wish to receive the output of this research upon its completion.

What will happen to the results of the study?

The output of this research will be used in the PhD thesis of Abdulelah Alshammari. In addition, the results of this study may be published in scientific journals and/or presented at conferences. Please provide your email on the consent form or contact the researcher via email, if you wish to receive the output of this research upon its completion.

Expenses and payments

Who is funding the research?

The study is being funded by the Saudi Arabia Higher Education Ministry represented by the Saudi Arabia Cultural & Educational Bureau in London.

Who is organising this study and how is my data being used?

Aston University is organising this study and acting as data controller for the study. Research data will be used only for the purposes of the study or related uses identified in this Information Sheet or Appendix A.

Who has reviewed the study?

This study was given a favourable ethical opinion by the Business & Social Sciences (BSS) Research Ethics Committee.

What if I have a concern about my participation in the study?

If you have any concerns about your participation in this study, please speak to the researcher and he will do his best to answer your questions. Contact details can be found at the end of this information sheet. If the research team are unable to address your concerns or you wish to make a complaint about how the study is being conducted you should contact the Aston University Research Integrity Office at research_governance@aston.ac.uk or via the University switchboard on +44 (0)121 204 3000. Researcher email address: 190228569@aston.ac.uk

***Consent Form**

- I confirm that I have read and understand the Participant Information Sheet (Version 1, 14/10/2022) for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

- I understand that my participation is voluntary and that I am free to withdraw at any time during the study by closing down the browser, without giving a reason and without my legal rights being affected
 - I understand that this study is anonymous and that I am not able to withdraw after submitting my answers.
 - I agree to my anonymised data being used by research teams for future research.
- ☐ I have read the 'Participant Information Sheet and Consent Form', and I agree to take part in this study.

Section One: Demographic Profile

1. What is your gender?

- ☐ Male
☐ Female

2. What is your age?

- ☐ 18 to 29
☐ 30 to 39
☐ 40 to 49
☐ 50 to 59
☐ 60 and over

3. What is the highest level of education you have completed?

- ☐ High school
☐ Bachelor
☐ Diploma
☐ Master
☐ Doctor of Philosophy
☐ Other

4. What work position do you hold in your organisation?

- ☐ Academic
☐ Administrative

5. How many years of experience do you have?

- ☐ < 1 year
☐ 1-3 years
☐ 3-5 years
☐ 5-10 years
☐ More than 10 years
☐

Section Two: Negative emotions

Please indicate to what extent you agree with the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I feel discourage in protecting my organisation's information resources from security threats.							
I feel uneasy in protecting my organisation's information resources from security threats.							
I feel angry in protecting my organisation's information resources from security threats.							

Section Three: Positive emotions

Please indicate to what extent you agree with the following statements.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I feel happy when thinking about protecting my organisation's information resources.					
I feel excited when thinking about protecting my organisation's information resources.					
I feel satisfied when thinking about protecting my organisation's information resources.					
I feel interested in compliance with cybersecurity procedures to protect my organisation's information resources.					
I feel strong in countering and avoiding any threats to protect my organisation's information resources.					
I feel active in countering threats to protect my organisation's information resources.					
I feel determined to counter any threats to protect my organisation's information resources.					
I feel alert about any threats to protect my organisation's information resources.					
I feel proud to avoid any threats to protect my organisation's information resources.					

Section Four: Self-efficacy.

Please indicate to what extent you agree with the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree

I have the necessary skills to protect myself from cybersecurity violations							
I have the expertise to implement preventative measures to stop people from getting my confidential information							
I have the skills to implement preventative measures to stop people from damaging my work computer							
I believe that it is within my control to protect myself from cybersecurity violations							
I can enable security measures on my work computer but only when I have manuals for reference							

Section Five: Employees' Cybersecurity Awareness.

Please indicate to what extent you agree with the following statements.

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly agree
I am aware of the requirements for computer use policies at my workplace					
I am aware of the computer use policies at my workplace.					
I am aware of the impact that a virus and other malicious software can have on my computer system					
I am aware that virus protection software can identify and remove viruses					
I am aware that virus protection software requires frequent updates					
I am aware that I should keep my passwords secure					
I am aware of the impact of responding to phishing emails (e.g. unsolicited emails asking for your bank information)					
I am aware that encryption can prevent unauthorized access to confidential information of the vulnerabilities associated with sharing devices such as files and drives					

Section Six: Protection motivation behaviours

Please indicate to what extent you agree with the following statements.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
I actively attempt to protect my organization's information resources.					
I try to safeguard my organization's information resources from security threats.					
I purposefully defend my organization from information security threats to its resources.					

CERTIFIED TRANSLATION



ترجمة معتمدة

Taha Mohammed Al-Edreesi for Translation

مكتب طه محمد الحسن الإدريسي للترجمة

C.R: 4030279920

License No.: 720

Chamber of Commerce Membership No.: 228194

س.ت: ٤٠٣٠٢٧٩٩٢٠

ترخيص رقم: ٧٢٠

رقم عضوية الغرفة التجارية: ٢٢٨١٩٤



مكتب عالم الترجمة الاحترافية



AFFIDAVIT

Dr. Taha Al-Edrisi Certified - Translation Office in Jeddah, Kingdom of Saudi Arabia hereby does certify that the attached Document is a true and Complete Translation for the original text without any responsibility for the contents thereof.

شهادة

بهذا يشهد مكتب د. طه محمد الحسن الإدريسي للترجمة المعتمدة بجدة، المملكة العربية السعودية أن الوثيقة المرفقة هنا هي ترجمة صحيحة وكاملة للنص الأصلي - المرفق صورة منه مع الترجمة - دون أدنى مسئولية عن محتوياتها.



Dr. Taha Mohammed Al-Edrisi

د. طه محمد الإدريسي

المدير العام



دعوة

ندعوك للمشاركة معنا في دراسة بحثية تشكل جزءاً من مشروع الدكتوراه المقدمة من السيد/ عبدالاله الشمري. قبل أن تقرر ما إذا كنت ترغب في المشاركة، خذ وقتاً لقراءة المعلومات التالية بعناية، وإذا كنت ترغب في ذلك، ناقشها مع الآخرين مثل عائلتك أو أصدقائك أو زملائك. إذا كان هناك أي شيء غير واضح أو إذا كنت ترغب في مزيد من المعلومات قبل اتخاذ قرارك يرجى التواصل مع الباحث عبر الايميل الموضح في اخر الصفحة .

ما هو الغرض من الدراسة؟

يتطرق هذا المشروع البحثي إلى تأثير مشاعر الموظفين وسمعتهم على سلوكهم الدافع لحماية الأمن السيبراني في مؤسسات التعليم العالي في المملكة العربية السعودية. يهدف بشكل أساسي إلى إنشاء نموذج لقياس الآثار العاطفية والآثار المتعلقة بالسمعة تجاه دافع حماية الموظفين من مخاطر الأمن السيبراني. يتم ذلك من خلال التحقيق في التأثير المباشر لهذه العوامل على سلوكهم الدافع لحماية الأمن السيبراني. استناداً إلى النتائج المتوقعة، سيوفر هذا البحث فهماً واضحاً للتأثيرات المباشرة للمشاعر والسمعة على دوافع حماية الأمن السيبراني للموظفين. وبالتالي، فإن النتائج سيكون لها آثار قيمة على النطاق العملي والعلمي.

لماذا تمت دعوتي؟

تم دعوتك للمشاركة في هذه الدراسة للأسباب التالية:

- لأنك تعمل في جامعة الملك عبدالعزيز ك/ أكاديمي أو إداري
- لأنك تستخدم الحاسوب لتحقيق أهداف عملك

ماذا سيحدث لي إذا شاركت؟

سيُطلب منك الإجابة عن الأسئلة المتعلقة بملفك الشخصي، آثار المشاعر السلبية والإيجابية في الأمن السيبراني، والوعي بالسمعة في مجال الأمن السيبراني، والكفاءة الذاتية، والوعي بالأمن السيبراني، وكيف يمكن لهذه العوامل أن تؤثر على سلوكك الدافع للحماية في الأمن السيبراني. يرجى ملاحظة أنه لا توجد إجابة صحيحة أو خاطئة. ساكون ممثلاً لو أمكنك توفير 10-15 دقيقة من وقتك للإجابة على هذا الاستبانة.

هل يجب على المشاركة؟

لا، الأمر متروك لك لتقرير ما إذا كنت ترغب في المشاركة أم لا. إذا قررت المشاركة، فسيُطلب منك تقديم موافقة مستنيرة. مشاركتك في هذا البحث تطوعية، ولك مطلق الحرية في الانسحاب في أي وقت أثناء الدراسة عن طريق إغلاق المتصفح، دون إبداء سبب ودون المساس بحقوقك القانونية. للتتويه، لا يمكنك سحب مشاركتك بعد إرسالها. هذا لأن البحث مجهول الهوية وإزالة مشارك من مجموعة البيانات غير ممكن، حيث لا يستطيع الباحث معرفة الإجابات التي تخصك.

هل ستبقى مشاركتي في هذه الدراسة سرية؟

نعم. سيتم إرفاق رمز بجميع البيانات المقدمة للحفاظ على إخفاء الهوية. سيتم إجراء تحليل لبياناتك باستخدام البيانات المشفرة. ستكون البيانات التي سيتم جمعها آمنة بما يتماشى مع إرشادات الجامعة بشأن حماية البيانات والخصوصية، وستظل ردودكم سرية للغاية وسيتم الإبلاغ عنها بشكل إجمالي فقط. ستم حماية البيانات بكلمة مرور قوية وسيتم تغييرها كل ستة أشهر، وسيتم الوصول إلى البيانات من قبل المشرفين فقط والباحث .

ما هي الفوائد الممكنة من المشاركة؟

قد لا تكون هناك فائدة مباشرة لك نتيجة لذلك. ومع ذلك، ستلعب دوراً مهماً في قياس تأثير عواطف الموظفين وسمعتهم على سلوكهم الدافع لحماية الأمن السيبراني في التعليم العالي في المملكة العربية السعودية. أمل أن تكون نتائج هذا البحث ذات قيمة في مجال أبحاث الأمن السيبراني، وبالتالي مشاركتك تعتبر جزء من مساهمة هذا البحث

ما هي المخاطر والأعباء المحتملة للمشاركة؟



ستكون مشاركتك في هذا البحث مجهولة المصدر؛ لن يتم جمع أي معلومات بخصوص الأسماء ورسائل البريد الإلكتروني الخاصة بك. علاوة على ذلك، لا يُتوقع أن تسبب لك المشاركة في البحث أي عيوب أو بحث مزعج.

ماذا سيحدث لنتائج الدراسة؟

ستستخدم مخرجات هذا البحث في أطروحة دكتوراه للطالب عبدالإله الشمري. بالإضافة إلى ذلك، يمكن نشر نتائج هذه الدراسة في المجلات العلمية أو تقديمها في المؤتمرات.

من يمول البحث؟

يتم تمويل الدراسة من قبل وزارة التعليم العالي في المملكة العربية السعودية ممثلة في المكتب الثقافي والتعليمي السعودي في لندن.

من ينظم هذه الدراسة وكيف يتم استخدام بياناتي؟

تنظم جامعة أستون هذه الدراسة وتعمل كمراقب بيانات للدراسة. سيتم استخدام بيانات البحث فقط لأغراض الدراسة أو الاستخدامات ذات الصلة المحددة في ورقة المعلومات هذه أو الملحق أ.

من قيم هذه الدراسة؟

أعطيت هذه الدراسة رأياً أخلاقياً إيجابياً من قبل لجنة أخلاقيات البحث في العلوم الاجتماعية والتجارية.

ماذا لو كان لدي قلق بشأن مشاركتي في الدراسة؟

إذا كانت لديك أية مخاوف بشأن مشاركتك في هذه الدراسة، فيرجى التحدث إلى الباحث وسوف يبذل قصارى جهده للإجابة على أسئلتك. يمكن التواصل مع الباحث عبر البريد الإلكتروني الموضح في الأسفل. إذا كان فريق البحث غير قادر على معالجة مخاوفك أو كنت ترغب في تقديم شكوى حول كيفية إجراء الدراسة، فيجب عليك الاتصال بمكتب نزاهة الأبحاث بجامعة أستون على research_governance@aston.ac.uk أو عبر لوحة مفاتيح الجامعة على +44 (0) 121204 3000.

ايمل الباحث

Email address: 190228569@aston.ac.uk

*

نموذج الموافقة

- أؤكد أنني قد قرأت وفهمت صحيفة معلومات المشاركين (الإصدار 2، 2022/11/10) للدراسة المذكورة أعلاه.
- لقد أتيت لي الفرصة للنظر في المعلومات وطرح الأسئلة وتمت الإجابة على هذه الأسئلة بشكل مرض.
- أفهم أن مشاركتي طوعية وأنني حر في الانسحاب في أي وقت أثناء الدراسة عن طريق إغلاق المتصفح، دون إبداء أسباب ودون المساس بحقوق القانون.
- أفهم أن هذه الدراسة مجهولة المصدر وأنني لا أستطيع الانسحاب بعد تقديم إجاباتي.
- أوافق على استخدام بياناتي مجهولة المصدر من قبل فرق البحث للبحث في المستقبل.

□ أؤكد أنني قد قرأت وفهمت ورقة معلومات المشاركين وقمت بتوقيع نموذج الموافقة"، وأوافق على المشاركة في

القسم الأول: النمط الديموغرافي

1- ما هو جنسك؟

☐ ذكر

☐ أنثى

2- ما هو عمرك؟



- ٢٩ إلى ١٨ ☐
- ٣٩ إلى ٣٠ ☐
- ٤٩ إلى ٤٠ ☐
- ٥٩ إلى ٥٠ ☐
- ٦٠ وما فوق ☐

3- ما هو أعلى مستوى تعليمي أكملته؟

- التعليم الثانوي ☐
- البكالوريوس ☐
- دبلومة ☐
- درجة الماجستير ☐
- درجة الدكتوراة ☐
- أخرى ☐

4- ما الوظيفة التي تشغلها في مؤسستك؟

- أكاديمية ☐
- إدارية ☐

5- كم عدد سنوات الخبرة لديك؟

- ١ سنة ☐
- 3-1 سنين ☐
- 5-3 سنين ☐
- 10-5 سنين ☐
- أكثر من 10 سنوات ☐

القسم الثاني: المشاعر السلبية

يرجى توضيح إلى أي مدى توافق على كل من العبارات التالية

أوافق بشدة	أوافق	أوافق لحد ما	لا أوافق ولا أختلف	لا أوافق إلى حد ما	أختلف	أختلف بشدة	
							أشعر بالإحباط في حماية بيانات موارد مؤسستي من التهديدات الأمنية.
							أشعر بالقلق في حماية بيانات موارد مؤسستي من التهديدات الأمنية.



							أشعر بالغضب في حماية بيانات موارد مؤسستي من التهديدات الأمنية.
--	--	--	--	--	--	--	---

القسم الثالث: المشاعر الإيجابية

يرجى توضيح إلى أي مدى توافق على كل من العبارات التالية

أوافق بشدة	أوافق	لا أوافق ولا أختلف	أختلف	أختلف بشدة	
					أشعر بالسعادة عندما أفكر في حماية بيانات موارد مؤسستي.
					أشعر بالإثارة عندما أفكر في حماية بيانات موارد مؤسستي.
					أشعر بالرضا عندما أفكر في حماية بيانات موارد مؤسستي.
					أشعر بالاهتمام بالامتثال لإجراءات الأمن السيرياني لحماية بيانات موارد مؤسستي.
					أشعر بقوة في مواجهة أي تهديدات وتجنبها لحماية بيانات موارد مؤسستي.
					أشعر بنشاط في مواجهة أي تهديدات لحماية بيانات موارد مؤسستي.
					أشعر بإصرار على مواجهة أي تهديدات لحماية بيانات موارد مؤسستي.
					أشعر بالهذر بشأن أي تهديدات لحماية بيانات موارد مؤسستي.
					أشعر بالفخر في مواجهة أي تهديدات وتجنبها لحماية بيانات موارد مؤسستي.

القسم الرابع: الكفاءة الذاتية

يرجى توضيح إلى أي مدى توافق على كل من العبارات التالية

أوافق بشدة	أوافق	أوافق لحد ما	لا أوافق ولا أختلف	لا أوافق إلى حد ما	أختلف	أختلف بشدة	
							أتمتع بمهارات ضرورية لحماية نفسي من انتهاكات الأمن السيرياني
							أتمتع بخبرة في تنفيذ التدابير الوقائية لتجنب الإفصاح عن معلوماتي السرية
							أتمتع بالمهارات في تنفيذ التدابير الوقائية لمنع الأشخاص من اتلاف جهاز الحاسب الآلي الذي أعتمد عليه في عملي.
							أعتقد أنه من اختصاصي حماية نفسي من انتهاكات الأمن السيرياني



						يمكنني تفعيل إجراءات الأمان على كمبيوتر العمل الخاص بي في حال الاحتفاظ بنسخة من المراجع.
--	--	--	--	--	--	--

القسم الخامس: توعية الموظفين بالأمن السيبراني.

يرجى توضيح إلى أي مدى توافق على كل من العبارات التالية

أوافق بشدة	أوافق	لا أوافق أو أختلف	أختلف	أختلف بشدة	
					أنا على دراية بمتطلبات سياسات استخدام الكمبيوتر في مكان عملي.
					أنا على دراية بسياسات استخدام الكمبيوتر في مكان عملي.
					أنا على دراية بالتأثير الذي قد يحدث لنظام جهاز الكمبيوتر الخاص بي من الفيروس والبرامج الضارة الأخرى.
					أدرك أن برامج الحماية من الفيروسات يمكنها التعرف على الفيروسات والتخلص منها
					أدرك أن برامج الحماية من الفيروسات تتطلب تحديثات متكررة
					أدرك أنه يجب تأمين كلمات المرور الخاصة بي
					أنا على دراية بتأثير الرد على رسائل البريد الإلكتروني الاحتمالية (مثل رسائل البريد الإلكتروني غير المرغوب فيها التي تطلب بيانات حسابك المصرفي)
					أدرك أن التشفير يمنع الوصول غير المصرح به إلى المعلومات السرية الخاصة بالثغرات الأمنية المرتبطة بمشاركة الأجهزة مثل الملفات ومحركات الأقراص

القسم السادس: سلوكيات تحفيز الحماية

يقصد بسلوك دافع الحماية الإجراءات المعرفية فيما يتعلق بنيتك في اتخاذ إجراءات وقائية في مواجهة تهديدات الأمن السيبراني.

يرجى توضيح إلى أي مدى توافق على كل من العبارات التالية

أوافق بشدة	أوافق	لا أوافق ولا أختلف	أختلف	أختلف بشدة	
					أحاول بنشاط حماية بيانات موارد مؤسستي.
					أحاول حماية بيانات موارد مؤسستي من التهديدات الأمنية.
					أدافع بشكل هادف عن موارد مؤسستي لحمايتها من تهديدات أمن المعلومات.



Appendix C: Ethical Approval



Aston University
Aston Triangle
Birmingham
B4 7ET
0121 204 3000

Date: 14th November 2022

Abdulelah Alshammari
Copy: **Vladlena Benson; Luciano Batista**
College of Business and Social Sciences

Dear Abdulelah Alshammari,

Study title:	Establish a Model for Measuring the Effect of Employees' Emotions and Reputation on their Cybersecurity Protection Motivation Behaviour in Saudi Arabia Higher Education
REC REF:	#BSS21012

Confirmation of Ethical Opinion

On behalf of the Committee, I am pleased to confirm a favourable opinion for the above research on the basis described in the application form, protocol and supporting documentation listed below.

Approved documents

The final list of documents reviewed and approved by the Committee is as follows:

Document	Version	Date
Ethics Application Form	2	11/11/2022
Participant Information Sheet	2	11/11/2022
Consent Form	2	11/11/2022
Questionnaire	2	11/11/2022
Letter of commitment	N/A	04/09/2022

With the Committee's best wishes for the success of this project.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Alexis Paton", with a long horizontal stroke extending to the right.

Dr Alexis Paton
Chair of the Business & Social Sciences Research Ethics Committee

Appendix D: Approvals From King Abdulaziz University

KINGDOM OF SAUDI ARABIA

Ministry of Higher Education

KING ABDULAZIZ UNIVERSITY

Faculty of Economics & Administration



6952000 - 6400000 Fax: 6401667



P.O. Box 80201 Jeddah 21589



المملكة العربية السعودية
وزارة التعليم العالي
جامعة الملك عبد العزيز
كلية الاقتصاد والإدارة

٦٤٠١٦٦٧ فاكس ٦٤٠٠٠٠٠ - ٦٩٥٢٠٠٠



ص.ب ٨٠٢٠١ جدة ٢١٥٨٩



Re: Mr. Abdulelah Alshammari

Date: Sep 4, 2022

To whom it may concern

I am pleased to endorse Mr. Abdulelah Alshammari's endeavours to pursue his data collection at King Abdulaziz University, and I would like to confirm that the Department of Management Information Systems (MIS) at the Faculty of Economics and Administration will support, guide, and facilitate Mr. Alshammari's data collection during his time in Saudi Arabia.

Would you require any further details, please feel free to contact me.

Sincerely Yours

Dr. Mohammad Y. Sarhan

Assistant Professor of Information System

Chair of Management Information Systems Department

Faculty of Economics and Administrations

King Abdul Aziz university

Email: mysarhan@kau.edu.sa

Attachment: المرفقات :

Date: / / التاريخ :

Number: الرقم :

Appendix E: Formal Letter of King Abdulaziz University's Deanship of Scientific Research

KINGDOM OF SAUDI ARABIA

Ministry of Higher Education

KING ABDULAZIZ UNIVERSITY

Faculty of Economics & Administration



المملكة العربية السعودية
وزارة التعليم العالي
جامعة الملك عبد العزيز
كلية الاقتصاد والإدارة

6952000 - 6400000 Fax: 6401667

P.O. Box 80201 Jeddah 21589

٦٤٠١٦٦٧ فاكس ٦٤٠٠٠٠٠ - ٦٩٥٢٠٠٠

ص.ب ٨٠٢٠١ جدة ٢١٥٨٩

سعادة وكيل الكلية للدراسات العليا والبحث العلمي المكلف

حفظه الله

السلام عليكم ورحمة الله وبركاته...

يطيب لقسم نظم المعلومات الإدارية ان يهدي سعادتك اطيب التحية والتقدير، ونشير إلى احالتكم لخطاب سعادة عميد البحث العلمي المكلف رقم: ٢٠٨٠٠٤/٤٤١٠٨٠٠٢ وتاريخ: ١٩/١٠/١٤٤٤هـ بشأن آلية التعامل مع طلبات تسهيل مهام الباحثين من داخل الجامعة.

عليه نرفق لسعادتك الطلب المقدم من عضو القسم المبتعث: أ. عبد الاله بن سليمان الشمري، وفقا للنموذج المطلوب، متضمنا موافقة لجنة اخلاقيات البحث في جامعة استون بمقر البعثة.

عليه نأمل من سعادتك التفضل بالاطلاع والتكرم بمخاطبة عمادة البحث العلمي لتسهيل نشر استبيان المبتعث لمنسوبي ومنسوبات الجامعة.

وتقبلوا خالص التحية والتقدير على جهودكم الكريمة،،،

رئيس قسم نظم المعلومات الإدارية

د. محمد بن ياسين سرحان



Encl: التوقيع Date: ٢٤٤/١٠/١٩ التاريخ Ref: ٤٤١٨٠٠٢/٤٤٤ الرقم

تعميم

الموضوع: بشأن نموذج تسهيل مهمة

حفظهم الله

سعادة عمداء وعميدات الكليات - المعاهد

السلام عليكم ورحمة الله وبركاته

عمادة البحث العلمي تهدي سعادتكم أطيب التحايا والتقدير، وإشارة إلى خطاب سعادة وكلية عمادة البحث العلمي رقم ٤٤١٨٠٠٢ بتاريخ ١٧/١٠/١٤٤٤ هـ، المشار فيه إلى ما يرد للعمادة من طلبات تسهيل مهام الباحثين من داخل وخارج الجامعة. وحرصاً على الاستمرار في تطوير إجراءات العمل بعمادة البحث العلمي، نرفق لسعادتكم نموذج تسهيل نشر أداة بحثية.

عليه نأمل تكرم سعادتكم بتعميم النموذج المرفق على الباحثين من أعضاء هيئة التدريس الراغبين بطلب "تسهيل مهمة" ليتسنى لنا اكمال اللازم مع شرط موافقة لجنة اخلاقيات البحث العلمي في الجامعة المعنية.

وتقبلوا خالص تحياتي وتقديري

عميد البحث العلمي المكلف

د/ سعيد بن علي باديش

١٠/١٨

صورة مع التحية ل: مكتبنا.

شعبه القدرى / ١٤٤٤ هـ





Encl : : المرفقات Date : 17/10/1444 التاريخ Ref : 44108002 الرقم :

حفظه الله

سعادة عميد عمادة البحث العلمي المكلف

السلام عليكم ورحمة الله وبركاته،،،

تهديكم عمادة البحث العلمي أطيب التحية والتقدير، وإشارة إلى ما يرد للعمادة من طلبات تسهيل مهام الباحثين من داخل وخارج الجامعة، وعدم تضمينها بعض البيانات الخاصة بالبحث، ووسائل التواصل مع مقدم الطلب، ورغبة منا في تنظيم المهام الادارية لوحدة الخدمات البحثية في العمادة
نأمل من سعادتك التكرم بتوجيه من يلزم بالتعميم بإرفاق نموذج تسهيل نشر أداة بحثية وفقا للنموذج المرفق أدناه إضافة إلى موافقة لجنة أخلاقيات البحث في الجامعة المعنية، ليتسنى لنا اكمال اللازم.

اسم الباحث	عبدالله سليمان عجلان الشمري
اسم الجامعة	Aston University
البريد الإلكتروني	190228569@aston.ac.uk
رقم الجوال	0543251888
عنوان البحث بالعربي	تأثير مشاعر الموظفين وسمعتهم على سلوكهم الدافع لحماية الأمن السيبراني
الفئة المستهدفة	موظفي جامعة الملك عبدالعزيز
الرابط الالكتروني للاستبيان	https://astonbusinessschool.qualtrics.com/jfe/form/SV_ewywi9gJn56wwYK?jfe=new
الباركود للاستبيان	

وتفضلوا بقبول فائق التحية والتقدير،،،

وكيلة عمادة البحث العلمي
١٤٤٤/١٠/١٧
د. ريم بنت عبد العزيز الثانية



Appendix F: King Abdulaziz University Email Survey



جامعة الملك عبد العزيز 5 Jul



to جامعة ^

From webmaster@kau.edu.sa جامعة الملك عبد العزيز

To webmaster@kau.edu.sa جامعة الملك عبد العزيز

Date 5 Jul 2023 at 7:16 AM



Standard encryption (TLS)

[Learn more](#)



تهديكم عمادة البحث العلمي أطيب التحايا ونأمل منكم التجاوب
في دعم الباحث بالمشاركة في تعبئة الاستبيان المرفق
عنوان البحث

تأثير مشاعر الموظفين وسمعتهم
على سلوكهم الدافع لحماية الامن السيبراني

https://cutt.us/dsr_4



شاكرين ومقدرين دعمكم للبحث العلمي والتطوير
وحدة الخدمات البحثية - عمادة البحث العلمي بشرط الطالبات
dsrw@kau.edu.sa للتواصل

IMPORTANT: PLEASE DO NOT REPLY TO THIS EMAIL. If you need assistance email dsrw@kau.edu.sa

هام : برجاء عدم الرد على هذا البريد . للتواصل يرجى المراسله على البريد

dsrw@kau.edu.sa

استبانة الباحث عبدالاله سليمان الشمري البريد الوارد x

☆ 11:03 من (قبل 4 ساعات)

جامعة الملك عبد العزيز <webmaster@kau.edu.sa>

جامعة



تهديكم عمادة البحث العلمي أطيب التحايا
ونأمل منكم تكرماً دعم الباحثين بالمشاركة في تعبئة الاستبيان المرفق

عنوان البحث

تأثير مشاعر الموظفين وسمعتهم على سلوكهم الدافع لحماية الامن السيبراني

الباركود



شاكرين ومقدرين دعمكم للبحث والتطوير

مع تحيات وحدة الخدمات البحثية بعمادة البحث العلمي
تحويلة 40127

