



**University of  
Nottingham**  
UK | CHINA | MALAYSIA

# **The Influence of Usable Security on Security Culture**

Thesis submitted to the University of Nottingham for the degree of  
**Doctor of Philosophy, January 2025**

Wesam Fallatah

20205841

Supervised by

Prof. Steven Furnell

Prof. Christian Wagner

# Abstract

Cybersecurity threats are becoming more complex, and organizations must implement security measures that are technically robust and practical. The lack of usability of these measures can lead to uncompliant behavior, risky workarounds, and a weak security culture, making the organization susceptible to security breaches. To improve cybersecurity posture and resilience, organizations need to understand and strengthen their security culture.

This study adopts a mixed-method approach to explore the influence of usable security on security culture. It centers on three core objectives. First, it seeks to understand the concepts of usability, usable security, and security culture by examining their representation in studies and authoritative sources. It also formulates a comprehensive set of definitions to identify the factors that influence these key elements. Second, it aims to characterize the relationship between usable security and security culture by framing the study variables and investigating whether usable security can positively impact security culture, drawing on both quantitative and qualitative analyses. To achieve this, a survey was conducted with over 200 participants, followed by interviews with a smaller sub-population. The study then employed statistical descriptive analysis and thematic analysis to understand the relationship between usable security and security culture. Third, it sought to design a means that leverages the influence of usable security, identifying specific areas where usability improvements can promote a stronger and positive security culture.

A thorough review of previous and related studies informs the study's direction and methodology, laying the groundwork for developing the instruments required to investigate the impact of usable security on security culture. An important outcome of this research is the development of a framework for fostering a strong security culture by employing usable security alongside other necessary elements. This framework, which forms a key contribution to the study, was validated by two groups: participants who completed the survey and interviews and a group of experts. The validation process highlighted the framework's practical value and contributed to enhancing the framework's clarity, presentation, and potential for integration.

The research intends that organizations may overcome pitfalls that hinder the development of a positive security culture by establishing a structured approach that addresses common usability barriers. Ultimately, the study has the potential to help organizations achieve greater compliance, reduce cybersecurity risks, and enhance their resilience to evolving threats.

# Acknowledgments

First and foremost, I am profoundly grateful to God, the Almighty, for granting me the strength to complete my PhD studies. I dedicate this work to my beloved parents, whose unwavering faith in me has been my cornerstone. They tirelessly encouraged me to strive for excellence, and I am beyond grateful for their endless support, prayers, and sacrifices. This PhD is but a single drop in the vast ocean of dedication they have given me.

To my wife and children: your love, patience, and support have been my guiding light throughout this journey. You are my foundation. You are my greatest source of motivation. This achievement is as much yours as it is mine.

To my sisters and brothers, who have cheered me every step of the way: your encouragement and belief in my potential have meant the world to me. You are a reminder that success is never a solitary endeavor, and I am fortunate to have you by my side.

My deepest gratitude to my supervisor, Prof. Steven Furnell, whose continuous and thoughtful guidance has been instrumental in shaping my research. Your mentorship has been both inspiring and delightfully memorable. I have learned so much from you, both academically and in life, and I will carry those lessons forward with pride and gratitude. My sincere thanks also go to Prof. Christian Wagner and Dr Ying He, who were part of my supervisory team. I would also like to sincerely thank Dr Joakim Kävrestad for the collaboration during my PhD, which greatly contributed to my research. Your insights and support have been an invaluable part of this journey.

To my colleagues in the CybSec research group: thank you for the many great memories and the bond we shared. Your companionship made this journey as enriching personally as it was professionally.

I also wish to express my appreciation to the study participants for providing their valuable insight and to members of the Human-centered Cybersecurity (HCC) group, whose contributions were critical in evaluating key aspects of my research. Your time and efforts were invaluable to this work.

Finally, I would like to acknowledge the support of the Ministry of Education in Saudi Arabia, whose scholarship made this study possible. I am grateful for the opportunity provided by this sponsorship.

# Publications

## **Refining the Understanding of Usable Security**

*Fallatah, W., Furnell, S. and He, Y., 2023, July. Refining the Understanding of Usable Security. In International Conference on Human-Computer Interaction (pp. 49-67).*

## **Cybersecurity Training Acceptance: A Literature Review**

*Kävrestad, J., Fallatah, W. and Furnell, S., 2023, July. Cybersecurity training acceptance: A literature review. In International symposium on human aspects of information security and assurance (pp. 53-63). Cham: Springer Nature Switzerland.*

## **Establishing a Model for the User Acceptance of Cybersecurity Training**

*Fallatah, W., Kävrestad, J., & Furnell, S. (2024). Establishing a Model for the User Acceptance of Cybersecurity Training. Future Internet, 16(8), 294.*



# Table of Contents

Chapter 1: Introduction .....	1
1.1 Introduction .....	2
1.2 Aim and Objectives .....	4
1.3 Thesis Structure .....	5
 Chapter 2: Exploring Security Culture.....	7
2.1 Introduction .....	8
2.2 Security Culture Definition .....	8
2.3 Security Culture Influential Factors .....	10
2.4 Measuring Security Culture.....	14
2.5 Chapter Summary .....	19
 Chapter 3: Cybersecurity Training .....	20
3.1 Introduction .....	21
3.2 Socio-technical Perspectives on User Acceptance of Cybersecurity Training.	21
3.3 Categorization of Studies that Discussed the Socio-technical Dimensions .....	23
3.3.1 Technical Dimensions .....	24
3.3.2 Organizational Dimension .....	25
3.3.3 User-centered dimension .....	25
3.4 A Model for Cybersecurity Training Acceptance .....	26
3.4.1 Components and Evolution of TAM and its Extensions.....	27
3.4.2 Literature Assessment Methodology .....	29
3.4.3 Results.....	31
3.4.4 Discussion.....	36
3.5 Chapter Summary .....	38

Chapter 4: Defining and Framing Usable Security .....	40
4.1 Introduction .....	41
4.2 Defining Usability .....	41
4.3 Current Usable Security Representation .....	49
4.4 Usable Security Definition and Framework .....	53
4.5 Chapter Summary .....	56
 Chapter 5: Investigating Usable Security and Security Culture in Organizational Settings.....	 57
5.1 Introduction .....	58
5.2 Data Collection Methods.....	58
5.2.1 Survey Design and Implementation.....	59
5.2.2 Semi-Structured Interviews .....	61
5.2.3 Ethical Considerations and Approval .....	62
5.2.4 Pilot Study.....	62
5.2.5 Participant Recruitment Techniques .....	63
5.3 Data Analysis Approaches .....	66
5.3.1 Quantitative Data Analysis .....	67
5.3.2 Qualitative Data Analysis .....	74
5.4 Chapter Summary .....	79
 Chapter 6: Quantitative Analysis and Findings.....	 81
6.1 Introduction .....	82
6.2 Survey Quantitative Findings.....	82
6.2.1 Participants' Demographic.....	82
6.2.2 Dimensions of Security Culture.....	94

6.2.3 Aspects of Usable Security .....	96
6.2.4 Impact of Usable Cybersecurity on Organisational Security Culture.....	104
6.2.5 Motivators for Cybersecurity Best Practices .....	105
6.2.6 Barriers to Cybersecurity Compliance.....	106
6.3 Hypotheses Testing Results .....	108
6.4 Chapter Summary .....	136
 Chapter 7: Qualitative Analysis and Findings.....	 137
7.1 Introduction .....	138
7.2 Findings from the Survey .....	138
7.3 Findings from the Semi-structured Interviews .....	149
7.4 Chapter Summary .....	155
 Chapter 8: Developing a Usability-focused Security Culture Framework .....	 156
8.1 Introduction .....	157
8.2 Insights from the Quantitative Findings.....	157
8.2.1 Survey Findings .....	157
8.2.2 Hypotheses Testing .....	158
8.3 Insights from Qualitative Findings.....	160
8.3.1 Open-ended Responses .....	160
8.3.2 Semi-structure Interviews .....	161
8.4 Overview of Issues Identified in Study Findings and Recommended Solutions .....	162
8.5 Introducing a Usability-focused Security Culture Framework .....	167
8.6 Framework Implementation Guidelines .....	169
8.7 Case Study Application .....	171
8.8 Chapter Summary .....	176

Chapter 9: Framework Evaluation .....	177
9.1 Introduction .....	178
9.2 Evaluators Recruitment .....	178
9.3 The Evaluation Process .....	180
9.4 Analysis and Reflection on the Evaluators' Feedback .....	181
9.4.1 Theme 1: Alignment with Key Issues and Practical Value .....	181
9.4.2 Theme 2: Clarity and Presentation.....	182
9.4.3 Theme 3: Scalability and Integration.....	183
9.4.4 General Reflection .....	188
9.5 Chapter Summary .....	188
 Chapter 10: Conclusions .....	189
10.1 Summary of Research Achievements and Contributions .....	190
10.2 Limitations of the research .....	196
10.3 Directions for Future Work.....	197
10.4 The Importance of Security Culture and Usable Security .....	198
 <b>References</b> .....	199
 <b>Appendices</b> .....	214
Appendix I: Ethical Approval.....	214
Appendix II: Survey .....	229
Appendix III: Interview Plan .....	249
Appendix IV: Feedback for the validation process .....	251
Appendix V: Posters & Flyers .....	259

## List of Tables

Table 2.1: Security Culture Definitions .....	9
Table 2.2: Security Culture Influential Factors Presented in Studies.....	12
Table 2.3: Measuring Approaches of Security Culture .....	15
Table 3.1: Categorization of Studies that Discussed the Socio-technical Dimensions .....	23
Table 3.2: Included publications and factors discussed .....	33
Table 4.1: Usability Definitions and Key Aspects .....	46
Table 4.2: Usable Security Definitions and the Key Aspects.....	51
Table 5.1: Pilot Participants .....	63
Table 5.2: SPSS Scale Reversal .....	74
Table 6.1: H1 <sub>A</sub> Overview .....	109
Table 6.2: H1 <sub>A</sub> Normality Test .....	109
Table 6.3: Q14 and Q16 Correlation .....	110
Table 6.4: Correlation of the individual items from Q14 and Q16 .....	111
Table 6.5: Correlation of H1 <sub>A</sub> Variables Based on the Employees Departments.....	118
Table 6.6: Correlation of Employees in Cybersecurity Dept. ....	118
Table 6.7: Correlation of Employees in IT Dept including Cybersecurity (if applicable) .....	118
Table 6.8: Correlation of Employees in Departments Other Than the Cybersecurity or IT Dept .....	119
Table 6.9: Employees who Selected Other .....	119
Table 6.10: Residuals Statistics for H1 <sub>A</sub> .....	120
Table 6.11: Model Summary of H1 <sub>A</sub> with Q16's Mean Being the Dependent Variable .....	120
Table 6.12: Correlation Coefficients (Dependent Variable: Q16 Mean).....	121
Table 6.13: Model Summary of H1 <sub>A</sub> with Q14's Mean Being the Dependent Variable .....	122
Table 6.14: Correlation Coefficients (Dependent Variable: Q14 Mean).....	122
Table 6.15: H2 <sub>A</sub> Overview .....	124
Table 6.16: H2 <sub>A</sub> Normality Test .....	124
Table 6.17: H2 <sub>A</sub> Test Summary .....	125
Table 6.18: H3 <sub>A</sub> Overview .....	128
Table 6.19: Model Summary of Q16's Mean Being the Independent Variable and Q11 the Dependent Variable .....	128
Table 6.20: Summary of H3 <sub>A</sub> 's ANOVA Test.....	129
Table 6.21: H3 <sub>A</sub> 's Correlation Coefficients (Dependent Variable: Cybersecurity Compliance).....	129
Table 6.22: H4 <sub>A</sub> Overview .....	131
Table 6.23: H4 <sub>A</sub> 's Prediction Classification Table .....	131
Table 6.24: H4 <sub>A</sub> 's Model Coefficients.....	132
Table 6.25: H4 <sub>A</sub> 's Variable in the Equation .....	132
Table 6.26: H5 <sub>A</sub> Overview .....	133
Table 6.27: H5 <sub>A</sub> 's Model Summary.....	134

Table 6.28: Summary of H5 <sub>A</sub> 's ANOVA Test.....	134
Table 6.29: H5 <sub>A</sub> 's Correlation Coefficients (Dependent Variable: Identifying and Reporting Cybersecurity Incidents) .....	135
Table 7.1: Interviews Participant Demographics .....	149
Table 8.1: Identified Themes and Subthemes of the Open-Ended Responses .....	160
Table 9.1: Participant Demographics for the Validation Process .....	179

# List of Figures

Figure 2.1: The number of Factors Influencing Security Culture .....	12
Figure 2.2: Security Culture Dimensions Scores (KnowBe4, 2020) .....	18
Figure 3.1: Technology Acceptance Model (TAM) and its External Factors .....	27
Figure 3.2: PRISMA flow diagram outlining the searching and screening process ..	31
Figure 3.3: Cybersecurity Training Acceptance Model (CTAM) .....	35
Figure 4.1: The Total Percentage of the Usability Key Aspects Iteration in Studies .	48
Figure 4.2: Word Cloud Denoting Prominence of Words Relating to Usability .....	48
Figure 4.3: The Total Percentage of the Usable Security Key Aspects Occurrence in Studies .....	52
Figure 4.4: Word Cloud Denoting Prominence of Words Relating to Usable Security .....	52
Figure 4.5: Usable Security Framework .....	54
Figure 5.1: Participant Recruitment Flowchart .....	65
Figure 5.2: Respondent Progress .....	66
Figure 5.3: Summary of Research Design .....	80
Figure 6.1: Age Distribution Among Participants .....	82
Figure 6.2: Educational Attainment Levels of Participants .....	84
Figure 6.3: Percentage of Participants with Disabilities Affecting Technology Use .	85
Figure 6.4: Participants' Roles/Positions within Their Organisations .....	87
Figure 6.5: Participant Distribution Across Organisational Departments .....	88
Figure 6.6: Primary Industries Represented by Participants' Organisations .....	90
Figure 6.7: Geographic Distribution of Participants' Organisations .....	91
Figure 6.8: Distribution of Participants' Organisation Sizes .....	93
Figure 6.9: Participant Agreement on the Impact of Shared Attitudes, Behaviours, and Beliefs about Cybersecurity within Their Organisation Promoting Shared Responsibility for Maintaining Cybersecurity .....	94
Figure 6.10: Participants' Confidence Levels in Various Aspects of Cybersecurity Competence .....	95
Figure 6.11: Percentage of Participants' Encounters with Usability Issues in Cybersecurity Technologies and Procedures within Their Organisation .....	96
Figure 6.12: Likelihood of Participants' Responses to Difficult Cybersecurity Actions .....	97
Figure 6.13: Percentage of Participant Bypassing of Cybersecurity Measures Due to Usability Issues .....	99
Figure 6.14: Participant Agreement with Usability Statements on Cybersecurity Measures .....	100
Figure 6.15: Reporting and Resolution of Cybersecurity Issues .....	102
Figure 6.16: Participant Agreement with Statements on the Impact of Usable Cybersecurity on Organisational Security Culture .....	104
Figure 6.17: Key Motivators Encouraging Participants to Follow Cybersecurity Best Practices .....	105
Figure 6.18: Factors Hindering Participant Adherence to Cybersecurity Best Practices .....	106
Figure 6.19: Difference between the Participants' "Yes" and "No" Participants Responses to the Security and Usability Balance Perspective .....	126

Figure 6.20: Difference between the Participants' "Yes" and "No" Participants Responses about the Organizational Support for Cybersecurity.....	127
Figure 8.1: Mediating Strategies .....	165
Figure 8.2: Usability-focused Security Culture Framework .....	168
Figure 8.3: Framework implementation Phases.....	171
Figure 9.1: Usability-focused Security Culture Framework .....	183



## Glossary of Abbreviations

BI	Behavioral Intention
BYOD	Bring Your Own Device
COVID-19	Coronavirus
CTAM	Cybersecurity Training Acceptance Model
HCI	Human-Computer Interaction
HRM	Human Risk Management
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
MPCU	The Model of PC Utilization
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
SA&T	Security Awareness and Training
SCT	Social Cognitive Theory
SETA	Security Education, Training, and Awareness
SPSS	Statistical Package for Social Sciences
TAM	Technology Acceptance Model
TPB	Theory of Planned Behavior
USCF	Usability-focused Security Culture Framework
UTAUT	Unified Theory of Acceptance and Use of Technology

# **Chapter 1:**

# **Introduction**

## 1.1 Introduction

There is an increasing recognition that human factors play an important role in cybersecurity. Even with today's technological advancements, human behavior and decisions around security measures continue to pose major risks in organizations. The importance of human-centric control is evident in a variety of industries, including technology, education, and healthcare, where human-centric controls play a significant role in managing cyber risks. There are a number of human factors that contribute to vulnerabilities, including apathy, ignorance, and unintentional mistakes. In order to reduce human errors, many organizations apply constraining approaches, which aim at limiting the influence of humans and the potential for error (Zimmermann *et al.*, 2024). While these constraints can arguably minimize mistakes to a certain level, organizations are still reliant on human judgment and decision-making, meaning that employees need to be empowered with the skills and knowledge to identify and defend against cyber threats targeting humans, such as phishing and social engineering.

Moreover, despite the significant advancements that have been made in developing technical security solutions that support safeguarding information in organizations, these solutions cannot solely protect organizations and stop cyber threats on their own. Human perceptions and behavior while interacting with security are essential to the overall security systems. Several reports assert that the human element is behind the majority of cybersecurity breaches (Forbes, 2020; The World Economic Forum, 2022; Verizon, 2022), highlighting the need to address human factors in cybersecurity. According to Verizon's Data Breach Investigations Report, 68% of these breaches are a result of non-malicious human errors (Verizon, 2024). As a result, security solutions need to be effectively integrated into people's habits and daily actions to enhance the collective perceptions, behaviors, and beliefs about cybersecurity. Organizations have increasingly recognized the significance of fostering a robust security culture, as such efforts play a critical role in safeguarding against breaches and other security threats. Establishing and maintaining a strong security culture requires identifying and promoting factors that encourage secure behavior and facilitate its transition into a broader organizational culture. Among these factors, one essential consideration is the role of usability in security practices.

Additionally, individual perception and interaction with security solutions and measures can significantly affect the effectiveness of security systems (Parsons *et al.*, 2010; Ng, Kankanhalli and Xu, 2009). Several studies have examined the characteristics of security cultures and their potential for mitigating risk. However, despite the importance of usable security being emphasized in numerous studies, prior research has not directly examined the relationship between usable security and security culture. This gap underscores the need for a deeper investigation of how usability factors can influence and strengthen organizational security cultures.

Furthermore, the cybersecurity industry has put considerable focus on Human Risk Management (HRM) during the past few years as a broad concept to increase the effectiveness of traditional Security Awareness and Training (SA&T) programs. Many organizations have advocated this change to reflect the growing recognition that addressing the human element of cybersecurity is key to successfully mitigating risk. Numerous security vendors and institutions have adopted the HRM concept, indicating an emerging paradigm shift in the cybersecurity industry. According to Forrester, HRM involves four key components: detecting and measuring risks, policy and training interventions, empowering employees with knowledge and tools, and fostering a positive security culture where cybersecurity becomes intuitive (Forrester, 2024).

Similarly, CybSafe defines HRM as “the identification, evaluation, and prioritization of human cyber risks, followed by coordinated and effective application of resources to (A) minimize, monitor, and control the likelihood or impact of harmful cyber events, or (B) maximize the realization of digital opportunities” (CybeSafe, 2024). This definition emphasizes HRM's focus on mitigating risks and enabling digital opportunities. Moreover, Gartner predicts that by 2025, 40% of cybersecurity programs will integrate socio-behavioral principles to reduce the negative impact of human behavior on cybersecurity risks (Gartner, 2024). Integrating socio-behavioral principles into cybersecurity practices underscores the necessity to investigate factors that effectively mitigate the risks posed by human behavior and result in a robust security culture.

This project examines and analyzes the relationship between the usability of security measures and security culture, which highlights the potential value for organizations

in understanding and acting upon these impacts. The research analyses the representation of security culture in existing studies, focusing on its definitions, influential factors, and measurement approaches. Moreover, the concept of usability is investigated to highlight key aspects of relevance. As a result, the research develops a usable security framework to guide the cybersecurity community in addressing usability concerns. This project then examines the interplay between usable security and security culture in organizational contexts, which resulted in designing a Usability-focused Security Culture Framework (USCF) that emphasizes usability as a foundational element in fostering a strong security culture.

## **1.2 Aim and Objectives**

Organizations should create suitable working conditions and supportive environments for people who may have an impact on security culture. One way to establish and maintain an effective security culture is to take a usability-focused approach as a key enabler. As stated in the previous section, the influence of usable security on security culture is largely unaddressed, and so this project aims to determine the influence in organizational contexts. The primary contribution is to examine how usable security contributes to fostering a robust security culture, which can also provide practical insights that organizations can rely on to enhance their overall security culture.

The resulting objectives of the project are identified as follows:

1. To examine prior studies and authoritative sources on usability, usable security, and security culture to define usable security and identify the key influencing factors of security culture.
2. To characterize the relationship between usable security and security culture by framing relevant study variables and assessing whether usable security positively influence security culture. This will be achieved through quantitative and qualitative means to produce validated findings that demonstrate the nature of this relationship.
3. To design and evaluate a framework that leverages usable security and related factors to identify usability improvements that enhance security behaviors and promote a positive security culture. The framework's effectiveness and relevance

will be measured through stakeholder engagement to ensure its practicality and alignment with organizational needs and security practices.

An important outcome of conducting the research is a framework for promoting a positive security culture by employing usable security and other necessary elements. By establishing a framework for fostering a robust security culture, organizations can overcome usability barriers that might otherwise hinder the development of such a culture. It also ensures that cybersecurity measures are designed with human factors in mind by aligning security and usability goals. This leads to more usable and effective cybersecurity systems, which ensure that all employees' actions in the workplace support a strong security culture.

### 1.3 Thesis Structure

The thesis is organized into ten chapters. The background and the aim and objectives are discussed in Chapter 1. The rest of the chapters will be as follows:

- **Chapter 2: Exploring Security Culture.** This chapter examines security culture, offering insights into its definitions, influential factors, and measurement approaches as discussed in previous studies. By identifying gaps in current practices, the chapter highlights opportunities to enhance security culture.
- **Chapter 3: Cybersecurity Training.** This chapter examines the role of cybersecurity training in fostering secure behaviors. It explores user acceptance of training through a socio-technical lens, analyzing factors related to the training itself, the organizational environment, and the users. The chapter concludes with the development of a model for user acceptance of cybersecurity training based on a review of existing literature.
- **Chapter 4: Defining and Framing Usable Security.** This chapter investigates the concepts of usability and usable security, addressing their definitions and representations in the literature. It examines whether current security research effectively incorporates usability aspects. A proposed framework for usable security is presented, capturing key elements identified in the literature.
- **Chapter 5: Investigating Usable Security and Security Culture in Organizational Settings.** This chapter outlines the research methodology

employed in the study, detailing data collection and analysis methods. It discusses the reliability, validity, and ethical considerations that guided the research process, ensuring a robust and credible investigation.

- **Chapter 6: Quantitative Analysis and Findings.** This chapter presents the results of the quantitative survey analysis. The findings are synthesized to provide meaningful insights into the relationship between usable security and security culture.
- **Chapter 7: Qualitative Analysis and Findings.** This chapter focuses on qualitative data analysis, including open-ended survey responses and interview transcriptions. It describes the thematic analysis process, detailing the generation of initial codes, identification of broader themes, and refinement of subthemes. The findings are discussed in relation to the research objectives, providing a rich understanding of the data.
- **Chapter 8: Developing a Usability-Focused Security Culture Framework.** This chapter integrates the quantitative and qualitative findings to address the research objectives. Patterns and relationships between the data sets are identified, leading to the development of the USCF.
- **Chapter 9: Framework Evaluation.** This chapter discusses the process of validating the USCF. It outlines the evaluation methods used to ensure the framework's practical relevance and utility in real-world contexts.
- **Chapter 10: Conclusions.** The final chapter summarizes the research achievements and contributions, discusses the study's limitations, and provides directions for future research, emphasizing the importance of usable security in strengthening security culture.

Additionally, the appendices contain essential supporting materials that complement the main text. These materials include ethical approval, survey instruments, the interview plan, and feedback collected during the validation process. Also, they show promotional materials like posters and flyers that were used for contributions to conferences and events. Each appendix is referred to within specific chapters where relevant. This research has also resulted in publications in international peer-reviewed conferences and journals, which reflect its contribution to advancing knowledge and alignment with the broader discussion in the field.

# **Chapter 2: Exploring Security Culture**



## 2.1 Introduction

Security culture has become increasingly important as a concept that helps enhance organizational resilience to cybersecurity threats. It creates an environment where cybersecurity becomes a shared responsibility beyond technological solutions. By exploring security culture, organizations can identify gaps, increase awareness, and encourage behaviors that mitigate risks. This chapter will explore security culture's meaning and look into how previous research examines factors that influence security culture. Also, an overview of how studies have measured security culture will follow, offering insights into the methodologies utilized by different studies.

## 2.2 Security Culture Definition

It is essential to underline definitions of security culture in order to establish a clear understanding of its scope and aspects. This will also ensure that efforts to enhance security culture are well-aligned and effective, as interpretations can vary based on the context. Table 2.1 highlights some of the definitions suggested in studies.

Source	Definition
Al Sabbagh and Kowalski (2012)	“The way our minds are programmed that will create different patterns of thinking, feelings and actions for providing the security process”
AlHogail and Mirza (2014a)	“The collection of perceptions, attitudes, values, assumptions and knowledge that guide how things are done in the organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees’ security behavior in a way that preserving the information security becomes a second nature.”
Carpenter and Roer (2022)	“the ideas, customs and social behaviors that impact the security of your organization.”
(CPNI, 2021)	“the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security. Getting security culture right will help develop a security conscious workforce, and promote the desired security behaviours you want from staff”
Da Veiga (2016b)	“the intentional and unintentional manner in which cyberspace is utilized at four levels, namely at international, national, organizational or individual level, which either promotes or inhibits the safety, security, privacy, and civil liberties of individuals, organizations or governments”
Da Veiga and Eloff (2010)	“the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e., incidents) evident in artifacts and creations that become part of the way things are done

Source	Definition
	in the organization to protect their information assets. This information security culture changes over time”
Da Veiga <i>et al.</i> (2020)	“Information security culture is contextualized to the behaviour of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and procedures and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives.”
Dhillon (2007)	“The collection of human attributes such as behaviors, attitudes, and values that facilitate the protection of all the information in the organization”
ENISA (2017)	“knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people’s behaviour with information technologies.”
Kraemer and Carayon (2007)	“Security culture is defined as aspects of the organizational security philosophy that directly or indirectly affects the overall security of the network”
Mahfuth <i>et al.</i> (2017)	“an integration process of beliefs, perceptions, attitudes, values, assumptions and knowledge that guide, direct and manage employees’ perceptions and attitudes to influence employees’ security behavior or to find an acceptable behavior for employees when they are interacting with the information assets in their organizations”
Malcolmson (2009)	“Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organization, and behaviours they perform, which could potentially impact on the security of that organization, and that may, or may not, have an explicit, known, link to that impact”.
Martins and Elofe (2002)	“the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization.”
Nasir, Arshah and Hamid (2019)	“a culture that emphasizes on the security of information assets by improving employees’ information security behavior”
Roer (2014)	“the ideas, customs, and social behavior of a particular people or society, that helps them being free from danger or threat”
Ross (2011)	“no security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted”. Indicating that if users are not relying on a culture they can approach security inadequately.
Schlienger and Teufel (2003)	“socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee”
Tang, Li and Zhang (2015)	Information Security Culture is defined “as the manifestation of [Information Security Management] ISM practices or information security behaviors evolving from the shared values and beliefs in information security within an organization.”
Thomson, Von Solms and Louw (2006)	“as ‘de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy’”

Table 2.1: Security Culture Definitions

Security culture does not appear to have a commonly accepted definition. Most studies, however, propose a working definition as a means of explaining how the working definition is related to their overall research. A common understanding of security culture suggests that it is the collective beliefs, values, assumptions, and behaviors of individuals that influence how security is perceived and practiced. Understanding security culture allows us to explore its influential factors. These factors determine the degree to which security culture is effectively embedded, which shapes the success of security-related efforts. Most importantly, examining these factors allows for the identification of areas for improvement to foster a robust security culture that mitigates risks and aligns human behavior with security goals.

## **2.3 Security Culture Influential Factors**

The research addresses a variety of shared characteristics when investigating factors that have an impact on establishing and maintaining a strong security culture. This section illustrates the most discussed factors influencing security culture by various studies conducted over the past ten years (as of the time of writing). The most discussed factors are:

- Management and leadership support (ML)
- Policies and Procedures (PP)
- Awareness and Knowledge (AK)
- Change Management (CM)
- Regulatory and Corporate Compliance (RC)
- Education & Training (ET)
- Communication (Co)
- Behavior (Be)
- Technical and Technological (TT)
- National Culture (NC)
- Accountability (Ac)
- Ethical Conduct (EC)
- Trust (Tr)
- Organisation System (OS)

- Commitment (Ct)
- Safety Culture (SC)

Table 2.2 and Figure 2.1 show the number of influential factors each study supports and the total iterations in which each factor was presented in the studies. These factors were identified as a result of empirical investigations and analyses concerning security culture. The investigation will help explore the extent to which usability is considered in security culture studies.

Sources	M L	P P	A K	C M	R C	E T	C o	Be	T T	N C	Ac	E C	Tr	O S	Ct	S C	No. of factors
Alfawaz, Nelson and Mohannak (2010)	✓	✓	✓			✓	✓					✓					6
AlHogail (2015)	✓				✓						✓						3
AlHogail and Mirza (2014a)	✓			✓		✓											3
AlHogail and Mirza (2014b)	✓				✓		✓			✓	✓	✓					6
AlKalbani, Deng and Kam (2015)					✓												1
Cruz (2022)			✓														1
D'Arcy and Greene (2014)							✓		✓						✓		3
Da Veiga (2018)	✓	✓	✓	✓													4
Da Veiga and Eloff (2010)	✓	✓		✓				✓									4
Da Veiga <i>et al.</i> (2020)	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓				10
Evrpidou <i>et al.</i> (2022)	✓	✓	✓			✓	✓		✓							✓	7
Georgiadou, Mouzakitis and Askounis (2022)			✓					✓	✓				✓	✓			5
Hassan and Ismail (2012)			✓	✓	✓			✓						✓			5
Hassan <i>et al.</i> (2017)	✓	✓	✓												✓		4
Ioannou, Stavrou and Bada (2019)	✓	✓					✓										3
Lopes and Oliveira (2014)	✓		✓		✓	✓			✓						✓		6
Mahfuth <i>et al.</i> (2017)								✓									1
Ruhwanya and Ophoff (2019)	✓									✓							2
Sherif, Furnell and Clarke (2015)	✓	✓	✓														3

Sources	M L	P P	A K	C M	R C	E T	C o	Be	T T	N C	Ac	E C	Tr	O S	Ct	S C	No. of factors
Tang, Li and Zhang (2015)	✓	✓			✓		✓				✓						5
Tolah, Furnell and Papadaki (2021)	✓	✓		✓		✓						✓					5
Wiley, McCormac and Calic (2020)	✓		✓		✓				✓								4
Total no. of occurrences	16	10	11	6	8	6	6	5	6	3	3	3	2	2	3	1	

Table 2.2: Security Culture Influential Factors Presented in Studies

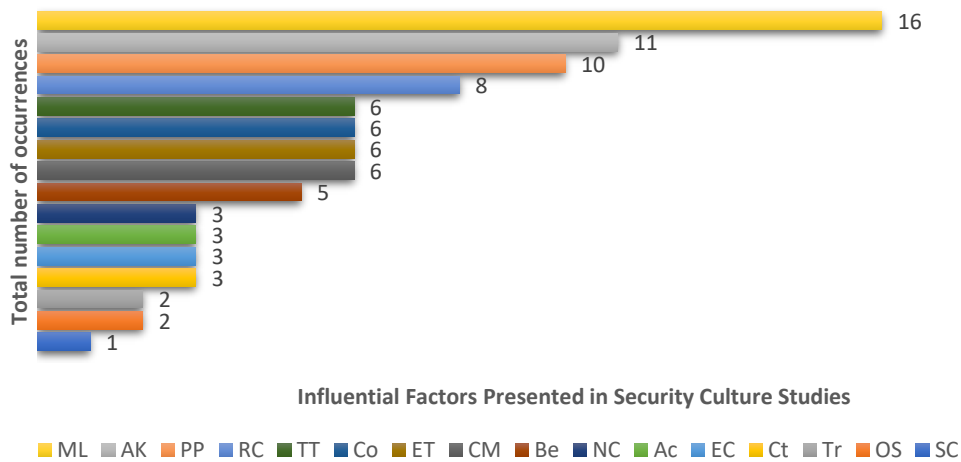


Figure 2.1: The number of Factors Influencing Security Culture

Studies indicate that many factors influence security culture in organizations. A large number of studies emphasize the importance of top management and leadership support. This support is arguably critical in enforcing and fostering other factors, such as increasing awareness and knowledge, applying policies and procedures, and complying with corporate governance (Mahfuth *et al.*, 2017; AlHogail and Mirza, 2014a; Da Veiga *et al.*, 2020). Cybersecurity activities may not seem important without the support from top management; therefore, management must guide employees' security culture efforts and manage resources effectively (Uchendu *et al.*, 2021). Policies and procedures also appear in many papers as a vital factor. It is also worth noting that policies and procedures are frequently associated with users' awareness and knowledge and the training programs organizations provide to their employees. For example, Chen, Ramamurthy and Wen (2015) assert that security education, training,

and awareness programs are key components that influence employees' understanding of organizational security policy and that the awareness will ultimately positively impact the overall security culture. By contrast, the lack of awareness and knowledge to implement the necessary policies and procedures might negatively impact the organization's security culture. However, despite top management's support for cybersecurity awareness and training programs, a study concludes that compliance is the primary driving factor while conducting awareness and training programs because regulations require businesses to provide regular cybersecurity awareness and training programs (Bada, 2022).

The remaining other factors, like change management, communication, trust, and technological aspects, appear in multiple articles. Nevertheless, a further important implication is to consider all internal and external factors while establishing and maintaining a robust security culture, besides determining the degree to which the organization's security culture is dependent on each of them (Da Veiga *et al.*, 2020). Noteworthy, no study has directly stated the usability of security and addressed it as a factor influencing security culture, although few studies identify usability as an integrated quality in other factors. For example, Furnell and Rajendran (2012) emphasize that usability is an aspect that can enhance user behavior, Padayachee (2012) asserts that usability increases the likelihood of compliance, and Hassan and Ismail (2012) discuss how change management improves security through multiple elements including usability. Although previous studies consider some aspects of usable security, no explicit connection has been identified between usable security and security culture.

## **2.4 Measuring Security Culture**

Research indicates that security culture can be measured. Measuring security culture is also an important step toward understanding the factors that influence it and eventually fostering a good security culture (Okere, Van Niekerk and Carroll, 2012). Different instruments have been used by researchers to measure culture. The summary of the approaches is shown in Table 2.3.

	Study approach				
	Quantitative	Qualitative			Mixed-method
Instrument	Questionnaire/Survey	Interview	Observation	Document analysis	(Quantitative + Qualitative) approaches
Sources	(Martins and Elofe, 2002); (Da Veiga and Eloff, 2010); (Al Natheer, Chan and Nelson, 2012); (D'Arcy and Greene, 2014); (AlHogail, 2015); (AlHogail and Mirza, 2015); (Da Veiga, 2016a); (Da Veiga and Martins, 2017); (Nævestad, Meyer and Honerud, 2018); (Nasir, Arshah and Hamid, 2019); (Nel and Drevin, 2019); (Georgiadou, Mouzakitis and Askounis, 2022)	(Alfawaz, Nelson and Mohannak, 2010)	(Alfawaz, Nelson and Mohannak, 2010); (Marotta and Pearlson, 2019)	(Alfawaz, Nelson and Mohannak, 2010)	(Schlienger and Teufel, 2003); (Da Veiga <i>et al.</i> , 2020); (Tolah, Furnell and Papadaki, 2021)

Table 2.3: Measuring Approaches of Security Culture



As shown in Table 2.3, questionnaires and surveys are the most dominant utilized instruments. Other tools such as interviews, observation, document analysis, or multiple instruments have also been employed with much less attention than questionnaires and surveys. The majority of studies used a five-point Likert scale to assess participants' responses. The targeted population in the majority of the studies (Schlienger and Teufel, 2003; Martins and Elofe, 2002; Alnatheer and Nelson, 2009; AlHogail and Mirza, 2015; Tolah, Furnell and Papadaki, 2021) varied from executives and senior management to staff in various job levels and disciplines.

Some approaches used in studies are based on the assessment situation. For example, during the coronavirus (COVID-19) pandemic, people were encouraged to stay home and work remotely. Meanwhile, fraud and cyber-attacks have dramatically increased in the same period<sup>1</sup>. To evaluate the security culture status while working remotely, Georgiadou, Mouzakis and Askounis (2022) created a targeted questionnaire and conducted a web-based survey on individuals from different countries and business domains based on a cyber security culture framework that focuses on assessing critical infrastructure during COVID-19 (Georgiadou, Mouzakis and Askounis, 2021). The authors considered the following steps:

- 1) Designing the survey taking into account that (i) the survey should be conducted while the COVID-19 legislation measures still existed, (ii) the survey has to be brief, i.e., 5 to 10 minutes, to respect participants' time during this difficult period, (iii) the survey needs to be digitalized so it can be accessible to participants around the globe, and (iv) the survey questions need to use simple language as it was targeting workers from different business domains and who might not be familiar some technological and security terms. Then, the authors created a web-based questionnaire with no more than 23 questions.

---

<sup>1</sup> According to the UK National Fraud & Cyber Security Centre, During the COVID-19 pandemic, fraud related to COVID-19 increased by 400% in March 2020, costing victims more than 800 thousand pounds only in one month (National Fraud & Cyber Crime Reporting Centre, 2020). This raises the question of whether security culture can be affected by such circumstances, given that cybercriminals are taking advantage of the great number of employees working from home and connecting to their organization's systems (Europol, 2020).

- 2) The questionnaire was validated through a focus group of 20 people from different backgrounds and experience levels to identify unclear instructions.
- 3) Selecting the study sample focusing on European critical national infrastructures (CNI) and representatives from different domains, e.g., utility, transport, banking, finance, and healthcare, as such fields needed a more robust security culture in order to maintain full functionality and minimize operations impact during this particularly demanding time.
- 4) Sending a special invitation email to the selected sample to carry out the main study.

The findings of the study suggest that, despite its importance, cyber security still has a long road until it becomes an integral part of the workforce and corporate operations and that great emphasis on personal security factors, including behavior, attitude, awareness, and compliance is demanded, besides the need to quantifying these primarily qualitative indicators to establish a trustworthy cultural approach to cyber security. However, according to Roer *et al.* (2022), while some factors might experience a noticeable decline for the past few years due to “COVID-19 exhaustion”, several sectors around the world have improved their security culture during the pandemic. In addition, Georgiadou, Mouzakitis and Askounis (2022)’s study is designed with particular attention to the COVID-19 situation, and then the tools and questionnaire would not necessarily be helpful in assessing security culture in different situations.

In another practical example of measuring security culture in organizations, KnowBe4 breaks culture down into measurable dimensions (Carpenter and Roer, 2022). They identify multiple dimensions of culture, including behaviors, attitudes, compliance, norms, and communication, and aim to assess those. It is notable that each of these dimensions has a level of influence on culture and can be used as a key indicator of cultural improvement. An example of how KnowBe4 quantifies the dimensions is shown in Figure 2.2.

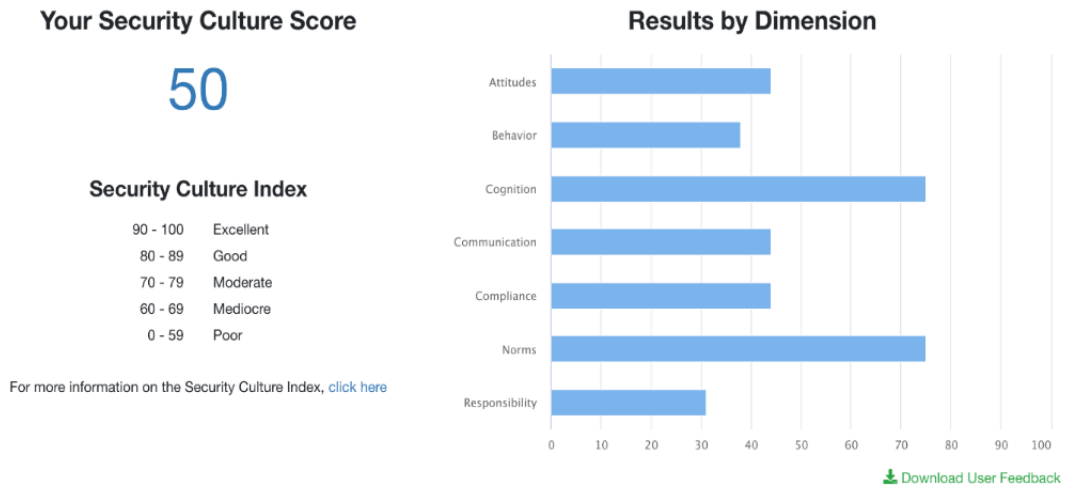


Figure 2.2: Security Culture Dimensions Scores (KnowBe4, 2020)

In the example above, seven dimensions are evaluated and displayed in the order corresponding to the organization's highest-scoring to lowest-scoring dimensions using a Security Culture Survey created by KnowBe4 (2020). The survey then allows organizations to compare their average score with other organizations in the same industry and to use the score as a benchmark to track how the organization's culture evolves over time. Still, all the dimensions in KnowBe4's approach and other methods to measure security culture do not directly take the usability of cybersecurity into account.

A practical implication is to assess the security culture in organizations and determine the extent to which specific factors impact cultivating a strong security culture. The available evidence suggests that security culture is measurable, with various instruments being utilized for this purpose. However, questionnaires and surveys are widely used, even though they might not always be the most optimal method. In other words, certain aspects of culture, such as the actual security behavior of users in an organization, can be challenging to measure using only quantitative approaches. Evaluating these factors through qualitative methods, such as interviews and observation, is ideal for obtaining meaningful results. Additionally, interviews can follow questionnaires to clarify misunderstandings and address potential gaps (Sas et al., 2021). Therefore, it is recommended that both quantitative and qualitative approaches be incorporated to evaluate every aspect of information security culture thoroughly.

Referring back to Table 2.2 in Section 2.3, which highlights the number of influential factors identified in each study and their recurrence, it is evident that Awareness and Knowledge (AK) has been recognized in 11 studies over the past decade, alongside six occurrences for Education and Training (ET). These factors emerge as the most frequently discussed contributors to shaping security culture in organizations. Furthermore, HRM incorporates critical components, including training programs designed to help employees recognize and mitigate the risks associated with their activities around security measures. Given the pivotal role of training in fostering a robust security culture, it is essential to discuss cybersecurity training and, more importantly, user acceptance of such training programs.

## 2.5 Chapter Summary

To sum up, there does not seem to be a single definition of security culture widely acknowledged. However, most publications include definitions to demonstrate how their working definitions fit into the wider research. Numerous studies have emphasized the necessity of top management and leadership support as an influential factor. Other aspects of security culture, such as compliance, awareness, and policies and procedures, are dependent on this support. Hence, there is a need for well-defined and easy-to-understand policies and procedures. Also, we must move beyond limiting human interaction with technology and viewing humans as problems (Zimmermann *et al.*, 2024) in order to prevent cyber incidents. People should be empowered to be a line of defense against cyber-attacks and not be viewed as the weakest link in the cybersecurity chain. A key point to highlight is that the provision of effective cybersecurity awareness, training, and education is widely regarded as the basis of establishing a strong security culture. In fact, some organizations may view it as the only requirement for developing such a culture. Thus, it is essential to explore the nature of cybersecurity training and evaluate its effectiveness from the user perspective, specifically whether users accept and engage with it. The next chapter will explore cybersecurity training and user acceptance in fostering a robust security culture.

# **Chapter 3:**

# **Cybersecurity Training**

### **3.1 Introduction**

Cybersecurity relies heavily on user behavior, and training is one of the most widely recommended methods for ensuring secure behavior (McCrohan, Engel and Harvey, 2010; Aldawood and Skinner, 2019). Nonetheless, it remains a challenge to ensure that users are engaged with such training. User acceptance of cybersecurity training can be viewed from a socio-technical perspective. It is determined by several factors, including the training itself, the organization in which it is deployed, and the users who expect to engage with it. This chapter provides an overview of the research conducted on user acceptance in the three social-technical dimensions and outlines the acceptance factors for cybersecurity training that have been discussed in the existing scientific literature. Then the chapter explores the application of the Technology Acceptance Model factors in the context of cybersecurity training acceptance, leading to the development of a Cybersecurity Technology Acceptance Model (CTAM).

### **3.2 Socio-technical Perspectives on User Acceptance of Cybersecurity Training**

Baxter and Sommerville (2011) describe that a socio-technical approach to system design leads to higher user acceptance and stakeholder value. Interpreted in the domain of this research, it can be argued that it increases user adoption of cybersecurity training and improves the outcomes of such training. A socio-technical approach assumes that a technology depends on itself, its users, and the organization in which it is used (Mumford, 2006). Prior user acceptance research in those dimensions is outlined below.

Technical aspects relating to the technology itself, have been extensively discussed, and summaries are provided by Venkatesh and Bala (2008) and Lee, Kozar and Larsen (2003). In the context of this research, technology refers to the cybersecurity training effort itself. Venkatesh and Bala (2008) and Lee, Kozar and Larsen (2003) highlight system quality as a contributor to user acceptance. System quality is further described as how easy and intuitive technology is to use and how well it supports the user's job performance. Those factors are to be considered in relation to other technologies with similar purposes. Users will adopt a technology that is comparatively better to a greater

extent. Technical aspects relating to cybersecurity training have been the focus of previous research. In Kävrestad *et al.* (2022), it is demonstrated that the implementation of cybersecurity training impacts users' willingness to adopt the training. A possible reason is described by Bello and Maurushat (2020), who argue that users are more prone to use intuitive and easy-to-use cybersecurity training. Similar findings are presented by Dahabiyeh (2021), who also emphasizes the quality of the presented content.

Aspects relating to the user include demographic aspects where age, nation of residence, and gender have been discussed as possible mediators of user acceptance (Kävrestad, Furnell and Nohlberg, 2021). Venkatesh and Bala (2008) and Lee, Kozar and Larsen (2003) further describe that a user's computer skills and attitude will also have an impact. Both a user's predisposition to try new technology and self-efficacy will also impact user acceptance. Organizational aspects first include availability, where time, support, and systems availability positively impact user acceptance (Venkatesh and Bala, 2008; Lee, Kozar and Larsen, 2003). Organizational culture will also have an impact, where user acceptance is impacted by managerial support and how the organization's members perceive a technology, i.e., subjective norms (Venkatesh and Bala, 2008; Lee, Kozar and Larsen, 2003). The impact of organizational aspects relating to cybersecurity training acceptance has received less attention from the research community. Nevertheless, Dahabiyeh (2021) suggested that management support, engagement from colleagues, and dedicated IT staff should positively impact the acceptance of cybersecurity training. Reeves, Calic and Delfabbro (2021) also describe colleagues as important positive or negative mediators of cybersecurity training acceptance.

A core component of a socio-technical approach to systems design is the view that performance is reliant on all socio-technical dimensions, which are highly intertwined (Baxter and Sommerville, 2011). A consequent property is that system goals can typically be addressed in more than one way. One can, for instance, assume that a certain technology may work well in one organization but less so in another. As an example, one can assume that users in a military organization may be more prone to adopt cybersecurity training than users in a more relaxed environment because of their predisposition to follow orders and strive for security. A solution with the same goals

may have to be designed differently, for instance, in a non-hierarchical startup company.

### 3.3 Categorization of Studies that Discussed the Socio-technical Dimensions

A structured review was conducted to examine the studies that discussed the socio-technical dimensions using the following search:

*(Cyber OR Information OR IT OR computer) AND security AND (training OR education) AND (adoption OR acceptance OR usage).*

The search string was applied to the following databases and indexes; ACM, IEEE Xplore, DBLP, Science Direct, and Scopus. The searches, conducted in 2023, were restricted to research papers published within the preceding ten years. A total of 16 studies were selected and were categorized according to what socio-technical dimensions they discussed. This search reveals that all papers discussed the training itself (i.e., the technical dimension). Five papers discussed the organizational dimension, and one paper discussed the social dimension. All included papers are shown in Table 3.1

Study	Technical	Organizational	User-Centered
Kävrestad <i>et al.</i> (2022)	X	X	X
Dahabiyeh (2021)	X	X	
Haney and Lutters (2018)	X	X	
Ma <i>et al.</i> (2019)	X	X	
Shillair (2016)	X		
Wash and Cooper (2018)	X		
Silic and Lowry (2020)	X		
Shen, Mammi and Din (2021)	X		
Wen <i>et al.</i> (2019)	X		
Jin <i>et al.</i> (2018)	X		
Kletenik <i>et al.</i> (2021)	X		
Cullinane <i>et al.</i> (2015)	X		
Gokul <i>et al.</i> (2018)	X		
Stockett (2018)	X		
Offor and Tejay (2014)	X		
Bélanger, Maier and Maier (2022)	X	X	

Table 3.1: Categorization of Studies that Discussed the Socio-technical Dimensions

The following subsection provides an overview of the extracted content for each dimension of cybersecurity training acceptance.



### 3.3.1 Technical Dimensions

The technical dimension was the most prominent dimension in the 16 papers included in this review. In fact, the nature of the training itself was, to some extent, discussed in all included papers. Five of those argue that user satisfaction is important for cybersecurity training efforts before developing training efforts and evaluating user satisfaction of them (Silic and Lowry, 2020; Shen, Mammi and Din, 2021; Wen *et al.*, 2019; Jin *et al.*, 2018). Shen, Mammi and Din (2021) describe that the properties of the training itself will greatly impact the user's perception of that training, which is further supported by Dahabiyeh (2021). Ma *et al.* (2019) and Cullinane *et al.* (2015) further show that user satisfaction impacts a user's willingness to use and re-use cybersecurity training tools and states that the perceived quality and fun of a training tool will influence the perception of it. The so-far presented papers discuss gamified training, and it can be concluded that user perception differs between cybersecurity games. Kävrestad *et al.* (2022) further show that user perception differs between different types of security training and suggests that contextual training is preferred over eLearning platforms and cybersecurity games. In contrast, Gokul *et al.* (2018) suggest that games are more engaging than training using mandatory quizzes.

To ensure that any cybersecurity training effort is positively perceived, it must be developed with its intended recipients in mind (Stockett, 2018). On that note, Offor and Tejay (2014) argue that cybersecurity training for adults must be developed using pedagogical principles for adults. Stockett (2018) further suggests that tailoring training to different user groups will facilitate adoption. Some suggestions pertaining to the content of the training can also be found in the included papers. Haney and Lutters (2018) argue that the material must be tailored to the recipient in a way that makes it easy to understand and convert into their daily life. Shillair (2016) also stresses the importance of understandable content and suggests that users have diverse preferences, which could be met by providing training in different formats. Making the material appear personal and mandatory is also described as a factor that can improve user adoption rates (Bélanger, Maier and Maier, 2022; Stockett, 2018).

A final interesting dilemma is reported by Wash and Cooper (2018), who discuss the timing of training. Wash and Cooper (2018) describe that phishing training is sometimes a part of a phishing exercise and is provided to users who act on the messages in those drills by clicking a link. While that may be effective for the users who click the links, other users would not be trained.

### **3.3.2 Organizational Dimension**

Organizational dimensions are discussed in five included publications and in two main themes. The first theme is trust in the security organization, which is described by Haney and Lutters (2018). They describe that trust in the source of a security message is imperative for users' willingness to listen to that message. Consequently, the security organization must build a reputation within the organization, leading to a higher degree of user adoption. Similarly, Dahabiyeh (2021) describes that commitment from various organizational stakeholders is needed to ensure user participation in training efforts. The notion of trust has also been found to impact user adoption in a survey with over 1400 respondents, who ranked trust in the sender of the training program as one of the most important factors for willingness to adopt cybersecurity (Kävrestad *et al.*, 2022).

The second theme can be described as informal culture, where Ma *et al.* (2019) describe that social influence is important for user stickiness, the degree to which users will continue to use a training effort. Social influence can assist in making training feel mandatory, which also contributes to user adoption (Bélanger, Maier and Maier, 2022).

### **3.3.3 User-centered dimension**

User-centered dimensions include how user demographics, abilities, and traits can impact user adoption of cybersecurity training. It is only explicitly studied in one of the included papers, i.e., (Kävrestad *et al.*, 2022). Kävrestad *et al.* (2022) research if worrying about cyberthreats impacts users' willingness to adopt cybersecurity training. While they find that to be the case, they also describe worry as a weak mediator. In addition, it can be mentioned that several papers included in this research argue that training should be tailored to various user groups, suggesting that user groups' different needs are understood. However, none of these describe how different groups should be trained.

### **3.4 A Model for Cybersecurity Training Acceptance**

Many models have been developed to explain user acceptance of technologies, introducing factors that affect user acceptance. These include widely recognized models such as the Technology Acceptance Model (TAM), The Model of PC Utilization (MPCU), the Theory of Planned Behavior (TPB), and the Social Cognitive Theory (SCT). Although most of these models offer valuable insights into technology adoption, they often introduce factors that may not be directly applicable to the specific context of cybersecurity training acceptance. By focusing on factors such as Perceived Usefulness (PU) and Perceived Ease of Use (PEOU), TAM may address the key elements that influence an individual's decision to engage in and accept cybersecurity training. This direct relevance makes TAM an ideal choice for this study, ensuring a focused and effective analysis of the factors that drive user engagement in the cybersecurity training context.

Most importantly, there is a lack of comprehensive literature on training acceptance that takes into account factors that contribute to user acceptance of cybersecurity training. To address this gap, this study seeks to answer the following question: How does current research relate to the factors mediating user acceptance of technology? The study utilizes the Technology Acceptance Model (TAM), a well-established theory initially introduced by Davis (1985) and subsequently reviewed and expanded upon by numerous studies, such as (Lee, Kozar and Larsen, 2003; Venkatesh and Davis, 2000; Venkatesh and Bala, 2008), to demonstrate how to encourage the acceptance and adoption of information systems.

The research proceeds to explore the application of TAM factors in the context of cybersecurity training acceptance. As a result, the study introduces a Cybersecurity Training Acceptance Model (CTAM) and underscores existing research gaps related to user acceptance of cybersecurity training. Equally important, this study highlights factors that have not been discussed in the context of cybersecurity training acceptance by previous research. Identifying the key factors that drive user acceptance of cybersecurity training contributes to informing the development of more effective cybersecurity training programs that engage users and improve organizational security

measures. This will ultimately support active participation and improve the broader cybersecurity culture.

### 3.4.1 Components and Evolution of TAM and its Extensions

The core components of TAM provide a foundational framework that helps understand how users accept a technology. The model explains that user adoption of technology is influenced by Behavioural Intention (BI), which is influenced by PU and PEOU. PEOU also has an influence on PU. PU, PEOU, and BI, as well as the relationships between those, are mediated by external factors, which are the focus of this chapter. The external factors outlined by Venkatesh and Davis (2000) and Venkatesh and Bala (2008), as well as what TAM constructs or relationships they mediate, are reflected in the model in Figure 3.1. Factors that mediate the same constructs or relationships are grouped together to increase readability.

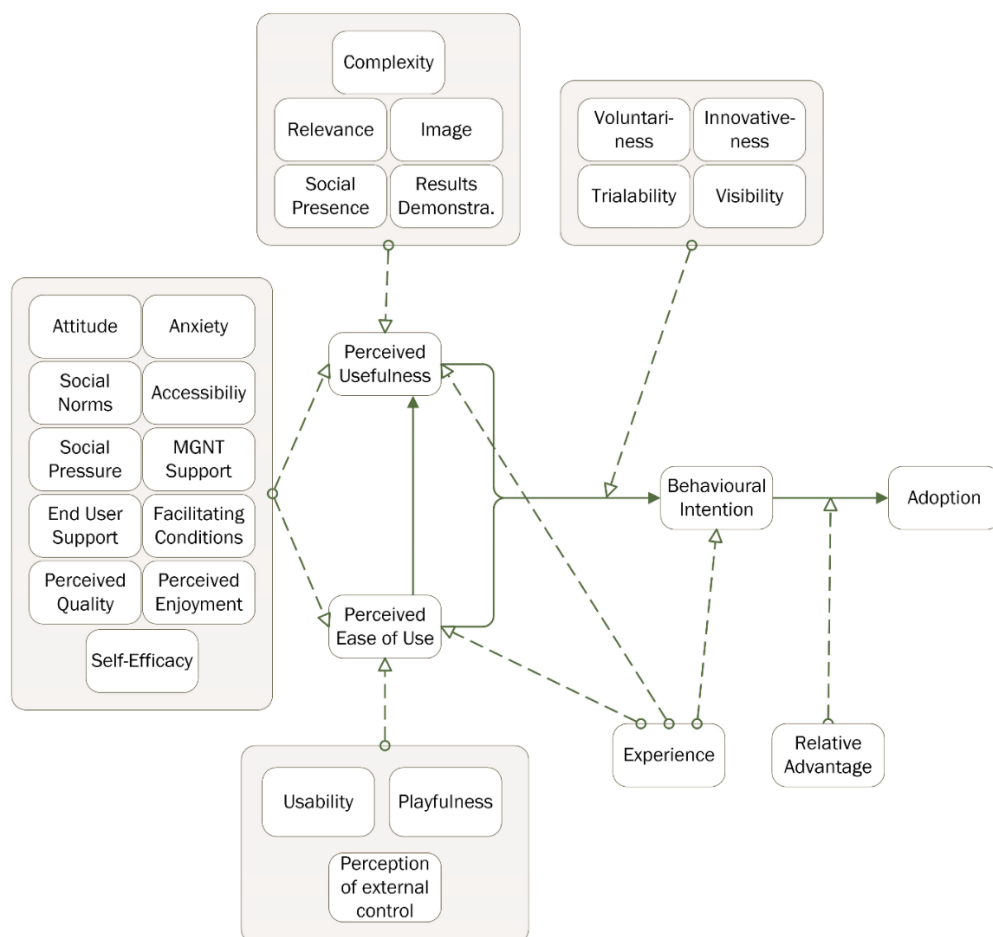


Figure 3.1: Technology Acceptance Model (TAM) and its External Factors

TAM has undergone a number of changes over the past few decades. For instance, Venkatesh and Davis (2000) proposed an update known as TAM2, in which they provided more detailed explanations of why technology users can find a given system useful. This update entailed the notion that users' perceptions of the usefulness of a given system are influenced by their mental assessment of how well the system corresponds to essential goals within the workplace (Venkatesh and Davis, 2000). The study results showed that TAM2 performed well both in voluntary and mandatory settings. Later, Lee, Kozar and Larsen (2003) reviewed TAM's evolution over time by assessing its impact and relevance in various contexts. The review is segmented into past, present, and future. The *past* section traces TAM's origins and early developments by highlighting how it emerged as a basic model for understanding user acceptance of technology using the initial constructs, namely PU and PEOU. The *present* section of the study discusses the numerous extensions and adaptations that have been proposed to enhance TAM's explanation and applicability. These extensions often integrate additional factors, including facilitating conditions and social influence, reflecting the dynamic of technology acceptance. The authors also evaluated TAM's performance across different user demographics and technological contexts. In the *future* section, Lee, Kozar and Larsen (2003) suggested potential directions for future research, including exploring emerging technologies and considering novel theoretical constructs.

In a subsequent development, Venkatesh and Davis (2000) presented an advanced version, TAM3, and proposed a research agenda focused on interventions to enhance technology acceptance. This was designed to address some of the limitations by incorporating an extensive set of factors influencing technology acceptance. This model integrates elements from TAM2 and the Unified Theory of Acceptance and Use of Technology (UTAUT), along with new concepts. Key additions include the influence of individual differences (e.g., perceptions of external control and computer self-efficacy), system characteristics (e.g., perceived enjoyment and objective usability), and contextual factors (e.g., experience and voluntariness).

TAM and its extensions have been extensively employed to understand user acceptance of technologies in a variety of contexts, demonstrating its adaptability and robustness in explaining technology adoption. Based on studies (Lee, Kozar and

Larsen, 2003; Venkatesh and Davis, 2000; Venkatesh and Bala, 2008), TAM has been found to be effective at predicting acceptance and usage behavior. However, TAM and its extended models have not been thoroughly explored in the context of cybersecurity training acceptance in spite of their widespread application. It is essential to recognize that cybersecurity involves unique challenges and user interaction paradigms fundamentally different from those associated with traditional technology use. As an example, user compliance with security measures may be driven by a variety of factors, including fear of breaches or potential legal implications, which are not considered primarily in TAM. It is imperative that research be conducted to adapt and validate TAM within the cybersecurity context to ensure that it adequately captures the distinct factors influencing the adoption of security technologies. Specifically, focusing on factors that influence users' acceptance of cybersecurity training can significantly foster greater user adherence to cybersecurity practices.

### 3.4.2 Literature Assessment Methodology

This research is conducted as a structured literature review following Paré and Kitsiou (2017) methodology. An inclusive approach was adopted to select databases and develop the search queries, as suggested by Meline (2006) and Jesson, Lacey and Matheson (2011). The literature review aimed to examine factors influencing users' acceptance of cybersecurity training and to identify relevant publications. To achieve this, the following query was developed:

*((cyber OR information OR computer OR IT) AND security)) AND (training OR education OR awareness) AND (adoption OR acceptance OR usage) AND [FACTOR].*

The intention was to capture all permutations of cybersecurity training combined with adapting words with similar meanings. Finally, terms for each factor in the TAM were appended. The search string was applied to the following databases and indexes: Scopus, Web of Science (WoS), IEEE Xplore, and ACM Digital Library, with minor modifications to the logic to meet the requirements of the respective databases. These databases and indexes provide comprehensive coverage within the fields of technology and computer science. It is also worth noting that Scopus and WoS are general indexing databases that provide a broad overview of peer-reviewed literature across various disciplines, including their extensive inclusion criteria and wide-ranging scope. This

ensures a diverse and multidisciplinary perspective on the research findings. On the other hand, IEEE Xplore and ACM Digital Library are publisher-specific repositories, which allows for more in-depth access to the latest advancements. While these databases are expected to yield different results due to their indexing criteria, there is a possibility of overlap. For instance, a paper published by ACM could potentially be retrieved from the ACM Digital Library, WoS, and Scopus, illustrating the varying coverage of these scholarly resources. Additional complementary searches with the same terms applied to the databases and indexes were also conducted on Google Scholar. The search approach resulted in 125 searches conducted on the listed databases and indexes. The papers resulting from the searches were screened for inclusion in a five-step process:

1. The hits from each search were screened based on titles and abstracts. The result of this step was a list of candidate papers. This step was completed by two researchers individually.
2. The lists of the two researchers were compared, and all papers included by one or both researchers were included for the next step.
3. The full body of the candidate papers was screened again by two researchers individually. The result was a refined list of candidate papers.
4. The lists of the two researchers were compared. Disagreements were solved by discussing each paper, where the researcher made different decisions until a consensus was reached. The output of this step was reviewed by a third researcher.
5. Backward snowballing was applied by considering all papers referenced by the set of papers from (4). Steps 1-4 were repeated for those papers, resulting in a final set of included publications.

The screening process is documented based on (Page *et al.*, 2021) and (Sarkis-Onofre *et al.*, 2021) in the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram displayed in Figure 3.2.

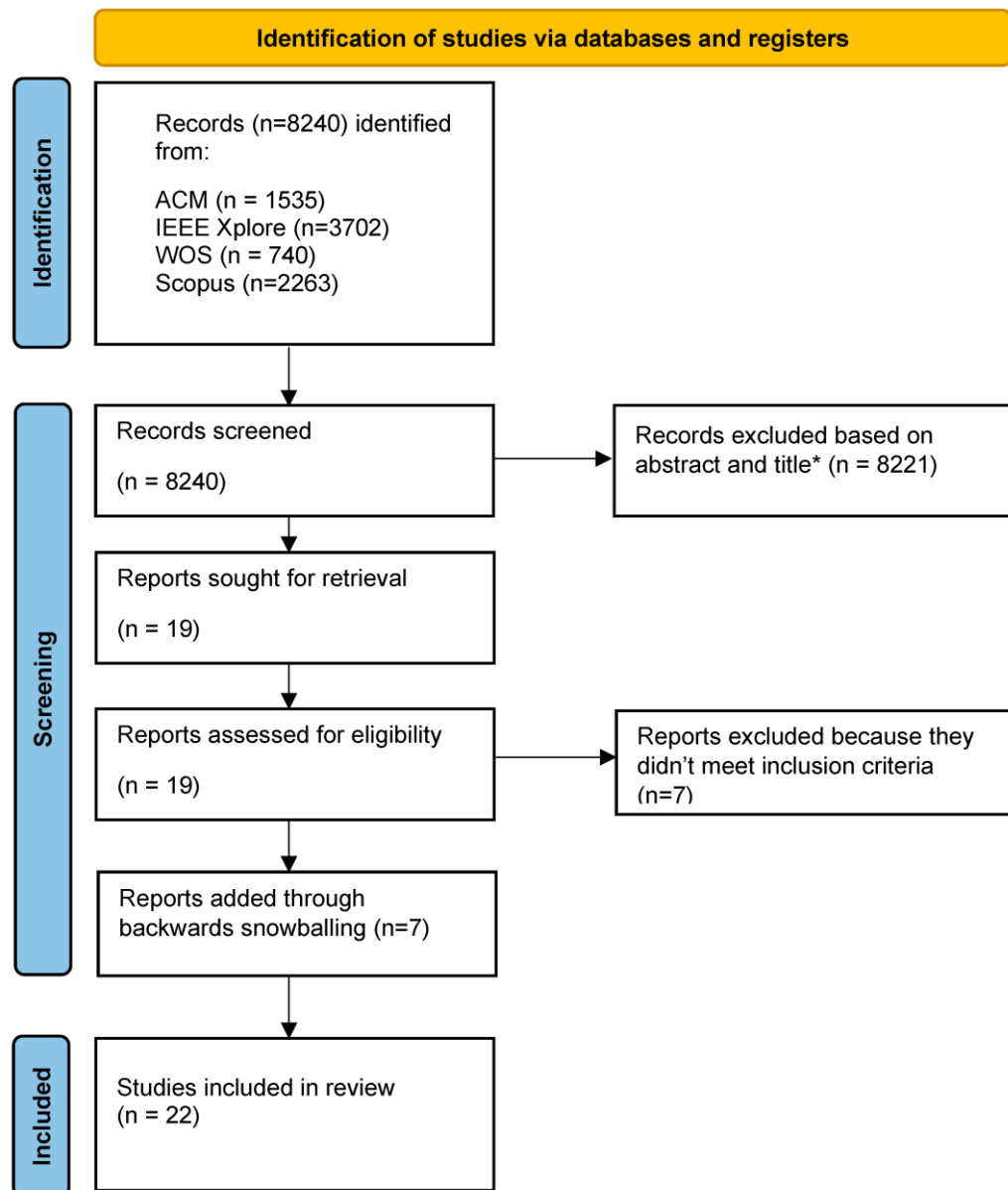


Figure 3.2: PRISMA flow diagram outlining the searching and screening process

### 3.4.3 Results

This section presents the results of the literature review aimed at identifying the factors influencing users' acceptance of cybersecurity training. First, an overview of the TAM and its various extensions is provided to establish a basis for identifying all possible factors influencing technology acceptance. Subsequently, a systematic literature review was conducted in order to examine how these factors have been discussed in cybersecurity training studies, both directly and indirectly. As part of the review, a number of studies were analyzed to determine whether TAM-related factors had been



empirically examined in the context of cybersecurity training. The direct factors are those explicitly identified in the studies, while the indirect factors are those discussed in broader terms, but which are relevant to cybersecurity training. In addition, the review identified gaps in the literature where certain TAM factors have not been examined for cybersecurity training. New factors unique to this context were also explored, providing a more comprehensive understanding of what influences cybersecurity training acceptance. These findings provide insight into the development of more effective cybersecurity training programs that increase user compliance and enhance the overall organizational security culture.

Table 3.2 lists the publications that were included and the factors each one discussed. Some included publications provide empirical data that show that one or more factors impact the acceptance of cybersecurity training. Other publications present findings that are indirectly related to the acceptance of cybersecurity training. That includes, for instance, the perception of cybersecurity training or willingness to adopt cybersecurity measures at large rather than training specifically.

<b>Paper</b>	<b>Directly Researched Factors</b>	<b>Indirectly Researched Factors</b>
Shukla <i>et al.</i> (2022)		Relevance, Experience, Management Support, Facilitating Conditions
Abawajy (2014)	Innovativeness	Usability
Mokwetli and Zuva (2018)		Management Support, Relevance, Regulatory control
Dang-Pham, Pittayachawan and Bruno (2017)	Trust, Social Presence	
Alhalafi and Veeraraghavan (2023)		Perceived Quality, Usability, Social Norms & Pressure, Facilitating Conditions, Accessibility
Lui and Hui (2011)		Self-efficacy
Bryan Foltz, Schwager and Anderson (2008)	Attitude, Apathy, Social Norms	Complexity
Gadzma (2014)		Management Support
Hart <i>et al.</i> (2020)	Perceived Enjoyment, Relevance	
Ma <i>et al.</i> (2019)	Perceived Quality, Social Norms, Perceived Enjoyment	
Rhee, Kim and Ryu (2009)	Self-efficacy	
Potgieter, Marais and Gerber (2013)		Usability, Relevance

<b>Paper</b>	<b>Directly Researched Factors</b>	<b>Indirectly Researched Factors</b>
Reeves, Calic and Delfabbro (2021)		Experience, Perceived Quality, Social Norms, Perception of External Control
Kävrestad <i>et al.</i> (2022)	Facilitating Conditions, Relative Advantage, Worry	
Shillair (2016)		Innovativeness, Relevance, Results Demonstrability
Shen, Mammi and Din (2021)		Perceived Enjoyment
Jin <i>et al.</i> (2018)		Perceived Enjoyment
Gokul <i>et al.</i> (2018)		Perceived Enjoyment
Talib, Clarke and Furnell (2010)	Perception of External Control	
Kajzer <i>et al.</i> (2014)		Image, Social Presence, Attitude, Self-Efficacy
Yasin <i>et al.</i> (2019)		Perceived Enjoyment
Aladawy, Beckers and Pape (2018)		Perceived Enjoyment

Table 3.2: Included publications and factors discussed

Several studies have examined the factors that directly influence users' acceptance of cybersecurity training. Abawajy (2014) suggests that combining different delivery methods of text-based, game-based, and video-based for awareness training is superior to an individual delivery method. This finding indicates that integrating diverse, engaging learning formats is effective. Also, participants in the same study preferred simpler text and video formats due to their lower complexity, even when game-based methods were used (Abawajy, 2014). Dang-Pham, Pittayachawan and Bruno (2017) found that users frequently seek advice from trusted colleagues or those who frequently assist them with computer issues, which illustrates the importance of social presence and trust. The study by Bryan Foltz, Schwager and Anderson (2008) identified attitude, apathy, and social trust as significant barriers to user participation in cybersecurity training and that using lengthy or complex language in materials may result in user fatigue, preventing some individuals from reading them. Hart *et al.* (2020) and Ma *et al.* (2019) examined perceived enjoyment in training, demonstrating that engaging training processes significantly enhance engagement. In addition, Ma *et al.* (2019) found that perceived content quality, social norms, and entertainment significantly influence user satisfaction. In turn, user satisfaction leads to increased

stickiness and security knowledge. Taking into account the perception of external control, Talib, Clarke and Furnell (2010) suggest that users are more likely to engage in training if they perceive strong organizational support, while Kävrestad *et al.* (2022) identified facilitating conditions, relative advantage, and worry as factors influencing user acceptance of cybersecurity training.

Other publications also present findings related to the acceptance of cybersecurity training, although indirectly related, such as the willingness to adopt cybersecurity measures in general rather than training specifically. Indirectly researched factors also played a significant role in understanding user acceptance. In their study, Shukla *et al.* (2022) emphasized the importance of training relevance, user experience, management support, and facilitating conditions. It should be noted, however, that these factors were discussed throughout the study rather than being empirically supported. Mokwetli and Zuva (2018) underlined the importance of management support, relevance, and regulatory control in the adoption of security culture, highlighting the importance of these factors to foster a positive environment for cybersecurity initiatives, including training. Alhalafi and Veeraraghavan (2023) investigated perceived quality, usability, social norms and pressure, facilitating conditions, and accessibility within the context of broader cybersecurity measures among IT professionals. Self-efficacy has been highlighted by Lui and Hui (2011) and Rhee, Kim and Ryu (2009), both of which note that it has a significant impact on the enhancement of security practices. The study by Rhee, Kim and Ryu (2009) found that individuals with a high level of self-efficacy practiced better security operations, including using security software, applying updates, and generally practicing good security behaviors. In their study, Reeves, Calic and Delfabbro (2021) examined how perceived quality, social norms, and perceived external control influence user acceptance. The study suggests that employees' perceptions of the SETA programs are shaped by these factors, which affect employees' behavior and can explain their engagement levels with cybersecurity training.

Furthermore, Shillair (2016) and Potgieter, Marais and Gerber (2013) emphasized the importance of relevance and usability, with Shillair (2016) also addressing innovativeness and results demonstrability within a qualitative context, while (Potgieter, Marais and Gerber, 2013) discussed how to present security information,

suggesting that usability and relevance are important for training to be effective. Several studies highlight that perceived enjoyment increases engagement and motivation, which influences users to embrace and participate in training programs (Shen, Mammi and Din, 2021; Jin *et al.*, 2018; Gokul *et al.*, 2018; Yasin *et al.*, 2019; Aladawy, Beckers and Pape, 2018). The model in Figure 3.3 below illustrates the factors identified in previous studies and highlights those that have been overlooked. The factors written in capital letters are factors that were not identified in the background presented in the section that discusses the TAM components, its evolution and its extensions, but new factors identified during the structured literature review.

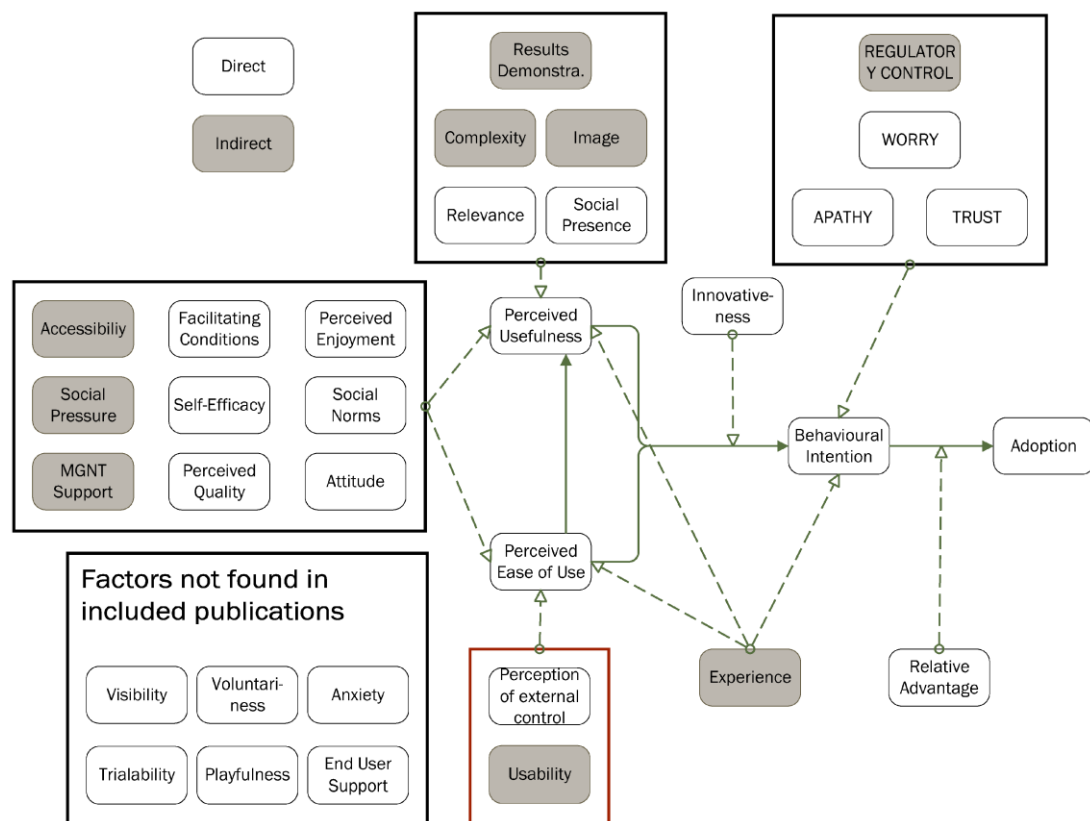


Figure 3.3: Cybersecurity Training Acceptance Model (CTAM)

### 3.4.4 Discussion

This study uses TAM as a theoretical framework to analyze users' adoption of technology. Specifically, the study investigates how TAM factors, which was first presented by Davis (1985) and later reviewed and extended by studies (Lee, Kozar and Larsen, 2003; Venkatesh and Davis, 2000; Venkatesh and Bala, 2008), can be applied to the acceptance of cybersecurity training. Consequently, this study proposes CTAM and identifies research gaps regarding user acceptance of cybersecurity training. TAM extended versions include a number of factors that are not addressed in the current literature regarding user acceptance of cybersecurity training, highlighting a need for further research in this area. These factors are Visibility, Voluntariness, Anxiety, Trialability, Playfulness, and End User Support. Visibility can assist in designing transparent training programs, thus making the benefits of the training clear to users. Voluntariness suggests that optional content in training could enhance user receptiveness. When cybersecurity training is voluntary, users may feel more motivated and autonomous to engage with it. Further, addressing anxiety by creating supportive atmospheres for users could improve training adoption rates. Trialability could facilitate the development of training sessions (e.g., exploratory or pilot sessions), increasing adoption and effectiveness. Users can remain committed and engaged if they are able to test out training modules without feeling pressured. An engaging and enjoyable training program could also be achieved through the use of playfulness, leading to increased participation and retention. Providing robust user support can encourage users to feel more confident and capable, thereby facilitating adoption. These factors can significantly contribute to user acceptance and engagement in cybersecurity training, resulting in more effective and widespread adoption.

As a key contribution, the study brought to light the influence of four factors (i.e., regulatory control, worry, apathy, and trust) on the users' BI to adopt cybersecurity training. These factors can play a vital role in determining the effectiveness of cybersecurity training programs. Firstly, regulatory control can be defined as a set of formal policies, rules, and regulations that govern cybersecurity practices within an organization. A structured and supportive environment for cybersecurity initiatives, including training, requires regulatory control. Providing users with a clear

understanding of legal and organizational expectations regarding cybersecurity practices promotes compliance and accountability. Cybersecurity training programs that consider regulatory control may result in higher compliance rates and a more conscious culture, whereas those that neglect regulatory control may result in a lack of enforcement and adherence to cybersecurity protocols, reducing the effectiveness of the training. Further, the second factor, “worry,” refers to the concern users feel about potential cybersecurity threats and their consequences. In some cases, worry may be a significant motivator for users to attend cybersecurity training. For example, when users are aware of the potential risks and dangers of cybersecurity breaches, they are more likely to take the training seriously and practice what they have learned. If this aspect is taken into consideration, then engagement and motivation could be enhanced, leading to a better retention of information and application of cybersecurity measures. However, Kävrestad *et al.* (2022) found that despite the possibility that worry may motivate users to engage in cybersecurity training, there was no meaningful linkage between worry and willingness to pay for or take up cybersecurity training. This finding suggests that worry alone does not drive the adoption of cybersecurity training, indicating that the combination of other factors is more likely to influence users’ willingness to engage in cybersecurity training. Thus, understanding worry and leveraging it in conjunction with other mediating factors may enhance the effectiveness and uptake of training.

Moreover, the third factor, “apathy,” refers to users’ lack of interest, enthusiasm, or concern for cybersecurity issues. The lack of interest in cybersecurity training represents a significant barrier to its effectiveness. No amount of training will be effective in changing a user’s behavior or improving their security practices if they do not care about cybersecurity. A cybersecurity program must find ways to motivate and engage different users, perhaps by emphasizing the stakes involved on a personal and organizational level. It is essential to keep this factor in mind when training users, as unengaged users are unlikely to adopt the necessary cybersecurity behaviors. Finally, trust refers to users’ confidence in the information, advice, and training provided by their organization or trusted colleagues. Trust is vital to ensure that cybersecurity training is accepted and effective. Users are more likely to follow and adopt guidelines and practices if they trust the source of information and the purpose of the training.

Cybersecurity practices can be significantly enhanced by establishing trust through transparent communication and credible training sources. The lack of trust may lead to skepticism and resistance, reducing the overall impact of training.

It is imperative that organizations adopt a multifaceted approach to cybersecurity training in order to increase user acceptance. A clear understanding of the benefits and importance of the training can significantly increase engagement (Venkatesh and Bala, 2008). It has also been shown that incorporating elements of choice within mandatory programs increases user receptivity since a feeling of autonomy enhances positive attitudes (Lee, Kozar and Larsen, 2003). In order to facilitate greater adoption rates of technology, it is essential to create a supportive and user-friendly environment (Venkatesh and Davis, 2000) in which anxiety can be reduced through accessible resources. It is also essential to address factors unique to cybersecurity training, such as fostering an environment that promotes compliance and accountability. Despite the fact that addressing users' concerns about cyber threats may not directly influence training adoption, it can still have a profound impact on engagement strategies. A proactive approach to combating user apathy involves emphasizing the personal and organizational stakes involved in cybersecurity. Establishing trust through transparent communication and credible training sources encourages adherence to guidelines and best practices.

### **3.5 Chapter Summary**

Organizations are increasingly dependent on robust security to protect their digital assets. To effectively protect these assets, cybersecurity training is essential in educating employees on safe practices to combat common threats. Although cybersecurity training has apparent benefits, organizations struggle to encourage employees to engage with it (Bada, Sasse and Nurse, 2019). Besides, there is a lack of comprehensive literature on user acceptance of cybersecurity training. One of this chapter's objectives is to synthesize existing research about user acceptance of cybersecurity training from a socio-technical perspective. To achieve this, a structured review was conducted, where 16 papers were included after database searches and screening. The results suggest that the majority of the existing research focused on the nature of the training interventions themselves. This research reveals a consensus that

user perception of cybersecurity training is imperative for the adoption of such training. Furthermore, included papers describe that easy-to-understand material that users can adopt in their daily routines is paramount for positive user perception. Furthermore, the included papers demonstrate a great variety of ways in which cybersecurity training can be implemented, with different results in terms of user perception. This suggests that employing design practices such as user-centric design can be beneficial. Several included papers further describe formal and informal cultures as important mediators for adoption. Trust in the security organization and social influence were the most prominent themes and show that awareness-raising stretches beyond the delivery or procurement of a measure. Rather, it is a matter of organizational culture. The impact of user demographics, abilities, or traits was implicitly acknowledged in several included papers that described individualization as important for cybersecurity training adoption. However, only a single paper researched how it could impact adoption and found worry about cyber threats to have a limited impact.

The other objective is to establish a model for acceptance of cybersecurity training. This study addresses the lack of comprehensive literature on user acceptance of cybersecurity training by exploring the application of TAM's factors in the context of cybersecurity training acceptance. Accordingly, the study identifies research gaps related to cybersecurity training acceptance and introduces CTAM. The study concluded that several TAM's factors have not previously been addressed in cybersecurity training acceptance research, including visibility, voluntariness, anxiety, trialability, playfulness, and end-user support. Most importantly, CTAM introduces four factors—regulatory control, worry, apathy, and trust—that influence users' BI to adopt cybersecurity training. Cybersecurity training programs can be designed to engage users effectively and enhance security measures by understanding these key drivers of user acceptance. This will ultimately foster active participation and strengthen the broader cybersecurity culture.



# **Chapter 4:**

## **Defining and Framing**

### **Usable Security**

## 4.1 Introduction

The conflict between usability and security has been extensively discussed in the literature for several decades. The U.S. Department of Homeland Security emphasizes that “*security must be usable by persons ranging from non-technical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security*” (U.S Department of Homeland Security, 2009). Despite the fact that most security practitioners acknowledge the importance of usable security, few are able to precisely define what it means in practice and the extent to which it influences end-user security behavior and the broader security culture of the organization. The purpose of this chapter is to examine how different sources characterize usability and usable security and to determine whether usability aspects are relevant in a cybersecurity context. Initially, the study establishes a broad catalogue of usability representations that capture the breadth of what is meant by usability and then explores whether the important aspects of usability are being recognized in current usable security research. This chapter then presents the definition of usable security along with a proposed framework by looking at the key aspects of usability that have been discussed in the literature.

## 4.2 Defining Usability

The usability of products is essential for functioning, and it affects how users achieve a desired task. In addition, users leave products that are difficult to use and choose alternatives (Nielsen, 2012). Thus, creating usable products attracts users and helps organizations benefit from users’ engagement. To create usable measures, it is vital to understand what characteristics usability entails. This section investigates the various ways in which different sources characterize usability as a foundation for later discussion of usable security. The goal is to identify what key aspects affect usability and determine the degree to which these aspects are then relevant in cybersecurity.

A comprehensive definition of usability can guide the creation of effective systems and services. Many definitions of usability and its related attributes have been introduced in the literature. It is imperative to note that usability is not a single-dimensional issue, but its attributes connect it to qualities covering many disciplines

(Nielsen, 1993). Although various usability definitions are discussed in the literature, they nonetheless have attributes in common. Therefore, it is helpful to investigate what characteristics of usability have been identified and what characteristics have the more significant impact on systems' usability in order to consider these while designing usable systems and services. Moreover, Quesenberry (2003) believes that it is important to utilize our understanding of each usability dimension to better generate usable products. The International Organization for Standardisation (ISO) defines usability as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (ISO, 2018). Still, ISO's definition is not 'universal,' and other studies have proposed various usability definitions.

Table 4.1 demonstrates an illustrative set of usability definitions in an IT/HCI context. The search string: *usability AND (definition OR meaning)* was formalized to query relevant online indexes and publisher repositories: Springer, Scopus, IEEE Xplore, Web of Science, and Google Scholar. In the search, we considered widely cited data sources that are related to IT/HCI and with free access. The list includes sources that suggest a usability definition. However, definitions that are derived from other sources are not taken into account. Finally, definitions from authoritative sources were also included in the list. For each identified source, the table directly quotes its main definition of usability and then abstracts what are considered to be the key aspects from it. These are then able to be used to show how frequently each aspect was recognized in prior definitions. Most importantly, the resulting data from Table 4.1 will be crucial in determining how the usability key aspects are relevant in a cybersecurity context and the extent to which these aspects are recognized in usable security studies.

Source	Definition	Key aspects
Abran <i>et al.</i> (2003)	"a set of multiple concepts, such as execution time, performance, user satisfaction and ease of learning ("learnability"), taken together"	<ul style="list-style-type: none"> <li>• Execution time/efficiency</li> <li>• Performance</li> <li>• User satisfaction</li> <li>• Ease of learning (learnability)</li> </ul>
Bevan and Macleod (1994)	"a) the product-centred view of usability: that the usability of a product is the attributes of the product which contribute towards the quality of use;	<ul style="list-style-type: none"> <li>• Product</li> <li>• Quality of use</li> <li>• Environment/context</li> <li>• User</li> <li>• Task</li> </ul>

Source	Definition	Key aspects
	<p>b) the context of use view of usability: that usability depends on the nature of the user, product, task and environment;</p> <p>c) the quality of use view of usability: that usability is the outcome of interaction and can be measured by the effectiveness, efficiency, and satisfaction with which specified users achieve specified goals in particular environments.”</p>	<ul style="list-style-type: none"> <li>• Interaction outcome</li> <li>• Effectiveness</li> <li>• Efficiency</li> <li>• User satisfaction</li> <li>• Goals</li> </ul>
Bevan, Kirakowskib and Maissela (1991)	“the ease of use and acceptability of a product for a particular class of users carrying out specific tasks in a specific environment.”	<ul style="list-style-type: none"> <li>• Ease of use</li> <li>• Acceptability</li> <li>• Product</li> <li>• Users</li> <li>• Tasks</li> <li>• Environment/context</li> </ul>
Constantine and Lockwood (1999)	<p>“Usability is influenced by many factors. Highly usable systems are easy for people to learn how to use and easy for people to use productively. They make it easy to remember from one use to another how they are used. Highly usable systems help people to work efficiently while making fewer mistakes. We can think of these characteristics as five facets of usability[...]:</p> <ul style="list-style-type: none"> <li>• Learnability</li> <li>• Rememberability</li> <li>• Efficiency in use</li> <li>• Reliability in use</li> <li>• User satisfaction”</li> </ul>	<ul style="list-style-type: none"> <li>• Systems</li> <li>• People (users)</li> <li>• Ease of learning (learnability)</li> <li>• Productivity</li> <li>• Fewer mistakes/Error tolerance</li> <li>• Ease of remembering (memorability/remembrance)</li> <li>• Efficiency of use</li> <li>• Reliability of use</li> <li>• User satisfaction</li> </ul>
Eason (1989)	“the degree to which users are able to use the system with the skills, knowledge, stereotypes and experience they can bring to bear”	<ul style="list-style-type: none"> <li>• Users</li> <li>• System</li> <li>• Users’ skills, knowledge, stereotypes, and experience (user literacy)</li> </ul>
EC (2022)	“Usability refers to how easy it is to navigate through your website. This is determined by aspects including the way your site arranges and displays information, as well as how comfortable it is for users to interact with it.”	<ul style="list-style-type: none"> <li>• Website</li> <li>• Ease of use</li> <li>• Information display/ user interface</li> <li>• Comfort of use</li> <li>• Interaction</li> </ul>
Edwards (2018) for Hewlett Packard (hp)	“When using HCI to develop new tech, it was agreed that four main components factor into the equation: the user, the task, the interface, and the context.”	<ul style="list-style-type: none"> <li>• User</li> <li>• Task</li> <li>• User interface</li> <li>• Environment/context</li> </ul>
Gould and Lewis (1985)	“Any system designed for people to use should be easy to learn (and remember), useful, that is, contain functions people really need in their work, and be easy and pleasant to use.”	<ul style="list-style-type: none"> <li>• System</li> <li>• People (users)</li> <li>• Ease of learning (Learnability)</li> <li>• Ease of remembering (memorability)</li> <li>• Useful functions</li> <li>• Use satisfaction</li> </ul>

Source	Definition	Key aspects
HHS and GSA (2004)	“the quality of a user’s experience when interacting with products or systems, including websites, software, devices, or applications. Usability is about effectiveness, efficiency and the overall satisfaction of the user”	<ul style="list-style-type: none"> <li>• User experience (user literacy)</li> <li>• Interaction</li> <li>• Product/system/websites/software/devices/applications</li> <li>• Effectiveness</li> <li>• Efficiency.</li> <li>• User satisfaction</li> </ul>
Holzinger (2005)	“usability is most often defined as the ease of use and acceptability of a system for a particular class of users carrying out specific tasks in a specific environment”	<ul style="list-style-type: none"> <li>• Ease of use</li> <li>• Acceptability</li> <li>• System</li> <li>• Users</li> <li>• Tasks</li> <li>• Environment/context</li> </ul>
IBM (2008)	“Usability is the discipline of applying scientific principles to ensure that the application or website being designed is easy to learn, easy to use, easy to remember, error tolerant, and subjectively pleasing”	<ul style="list-style-type: none"> <li>• Application/website</li> <li>• Ease of learning (learnability)</li> <li>• Ease of remembering (memorability)</li> <li>• Error tolerance</li> <li>• User satisfaction</li> </ul>
IEEE (1990)	"The ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component."	<ul style="list-style-type: none"> <li>• Ease of learning (learnability)</li> <li>• User</li> <li>• Input preparation/Output interpretation/ task performance</li> <li>• System/component</li> </ul>
(IEEE, 2022)	“the extent to which a product can be used by intended users to achieve specified goals with effectiveness, efficiency, and satisfaction”	<ul style="list-style-type: none"> <li>• Product</li> <li>• Users</li> <li>• Goal achievement</li> <li>• Effectiveness of use</li> <li>• Efficiency of use</li> <li>• User satisfaction</li> </ul>
Interaction Design Foundation (2022)	“Usability is a measure of how well a specific user in a specific context can use a product/design to achieve a defined goal effectively, efficiently and satisfactorily”	<ul style="list-style-type: none"> <li>• User</li> <li>• Environment/context</li> <li>• Product/design</li> <li>• Goal achievement</li> <li>• Effectiveness of use</li> <li>• Efficiency of use</li> <li>• User satisfaction</li> </ul>
(ISO, 2018) <i>Also adapted by HCI experts and organisations including (HFES, 2021; ANSI, 2022; BSI, 2022; Jordan et al., 1996; IEC, 2018)</i>	“extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”	<ul style="list-style-type: none"> <li>• System/product/service</li> <li>• Users</li> <li>• Goals achievement</li> <li>• Environment/context</li> <li>• Effectiveness of use</li> <li>• Efficiency of use</li> <li>• User satisfaction</li> </ul>

Source	Definition	Key aspects
Krug (2000)	“making sure that something works well: that a person of average (or even below average) ability and experience can use the thing—whether it’s a Web site, a fighter jet, or a revolving door—for its intended purpose without getting hopelessly frustrated”	<ul style="list-style-type: none"> <li>• Person (users)</li> <li>• Experience (user literacy)</li> <li>• User satisfaction</li> </ul>
Microsoft (2019)	“Usability is a measure of how easy it is to use a product to perform prescribed tasks.”	<ul style="list-style-type: none"> <li>• Ease of use</li> <li>• Product</li> <li>• Performance</li> <li>• Tasks performance</li> </ul>
Nielsen (1993)	<p>“usability is not a single, one-dimensional property of a user interface. Usability has multiple components and is traditionally associated with these five usability attributes:</p> <ul style="list-style-type: none"> <li>• Learnability</li> <li>• Efficacy</li> <li>• Memorability</li> <li>• Errors</li> <li>• Satisfaction.”</li> </ul>	<ul style="list-style-type: none"> <li>• User interface</li> <li>• Ease of learning (learnability)</li> <li>• Efficacy</li> <li>• Memorability</li> <li>• Errors tolerance</li> <li>• User satisfaction</li> </ul>
Preece (1993)	“a measure of the ease with which a system can be learned or used, its safety, effectiveness and efficiency, and the attitude of its users towards it”	<ul style="list-style-type: none"> <li>• Ease of use</li> <li>• Ease of learning (learnability)</li> <li>• System safety</li> <li>• System effectiveness</li> <li>• System efficiency</li> <li>• User attitude/user satisfaction</li> </ul>
Quesenberry (2003)	<p>“For each of the five dimensions of usability (the 5Es), we think about how it is reflected in requirements for each of the user groups. The 5Es are:</p> <p><b>Effective:</b> How completely and accurately the work or experience is completed or goals reached.</p> <p><b>Efficient:</b> How quickly this work can be completed.</p> <p><b>Engaging:</b> How well the interface draws the user into the interaction and how pleasant and satisfying it is to use.</p> <p><b>Error Tolerant:</b> How well the product prevents errors and can help the user recover from mistakes that do occur.</p> <p><b>Easy to Learn:</b> How well the product supports both the initial orientation and continued learning throughout the complete lifetime of use.”</p>	<ul style="list-style-type: none"> <li>• Effectiveness</li> <li>• Efficiency</li> <li>• Interaction</li> <li>• Users</li> <li>• Goals achievement</li> <li>• User interface</li> <li>• Interaction</li> <li>• User satisfaction</li> <li>• Product</li> <li>• Error tolerance</li> <li>• Ease of learning (learnability)</li> </ul>
Schumacher, Lowry and Schumacher (2010) for the National Institute of Standards and Technology (NIST)	“the effectiveness, efficiency, and satisfaction with which the intended users can achieve their tasks in the intended context of product use”	<ul style="list-style-type: none"> <li>• Effectiveness</li> <li>• Efficiency</li> <li>• User satisfaction</li> <li>• Task</li> <li>• Environment/context</li> <li>• Product</li> <li>• User</li> </ul>
Shackel (2009)	“the capability in human functional terms to be used easily and effectively by the specified range of users, given specified training and user support,	<ul style="list-style-type: none"> <li>• Users</li> <li>• User literacy</li> <li>• Ease of use</li> </ul>

Source	Definition	Key aspects
	to fulfil the specified range of tasks, within the specified range of environmental scenarios. A convenient shortened form for the definition of usability might be ‘the capability to be used by humans easily and effectively’, where Easily = to a specified level of subjective assessment. Effectively = to a specified level of (human) performance.”	<ul style="list-style-type: none"> <li>• Effectiveness of use</li> <li>• User support</li> <li>• Tasks</li> <li>• Performance</li> <li>• Environment/context</li> </ul>
Sharp, Rogers and Preece (2019)	<p>“usability is generally regarded as ensuring that interactive products are easy to learn, effective to use, and enjoyable from the user's perspective. It involves optimizing the interactions people have with interactive products to enable them to carry out their activities at work, school, and in their everyday life. More specifically, usability is broken down into the following goals:</p> <ul style="list-style-type: none"> <li>• effective to use (effectiveness)</li> <li>• efficient to use (efficiency)</li> <li>• safe to use (safety)</li> <li>• have good utility (utility)</li> <li>• easy to learn (learnability)</li> </ul> <p>easy to remember how to use (memorability).”</p>	<ul style="list-style-type: none"> <li>• Products</li> <li>• People (users)</li> <li>• Interaction</li> <li>• Activities/tasks</li> <li>• Environment/context</li> <li>• Effectiveness of use</li> <li>• Efficiency of use</li> <li>• Safety</li> <li>• Utility</li> <li>• Ease of learning (learnability)</li> <li>• Ease of remembering (memorability)</li> <li>• User satisfaction</li> </ul>
Shneiderman and Plaisant (2010)	<p>“1. <b>Time to learn:</b> How long does it take for typical members of the community to learn relevant task? 2. <b>Speed of performance:</b> How long does it take to perform relevant benchmarks? 3. <b>Rate of errors by users:</b> How many and what kinds of errors are made during benchmark tasks? 4. <b>Retention over time:</b> Frequency of use and ease of learning help make for better user retention 5. <b>Subjective satisfaction:</b> Allow for user feedback via interviews, free-form comments and satisfaction scales”</p>	<ul style="list-style-type: none"> <li>• Time of learning/ Ease of learning (learnability)</li> <li>• Speed of performance/ Efficiency</li> <li>• Rate of errors/ Error tolerance</li> <li>• User satisfaction</li> <li>• Task</li> <li>• Users</li> </ul>
Usability Professionals Association (2010)	“the degree to which something - software, hardware or anything else - is easy to use and a good fit for the people who use it.”	<ul style="list-style-type: none"> <li>• Software/hardware</li> <li>• Ease of use</li> <li>• User satisfaction</li> </ul>
Usability.gov (2022)	“How effectively, efficiently and satisfactorily a user can interact with a user interface.”	<ul style="list-style-type: none"> <li>• User interface</li> <li>• Effectiveness</li> <li>• Efficiency</li> <li>• User satisfaction</li> <li>• Interaction</li> </ul>

Table 4.1: Usability Definitions and Key Aspects

Table 4.1 establishes a broad catalogue of usability representation that captures the extent of what it is considered to mean. Hence, we opt to have consistent vocabularies for the key aspects across all of the sources we are examining, as some of the different terminologies can / may end up being combined together. For instance, systems, products, websites, software, devices, applications, and services can be characterized as touchpoints. Also, cognitive load, consciousness, and mental image are all defined as ‘mental models.’ The result of this investigation supports the conclusion drawn from usability studies, including a systematic review of usability, which covers 790 papers from 2001 to 2018 (Weichbroth, 2020). The study confirms that the HCI community has primarily adopted ISO’s definition of usability and standardized it in an unchanged form. The study also asserts that the most frequently identified usability aspects are “efficiency (70%), satisfaction (66%) and effectiveness (58%)”, which are derived directly from the ISO definition. Figure 4.1 shows the total percentage of the key aspects of the most identified usability highlighted in our study, while Figure 4.2 provides a visual insight concerning the most common terms associated with ‘usability’ using a Word Cloud tool (Davies). This study suggests that the ‘touchpoint’ is the most considered aspect in usability studies. Also, facets such as ‘user satisfaction’, ‘user’, ‘efficiency’, and ‘effectiveness’ have been mentioned more repetitively than the other usability aspects.



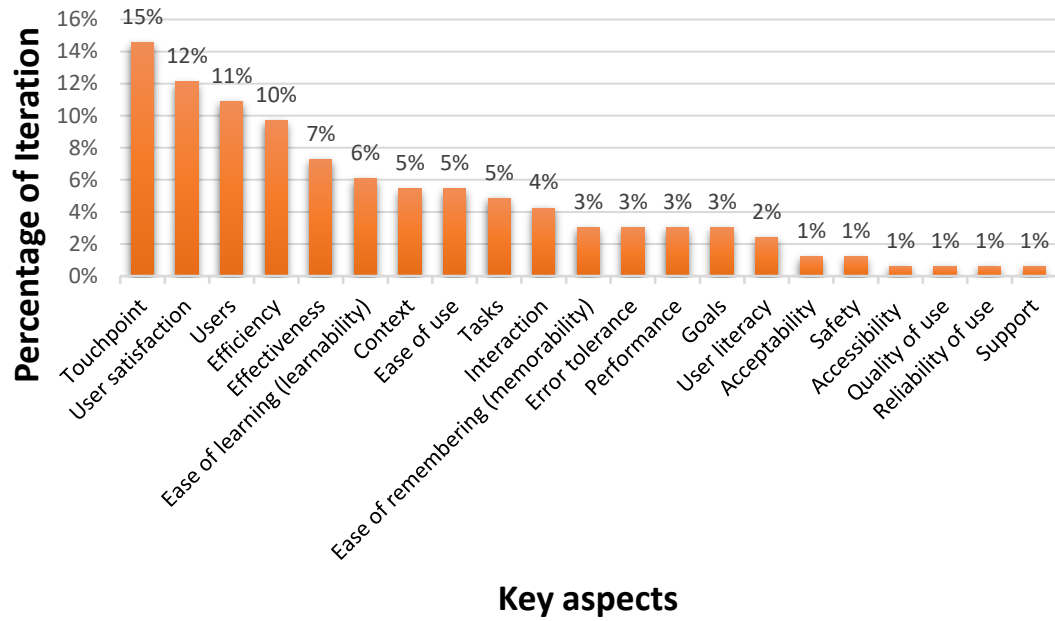


Figure 4.1: The Total Percentage of the Usability Key Aspects Iteration in Studies



Figure 4.2: Word Cloud Denoting Prominence of Words Relating to Usability

### 4.3 Current Usable Security Representation

Having determined the key aspects of usability definitions, next, we examine how different sources also address usable security to see how the usability aspects are relevant in the cybersecurity context. To identify sources that define usable security, the study took the same approach presented in 4.2 above but by using the search string: (*“Usable security” OR “Cybersecurity usability” OR “security usability”*) AND (*definition OR meaning*). Unlike ‘usability’ definitions, there do not seem to be many definitions that specifically focus on what it means for a system or service to be both ‘usable’ and ‘secure’. Table 4.2 presents usable security definitions and the associated key aspects.

Source	Definition	Key aspects
(Garfinkel and Spafford, 1991)	“A computer is secure if you can depend on it and its software to behave as you expect”	<ul style="list-style-type: none"> <li>• Reliability</li> <li>• Compute /Software</li> <li>• Behaviour</li> </ul>
(Hof, 2015)	<p>“usability of security mechanisms is often the afterthought of an afterthought.” “The following set of nine design guidelines coming from the field [usable security] may be of help for software developers:</p> <ul style="list-style-type: none"> <li>• Understandability, open for all users: Usable security should be available for all users. It should especially not discriminate people.</li> <li>• Empowered users: Security mechanisms should allow the user to execute activities in any way he wants.</li> <li>• No jumping through hoops: Users should only be forced to execute as little tasks as possible that exist only for I.T. security reasons. Otherwise, users get annoyed and refuse collaboration with I.T. security mechanisms.</li> <li>• Efficient use of user attention and memorization capability:</li> <li>• Only informed decisions: Security mechanisms should only require as little interaction with the user as possible. The security mechanism should only requests the attention of the user if it is absolutely necessary.</li> <li>• Security as default: Good usability requires efficiency. Hence, the user should not have to configure security when he first starts an application.</li> <li>• Fearless System: The security system should support a positive attitude of the user towards the security system. A user with a positive attitude towards security mechanisms is cooperative and more likely to not feel interrupted by security mechanisms.</li> <li>• Security guidance, educating reaction on user errors: A security system should guide the user in the usage of security mechanisms. Errors should be prevented and there should be ways to “heal” errors.</li> </ul>	<ul style="list-style-type: none"> <li>• Consciousness</li> <li>• Availability/un understandability</li> <li>• Empowerment</li> <li>• Activities/Tasks</li> <li>• Interaction</li> <li>• Efficiency</li> <li>• Ease of remembering (memorability)</li> <li>• Interaction</li> <li>• System/application</li> <li>• Support</li> <li>• User satisfaction</li> <li>• Error tolerance</li> <li>• Consistency</li> <li>• Users</li> </ul>

Source	Definition	Key aspects
	<ul style="list-style-type: none"> <li>• Consistency: Consistency allows users to efficiently fulfill their tasks.”</li> </ul>	
(Johnston, Eloff and Labuschagne, 2003)	<p>The authors propose 6 design criteria for a “successful HCI applied in the area of security:</p> <ol style="list-style-type: none"> <li>1) Convey features: The interface needs to convey the available security features to the user.</li> <li>2) Visibility of system status: It is important for the user to be able to observe the security status of the internal operations.</li> <li>3) Learnability: The interface needs to be as non-threatening and easy to learn as possible.</li> <li>4) Aesthetic and minimalist design: Only relevant security information should be displayed.</li> <li>5) Errors: It is important for the error message to be detailed and to state, if necessary, where to obtain help.</li> <li>6) Satisfaction: Does the interface aid the user in having a satisfactory experience with a system?</li> </ol> <p>Does the interface lead to trust being developed? Trust: It is essential for the user to trust the system. This is particularly important in a security environment.”</p>	<ul style="list-style-type: none"> <li>• User interface / Aesthetic/minimalist design</li> <li>• Visibility</li> <li>• Users</li> <li>• Learnability</li> <li>• Error</li> <li>• User satisfaction</li> <li>• Trust</li> <li>• Environment</li> </ul>
(Nurse <i>et al.</i> , 2011)	<ul style="list-style-type: none"> <li>• “Cybersecurity usability should be considered early on</li> <li>• Accommodate all types of users.</li> <li>• Give informative feedback.</li> <li>• Provide help, advice and documentation.</li> <li>• Error prevention, handling and recovery/Undo</li> <li>• Allow for visibility of system state.</li> <li>• Make security functionality visible and accessible.</li> <li>• Reduce cognitive load associated with system activities.</li> <li>• Give guidance on what tasks users need to perform and where necessary, provide recommendations support.</li> <li>• Emphasize a positive system experience and good levels of user satisfaction.</li> <li>• Aesthetic and minimalistic design.</li> <li>• Design for learnability.</li> <li>• Reduce use of technical and security-specific terms and jargon.</li> <li>• Facilitate the creation of an accurate mental model.</li> <li>• Design security into all application layers.</li> <li>• Design such that security does not reduce performance.</li> <li>• Tools are not solutions.</li> <li>• Separate distinct concepts.</li> </ul> <p>Note that security management interfaces may need additional usability considerations.”</p>	<ul style="list-style-type: none"> <li>• Accessibility</li> <li>• Users</li> <li>• Support</li> <li>• Error prevention</li> <li>• Visibility</li> <li>• Cognitive load</li> <li>• System/application</li> <li>• Tasks</li> <li>• Users</li> <li>• Performance</li> <li>• User satisfaction</li> <li>• Aesthetic/minimalistic design/user interface</li> <li>• Technical terms</li> <li>• Mental model</li> <li>• Tools</li> </ul>
(Saltzer and Schroeder, 1975)	<p>“It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user’s mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized”</p>	<ul style="list-style-type: none"> <li>• User interface</li> <li>• Users</li> <li>• Ease of use</li> <li>• Protection</li> <li>• Mental image</li> <li>• Mechanisms</li> <li>• Goals</li> <li>• Rate of errors/mistakes</li> </ul>
(Theofanos, 2020)	<p>“To date, we have no formal definition of usable security; instead, the field has focused on applied problems and the interactions of cybersecurity and usability.”</p>	<ul style="list-style-type: none"> <li>• Cybersecurity and usability interaction</li> </ul>

Source	Definition	Key aspects
(Whitten and Tygar, 1999)	<p>“Security software is usable if the people who are expected to use it:</p> <ol style="list-style-type: none"> <li>1. are reliably made aware of the security tasks they need to perform;</li> <li>2. are able to figure out how to successfully perform those tasks;</li> <li>3. don’t make dangerous errors; and</li> <li>4. are sufficiently comfortable with the interface to continue using it.”</li> </ol>	<ul style="list-style-type: none"> <li>• People (users)</li> <li>• Reliability</li> <li>• Tasks</li> <li>• Performance</li> <li>• Errors</li> <li>• User satisfaction</li> <li>• User interface</li> </ul>
(Yee, 2002)	<p>In order to have a chance of using a system safely in a world of unreliable and sometimes adversarial software, I need to have confidence in the following statements:</p> <ul style="list-style-type: none"> <li>• Things don’t become unsafe “all by themselves” (Explicit Authority)</li> <li>• I can know whether things are safe (Visibility)</li> <li>• I can make things safer (Revocability)</li> <li>• I don’t choose to make things unsafe (Path of Least Resistance)</li> <li>• I know what the system can do for me (Expected Ability)</li> <li>• The system can safely do what I want (Appropriate Boundaries)</li> <li>• I can tell the system what I want (Expressiveness)</li> <li>• I know what I’m telling the system to do (Clarity)</li> <li>• The system protects me from being fooled (Identifiability, Trusted Path)”</li> </ul>	<ul style="list-style-type: none"> <li>• System/ Software</li> <li>• Explicit Authority (safety related)</li> <li>• Visibility (safety related)</li> <li>• Revocability (safety related)</li> <li>• Path of Least Resistance (safety related)</li> <li>• Expected Ability</li> <li>• Boundaries Appropriation (safety related)</li> <li>• Expressiveness</li> <li>• Clarity</li> <li>• Identifiability, Trusted Path (safety/protection related)</li> </ul>
(Zurko and Simon, 1996)	<p>“security models, mechanisms, systems, and software that have usability as a primary motivation or goal.”</p>	<ul style="list-style-type: none"> <li>• Security models/mechanisms/system/software</li> <li>• Goal</li> </ul>

Table 4.2: Usable Security Definitions and the Key Aspects

A considerable body of research examines usable security. Although there are different perspectives when addressing usable security, no widely accepted formal definition has been observed so far. In addition, few studies clearly outline the different dimensions that may contribute to understanding usable security despite some efforts.



important usability aspects such as efficiency and learnability are still considered outliers in usable security studies. The ‘context of use’, which has a degree of importance in usability studies, also is not given the required attention in the usable security community. The lack of consistency in defining and presenting usable security motivates this work to create an initial definition, which will be discussed in the next section.

#### **4.4 Usable Security Definition and Framework**

To refine the understanding of usable security, a definition was developed through a structured analysis of existing studies. As mentioned in sections 4.2 and 4.3, the process began by reviewing established definitions of usability. Key usability aspects such as touchpoints, effectiveness, efficiency, satisfaction, and context of use, and goals were highlighted. A parallel analysis was conducted on existing usable security studies, which lack a widely accepted formal definition. Certain usability concepts such as user satisfaction, touchpoints, and user are also emphasized in usable security research, but other aspects, like context of use, still underrepresented in the cybersecurity domain. The outcomes, along with the understanding that the cybersecurity domain is increasingly adopting concepts long established in HCI, resulted in the development of a holistic definition:

**“Usable security is utilizing usability concepts to enable cybersecurity concepts.”**

**Where usability concepts = all usability key aspects and requirements,  
and cybersecurity concepts = all cybersecurity aspects and requirements.**

The definition intentionally connects the two domains by incorporating all essential usability and cybersecurity criteria. Furthermore, a primary result arising from assessing usability and usable security studies is establishing a framework of usable security by looking at the different aspects identified in the literature. The perspective of this definition is to be detailed in the usable security framework presented in Figure 4.5.

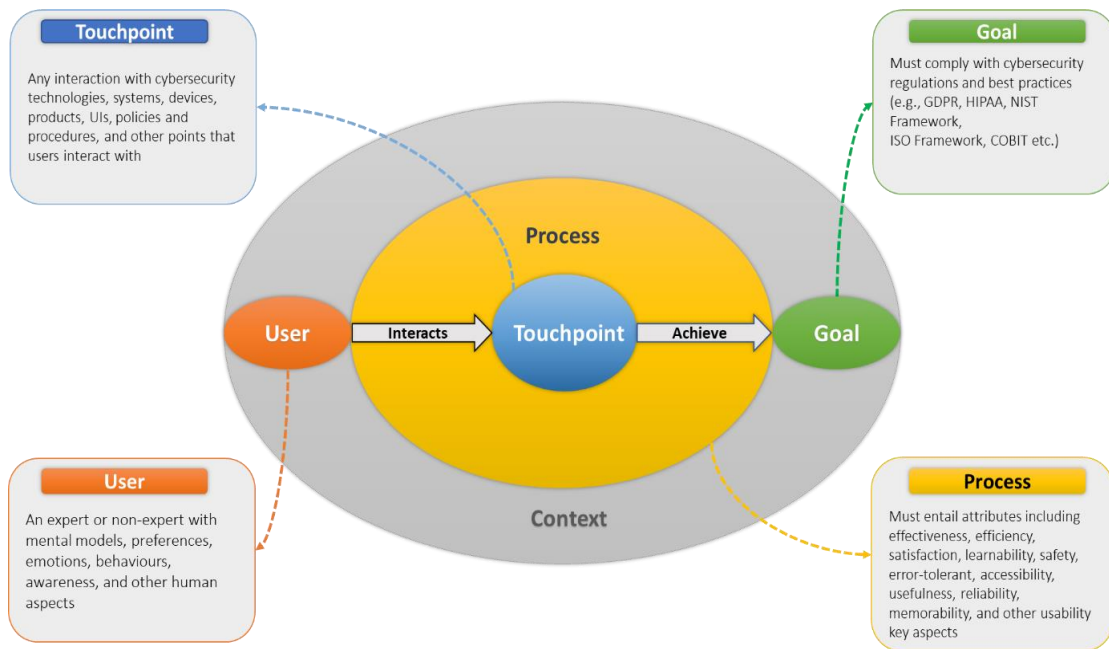


Figure 4.5: Usable Security Framework

An outcome of reviewing usable security representations is a framework that characterizes the relationship between different aspects of usable security. The framework provides a means to operationalize usable security definition, taking into account all important facets of usability from both HCI and cybersecurity perspectives

The main elements of this framework are as follows:

- **User:** a person (expert or non-expert) with expectations, perceptions, and beliefs about the touchpoint they will interact with.
- **Touchpoint:** any point that the user interacts with and creates their experience. This includes digital and physical systems, cybersecurity policies, and procedures.
- **Process:** The action(s) constructed for the user to achieve a goal. The process should be centered on users' needs and meet the usability key aspects based on the context of use.
- **Goal:** a specific aim that users or organizations aim to achieve while considering cybersecurity best practices, each in their context.

- **Context:** the set of conditions that accommodate the process to achieve the goal.

The framework provides a mechanism to define usable security, taking into consideration all the key aspects of usability from both HCI and cybersecurity perspectives. The mechanism implies that a user with a level of experience, awareness, emotions, or specific behavior interacts with a touchpoint (technology, device, product, or user interface) to achieve a goal that should comply with the cybersecurity best practices and requirements in a specified context of use. The process of interaction to achieve the goal should fulfill a set of multiple attributes (e.g., effective, efficient, satisfactory, safe, simple, accessible, reliable, error tolerance, trustworthy, or aesthetic). Organizations can use the existing evaluation methods to assess if the process meets these attributes or if they should value one quality over another based on the context of use and threat modeling process. Also, designers and policy and procedure makers should keep in mind that the touchpoint they create for the user to interact with should make the process cybersecurity compliant.

One example to clarify the operation in the proposed framework is that a user interacts with a banking application using a biometric signature to log into the system to make a bank transfer. In this context, biometric authentication facilitates a simple, secure, and efficient interaction with the application (touchpoint) to achieve a certain goal in accordance with the best cybersecurity practices. The journey of the user experience once they log in to the system until they make the transfer holds a number of attributes that would leave the user with a positive experience while complying with cybersecurity requirements. Another example is an organization with a clean desk and clear screen policy, which requires all users to clear their desks at the end of the day and lock their devices' screens as they leave their offices. In this case, the policy is the touchpoint. If a user has to deal with this policy, the organization is responsible for making the process effective, efficient, and satisfactory. For example, while implementing such a policy, the organization should provide the employees with clean desk equipment, such as lockable drawers and storage boxes, as an alternative to keeping documents lying on the desk.



If the users' interaction with the touchpoint is not usable, there will be no guarantee that the goal they are trying to achieve will comply with best cybersecurity practices because users are always going to find ways to make the touchpoint usable for themselves, which can sometimes damage the whole security system. In many cases, the user cannot be blamed for not abiding by the cybersecurity policies and rules set by organizations if these are not usable while there is a less secure and more usable way to complete a task. Further, some users would be encouraged to bypass the unusable security rules to achieve more important goals. For example, a doctor bypassing or ignoring the security system to access a patient record to save their life.

## **4.5 Chapter Summary**

It has been a significant achievement to develop technical security solutions that enable organizations to mitigate serious security risks. Nevertheless, these solutions do not provide adequate protection against all types of threats on their own. The effectiveness of the overall security systems depends on people's perception and behavior around security measures. Usable security is one way to maintain people's behaviors in organizations. This chapter proposes a usable security definition. The definition is then accompanied by a usable security framework that helps provide a structured approach to supporting prior studies' efforts and ensuring that all relevant usability aspects are considered when implementing security measures. The framework asserts that the notion of human-centric must be considered and applied to all interactions with security processes and technological measures. After exploring usable security and security culture in this chapter and Chapter 2, the next chapter presents the methodological approach for investigating the factors influencing their relationship.

# **Chapter 5: Investigating Usable Security and Security Culture in Organizational Settings**

## **5.1 Introduction**

This chapter explains the methodological approach underpinning the investigation conducted in this research. It begins by detailing the data collection methods and how they were designed to effectively address the research objectives. Next, it describes the data analysis techniques employed to interpret and draw meaningful input from the collected data. In addition, the chapter examines the measures taken to ensure the research process's reliability and validity, highlighting the ethical considerations observed throughout the study and emphasizing the commitment to conducting research with integrity.

## **5.2 Data Collection Methods**

Data can be facts, numbers, letters, or symbols that report factors (National Academies Press, 1999), and collecting data is crucial for the research to understand the current state of studies and practice in a particular domain, such as security culture and the associated factors. It also enables the identification of trends within a large sample across different settings and the exploration of the context and reasons behind people's behaviors and attitudes towards a given situation. This study employed a mixed-method approach to data collection, utilizing both quantitative and qualitative methods to collect data.

The process began with reviewing studies, as shown in Chapter 2, to identify practical approaches for studying security culture and its related factors. The review provided crucial insights into existing research and best practices relevant to this study's objectives. The review process was followed by designing the required methods to gather insights based on people's cybersecurity experiences and how usability influences their behavior in managing it within their organizations. This involved conducting a survey study followed by semi-structured interviews. The goal of combining these methods is to strengthen the study's conclusions (Schoonenboom and Johnson, 2017). Therefore, following the literature review, the study combined quantitative and qualitative methodological approaches through a survey and semi-structured interviews to measure the extent to which the usability of security influences

---

security culture. This mixed-method approach supports the study and helps in achieving an extensive breadth and depth goal.

### **5.2.1 Survey Design and Implementation**

Surveys are one of the most widely utilized forms of measurement and observation that have been used in studies. They can be employed to evaluate how a particular population behaves or perceives a certain concept (Sinkowitz-Cochran, 2013), helping the researchers obtain knowledge of the topic being studied. The topic of the study could be individuals, teams, organizations, communities, or applications and systems (Pinsonneault and Kraemer, 1993). There are various methods to carry out surveys, including in-person, over the phone, via interactive voice response, email, or online platforms. The resources available to the researcher and the topic/population being studied all play a major role in the mode selection (Sinkowitz-Cochran, 2013).

Moreover, it is essential to set the goal of the survey and the type of data that must be generated from the survey in order to obtain meaningful data (Dillman, 2011). The survey in this study was designed to collect participants' perceptions of usable security measures and their relation to the wider security culture in their organizations. These participants are from different industries, roles, and levels of IT literacy. Despite numerous surveys were reviewed during the initial phase, they do not address the specific objectives of this research sufficiently. The literature indicates that many factors, including organizational support and user behavior are becoming increasingly important in forming a security culture, but it also showed that there is a notable gap in understanding the role of usable security in this context. As a result, the survey was created from the ground up to also fit with the study's hypotheses stated in subsection 5.3.1.2 rather than adapting existing instruments. The purpose of the questions was to gather users' views about usable security and to determine how these views might affect how they interact with security measures. This approach ensures that the survey could yield relevant data and hypothesis-driven details while also addressing an underexplored area in cybersecurity research.

The survey was conducted using Jisc Online Survey (JOS), a GDPR-compliant platform. The survey consists of different sections, including:

- Demographic questions to gather information about participants' age, gender, background, education level, job title, geographic location, and the organization's industry.
- Security culture-related questions with several Likert scale items and an open-ended question to assess participants' perceptions of how usable security and other factors impact security culture in their organizations.
- Usable security-related questions, including Likert scale items, open-ended questions, and close-ended questions, are used to obtain preliminary insight into people's perceptions of usable security and its impact on their organization's culture.
- A section with a Likert scale question and an open-ended question to determine how the study participants assess the impact of usable security on their organizations' security culture.
- A final section with multiple-choice and open-ended questions was designed to determine the main drivers and barriers for people to comply with cybersecurity practices in their organizations.

The survey's open-ended questions and free-text fields enable participants to elaborate more or provide further insights if needed. Overall, the survey consists of 25 items, including an invitation to the second part of the study, and it was estimated to be completed in approximately eight to ten minutes. Several survey questions were designed to address the hypotheses detailed in subsection 5.3.1.2. Furthermore, participants were provided with definitions of key terms used in the survey to enhance comprehension and ensure uniform interpretation of these terms. The following terms and their corresponding definitions were provided to participants:

- **Cybersecurity usability issues** are difficulties users encounter while using security-related tools or systems, such as lengthy security procedures that hinder productivity, confusing user interfaces, or difficulty remembering processes (e.g., complex passwords).
- **Cybersecurity actions** refer to user behaviors to safeguard systems and data, including regular software updates, strong passwords, data backup, and identifying suspicious emails or messages.

- **Cybersecurity technologies** encompass tools, software, and hardware solutions like firewalls, antivirus software, and encryption mechanisms protecting systems, networks, and data.
- **Cybersecurity procedures** include documented processes and guidelines addressing security risks and maintaining a proactive security posture, such as access control policies and security training and awareness sessions.

The survey aimed to obtain detailed insights into the perceptions of the usability of security measures within their workplace and a means of understanding the complex dynamics of security practices in the organization's settings. This data collection strategy aligns with the study's objectives and offers a foundation for further analysis and interpretation in later phases of the research.

### 5.2.2 Semi-Structured Interviews

Incorporating semi-structured interviews has been shown to be beneficial in prior research (Kallio *et al.*, 2016). With the use of open-ended questions and follow-up questions, the researcher can explore specific concerns that the participants did not have the chance to articulate during the survey phase (Timans, Wouters and Heilbron, 2019). Moreover, interviews facilitate more exploration than is typically achievable with the surveys alone. Traditionally, interviews have been conducted face-to-face, but they have increasingly transitioned to online modes (Kvale and Brinkmann, 2009), and they continued to transfer online, especially after the global COVID-19 pandemic (Sah, Singh and Sah, 2020). The shift to online interviews offers various advantages, including reaching a wider geographical location and the convenience of interacting with participants globally. This is particularly valuable, given the constraints on participants' availability for face-to-face meetings, although there are challenges associated with online meetings, such as the lack of non-verbal cues and the possibility of less personal interactions.

Participants had the option to participate in the survey only by filling it out or in the survey and the interview by completing the survey and providing their contact details for a follow-up interview. The part involved follow-up interviews aimed at gaining deeper insight into users' behaviors and attitudes towards security usability in their

workplace, identifying areas that could promote a positive security culture. The interview process started by revisiting noticeable parts from the open-ended responses to enable the participants to express their thoughts further. That was followed with an open-to-close question format, with questions encouraging participants to share their opinions and concerns openly. This planned yet customizable approach is helpful for gathering in-depth data (Kvale and Brinkmann, 2009), making semi-structured interviews an essential supplement to the survey discussed in the previous section. The interpretations will then be drawn based on the combined strength of both approaches.

### **5.2.3 Ethical Considerations and Approval**

Participation in the survey involved using an online data storage platform; however, the collection process did not gather any sensitive information about the participants or their organization, minimizing risk. The data collected, which is anonymized, was stored on the University of Nottingham's OneDrive server. Participants were informed that providing contact information during the survey would only be used to invite them to join the interview part. The participants involved in this study adhered to the ethical guidelines established by the University of Nottingham. Participants were invited to consent to participate voluntarily and were informed that they had the right to withdraw from the study at any time. Anonymity was guaranteed for all participants, and the collected data was solely used for research purposes. Ethical approval for this study was granted under application reference number **CS-2022-R32**, as shown in Appendix I.

### **5.2.4 Pilot Study**

The survey questions and the interview method were piloted with twenty participants, ten of whom provided feedback through the online survey platform, while the other ten, including three involved in pilot interviews, submitted their feedback via emails and in-person meetings. The pilot study engaged professionals and academics from the information technology and cybersecurity community and users from other fields who regularly use technology in corporate settings. The participants in the pilot were selected to ensure a diverse range of backgrounds, thereby enhancing the validity and applicability of the survey questions. Table 5.1. details the pilot participants

information. Subsequently, the survey was refined based on participants' feedback from the pilot test before its official distribution.

<b>Pilot Participant No.</b>	<b>Gender</b>	<b>Age Group</b>	<b>Mode of Participation</b>	<b>Industry Field</b>
PP1	Male	45-54	Online surveys	Energy supply
PP2	Male	35-44	Online surveys	Education
PP3	Male	35-44	Online surveys	Education
PP4	Male	45-54	Online surveys	IT
PP5	Female	55-64	Online surveys	Education
PP6	Female	35-44	Online surveys	Education
PP7	Female	25-34	Online surveys	IT
PP8	Male	35-44	Online surveys	Energy supply
PP9	Female	45-54	Online surveys	Education
PP10	Male	25-34	Online surveys	Energy supply
PP11	Male	45-54	Online surveys & Email feedback	IT
PP12	Male	35-44	Online surveys & Email feedback	Education
PP13	Female	45-54	Online surveys & Email feedback	Education
PP14	Male	25-34	In-person	IT
PP15	Female	25-34	In-person	Education
PP16	Male	45-54	In-person	IT
PP17	Male	55-64	In-person	IT
PP18	Male	45-54	In-person	IT
PP19	Female	25-34	In-person	Education
PP20	Female	35-44	In-person	Education

Table 5.1: Pilot Participants

### 5.2.5 Participant Recruitment Techniques

The study utilized a combination of convenience sampling and snowball sampling techniques to recruit participants:

1. Convenience Sampling: this approach involves selecting individuals who are accessible to the researcher for survey distribution (Brewerton and Millward, 2001), and this is the most common sampling method used by researchers (Acharya *et al.*, 2013). The survey was distributed via emails, direct messages, various social media platforms, such as LinkedIn and WhatsApp, and by using posters and flyers at conferences and events to recruit participants.



2. Snowball Sampling: in this approach, researchers request initial participants to recommend others who meet the research criteria, who then recommend other participants who fit the criteria, and so on (Parker, Scott and Geddes, 2019). Therefore, initial participants were asked to suggest and recommend more eligible individuals who fit the study's criteria and are willing to take part. This approach was mainly used by asking social networks to invite their connection to take part and also during the qualitative part of the study by requesting interviewees to invite others.

It is worthwhile to note that convenience and snowball sampling are both valuable recruitment strategies in studies with limited resources and time. Convenience sampling, in which readily available and willing participants are selected, is practical and cost-effective, particularly in exploratory research phases or preliminary studies, since it requires minimal planning and expense (Emerson, 2021). As a further advantage, snowball sampling is particularly effective at engaging hard-to-reach populations through the use of existing participants and networks. Hence, increasing engagement (Naderifar, Goli and Ghaljaie, 2017; Valerio *et al.*, 2016). Furthermore, combining these sampling methods results in a more diverse and representative sample, allowing detailed data to be collected from individuals who might not be accessible with one of these methods alone (Kirchherr and Charles, 2018; Petersen and Valdez, 2005). Figure 5.1 illustrates the flowchart detailing the participant recruitment

process.

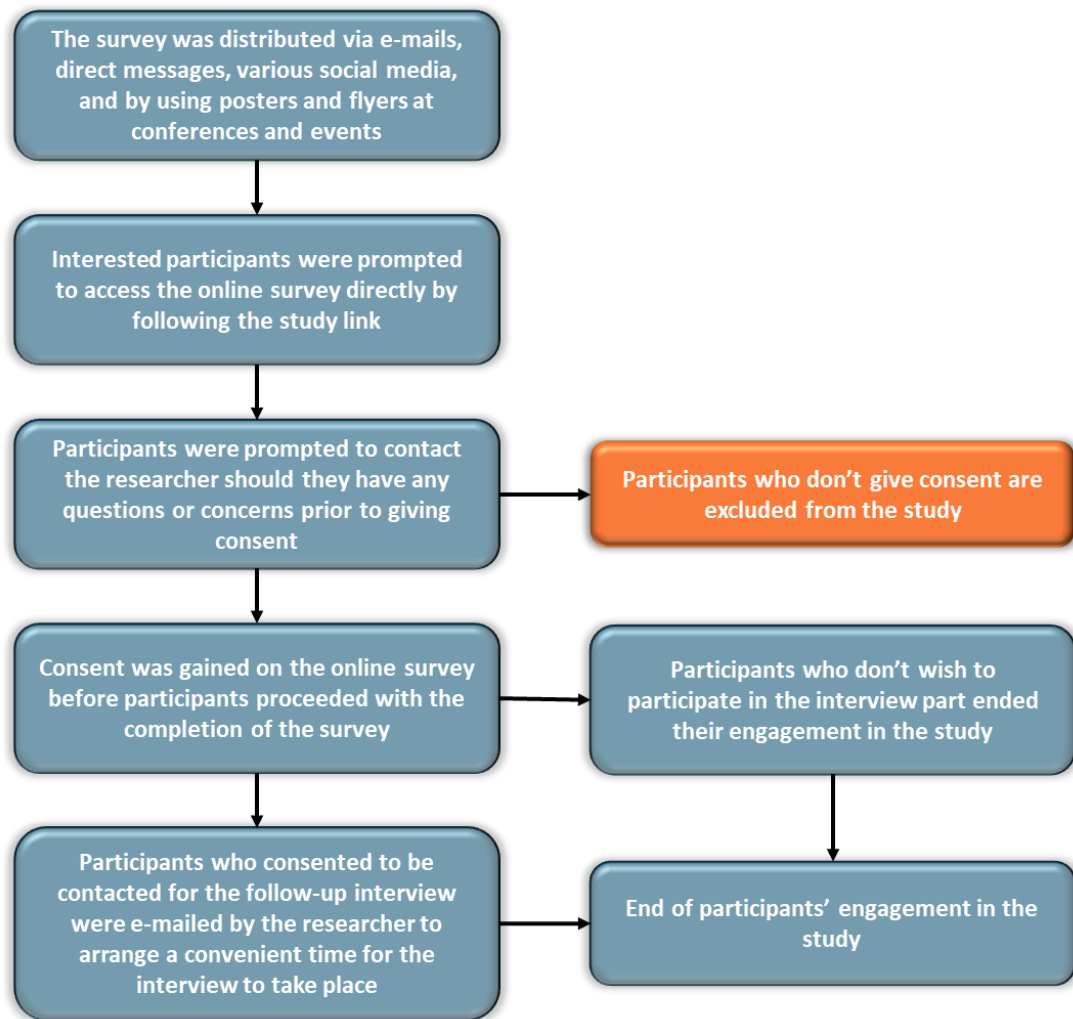


Figure 5.1: Participant Recruitment Flowchart

Interested individuals were encouraged to contact the researcher with any questions or concerns before providing consent to participate in the study. Participants who did not consent were not able to proceed with the survey and were excluded from further participation. Consent was obtained online at the beginning of the survey before participants proceeded with its completion. At the end of the survey, participants were able to provide their email addresses if they were willing to be contacted for an approximately 20-minute interview. Those who opted out of the interview phase could conclude their engagement by clicking 'Finish' to end the survey. Participants who consented to a follow-up interview were contacted via email after survey completion to schedule a convenient interview time. The interviews were conducted with eight

participants. The conclusion of the interviews marked the end of the participant's involvement in the study, although they were welcome to reach out with additional thoughts or questions.

Respondent progress							
p.1	p.2	p.3	p.4	p.5	p.6	p.7	p.8
948	54	19	22	8	5	7	203

Figure 5.2: Respondent Progress

Figure 5.2 presents an overview of the survey participation, indicating the instances when respondents initiated but did not finish the survey and the specific pages at which they discontinued their participation. The respondent progress table describes the final page participants visited before exiting the survey. For example, a count of '948' under 'p.1' indicates that 948 people accessed the study's link but chose not to proceed. Similarly, '54' under 'p.2' shows that 54 respondents reached the second page before abandoning their participation. Notably, 203 people successfully navigated to 'p.8' and submitted their responses. The respondent progress figure suggests that the total number of people who accessed the survey (i.e., from those who stopped at page 1, up to and including those who completed it) is 1266 participants, and the overall completion percentage is 16.03%. While dropouts from surveys can occur for a variety of reasons, including connectivity issues, interruptions, or lack of interest in the topic, JISC (2024) suggests that a high dropout rate on the second last page may indicate unclear instructions. Notably, only seven respondents left the survey at this point in the study, suggesting that the survey instructions were clear.

### 5.3 Data Analysis Approaches

It is important to highlight the methods employed in this study to ensure clarity in the data analysis process. As indicated in the data collection section, this study utilizes a mixed-method approach, integrating quantitative and qualitative methods to effectively evaluate the impact of cybersecurity usability on the overall security culture in organizations. Quantitative data acquired via a survey instrument was analyzed using statistical methods such as descriptive statistical analysis and correlation and

regression tests in the Statistical Package for the Social Sciences (SPSS) to test the study hypotheses and investigate correlations between relevant variables derived from closed-ended survey questions. Furthermore, qualitative data from open-ended survey responses and the semi-structured interviews were analyzed by NVivo, a qualitative data analysis software that helps discover themes and insights from participants' input (NVivo, 2024). This mixed-method approach helps provide an in-depth perspective of the research topic by combining the breadth of the quantitative analysis and the depth of the qualitative interpretation. The following sections reflect the data analysis process.

### **5.3.1 Quantitative Data Analysis**

The quantitative data obtained from the investigation process is analyzed using descriptive statistical analysis. This facilitates a comprehensive understanding of the data, the relationships identified through the research, and the significance of the results.

#### ***5.3.1.1 Descriptive analysis of the survey responses***

A descriptive statistical analysis was used to analyze the data acquired from the survey responses. The analysis is focused on summarizing the numerical results from the responses to provide a clear and concise understanding. The study employs visual representations, such as pie charts, column charts, and other graphical representations in order to communicate key findings within the data. These figures are accompanied by a detailed explanation that highlights the patterns and insights revealed by the data.

#### ***5.3.1.2 Hypotheses Testing***

The increasing reliance on humans to adopt and adhere to cybersecurity measures underscores the importance of their behavior in improving security outcomes. However, research indicates that users frequently encounter hurdles that hinder their capacity to make appropriate security decisions (Furnell *et al.*, 2018). Factors such as time pressures exacerbate this issue, compelling users to rely on quick alternatives, which increase the likelihood of errors and non-secure workarounds (Chowdhury, Adam and Teubner, 2023). These challenges raise the question of whether integrating

---

usable security solutions could address these limitations and encourage better security practices.

Research further suggests that user behavior significantly influences cybersecurity outcomes, particularly in minimizing the impact of security incidents (Moustafa, Bello and Maurushat, 2021). Also, familiarity with workplace cybersecurity policies and procedures can enable users to manage cybersecurity tasks more effectively, increasing their adherence to security measures (Li *et al.*, 2019). Therefore, well-informed and supported users are more likely to make secure decisions, which highlights the potential of usability-focused interventions to drive behavioral change. Additionally, organizational support has been identified as a critical factor in promoting cybersecurity compliance (Guo *et al.*, 2011). Despite these evidences, the role of usable security solutions in directly addressing these challenges has received limited attention.

While general research highlights the influence of user behavior and organizational support on cybersecurity, there remains a gap in understanding the contribution of usable security. By examining the effect of usable security and users' perception of usability on user confidence, motivation, and compliance, hypotheses H1<sub>A</sub> through H5<sub>A</sub> aim to address these gaps. For each, a null hypothesis (H<sub>0</sub>) is also defined:

- **H1<sub>A</sub>:** *There will be a positive correlation between users' perception of usable security measures and their behavior towards unusable security measures within the organization.*
- **H1<sub>0</sub>:** *There is no significant correlation between users' perception of usable security measures and their behavior towards unusable security measures within the organization.*

H1<sub>A</sub> assesses the relationship between users' views of usable security measures and their behavior towards unusable security measures within the corporation. This hypothesis aims to determine whether a user's perception of usable or unusable security measures affects their overall security behaviors and attitudes. Variables of interest:

- *Independent Variable:* Perception of usable security measures within the organizations. This variable evaluates participants' views on the usability of cybersecurity measures implemented in their workplace.
- *Dependent Variable:* Security behaviors and attitude. This variable reflects the actions and attitudes towards security protocols that are perceived as complex or ineffective. It captures the extent of users' adherence to these measures.

The correlation test is used to determine the strength and direction of the link between users' perceptions of usable security and their behavioral responses to unusable security measures. For example, a positive correlation coefficient would imply that a more positive perception of usable security measures is related to more positive or compliant behavior. Following the correlation analysis, regression testing is used to determine the predictive potential of perceived usable security on security behaviors and attitudes. The regression analysis assists in determining how much variation in security behavior and attitudes may be explained by perceptions of usable security. It can, most importantly, be used to predict which usability aspect might affect security culture. Conducting such tests is essential to understand how perceptions of cybersecurity measures in organizations influence the actual behavior and attitude among employees. Understanding usable security elements that significantly impact employee behavior can inform cybersecurity initiatives such as training or awareness programs to focus on the problem and create tailored programs that address these aspects, resulting in higher compliance rates and a more robust security culture.

- *H2A: A positive perception of usable security is negatively associated with the frequency of reported incidents of bypassing security measures.*
- *H2o: There is no significant association between users' positive perception of usable security and the frequency of reported incidents of bypassing security measures.*

**H2A** suggests that the favorable perception of usable security measures negatively correlates with reported incidents of bypassing security measures. This hypothesis seeks to determine whether usable security measures are associated with fewer bypassing of these measures. Variables of interest: H2A

- 
- *Independent Variable:* Bypassing security measures. This variable is categorical with binary responses “Yes” or “No,” denoting whether respondents have bypassed security measures. It is worth noting that there is a high probability that people might not be comfortable acknowledging or admitting to bypassing security measures. However, the hypothesis will test the reported incident.
  - *Dependent Variable:* Positive perception of usable security measures within the organizations. This variable looks into how employees perceive the usability of security measures implemented in place.

Since this hypothesis includes a categorical (binary) variable, a normality test was used to determine whether traditional parametric tests, such as t-tests, are suitable. The p-value running the normality test is 0.015, indicating that data is not normally distributed; the Mann-Whitney U test is accordingly selected. This test will evaluate if there is a statistically significant difference in respondents’ perceptions of usable security measures between those who have bypassed security measures and those who have not. The Mann-Whitney test is appropriate for comparing differences between two independent groups.

- *H3<sub>A</sub>: Ease of understanding and performing security actions predicts users’ confidence with security policies within organizations.*
- *H3<sub>B</sub>: Ease of understanding and performing security actions does not significantly predict users’ confidence in organizational security policies.*

**H3<sub>A</sub>** posits that the ease of understanding and performing security actions predicts users’ confidence in complying with security requirements within organizations. This hypothesis aims to investigate whether the perceived ease of understanding of security actions has significant influences on users’ confidence in their ability to effectively comply with security requirements. Variables of interest:

- *Independent Variable:* Perceived ease of understanding and performing security actions within the organization. This variable assesses employees’ perception of how cybersecurity measures are clear and easy for them to adopt.

- *Dependent Variable:* Confidence in following cybersecurity requirements. This variable measures employees' confidence in their capacity to follow the cybersecurity measures established within their organizations.

Simple linear regression is used to test H3<sub>A</sub>, which helps quantify the variations in the perception of the usability of security actions and how that can explain changes in users' confidence in following cybersecurity requirements. The theory here is that higher confidence among employees in their ability is likely to result in higher compliance rates. The regression analysis is suitable since it helps quantify if usability predicts employees' confidence in following security requirements. The findings can inform organizational decisions regarding enhancing usability if they wish to boost employees' confidence in following security measures. By testing the relationship between the independent and dependent variables in the hypothesis, it is possible that the analysis can support creating more usable security practices and enhance the overall security culture.

- *H4<sub>A</sub>: Ease of understanding and performing security actions is negatively associated with the frequency of reported security incidents.*
- *H4<sub>B</sub>: Ease of understanding and performing security actions is not significantly associated with the frequency of reported security incidents.*

H4<sub>A</sub> proposes that the ease of understanding and performing security actions is negatively correlated with the frequency of reported security incidents within organizations. This hypothesis examines whether clearer and simpler security measures can lead to more frequent reporting of security incidents, possibly as a result of increased awareness and feeling of responsibility among employees. Variables of interest:

- *Independent Variable:* Perceived ease of understanding and performing security actions within the organization. This variable assesses employees' perception of how cybersecurity measures are clear and easy for them to adopt.
- *Dependent Variable:* Frequency of reported security incidents. This variable assesses the frequency with which respondents say that they have reported security incidents or not.



Logistic regression is chosen for this analysis to explore the relationship between the perceived usability of security and the likelihood of reporting incidents. This analysis enables the examination of whether the perceived usability might affect the probability of encouraging employees to report security incidents, possibly due to greater awareness or a lower barrier to reporting incidents. Understanding this relationship is vital for organizations that aim to enhance their response strategies. The assumption is that empowering their employees to understand and perform security measures will result in increased incident reports, allowing for quicker responses. That is to say, usable security improves security incident management.

- *H5<sub>A</sub>: Organizational support and policies promoting reporting usable security issues positively influence employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches.*
- *H5<sub>o</sub>: Organizational support and policies promoting the reporting of usable security issues have no significant influence on employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches.*

H5<sub>A</sub> hypothesizes that organizational support and policies that promote reporting usable security issues influence employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches. This hypothesis aims to assess whether the support provided to the employees within an organization can boost their confidence in effectively handling security issues. Variables of interest:

- *Independent Variable:* Organizational support for reporting usable security issues. This variable assesses respondents' perceptions of the support provided by the organizations to employees for reporting issues related to security usability.
- *Dependent Variable:* Employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches. This variable evaluates employees' confidence in their capacity to identify possible security threats and report them effectively.

Regression analysis is used to evaluate the impact of organizational support on employees' confidence and readiness to identify and report threats. This analysis helps

understand the direct relationship between organizational support for security measures and employees' confidence in identifying any risks or flaws that might negatively affect their organization's cybersecurity posture. The hypothesis tests whether higher confidence is linked to more proactive behavior in reporting vulnerabilities. The findings can provide insights for organizational leaders and policymakers to craft or revise their initiatives to support employees, resulting in the overall effectiveness of the cybersecurity measures. Most importantly, it could show if the impact of supportive policies and empowerment steps improves security and fosters a culture of accountability.

In each of the hypotheses, the independent variables are the variables that are considered to impact or predict change, whereas the dependent variables are the outcomes that are being measured. The purpose of determining independent and dependent variables is to examine the strength, direction, and nature of the relationships between the variables. For example, whether improvements in usability lead to increased compliance, confidence, or fewer security incidents. This enables us to verify the study's hypotheses and draw meaningful conclusions regarding cause-effects and potential associations between users' behaviors and security culture.

### ***5.3.1.3 Data Processing and Cleaning***

For quantitative data analysis in SPSS, numerical values are recommended to be used to code different variables (DeCoster and Claypool, 2004). Additionally, specific scales needed to be reversed for some survey variables because the wording does not align consistently with other variables. Some questions in the survey have negative phrasing, or what is considered a 'good' outcome is a high score on one variable and low on another. The object of reversal enables comparing descriptive stats, such as means or medians, across all questions regardless of whether they are positively or negatively phrased. For example, in Question 14 (as shown in Appendix II), participants were asked to rate the likelihood of taking specific actions when finding a cybersecurity task difficult to perform. One option is "Complain/report to the responsible person or team (e.g., supervisor, I.T. department, cybersecurity team)," while another option is "Find my own ways around the action." The different likelihood ratings for these actions have varied implications for the organization's

cybersecurity. Complaining or reporting demonstrates awareness and aids in addressing usability issues for enhanced cybersecurity practices. On the other hand, users finding their own ways around actions introduces security vulnerabilities and risks. The values of the second option were reversed to standardize the scale as follows:

Old Value	New Value
1	5
2	4
3	3
4	2
5	1

Table 5.2: SPSS Scale Reversal

This concept is applied to all responses which need scale reversal. Also, all the “I don’t know / Not able to comment” responses were excluded from the analysis as they don’t contribute to the main rating scale.

### 5.3.2 Qualitative Data Analysis

Qualitative research plays a critical role in offering depth and context for the study overall and understanding the underlying reasons behind the quantitative findings presented in numerical form (Rouder *et al.*, 2021). The qualitative part of the study focuses on analyzing open-ended responses from the survey and data collected through semi-structured interviews. Throughout this study, the qualitative data was subjected to a thematic analysis, which is a qualitative method of analysis designed to identify and explore patterns of meaning within a dataset (Braun and Clarke, 2006). There has been substantial growth in the use of thematic analysis, and it is now recognized as an integral approach to qualitative research (Guest, MacQueen and Namey, 2012; Vaismoradi *et al.*, 2016). Themes are identified through inductive and deductive means, where inductive themes are derived organically from the data itself, and deductive themes are based on pre-existing models and theories (Braun and Clarke, 2006). Using thematic analysis allows researchers to explore data without being restricted by pre-existing theoretical assumptions (Braun and Clarke, 2021). Thematic analysis is thus suitable for a wide range of research questions and contexts, especially when investigating broader themes across multiple participants (Guest, MacQueen and Namey, 2012; Terry *et al.*, 2017; Nowell *et al.*, 2017). This study benefited from the

adaptability and practicality of thematic analysis. Although there are a number of different thematic analysis methods, the steps advocated by Braun and Clarke (2006) remains one of the most influential and this research follows their approach to thematic analysis. While valuable, thematic analysis may raise concerns due to subjectivity in theme identification and interpretation, influenced by researchers' biases (Vaismoradi and Snelgrove, 2019). However, rigorous coding, peer review, and reflexivity can mitigate potential biases (Braun and Clarke, 2022) and all these aspects were considered in the study.

First, the researcher began by collecting all open-ended responses and transcribing the recordings obtained from the interviews. This was followed by actively reading the dataset to become familiar with the data. Next, the researcher generated initial codes, which were helpful in identifying broader themes. Then, the researcher explored the relationships between codes by carefully examining the data to identify potential connections and patterns, which helped to reveal common themes and connections within the dataset. As themes began to emerge, the researcher identified contestant themes based on the initial codes and deeply explored the data to gain further insights. Subsequently, the researcher started the refining process by reviewing the identified themes for accuracy and ensuring that the represented data was aligned with the research objectives. Subthemes were also generated where applicable, and some themes were merged to refine and solidify their conceptual clarity. NVivo played a crucial role in facilitating the management and organization of the data as it allowed for efficient coding, categorizing, and retrieval of data segments related to specific themes. A second rater was involved in enabling critical discussions and improving the rigor and credibility of the analysis by helping enhance the researcher's reflexivity and overcome bias. The following two sections detail the data analysis process of the open-ended responses and semi-structured interviews.

### ***5.3.2.1 Open-ended responses***

Open-ended responses are designed to help explore different aspects related to usable security and organizational security culture. The open-ended part of the survey included a range of questions that addressed various aspects of security culture and the usability of cybersecurity, allowing respondents to express their views or feedback

related to their organization's security culture. For example, one question asked if the participants had ever bypassed cybersecurity technologies or procedures due to usability issues, requesting a brief description of the circumstances surrounding the event in order to understand the nature of the incident. Also, participants were asked if they had reported any difficulties using cybersecurity technologies or following procedures to the responsible person or team, along with an explanation of the challenges they faced. The purpose of this was to record instances in which usability issues were formally communicated to the responsible team or person. Additionally, respondents were encouraged to comment on the relationship between usable security and security culture within their workplace, as well as to provide general feedback on the usability of cybersecurity measures in their workplace. Further, the questionnaire included a question regarding the primary drivers of adherence to cybersecurity best practices, with the option to specify other drivers if they were not listed. In contrast, another question asked about potential barriers to following these practices. Again, other reasons could be listed. Ultimately, respondents were asked for suggestions on improving cybersecurity usability within their organization in order to gather practical recommendations for improving cybersecurity usability within the corporate settings.

All responses are anonymized to ensure the protection and confidentiality of participants. The input from the responses was then imported into NVivo. Each response was read thoroughly to capture key concepts and ideas raised by respondents under each question and to generate codes directly from the provided text based on their relation to specific survey questions. Within each group of codes, subthemes were further developed to provide more insights into the wider topics of each survey question. These themes and subthemes were continuously refined to ensure their accuracy in representing the data provided and generate meaningful insights into the research aim and objectives.

### ***5.3.2.2 Semi-structured interviews***

The semi-structured interviews performed as part of this research provide substantial insights into the impact of usability on cybersecurity measures across organizational contexts. Eighteen participants expressed their interest in the semi-structured interviews and were contacted via email accordingly. However, several of them did

not reply and continued their engagement in the study. Consequently, the interviews were conducted with eight participants (four males and four females): four academics, three industry professionals, and one PhD candidate with an industry background. Participants were from the U.K., Saudi Arabia, South Africa, Finland, Estonia, Armenia, Sweden, and the U.S., offering a diverse perspective on cybersecurity across different cultures and regulatory contexts. The interviews were conducted via Microsoft Teams to enable the possibility of international participation without any geographic constraints. Participants were informed that their interviews would be recorded and transcribed later, allowing the researchers to revisit the data and support a thorough analysis.

The interviews commenced with parts that needed further investigation or issues on which participants wanted to elaborate. The average duration for each interview was 20 minutes. Following the initial focused discussion, an open conversational approach was taken, inviting participants to openly express their opinions and share insights, increasing the depth of qualitative data. The questions varied depending on the context of the conversation, allowing for a responsive and dynamic interview process that adjusted to the flow of dialogue. The questions included during the interview, depending on the context of the conversation, were:

- Do you feel that cybersecurity usability issues affect your overall productivity and effectiveness in carrying out your day-to-day tasks?
- Can you tell me if there are any specific cybersecurity actions or processes that you find more challenging than others due to issues related to usability? How would you suggest improving them?
- Does management and leadership support affect the implementation of usable security measures? What actions have been taken or could be taken in this regard? (e.g., invest in alternative technologies, provide training to offset usability difficulties (i.e., so that users know how to do things and find them less difficult)
- What strategies can effectively balance usability and cybersecurity measures in your organization?

- Do you believe the usability of cybersecurity measures impacts your ability (or your colleagues') to comply with security expectations or good practices?
- Can you share an example from your organization where the usability of cybersecurity has positively or negatively impacted security culture?
- Considering your organization's geographical location, are there cultural or regional factors influencing security culture and the usability of cybersecurity?  
How can these factors be considered in improving security practices?

The recorded interviews were transcribed, ensuring that every element of the discussions was accurately captured for analysis. The transcriptions were coded using NVivo and then used to identify key themes and subthemes, which were then thoroughly extracted from the data.

Moreover, a second rater was included in the analysis process in order to improve the reliability and credibility of the qualitative data analysis based on semi-structured interviews. This engagement offers an important degree of dependability, assuring consistency and objectivity in data's thematic categorization and coding. The second rater verified the integrity of the semi-structured interviews' theme results. The main responsibilities included thoroughly analyzing the transcribed interviews to check the themes previously identified by the primary researcher. Additionally, the researcher took careful measures to anonymize the transcripts, ensuring that no personal information about the individuals is identifiable.

It is worth to note that although the sample size of  $n=203$  participants for the survey and  $n=8$  for interviews may seem relatively small compared to the potential global population of I.T. users in organizations, it can still provide valuable insights and generate meaningful data since several conditions were taken into account. The study targeted I.T. users in organizations worldwide to ensure that participants come from diverse backgrounds, industries, and geographic locations. This factor can increase the likelihood that the findings are applicable to the population represented by the participants. The study also utilizes hypothesis testing using statistical techniques, which are helpful in assessing the reliability and significance of the findings (Nickerson, 2000; Bonett and Wright, 2015). Further, the study's main aim was narrowed down to focus on specific variables of human aspects of cybersecurity and

the tools used in organizations, including technology and processes, to help maximize the effectiveness of the sample size. Focusing on key variables of interest resulted in allocating resources more efficiently and obtaining precise insights within the available sample size. Moreover, the interviews with eight participants provided deeper insights, which complements and enriches the quantitative findings from the survey, enabling the study to uncover concepts and complexities that the surveys might not capture. The next two chapters will illustrate the findings of the quantitative and qualitative data. The findings then are synthesized to provide insights into the relationship between usable security and security culture.

## **5.4 Chapter Summary**

This chapter described the research methodology utilized in the study, detailing data collection and analysis methods. It also detailed what type of questions the participants were asked to obtain meaningful insights. A summary of the research design is shown in Figure 5.3.



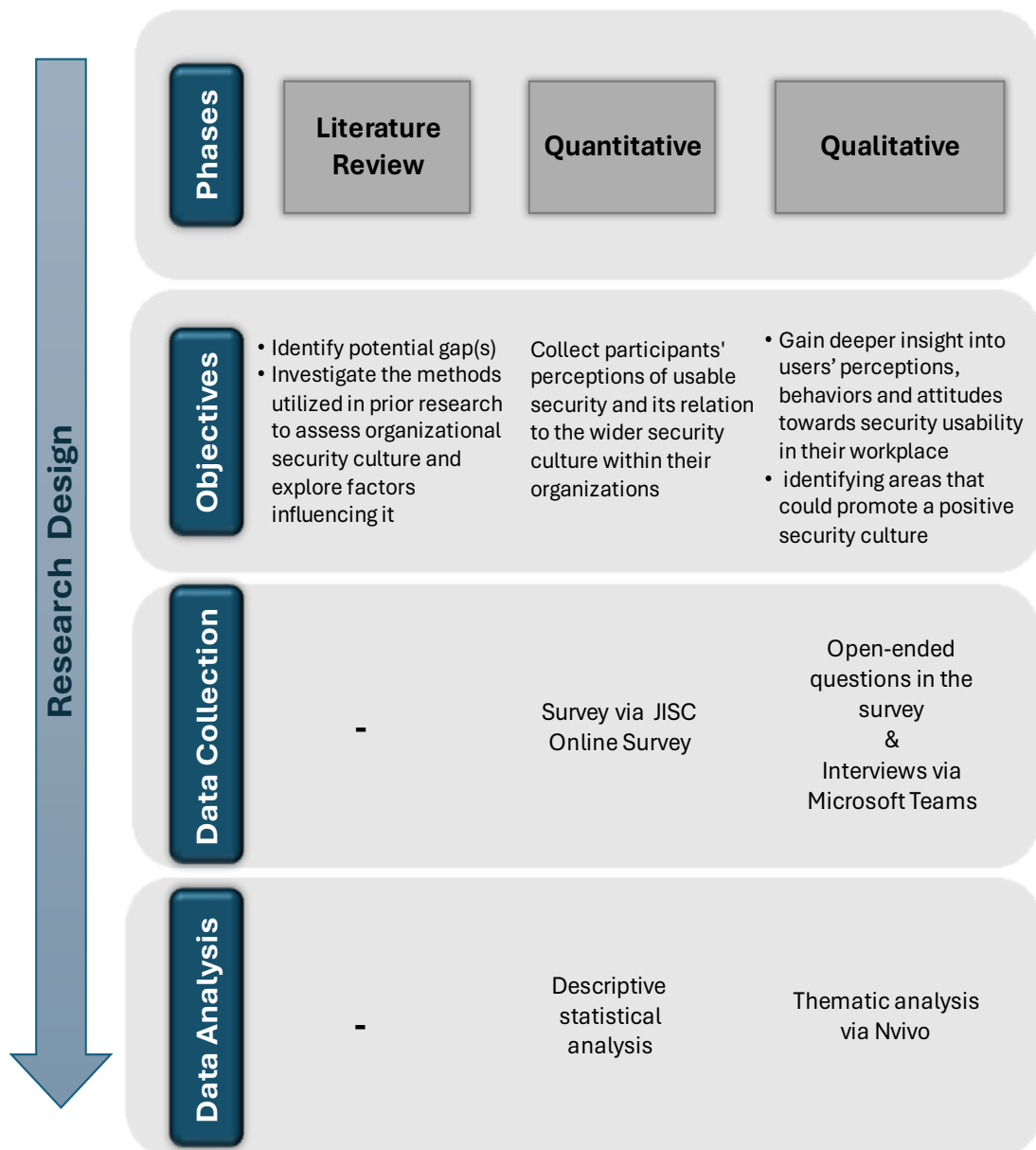


Figure 5.3: Summary of Research Design

# **Chapter 6: Quantitative Analysis and Findings**

## 6.1 Introduction

This chapter presents the findings derived from the analysis of the quantitative data collected through the survey. It covers both the participants' responses and the results of hypotheses testing. The analysis employs descriptive statistical techniques to summarize and ensure that key findings are effectively highlighted. Survey responses are visually represented through a variety of figures and accompanied by detailed interpretations to provide a clear understanding of the results. Furthermore, the study's hypotheses were tested using SPSS software, with each test accompanied by an interpretation.

## 6.2 Survey Quantitative Findings

An overview of the responses from the survey is presented in this section.

### 6.2.1 Participants' Demographic

#### 6.2.1.1 Age Distribution

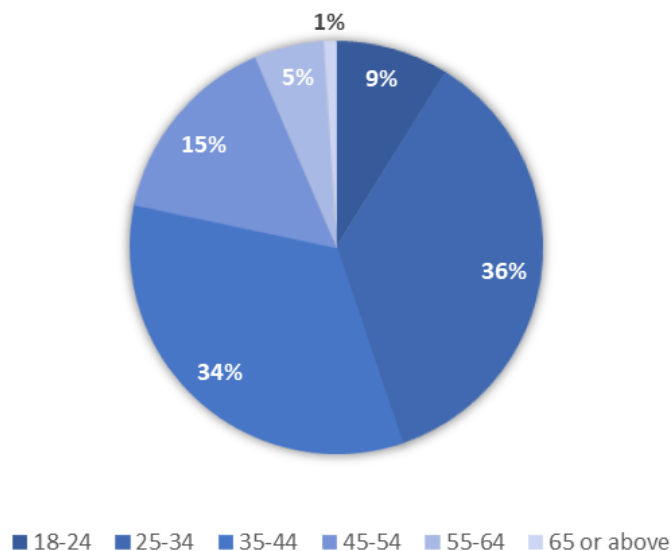


Figure 6.1: Age Distribution Among Participants

The age distribution of participants offers insight into their demographic profile in terms of the cybersecurity behaviors and attitudes of certain ages. As shown in Figure 6.1, the majority of the survey respondents (70%) are between the ages of 25 and 44. This implies a mostly middle-aged workforce, which is important because these people

are likely in the middle of their careers and may hold positions of varied responsibility. They are also more likely to be technologically aware and have experience with cybersecurity procedures in a professional setting.

The results also reflect less representation of the younger and older age groups. Only 9% of participants are between the ages of 18 and 24, indicating that there is a lack of input from younger participants who may be new to the workforce or still enrolled in university or educational settings. Although they are likely to be more familiar with technology than other age groups, their cybersecurity behaviors and attitudes may differ considerably due to differences in technology exposure and educational curriculum emphasizing that newer cybersecurity challenges and solutions could exist. Similarly, participants aged 55 and above account for only 6% of the sample, showing that people approaching or having reached retirement age are less likely to be involved. This age group might show different patterns in cybersecurity behavior, presumably indicating less knowledge of modern technologies and security measures compared to younger age groups.

The age distribution helps shape our understanding of how different users adopt cybersecurity practices and perspectives. It also highlights the importance of a tailored strategy in organizational cybersecurity initiatives, which considers the traits of the majority age groups while not omitting the specific needs and behaviors of the other groups. For example, cybersecurity training and guidelines may need to be tailored to better suit middle-aged employees' learning preferences and knowledge levels while simultaneously taking into account measures to bring younger and older workers up to speed.

### ***6.2.1.2 Gender Distribution***

The gender distribution of the survey participants shows 113 males (56% of the participants), 89 females (44% of the participants), and one participant who identified as 'Other.' A reasonably balanced gender distribution adds credibility to the study's findings by ensuring that both male and female perspectives on cybersecurity are effectively reflected, meaning that the survey results can reasonably reflect the different gender dynamics inside organizations, making the conclusions applicable to both genders. Moreover, analyzing data from a gender perspective may reveal specific

challenges or benefits each gender faces in cybersecurity practices, thereby leading to tailored interventions. These findings can help organizations determine if their current cybersecurity policies effectively reflect the demands and habits of both male and female employees. For example, if additional research finds that one gender is less confident in using specific security systems, specialized instructional programs can be devised.

### 6.2.1.3 Educational levels

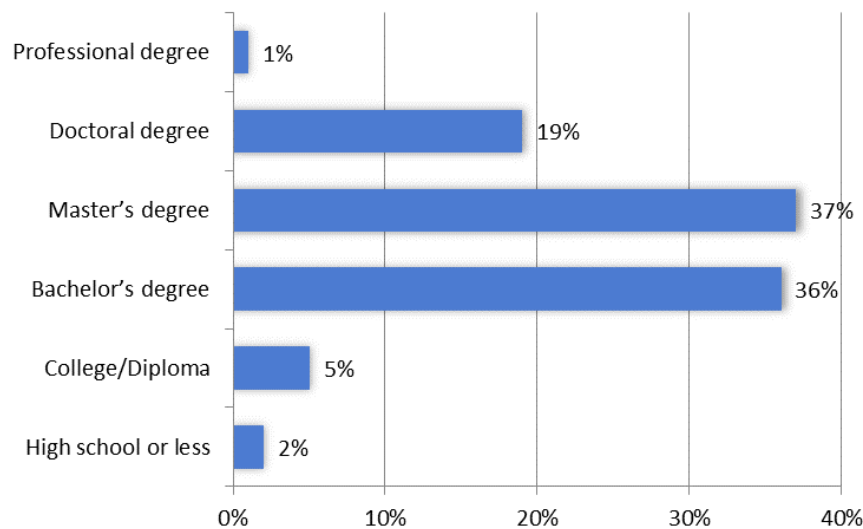


Figure 6.2: Educational Attainment Levels of Participants

The survey participants' educational attainment levels reflect a highly educated population with a strong focus on higher education degrees. It is hard to estimate the percentage of the world's population that holds a university degree because different countries apply different methods for collecting and reporting data. However, approximately 44% of people in the OECD's member countries who are between the ages of 25 and 34 have a university degree (OECD, 2023). This statistic may not fully reflect the global average since the 38 members of the OECD are mostly industrialized countries. In which case, the distribution of education level amongst the survey respondents indicates that they are with an above-average level of education compared to the general populous. In Figure 6.2, one can observe that a total of 92% of participants at least have a bachelor's degree, 37% have a master's degree, and 19% hold a doctorate. This indicates that the majority of respondents are well-educated, which may influence their perceptions and interactions with measures related to

cybersecurity. High educational attainment may also be correlated with a greater understanding of cybersecurity threats and more sophisticated approaches to controlling these threats.

In contrast, only 7% of participants have a high school or college degree, limiting the breadth of data into how less academically trained workers approach and interact with cybersecurity processes. This underrepresentation could bias the findings toward the views and behaviors of those with higher education, and it may not fully reflect the perspectives of all organizational members, particularly those in positions that require less education. Organizations need to ensure that cybersecurity policies and procedures are accessible and inclusive to all their members, regardless of their educational level. The results may indicate the necessity to measure educational levels and competencies in order to differentiate cybersecurity approaches and programs that cater to the various degrees of baseline understanding and learning styles associated with diverse educational backgrounds.

#### 6.2.1.4 Accessibility Challenges

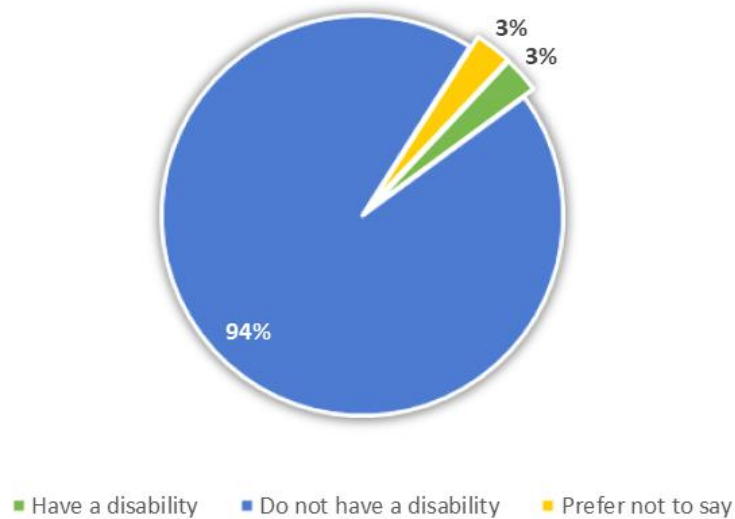


Figure 6.3: Percentage of Participants with Disabilities Affecting Technology Use

Figure 6.3 shows that only 3% of the respondents mentioned having disabilities that impact their usage of technology. This small proportion is not a sufficient basis from which to generalize results to the larger community, which has a more significant number of people with certain disabilities. It most importantly raises the question about

the inclusivity and accessibility of cybersecurity measures since users with disabilities might not have been enabled and empowered to interact with cybersecurity measures within corporate contexts. Among the disabilities mentioned are Attention-deficit/hyperactivity disorder (ADHD), Short-sightedness (myopia), dyslexia, and stuttering. Each of these may have an effect on how people use cybersecurity technologies since the study participants reported them. The definitions and the possible interpretation of participants mentioning these difficulties could be:

- ADHD is the most prevalent neurodevelopmental disorder in children, and research has shown that a significant percentage of adults with ADHD still have impairments from their condition (Sibley, Mitchell and Becker, 2016). This disorder might affect attention and the ability to focus on complex security measures.
- Myopia is a common eye condition that causes blurry vision in far objects(NHS, 2022). Myopia could affect visual interaction with some security interfaces.
- Dyslexia is a learning disorder that mainly impacts reading and writing abilities, which affect information processing and can have an effect on other areas, such as organizational abilities (BDA, 2010). This may make understanding textual guidelines or warnings challenging, potentially affecting compliance with security measures.
- Stuttering is a speech condition that causes the repetition of sounds, syllables, or words and can have a negative impact on work efficiency and opportunities (NIH, 2017). While it generally affects speech, stuttering may indicate broader conditions that might impact cognitive processing toward security in the workplace.

Designing cybersecurity technologies that are both usable and accessible to people with a variety of abilities is crucial. These approaches increase accessibility and support the usability of security's main objective. Examples of practical integration of these principles include implementing screen readers for visually impaired users, designing interfaces that use simpler language, adjustable text sizes, introducing customised training sessions with contextual explanations, and voice commands for security-related tasks that consider individual differences in cognition and learning.

These training could assist in reducing the specific obstacles that may result from the disabilities described, which ensures that all employees are similarly competent in handling cybersecurity issues. The small percentage of respondents who reported disabilities in this survey points to a possible subject for additional investigation and advancement in organizational cybersecurity procedures.

### 6.2.1.5 Organizational Roles

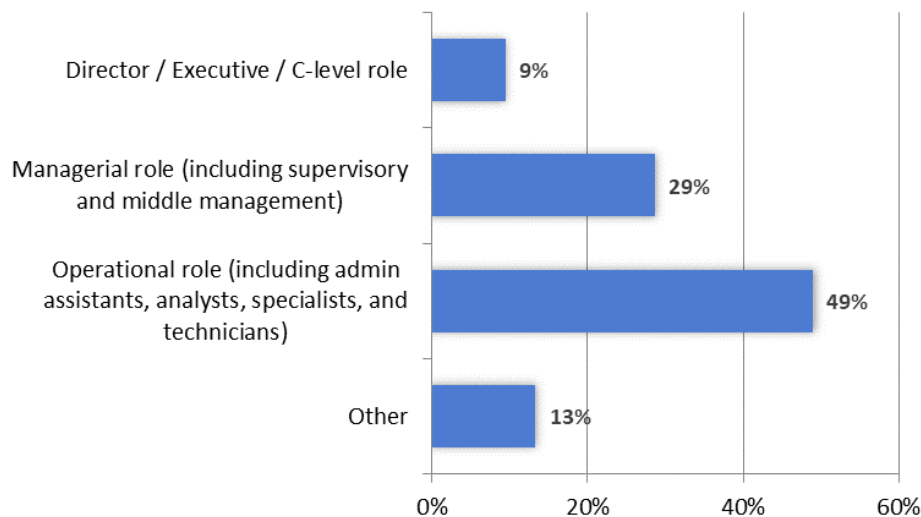


Figure 6.4: Participants' Roles/Positions within Their Organisations

The distribution of participants' roles within their organizations offers an overview of the responsibility level and the potential influence on organizational practices and culture. As shown in Figure 6.4, 49% of participants hold operational roles (e.g., administrative assistants, analysts, specialists, or technicians). This group of employees forms the backbone of the day-to-day activities in their departments and is likely to interact with cybersecurity measures frequently. This suggests that the experiences and feedback from this group are crucial. Participants in managerial roles, who make up 29% of the survey, are also vital to interpreting how people in middle management perceive cybersecurity policies and procedures. In addition, these individuals play an essential role in bridging the gap between executive decisions from the higher management and operational execution. Directors, executives, or C-level respondents represent 9% of participants. Their roles offer perspectives that are important for understanding the strategic priorities or challenges related to security measures at the highest levels of decision-making. The 'Other' category includes a



diverse mix of academics, researchers, and retired people, who constitute 13% of participants. This variety enriches the study dataset with a wide range of views.

The participants' different responsibilities can highlight the importance of customized cybersecurity policies that consider the specific needs and degrees of interaction of various positions and roles inside the corporation. Additionally, the comprehensiveness and efficacy of cybersecurity strategies are improved when they integrate insights from executives to operational workers across the entire organization. The establishment of efficient communication channels is crucial in ensuring that cybersecurity rules are effectively understood and applied consistently across all positions. Further, mechanisms for capturing feedback from various roles should be in place to continuously improve security measures. This will ensure that cybersecurity measures are understandable, accessible, and practical for all organizational roles and positions, contributing to building a robust cybersecurity culture.

#### ***6.2.1.6 Departmental Representation***

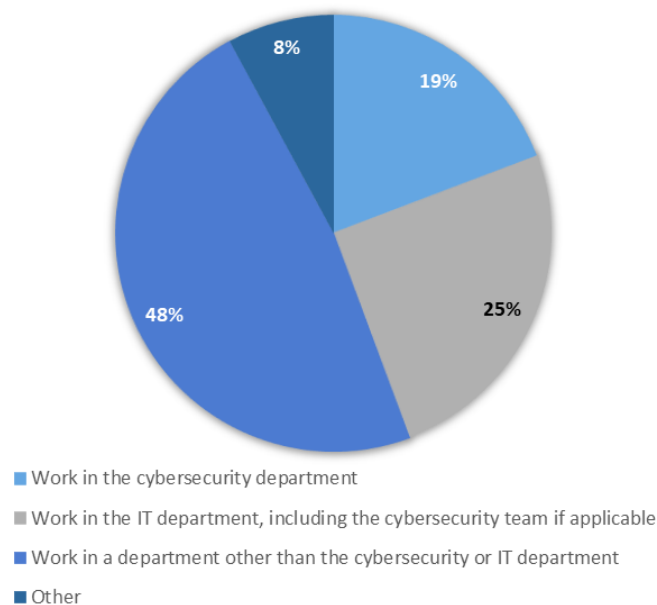


Figure 6.5: Participant Distribution Across Organisational Departments

Understanding the distribution of participants across various departments provides a valuable landscape to extract detailed insights into how cybersecurity practices might

vary based on departmental roles and people's direct or indirect interaction with cybersecurity measures, all of which influence organizational cybersecurity culture. The diverse departmental involvement noted in survey responses demonstrates the need to integrate security measures at all levels of an organization. Understanding diverse departments' perspectives strengthens the organization's defenses against cyber threats and creates more informed and aware individuals. Respondents from Cybersecurity Departments, who represent 19% of participants, as shown in Figure 6.5, are directly responsible for security-related roles, including implementing and monitoring cybersecurity measures within the organization. Their perspectives are vital in assessing the effectiveness of current cybersecurity strategies and tools. The responses from the IT Departments who may also be part of the cybersecurity team (25%) are also significant since they are involved in the day-to-day IT operations and support, including implementing cybersecurity measures. Other departments (48%), which is the largest group and can form a broad non-technical representation, include employees whose feedback is invaluable for evaluating the broader impact of cybersecurity practices across the organization.

Additionally, the diverse insights from the 'Other' category (8%) encompass a variety of fields such as education, marketing, medical, and more. The departments' distribution underscores the necessity for cross-departmental views and considerations, e.g., cross-departmental training that caters to the specific needs and exposure levels of various departments in order to address the unique vulnerabilities of different departments. Also, including representatives from all organization departments in the cybersecurity policy formulation process can ensure that policies are practical and applicable across the entire organization.

### 6.2.1.7 Industry Representation

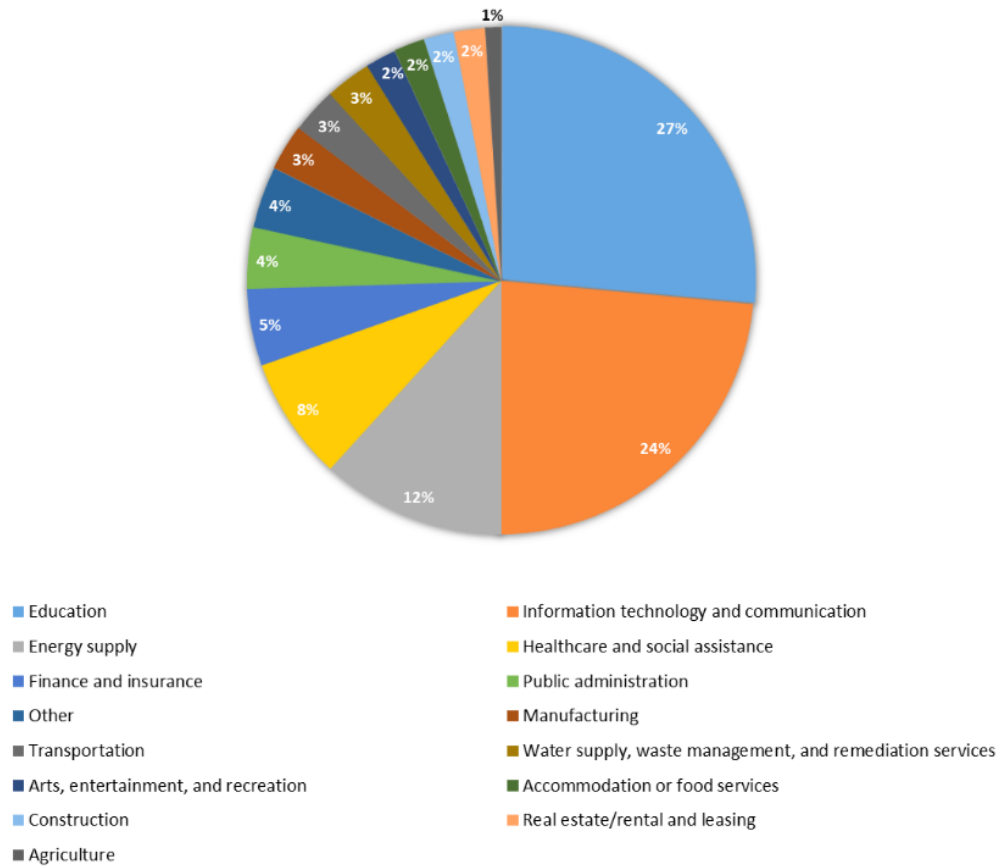


Figure 6.6: Primary Industries Represented by Participants' Organisations

Having a clear understanding of the varied sectors in which cybersecurity measures are implemented and evaluated is crucial to understanding sector-specific challenges and best practices. This study's findings may be influenced by the prominence of the education sector (27%) as can be inferred from Figure 6.6. In addition, a high percentage of IT and communication companies (24%) can provide valuable feedback to set benchmarks in cybersecurity measures. Energy supply (12%) and healthcare and social assistance (8%) are critical since these sectors provide public services and manage sensitive information. Cybersecurity impacts essential services and imposes far-reaching consequences, so having representation from these sectors can provide valuable insights. Other sectors, which are represented by only a small percentage, bring diverse perspectives on how cybersecurity is integrated into operational frameworks and regulatory environments. It is important to remember that each industry faces unique cybersecurity challenges. Healthcare and finance, for instance,

require strict data protection measures due to regulatory compliance requirements (like HIPAA in healthcare or GDPR in finance). Organizations can benefit when cybersecurity practices and lessons from one sector are applied to another. Public administration techniques can be adapted from risk assessment techniques used in the energy sector. To ensure cybersecurity policies are robust, versatile, and adaptable to any operational or regulatory context, they should be developed with input from diverse industries. Each industry has its own cybersecurity challenges and workforce needs, so tailored training programs are essential. Regularly updating these programs is necessary to stay on top of industry-specific threats and technological advances. One strategy for sharing cybersecurity practices between industries is establishing cross-industry collaboration platforms or forums where representatives from different sectors can exchange knowledge (Neisse *et al.*, 2020).

#### 6.2.1.8 Geographic Diversity

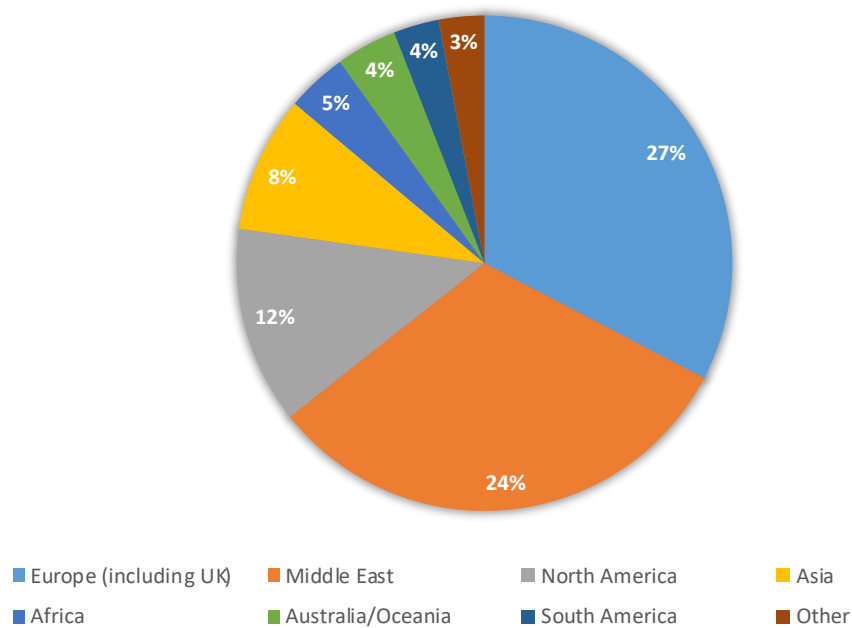


Figure 6.7: Geographic Distribution of Participants' Organisations

Survey participants' geographic distribution demonstrates the global nature of cybersecurity challenges. It emphasizes the importance of adaptable, inclusive strategies that respect and accommodate regional differences. A comprehensive analysis of cybersecurity practices globally can be provided by taking into account a

wide range of environmental, cultural, and legal factors. Moreover, it is important to understand how cybersecurity is affected by regional factors such as local laws, cultural attitudes toward security, and technological advancements. Figure 6.7 illustrate that a strong representation of respondents from Europe and the Middle East (33%) and (32%), respectively, provides an in-depth view, particularly from these regions where cybersecurity environments are rapidly evolving. Even though North American organizations contribute less than their European and Middle Eastern counterparts, their input is crucial, given their leadership in technological innovation and cybersecurity. Also, aspects of cybersecurity challenges are understood differently in different economic and technological contexts in Asia (9%), Africa (4%), Australia/Oceania (4%), and South America (3%), respectively. It can guide cybersecurity strategies that are adaptable to different regional laws, cultural norms, and technological landscapes. As an example, what works in Europe with its strict privacy laws might need to be adjusted to be applicable in areas with less restrictive laws. Furthermore, organizations should consider customizing global cybersecurity practices to suit regional needs. With this approach, security standards can be consistent while still being flexible enough to meet local needs, and organizations can improve their cybersecurity posture by considering regional specifics.

### 6.2.1.9 Organisational Size Distribution

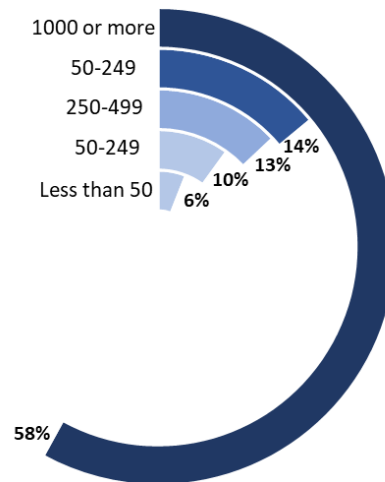


Figure 6.8: Distribution of Participants' Organisation Sizes

Figure 6.8 reveals that a considerable number of larger companies are represented in the study. Specifically, the vast majority of participants come from large organizations with 1000 employees or more. These companies probably have more complex IT systems and may have greater resources available for cybersecurity. They might also be targeted by more advanced cybersecurity attacks because of their size and importance. This is not to discount the significance of cybersecurity measures in smaller and mid-sized businesses, where resources and expertise may be less than in more prominent companies. These businesses' cybersecurity policies may be different from those of larger corporations, sometimes emphasizing more affordable solutions and dealing with certain challenges. Cybersecurity measures must be scalable across different organization sizes. Larger enterprises may benefit from more extensive, integrated security solutions, whereas smaller businesses may require simpler, more cost-effective alternatives. Encouraging knowledge sharing among businesses of varying sizes may enable smaller firms to adopt best practices from larger ones, thereby utilizing economies of scale and advanced expertise. In contrast, large enterprises can benefit from the agility and innovative ideas that are typically applied in smaller settings.

## 6.2.2 Dimensions of Security Culture

### 6.2.2.1 Security Culture Consensus

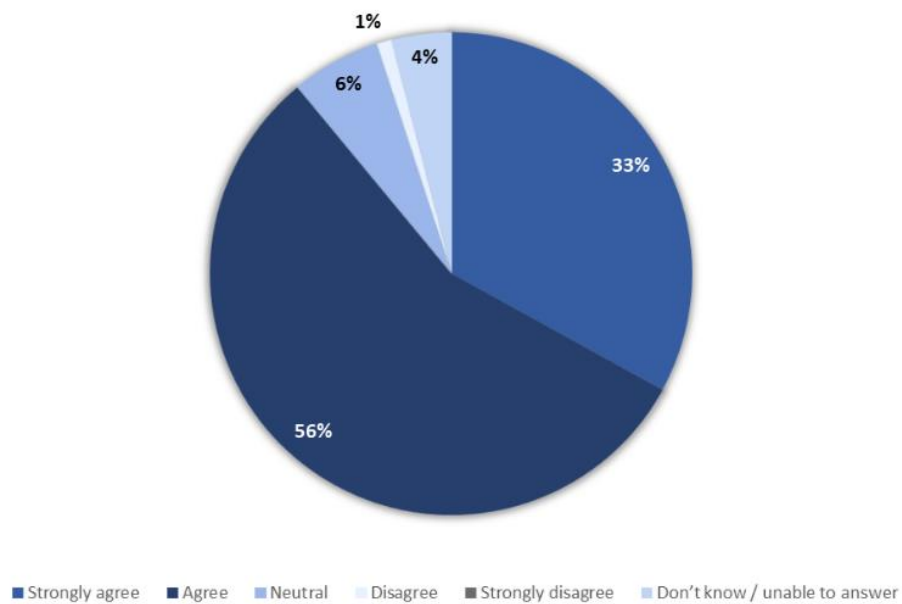


Figure 6.9: Participant Agreement on the Impact of Shared Attitudes, Behaviours, and Beliefs about Cybersecurity within Their Organisation Promoting Shared Responsibility for Maintaining Cybersecurity

The responses to the influence of shared attitudes, behaviors, and beliefs about cybersecurity within their organizations demonstrate the perceived relevance of a collaborative approach to cybersecurity. The overwhelming majority of participants agreed that company culture plays a key influence in cybersecurity success. According to Figure 6.9, a total of 89% of participants agree or strongly agree that common attitudes, behaviors, and beliefs related to cybersecurity encourage shared accountability. This demonstrates a shared belief that a positive security culture is essential and can indicate that people understand the value of everyone in the organization being on the same page when it comes to cybersecurity norms and practices. The findings highlight the importance of corporations establishing a strong cybersecurity culture that actively promotes common attitudes and behaviors. For example, training programs must emphasize the "how" of cybersecurity and the "why" to enhance the collective understanding and responsibility for security measures. For people who are neutral or unsure about the importance of shared behaviors and attitudes towards cybersecurity, more targeted methods of communication may be

required to clearly describe the benefits of a shared cybersecurity culture as well as how each individual's behavior affects the organization's overall security.

### 6.2.2.2 Cybersecurity Competence Confidence within the Organization

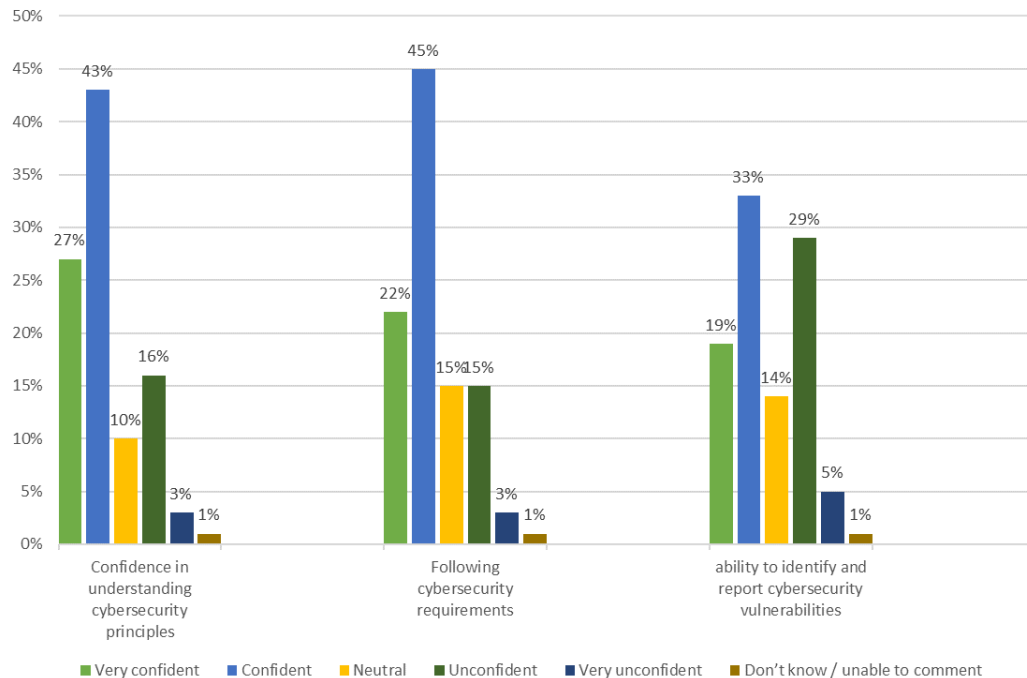


Figure 6.10: Participants' Confidence Levels in Various Aspects of Cybersecurity Competence

While the study respondents report a high foundational knowledge and compliance confidence as depicted in Figure 6.10, there is a clear indication that additional focus is needed on identifying and reporting vulnerabilities. Enhancing skills in this area could significantly improve organizational cybersecurity resilience. This could include hands-on workshops, simulation exercises, and more comprehensive incident response training. However, self-reporting of knowledge or skills can come with disadvantages that might affect the accuracy and reliability of the collected data. For example, individuals may underestimate or overestimate their knowledge or skills due to personal biases or lack of self-awareness. Also, self-assessment can vary between different respondents if no standardized metric is applied, e.g., what one person considers only basic might be considered proficient by another. Besides, some participants may lack the required insight into their abilities simply because they are unaware of all aspects of the cybersecurity domain.



### 6.2.3 Aspects of Usable Security

#### 6.2.3.1 Usability Challenges in Cybersecurity

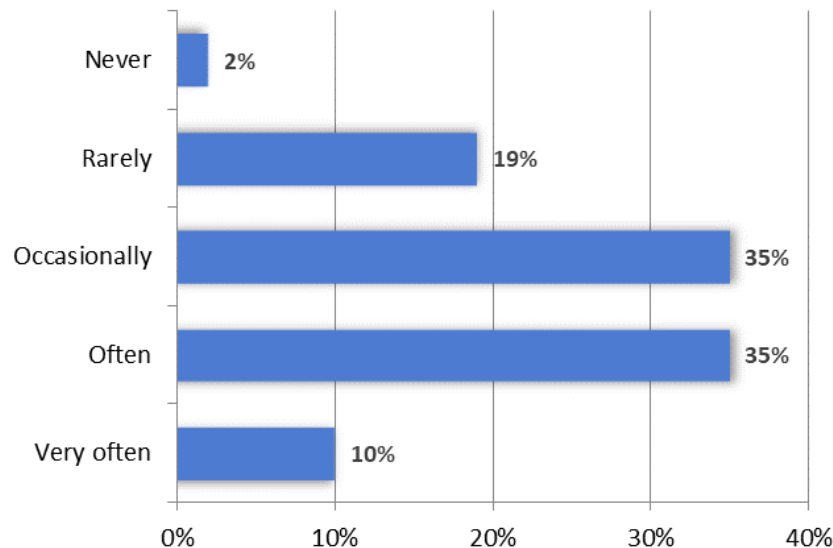


Figure 6.11: Percentage of Participants' Encounters with Usability Issues in Cybersecurity Technologies and Procedures within Their Organisation

The data on how frequently participants encounter usability issues in cybersecurity technologies and procedures within their organizations provides valuable insight into employees' operational challenges. Figure 6.11 shows that almost half of participants (45%) report encountering usability issues very often (10%) or often (35%). The significant percentage suggests that a large percentage of the workforce has difficulty using cybersecurity systems on a regular basis. This can hinder the effective implementation of security practices and may lead to non-compliance or workarounds that compromise security. A further 35% of participants experience occasional problems with usability. Even though this is not as frequent, it still indicates that more than one-third of the workforce encounters problems that can disrupt their workflow and negatively impact their efficiency in maintaining cybersecurity procedures. On the other hand, 19% of the workforce rarely encounters usability issues, and 2% do not encounter them at all. The findings suggest that, although some parts of the organization have effective and user-friendly cybersecurity measures in place, there may be disparities in experience between different departments or areas.

As a significant majority of participants reported usability issues, organizations should invest in cybersecurity technologies and procedures that are more user-friendly. By improving usability, we can increase compliance, reduce error rates, and increase the effectiveness of security measures. It is recommended that organizations conduct detailed user experience studies within their workforce to identify specific pain points associated with cybersecurity procedures and technologies. When these issues are addressed with targeted improvements, the reporting of usability problems can be greatly enhanced. It is important to establish robust feedback mechanisms so that employees can report usability issues without fear of reprisal or dismissal to assist IT departments and cybersecurity teams in understanding and prioritizing areas of improvement. Taking this approach can enhance the usability of the system proactively. According to the data, usability issues are common among a large segment of the workforce when interacting with cybersecurity technologies and procedures. This affects not only the effectiveness of these systems but also the morale of employees and the general security culture within the organization.

### 6.2.3.2 Responses to Difficult Cybersecurity Actions

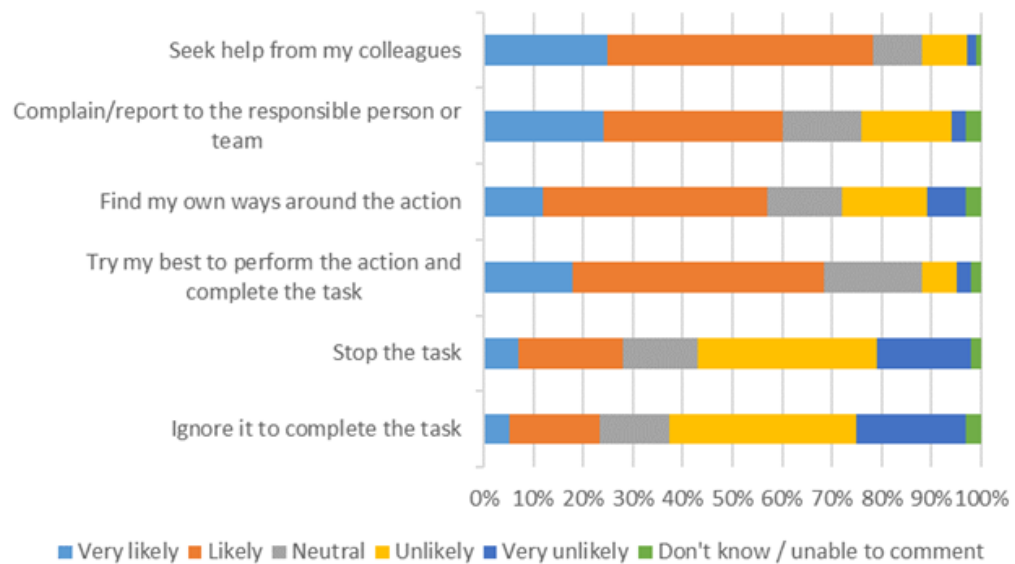


Figure 6.12: Likelihood of Participants' Responses to Difficult Cybersecurity Actions

In this survey question, participants were allowed to select all applicable responses, so the percentage of responses does not equal 100%. The chart provides insights into participants' reactions when they are encountered with a complex cybersecurity

measure. As shown in Figure 6.12, the majority of respondents indicated that they would seek assistance from their colleagues when faced with challenging cybersecurity tasks. While this can demonstrate a proactive tendency toward collaborative problem-solving, it might show the lack of direct communication with the responsible team to receive the required guidance. Additionally, 69% of the respondents said they would do their best to perform the task (very likely + likely), demonstrating a high level of initiative and a commitment to adhering to security protocols in challenging circumstances. Moreover, 60% of participants would report issues to the responsible person or team (very likely + likely), indicating that a significant portion would take formal steps to resolve issues.

Nonetheless, 57% of participants express a high probability of finding a way around the action, raising concerns about potential security breaches that could put the organization at risk. A significant 23% of respondents indicated that they would ignore security measures in order to complete broader tasks, indicating a willingness to bypass cybersecurity measures to maintain productivity, which could compromise the overall security of the organization. Additionally, 28% of respondents indicated they would likely or very likely stop the task, indicating usability or security concerns that may prevent the completion of this task and indicating that cybersecurity measures may be too restrictive or poorly integrated.

According to these responses, some security measures may be overly complex or inadequately integrated into daily workflows. It is imperative that these measures are reviewed to ensure that they do not impede productivity while maintaining security. Additionally, the data suggests that a small but significant percentage of employees may disregard security protocols in order to complete their tasks, suggesting a need to clarify communication regarding the importance of compliance and the potential risks associated with non-compliance. A variety of strategies can be employed, including the use of more frequent communications and targeted training.

### 6.2.3.3 Bypassing Cybersecurity Measures

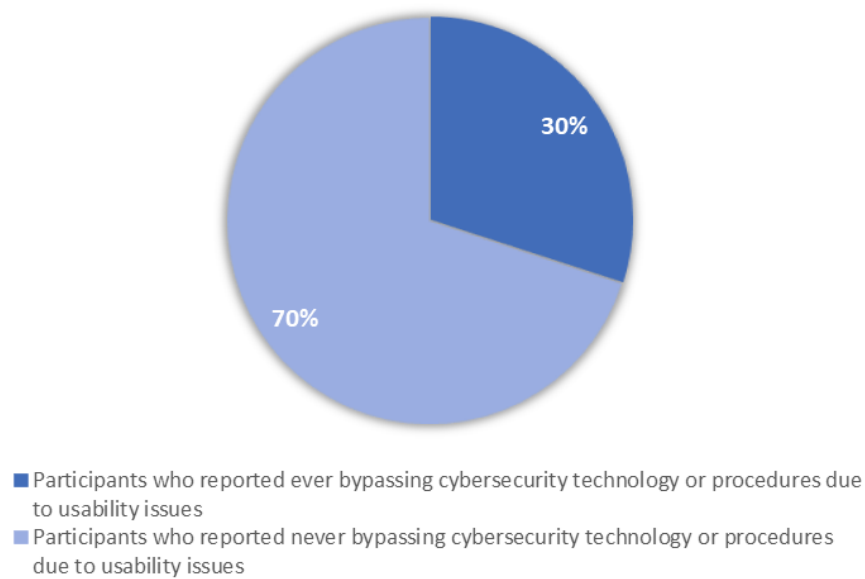


Figure 6.13: Percentage of Participant Bypassing of Cybersecurity Measures Due to Usability Issues

The survey data reports the percentage of participants bypassing cybersecurity measures due to usability issues, shown in Figure 6.13. This provides insight into employees' challenges when dealing with complex cybersecurity measures. The fact that 30% of participants admitted to bypassing cybersecurity measures because of usability problems is a cause for concern because this percentage suggests that usability issues exist and can hinder employees' ability to effectively complete their tasks without circumventing cybersecurity measures. Bypassing cybersecurity measures can expose organizations to significant risks, such as vulnerabilities that may be exploited. As a result, it emphasizes the need for cybersecurity solutions that are not only robust but also usable. Despite the fact that 70% of participants reported never bypassing cybersecurity measures, this figure should be interpreted with caution. It is possible that this statistic reflects a compliance culture in which employees are aware of the risks associated with bypassing security measures or that cybersecurity measures are adequately integrated and do not impede productivity. However, it is also possible that some participants chose not to disclose their actual behavior in light of the sensitive nature of admitting non-compliance.

Accordingly, organizations should place a high priority on the usability of cybersecurity technologies and procedures. Security measures that are too complex or unusable may be bypassed by employees, which may increase the organization's risk. Testing usability as part of the cybersecurity implementation process can assist in identifying and mitigating these problems. Furthermore, organizations can remain proactive in addressing these issues by establishing regular review processes for cybersecurity measures and creating feedback loops where employees can report usability issues. As a result, bypassing behaviors can be reduced. Also important is the creation of an organizational culture that fosters open communication where employees feel comfortable reporting usability problems without fear of retribution, which can result in more honest feedback and a more accurate assessment of the frequency of bypassing behaviors. This openness can also develop trust between employees and cybersecurity teams as a result.

#### 6.2.3.4 Agreement on the Usability of Cybersecurity Measures

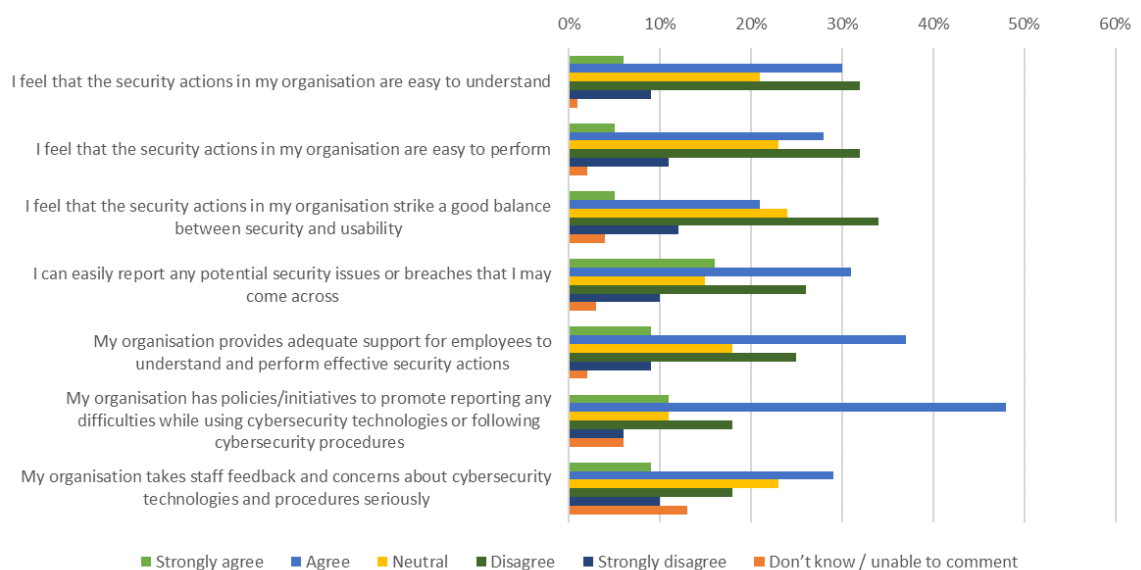


Figure 6.14: Participant Agreement with Usability Statements on Cybersecurity Measures

The participants' responses regarding their agreement with various statements regarding cybersecurity usability in their organizations reveal significant information about the participants' experiences and perceptions regarding security measures. From Figure 6.14, it is evident that a significant portion of participants feel that security actions are neither easy to understand (41% disagree or strongly disagree) nor easy to

perform (43% disagree or strongly disagree). This indicates that usability issues may hinder effective security practices. According to the responses, security protocols should be simplified and integrated into daily workflows in order to improve both comprehension and implementation. In addition, only 26% of respondents (21% agree + 5% strongly agree) believe that their organization strikes a good balance between security and usability, while 46% (34% disagree + 12% strongly disagree) feel this balance is lacking. This highlights a critical area where security measures may be perceived as too restrictive or complex, possibly compromising compliance and efficiency.

According to the survey, more participants feel positive about the ease of reporting cybersecurity issues (47% agree or strongly agree) than other areas. Nevertheless, 36% of respondents find it challenging (26% disagree + 10% strongly disagree), indicating that while mechanisms for reporting may already be in place, they could be improved in terms of accessibility or communication. Furthermore, while participants feel generally supported in understanding and performing security actions (46% agree or strongly agree), nearly a third (34%) do not feel adequately supported, which may affect their ability to adhere to security protocols. There are significant areas for improvement in making cybersecurity measures more accessible and better understood across organizations, despite the foundation of support and some good practices in place. Additionally, a significant majority of respondents (59% agree or strongly agree) acknowledge that their organization has policies to identify and address usability issues related to cybersecurity measures.

Moreover, the participants' feedback on how their organizations handle staff feedback on cybersecurity measures underscores the importance of this process in ensuring the usability of security systems. While 38% feel that their organization takes staff feedback seriously, a significant 28% disagree, and 13% are unsure, indicating room for improvement in how feedback is collected, valued, and acted upon. It is essential to establish more robust systems for collecting and acting on employee feedback. This can help organizations adjust their cybersecurity measures more dynamically and ensure they meet user needs effectively.

### 6.2.3.5 Reporting and Resolution of Cybersecurity Issues

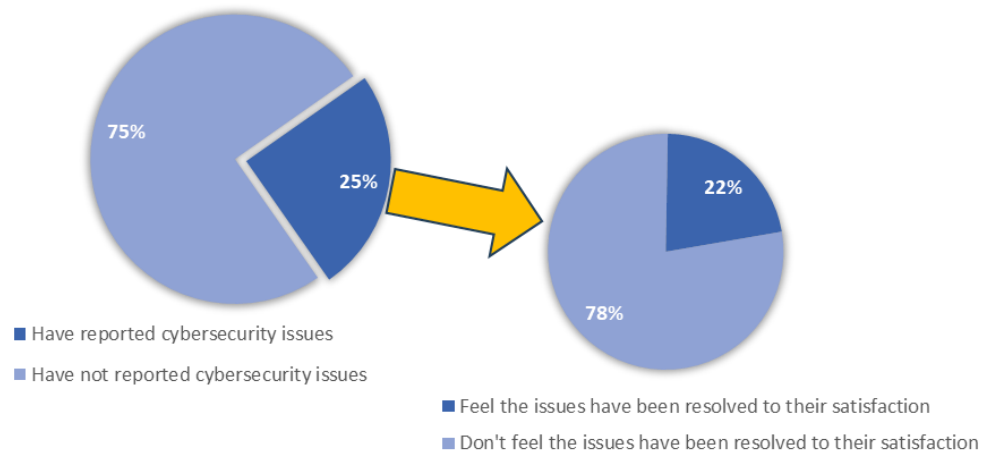


Figure 6.15: Reporting and Resolution of Cybersecurity Issues

Reporting and resolving cybersecurity incidents provide important evidence of the effectiveness of organizational processes for managing cybersecurity incidents. A breakdown of participants' viewpoints about how cybersecurity issues are reported and resolved reveals significant gaps between how issues are reported and how they are resolved. As evidenced in Figure 6.15, only a quarter of participants have reported cybersecurity concerns. This relatively low percentage may be indicative of a lack of understanding about how and when to report issues, concerns about retribution, or a perception that reporting may not result in meaningful action. In other words, the large number of respondents who do not report issues is concerning as it may indicate issues that are not being reported, which could result in unresolved security vulnerabilities. Even when issues are reported, a very small fraction of respondents (22%) feel that these issues have been resolved to their satisfaction. The low satisfaction rate of employees can negatively affect their trust in cybersecurity management. The high level of dissatisfaction indicates significant shortcomings in the handling of reported issues. In turn, this dissatisfaction can discourage future reporting and undermine the effectiveness of cybersecurity measures. A number of implications can be derived from this:

- The need to improve reporting mechanisms: Organizations should make reporting mechanisms more visible and accessible in order to encourage more

employees to report issues. There are several ways in which this can occur, including visible reminders of the process, targeted training sessions on how to report issues, and reassurances that reporting is valued and encouraged.

- Resolving issues more effectively: The high rate of dissatisfaction with how issues are resolved indicates that the resolution process should be revised. To effectively resolve reported issues, organizations should ensure that they have clearly defined, efficient, and effective procedures. This might involve setting up specialized teams to handle reports and ensuring they have the resources needed to investigate and address issues promptly.
- Establishing trust between employees and cybersecurity departments: To ensure that employees who report issues are kept informed about the status of their resolution, organizations could implement transparent follow-up procedures. It may also be appropriate to introduce feedback loops to allow employees to participate in the resolution process.
- The need for regular reviews and feedback: Organisations should regularly evaluate the effectiveness of their processes for reporting and resolving cybersecurity issues. The feedback could be provided through multiple means, such as periodic user feedback or suggestion boxes that allow employees to provide anonymous feedback on these processes.

Overall, these findings highlight the need for organizations to address gaps in reporting and resolving cybersecurity incidents. Developing these areas is essential for maintaining robust cybersecurity defenses, fostering a proactive cybersecurity culture, and ensuring employees are confident in the organization's ability to effectively manage cyber risks.



## 6.2.4 Impact of Usable Cybersecurity on Organisational Security Culture

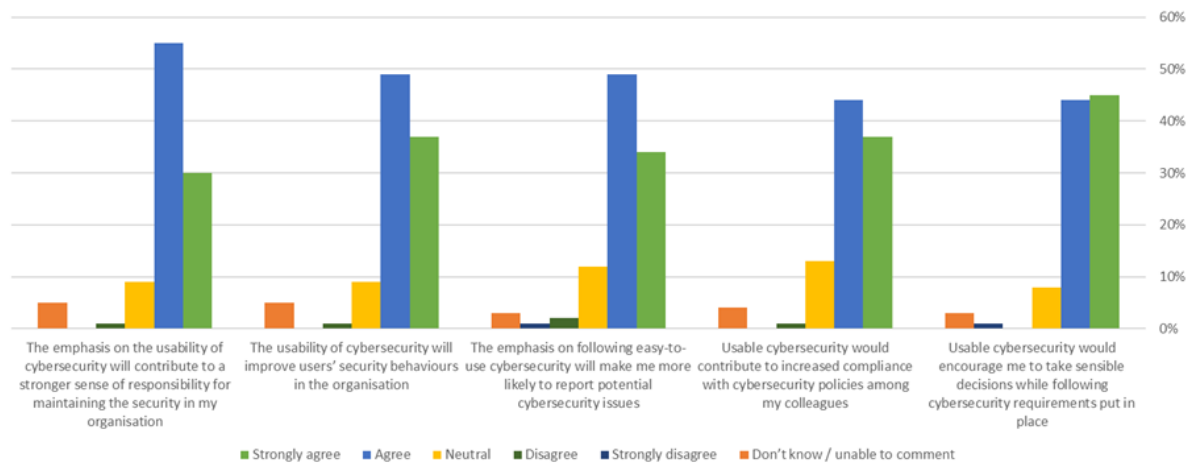


Figure 6.16: Participant Agreement with Statements on the Impact of Usable Cybersecurity on Organisational Security Culture

There is a strong consensus among participants that usable cybersecurity has a positive impact on organizational security culture. This suggests that improving the usability of cybersecurity measures will have a significant and positive impact on how organizations perceive and adopt these measures. Figure 6.16 highlights that the vast majority of respondents (89% combined strongly agree and agree) believe that usable cybersecurity would encourage them to make sensible decisions while adhering to security protocols. Individual compliance can be significantly influenced by usability by making security actions more intuitive and less burdensome. Likewise, the rest of the statements indicate that usable security measures positively impact organizational contexts. 81% of participants believe that a usable cybersecurity system would result in an increase in compliance among their colleagues. This illustrates the importance of usability in supporting a compliance-oriented culture, where security measures are naturally integrated into daily activities rather than just enforced. There are also 83% of respondents who report that they are more likely to report security issues if cybersecurity is made easier to use. Hence, employees are more likely to participate in security governance when security processes are intuitive and accessible.

In addition, 86% of respondents believe that improvements in the usability of cybersecurity tools and procedures would lead to improved security behaviors

throughout the organization. According to this viewpoint, usable security measures can directly influence the overall effectiveness of an organization's security practices. There is a strong consensus among 85% of respondents that emphasizing the usability of cybersecurity enhances employees' commitment to the security culture, which indicates that usability affects compliance as well as employee commitment to the security culture. It is evident from the data that organizations should prioritize usability when designing their cybersecurity tools and policies. Organizations can increase engagement, improve compliance, and stimulate more proactive security behavior by improving usability. This can involve aligning cybersecurity initiatives with employees' needs and organizational workflows. The results highlight the fact that organizations that invest in making cybersecurity tools and procedures more usable are likely to see a range of benefits. These benefits range from increased compliance and better security behaviors to a more ingrained sense of responsibility among employees.

### 6.2.5 Motivators for Cybersecurity Best Practices

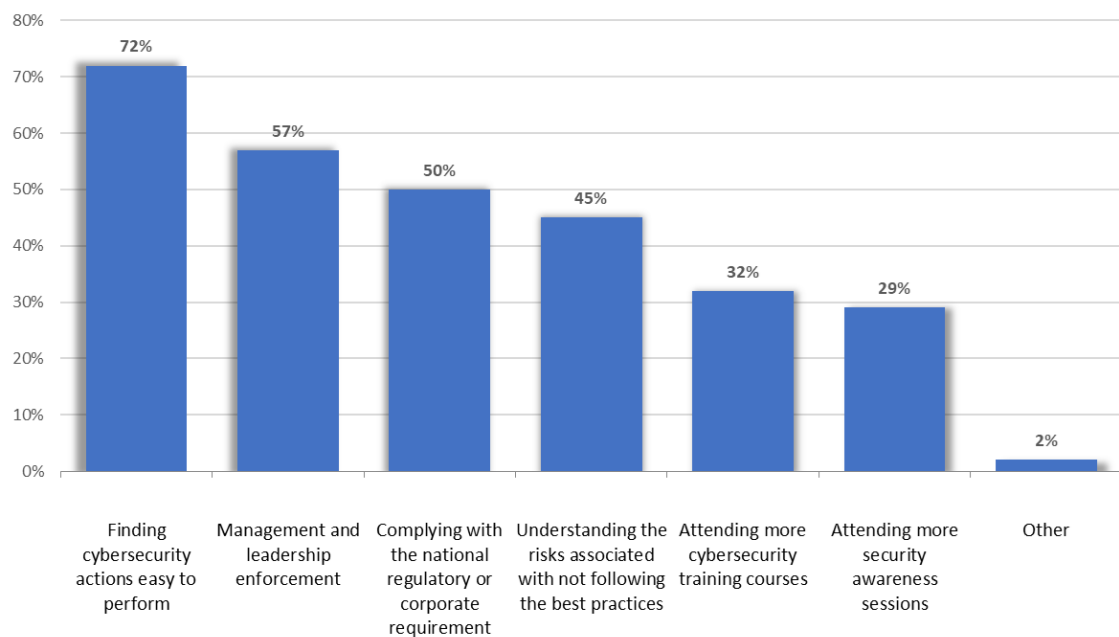


Figure 6.17: Key Motivators Encouraging Participants to Follow Cybersecurity Best Practices

Data on the key motivators encouraging participants to follow cybersecurity best practices can be used to gain insight into what drives compliance and engagement with security protocols within organizations. Understanding these motivators can help tailor

more effective cybersecurity policies and initiatives. Figure 6.17 illustrates that most participants find cybersecurity actions that are easy to perform is their top motivator. This illustrates the crucial role usability plays in cybersecurity tools and procedures. Compliance naturally follows usable security measures, reinforcing the need for ease of use and security practices. Following usability, management and leadership enforcement account for over half of the responses, indicating that when management promotes and enforces cybersecurity measures, it significantly impacts employee behavior. It is important for leaders in the workplace to be visible in their commitment to cybersecurity, perhaps through regular communication and participation. Interestingly, motivation for training or awareness sessions is lower than that for other factors, indicating the need to improve these programs and make them more engaging and relevant training could potentially have a greater impact. The 'Other' category includes unique motivators such as "the need for cybersecurity to support student education." One respondent mentioned that "the fear of being vulnerable or a victim of a cyberattack" can motivate adherence to cybersecurity best practices.

### 6.2.6 Barriers to Cybersecurity Compliance

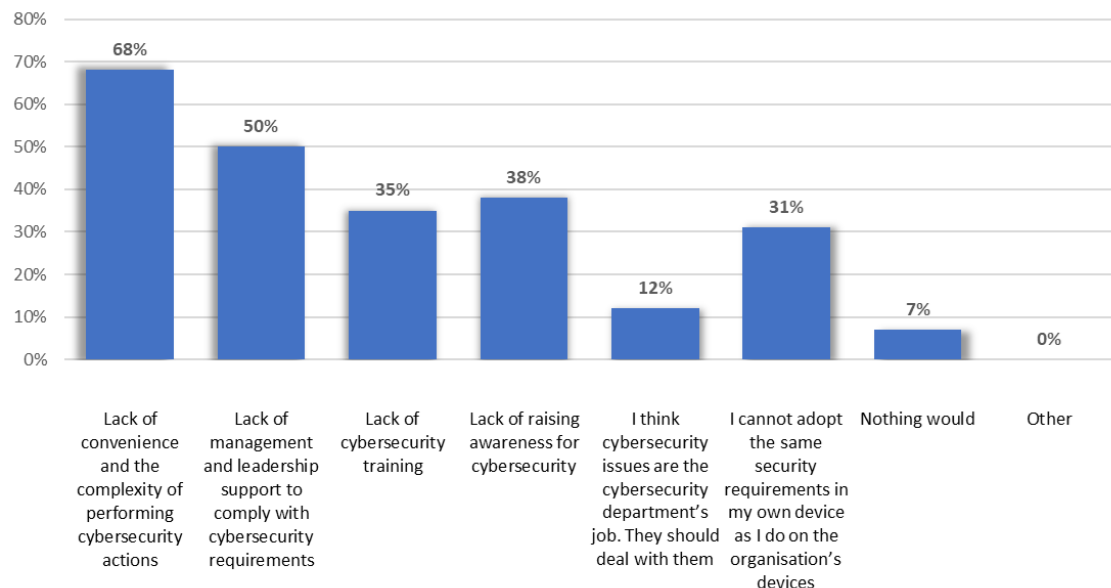


Figure 6.18: Factors Hindering Participant Adherence to Cybersecurity Best Practices

The information about what prevents participants from adhering to cybersecurity best practices gives a clear picture of the obstacles that workers must overcome to continue practicing effective security. Improving these issues is essential to improving an organization's overall cybersecurity posture. The majority of participants (68%), as shown in Figure 6.18, believe that the complexity of cybersecurity measures and their lack of convenience are the main barriers. This emphasizes how important it is to simplify cybersecurity procedures and make sure that security measures don't unnecessarily interfere with day-to-day operations. Of the participants, half believe that their inability to comply with cybersecurity regulations is caused by a lack of support from management and leadership. This suggests a lack of leadership engagement, which might be overcome by higher-level involvement and communication.

Over a third of participants say they are unable to follow best practices because they have not received adequate cybersecurity training. This indicates that more effective and intuitive training programs are required. Almost one-third of respondents found it challenging to apply the same security rules to their personal devices as to corporate devices, confirming issues in mobile and remote working contexts. A small proportion of individuals believe that nothing would hinder their compliance, indicating that they could be well-supported or highly motivated.

### 6.3 Hypotheses Testing Results

The study employed an analytical approach incorporating various statistical techniques to evaluate the hypotheses. The relationships between the key variables were examined using correlation analysis. Additionally, regression analysis was helpful in assessing the impact of predictor variables on the outcome variable. Also, logistic regression was applied to model binary outcome variables and identify significant predictors. For comparisons between groups, nonparametric tests for independent samples, such as the Mann-Whitney U test, were used. Field (2013) was a key reference for choosing the proper tests and interpreting the majority of the results. Overall, the purpose of using these methods is to provide reliability and validity for the findings.

<b>H1A: There will be a positive correlation between users' perception of usable security measures and their behavior towards unusable security measures within the organization.</b>		
<b>Variables of Interest</b>	<b>Relevant Survey Questions</b>	<b>Analytical Approach(es)</b>
<b>Independent Variable:</b> Perception of usable security measures within the organizations	<b>(Q16)</b> To what extent do you agree or disagree with the following statements:  a. I feel that the security actions in my organization are easy to understand b. I feel that the security actions in my organization are easy to perform c. I feel that the security actions in my organization strike a good balance between security and usability d. I can easily report any potential security issues or breaches that I may come across e. My organization provides adequate support for employees to understand and perform effective security actions f. My organization has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures g. My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously	Correlation & Multiple Linear Regression
<b>Dependent Variable:</b> Security behaviors.	<b>(Q14)</b> How likely would you do the following if you found a cybersecurity action difficult to perform:  a. Ignore it to complete my wider task b. Stop the task as I can't complete the action	

	c. Try my best to perform the action and complete the task d. Find my own ways around the action e. Complain/report to the responsible person or team (e.g., my supervisor, the IT department, or the cybersecurity team) f. Seek help from my colleagues	
--	--	--

Table 6.1: H1<sub>A</sub> Overview

### Correlation

We can look at the relation between Q16 and Q14 by performing a correlation test to see the direction (i.e., positive or negative) and the strength of the correlation if they are correlated {Field, 2013 #430}. First, a normality test was applied to determine the appropriate correlation test to correlate Q14 and Q16.

Tests of Normality						
	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q14 MEAN	0.161	199	<b>0.000</b>	0.970	199	<b>0.000</b>
Q16 MEAN	0.074	199	<b>0.009</b>	0.981	199	<b>0.009</b>
a. Lilliefors Significance Correction						

Table 6.2: H1<sub>A</sub> Normality Test

A Kolmogorov-Smirnov test and a Shapiro-Wilk test were conducted to assess the normality of the Q14 and Q16 mean scores. While Shapiro-Wilk is more sensitive, especially for such a sample size, Kolmogorov-Smirnov is widely used and included for completeness {Razali, 2011 #440}, and SPSS includes both test by default.

For Q14, the Kolmogorov-Smirnov test shows  $D(199) = 0.161$ ,  $p < .001$ , and the Shapiro-Wilk test also suggested a significant deviation from normality,  $W(199) = 0.970$ ,  $p = 0.000$ . Similarly, for Q16, the Kolmogorov-Smirnov test indicated that the distribution was significantly different from normal,  $D(199) = 0.074$ ,  $p = 0.009$ , and the Shapiro-Wilk test also suggested a significant deviation from normality,  $W(199) = 0.981$ ,  $p = 0.009$ . This means that the data is not normally distributed. Since the data is not normally distributed, we must use a suitable test to examine the correlation. Such data can be analyzed using Spearman rank correlation for non-parametric, which is also relatively robust even with outliers (Schober, Boer and Schwarte, 2018).

Correlations				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	.179*
		<b>Sig. (2-tailed)</b>		<b>0.011</b>
		N	200	199
	Q16 MEAN	Correlation Coefficient	.179*	1.000
		<b>Sig. (2-tailed)</b>	<b>0.011</b>	
		N	199	202
*. Correlation is significant at the 0.05 level (2-tailed).				

Table 6.3: Q14 and Q16 Correlation

The relationship between participants' perceptions of the usability of security measures (Q16 mean scores) and their behavior towards unusable security measures (Q14 mean scores) was analyzed using Spearman's rank-order correlation. The test shows that there is a statistically significant, positive correlation between the two variables,  $r_s(199) = .179$ ,  $p = .011$  (two-tailed). There is evidence that higher perceptions of usability are associated with more positive security behaviors, which is consistent with the research and supports H1<sub>A</sub>.

Further, Spearman's correlation test was performed between various perceptions of usability security measures and security behaviors and attitudes (the individual items from Q14 and Q16). Table 6.4 displays the results of the correlation.

Correlations									
		I feel that the security actions in my organisation are easy to understand	I feel that the security actions in my organisation are easy to perform	I feel that the security actions in my organisation strike a good balance between security and usability	I can easily report any potential security issues or breaches that I may come across	My organisation provides adequate support for employees to understand and perform effective security actions	My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures	My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously	
Spearman's rho	Ignore it to complete my wider task <i>(Scale reversed)</i>	Correlation Coefficient Sig. (1-tailed) N	0.035 0.311 196	0.052 0.235 196	<b>-.128<sup>*</sup></b> <b>0.039</b> <b>189</b>	<b>.198<sup>**</sup></b> <b>0.003</b> <b>191</b>	0.081 0.131 194	0.100 0.087 184	0.037 0.317 171
	Stop the task as I can't complete the action	Correlation Coefficient Sig. (1-tailed) N	<b>.244<sup>**</sup></b> <b>0.000</b> <b>198</b>	<b>.192<sup>**</sup></b> <b>0.003</b> <b>198</b>	<b>.210<sup>**</sup></b> <b>0.002</b> <b>191</b>	<b>.207<sup>**</sup></b> <b>0.002</b> <b>194</b>	<b>.141<sup>*</sup></b> <b>0.024</b> <b>197</b>	0.053 0.235 187	<b>.176<sup>*</sup></b> <b>0.010</b> <b>174</b>
	Try my best to perform the action and complete the task	Correlation Coefficient Sig. (1-tailed) N	<b>-.130<sup>*</sup></b> <b>0.034</b> <b>198</b>	<b>-.125<sup>*</sup></b> <b>0.039</b> <b>198</b>	-0.041 0.285 191	0.031 0.335 194	0.015 0.416 197	<b>.127<sup>*</sup></b> <b>0.042</b> <b>187</b>	0.007 0.465 174
	Find my own ways around the action <i>(Scale reversed)</i>	Correlation Coefficient Sig. (1-tailed) N	<b>.131<sup>*</sup></b> <b>0.034</b> <b>196</b>	0.111 0.061 196	-0.054 0.228 190	0.035 0.313 192	0.040 0.290 194	-0.020 0.394 185	<b>.192<sup>**</sup></b> <b>0.006</b> <b>172</b>
	Complain/report to the responsible person or team	Correlation Coefficient Sig. (1-tailed) N	<b>.140<sup>*</sup></b> <b>0.026</b> <b>195</b>	<b>.119<sup>*</sup></b> <b>0.050</b> <b>194</b>	<b>.120<sup>*</sup></b> <b>0.049</b> <b>189</b>	<b>.437<sup>**</sup></b> <b>0.000</b> <b>191</b>	<b>.279<sup>**</sup></b> <b>0.000</b> <b>194</b>	<b>.225<sup>**</sup></b> <b>0.001</b> <b>185</b>	<b>.237<sup>**</sup></b> <b>0.001</b> <b>174</b>
	Seek help from my colleagues	Correlation Coefficient Sig. (1-tailed) N	0.022 0.380 199	-0.037 0.301 199	0.019 0.399 192	0.102 0.079 195	0.070 0.164 198	0.074 0.157 188	0.044 0.280 175
	**. Correlation is significant at the 0.01 level (1-tailed). *. Correlation is significant at the 0.05 level (1-tailed).								

Table 6.4: Correlation of the individual items from Q14 and Q16



For each of the items, the following six points highlight the correlation results between each item from the two variables with more focus on the results that are significant, although the majority of the correlations are weak:

1. **Ignore it to complete my wider task (Scale reversed):**

There is a significant negative correlation between "I feel that the security actions in my organization strike a good balance between security and usability" and "Ignore it to complete my wider task"  $\rho(189) = -.128, p = .039$ . A correlation coefficient of -0.128 suggests a weak negative correlation, but the p-value of 0.039 is less than 0.05, which means the correlation is statistically significant. This significance implies that the negative correlation is unlikely to have occurred by chance, and there could be a meaningful relationship between the two variables. The negative value here indicates that there is an inverse relationship between the two variables. This correlation shows a weak negative relationship between employees' feelings about their organization's usable security measures and their tendency to ignore them to complete other tasks. In other words, when employees perceive a better balance between security and usability, they are less likely to disregard security to accomplish other tasks. This means that improving the perceived balance between security and usability may help reduce the tendency to bypass security measures.

In addition, there is a significant positive correlation between "I can easily report any potential security issues or breaches that I may come across" and "Ignore it to complete my wider task"  $\rho(191) = .198, p = .003$ . The correlation coefficient of 0.198 indicates a weak positive correlation, meaning that as the ease of reporting security issues increases, the tendency to ignore security measures to complete other tasks slightly increases, and vice versa. The p-value of 0.003 indicates that the correlation is statistically significant. The finding implies a statistically significant, albeit weak, positive correlation between employees' ability to easily report potential security issues or breaches and their tendency to overlook these vulnerabilities to continue performing other tasks. In other words, when employees find it easier to report security breaches, they are slightly more inclined to disregard security measures in order to complete their wider tasks. This may

appear contradictory, but it is possible that employees who are more aware of the reporting procedure are also more conscious of other factors or consequences of reporting and may opt to disregard them to retain productivity.

## **2. Stop the task as I can't complete the action:**

There are significant positive correlations between "Stop the task as I can't complete the action" and several usability perceptions:

- "I feel that the security actions in my organization are easy to understand"  $\rho(198) = .244, p < .001$ . A positive correlation of 0.244 indicates a moderate positive relationship. As employees generally understand security actions easier, they are also more likely to stop their tasks when they aren't able to complete them due to a complex security measure.
- "I feel that the security actions in my organization are easy to perform"  $\rho(198) = .192, p = .003$ . A positive correlation of 0.192 suggests a weak positive relationship, implying that when employees find security actions easier to perform, they still tend to stop their tasks when they are unable to complete an action due to complex security measures.
- "I feel that the security actions in my organization strike a good balance between security and usability"  $\rho(191) = .210, p = .002$ . A positive correlation of 0.210 indicates a weak to moderate positive relationship. This relation means that when employees perceive a good balance between security and usability within their working settings, they are slightly more likely to stop their task if they can't complete it because of security constraints.
- "I can easily report any potential security issues or breaches that I may come across"  $\rho(194) = .207, p = .002$ . A positive correlation of 0.207 also reflects a weak to moderate positive relationship. This indicates that when employees find it easy to report security issues, they are more likely to stop their task if they can't complete an action due to security reasons.
- "My organization provides adequate support for employees to understand and perform effective security actions"  $\rho(197) = .141, p = .024$ . A positive correlation of 0.141 indicates a weak positive relationship. This can mean employees who feel they receive adequate support for understanding and

performing security actions tend to stop their tasks when encountering complex security issues.

- "My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously"  $\rho(174) = .176, p = .010$ . A positive correlation of 0.176 suggests a weak positive relationship. This means that when employees feel their feedback and concerns are taken seriously by the organization, they are slightly more committed to stopping a task when they can't comply with security measures due to their complexity.

These correlations suggest that when employees perceive security actions as easier to understand, perform, balanced, easy to report, supported, and responsive to feedback, they also tend to comply strictly with these measures by stopping their tasks in order to avoid bypassing or improperly handling security practices.

### **3. Try my best to perform the action and complete the task**

There are significant negative correlations between "Try my best to perform the action and complete the task" and usability perceptions:

- "I feel that the security actions in my organization are easy to understand"  $\rho(198) = -.130, p = .034$ . A negative correlation of -0.130 indicates a weak inverse relationship, meaning that as employees find security actions easier to understand, they are slightly less likely to try their best to perform the action and complete the task when faced with unusable security measures.
- "I feel that the security actions in my organization are easy to perform"  $\rho(198) = -.125, p = .039$ . A negative correlation of -0.125 also indicates a weak inverse relationship. This relationship implies that as employees find security actions easier to perform, they are slightly less likely to try their best to perform the action and complete the task when unusable security measures are involved.

The results indicate that there are significant, although weak, negative relationships between employees' perception of the ease of performing security actions and their tendency to persist in completing tasks when facing unusable security measures. It might suggest that employees are slightly less likely to put additional effort into overcoming complex security practices even when they perceive security actions to be easier to understand and perform.

**4. Find my own ways around the action (scale reversed):**

- There is a significant positive correlation between "Find my own ways around the action" and "I feel that the security actions in my organization are easy to understand"  $\rho(196) = .131, p = .034$ . A correlation coefficient of 0.131 suggests a weak positive correlation. This means that as employees find the security actions easier to understand, they are slightly more likely to find their own ways around these actions. This finding is statistically significant, though weak, and shows a positive relationship between employees' understanding of security actions and their tendency to find their own ways around these actions. That is to say, when employees find the security measures easier to understand, they are still slightly more likely to circumvent them. A possible explanation is that employees who have a thorough understanding of security actions may also feel more confident in their ability to navigate around them without causing any significant harm. In such a situation, it may be possible that they feel empowered to bypass certain actions if they perceive them as a hindrance. Understanding security actions does not necessarily equate to adhering to them, as indicated by the positive correlation.
- There is a significant positive correlation between "Find my own ways around the action" and "My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously"  $\rho(172) = .192, p = .006$ . A correlation coefficient of 0.192 again suggests a weak positive correlation. The interpretation is that as employees perceive that their organization takes their feedback and concerns about cybersecurity seriously, they are also slightly more likely to find their way around security actions. Employees who feel that their feedback is valued might also believe that the organization trusts them to make informed decisions and may feel more empowered to take the initiative. Organizations should ensure that these decisions are taken based on security best practices.

**5. Complain/report to the responsible person or team:**

There are significant positive correlations between "Complain/report to the responsible person or team" and several usability perceptions:

- "I feel that the security actions in my organization are easy to understand"  $\rho (195) = .140, p = .026$ . A positive correlation of 0.140 indicates a weak positive relationship. This implies that as employees find security actions easier to understand, they are slightly more likely to complain or report issues to the responsible person or team.
- "I feel that the security actions in my organization are easy to perform"  $\rho (194) = .119, p = .050$ . A positive correlation of 0.119 indicates a weak positive relationship. This implies again that when employees find security actions easier to perform, they are also slightly more likely to complain or report issues.
- "I feel that the security actions in my organization strike a good balance between security and usability"  $\rho (189) = .120, p = .049$ . A positive correlation of 0.120 indicates a weak positive relationship, implying that employees are slightly more likely to complain or report issues when they perceive a good balance between security and usability.
- "I can easily report any potential security issues or breaches that I may come across"  $\rho (191) = .437, p < .001$ . A positive correlation of 0.437 indicates a moderate to strong positive relationship. This relation suggests that when employees find it easy to report security issues, they are much more likely to complain or report issues to the responsible person or team.
- "My organization provides adequate support for employees to understand and perform effective security actions"  $\rho (194) = .279, p < .001$ . A positive correlation of 0.279 indicates a weak to moderate positive relationship. This result ensures that when employees feel they receive adequate support for understanding and performing security actions, they are more likely to complain or report issues.
- "My organization has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures"  $\rho (185) = .225, p = .001$ . A positive correlation of 0.225 indicates another weak

to moderate positive relationship. This suggests that when employees perceive that the organization has initiatives to promote reporting difficulties, they are more likely to complain or report issues.

- "My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously"  $\rho(174) = .237, p = .001$ . A positive correlation of 0.237 shows a weak to moderate positive relationship, suggesting that when employees feel their feedback and concerns are taken seriously by the organization, they are more likely to complain or report issues.

#### **6. Seek help from my colleagues:**

No significant correlations were found between "Seek help from my colleagues" and any usability perceptions in the study.

Based on the study's results, it appears that there is a positive correlation between the perception of usable security measures and users' behavior towards those measures that are deemed unusable. Specifically, positive perceptions of security measures' usability are associated with more proactive security behaviors, such as reporting security issues and completing tasks, and less avoidance or workarounds of security issues. A negative perception of usability or difficulty with usability is associated with actions, such as ignoring tasks or stopping/slowing down their completion.

In addition, a separate analysis for H1<sub>A</sub> was performed to examine the correlation between the H1<sub>A</sub> variables, considering the different departments (i.e., the cybersecurity department, IT department, and other departments) where the respondents work. Evaluating the correlation across different departments enables the investigation of subgroup differences, as perceptions and behaviors may differ between people who work with cybersecurity and those who do not. It also increases contextual validity because users in non-technical departments may interpret usable security differently. In addition, the evaluation enhances interpretation. For example, if there is a substantial correlation in the "other departments" group but not in the cybersecurity group, it may indicate that usable security has a greater impact on non-experts. Table 6.5 displays the frequency and valid percent of responds from the different departments, while Tables 6.6 - 6.9 show the correlation of H1<sub>A</sub> variables based on the employees departments.

	Frequency	Valid Percent
I work in the cybersecurity department	39	19.2
I work in the IT department, including the cybersecurity team if applicable	51	25.1
I work in a department other than the cybersecurity or IT department	97	47.8
Other	16	7.9
Total	203	100.0

Table 6.5: Correlation of H1<sub>A</sub> Variables Based on the Employees Departments

More than half of respondents are from departments other than the cybersecurity or IT departments  $47.8\% + 7.9\% = 56\%$

Correlations <sup>a</sup>				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	-0.090
		<b>Sig. (1-tailed)</b>	<b>0.293</b>	
		N	39	39
	Q16 MEAN	Correlation Coefficient	-0.090	1.000
		<b>Sig. (1-tailed)</b>	<b>0.293</b>	
		N	39	39
<b>a. Please select what applies to you from the following: = I work in the cybersecurity</b>				

Table 6.6: Correlation of Employees in Cybersecurity Dept.

Correlations <sup>a</sup>				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	0.146
		<b>Sig. (1-tailed)</b>	<b>0.153</b>	
		N	51	51
	Q16 MEAN	Correlation Coefficient	0.146	1.000
		<b>Sig. (1-tailed)</b>	<b>0.153</b>	
		N	51	51
<b>a. Please select what applies to you from the following: = I work in the IT department, including the cybersecurity team if applicable</b>				

Table 6.7: Correlation of Employees in IT Dept including Cybersecurity (if applicable)

The results show no significant correlation between the variables of H1<sub>A</sub> for people who work either in the cybersecurity department or the IT department.

Correlations <sup>a</sup>				
			Q14 MEAN	Q16 MEAN
Spearman 's rho	Q14 MEAN	Correlation Coefficient	1.000	.255 **
		<b>Sig. (1- tailed)</b>	<b>0.007</b>	
		N	95	94
	Q16 MEAN	Correlation Coefficient	.255 **	1.000
		<b>Sig. (1- tailed)</b>	<b>0.007</b>	
		N	94	96
**. Correlation is significant at the 0.01 level (1-tailed).				
a. Please select what applies to you from the following: = I work in a department other than the cybersecurity or IT department				

Table 6.8: Correlation of Employees in Departments Other Than the Cybersecurity or IT Dept

Correlations <sup>a</sup>				
			Q14 MEAN	Q16 MEAN
Spearman 's rho	Q14 MEAN	Correlation Coefficient	1.000	-.523 *
		<b>Sig. (1- tailed)</b>	<b>0.023</b>	
		N	15	15
	Q16 MEAN	Correlation Coefficient	-.523 *	1.000
		<b>Sig. (1- tailed)</b>	<b>0.023</b>	
		N	15	16
*. Correlation is significant at the 0.05 level (1-tailed).				
a. Please select what applies to you from the following: = Other				

Table 6.9: Employees who Selected Other

The results from tables 6.8 and 6.9 show a significant correlation between the variable of H1<sub>A</sub> for people who work in departments other than the cybersecurity department or the IT department.

## Regression

According to Field (2013), correlation is often an important starting point for determining whether a relationship exists. However, a regression model is recommended to explain or predict an outcome (behavior, in this case) using multiple predictors. To perform a further investigation, Multiple Linear Regression (MLR) is a robust test even with violations of normality, particularly with large samples (Ghasemi and Zahediasl, 2012) (e.g., N>30) and residual diagnostics are critical to confirming model assumptions. Table 6.10 shows the residual statistics for H1<sub>A</sub>.



Residuals Statistics <sup>a</sup>					
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.2657	3.8082	2.9717	0.32725	191
Residual	-1.99309	2.38795	0.00000	0.83194	191
Std. Predicted Value	-2.157	2.556	0.000	1.000	191
Std. Residual	-2.358	2.825	0.000	0.984	191
a. Dependent Variable: Q16 MEAN					

Table 6.10: Residuals Statistics for H1<sub>A</sub>

The mean residual is 0.00, which is ideal since residuals in a well-fitting regression model should be around zero. Standardized residuals range from -2.358 to 2.825, i.e., within  $\pm 3$ , indicating no extreme outliers and supporting the validity of MLR. Also, 191 observations ensure robustness against deviations from normality. Thus, MLR analysis was performed to understand further the relationship between people's security-related behavior and their perceptions of the usability of cybersecurity measures within their workplace. Here, we have all of the Q14 items as predictors, and Q16 is the dependent variable, i.e., Q16 mean scores (participants' perceptions of the usability of security measures) based on their responses to various cybersecurity behaviors (Q14 items).

Model Summary <sup>b</sup>									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.366 <sup>a</sup>	0.134	0.106	0.845	0.134	4.745	6	184	0.000
a. Predictors: (Constant): - Ignore it to complete my wider task ( <u>Scale reversed</u> ). - Seek help from my colleagues. - Stop the task as I can't complete the action. - Find my own ways around the action ( <u>Scale reversed</u> ). - Complain/report to the responsible person or team. - Try my best to perform the action and complete the task.									
b. Dependent Variable: Q16 MEAN									

Table 6.11: Model Summary of H1<sub>A</sub> with Q16's Mean Being the Dependent Variable

As shown in Table 6.11, the model was statistically significant,  $F(6,184) = 4.745$ ,  $p < .001$ , and accounted for approximately 13.4% of the variance in Q16 mean scores (Adjusted  $R^2 = .106$ ), so the model explained approximately 10.6% of the variance in

the dependent variable. Also, as shown in Table 6.12 below, it appears that there is no issue with multicollinearity because all the VIFs are  $< 5$ .

Coefficients <sup>a</sup>								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
	(Constant)	1.643	0.390		4.218	<b>0.000</b>		
	Ignore it to complete my wider task (Scale reversed)	0.002	0.061	0.002	0.028	0.977	0.728	1.374
	Stop the task as I can't complete the action	0.144	0.052	<b>0.197</b>	2.755	<b>0.006</b>	0.921	1.085
	Try my best to perform the action and complete the task	0.008	0.071	0.009	0.114	0.909	0.843	1.186
	Find my own ways around the action (Scale reversed)	0.077	0.062	0.099	1.231	0.220	0.722	1.384
	Complain/report to the responsible person or team	0.209	0.058	<b>0.267</b>	3.629	<b>0.000</b>	0.872	1.147
	Seek help from my colleagues	0.030	0.070	0.032	0.432	0.666	0.885	1.130
a. Dependent Variable: Q16 MEAN								

Table 6.12: Correlation Coefficients (Dependent Variable: Q16 Mean)

The significant predictors are:

- “Stop the task as I can’t complete the action” ( $\beta = .197$ ,  $p = .006$ ) indicates that stopping a task due to unusable security measures significantly predicts better perceptions of cybersecurity usability.
- “Complain/report to the responsible person or team” ( $\beta = .267$ ,  $p < .001$ ), suggesting that those who are proactive in reporting issues perceive better usable security measures.

Other variables were not significant predictors, as their p-values exceeded 0.05.

Next, we perform the opposite to investigate the relationship between various perceptions of security actions and the dependent variable, Q14’s mean. The model summary and the correlation coefficient are shown in Table 6.13 and Table 6.14 respectively.

Model Summary <sup>b</sup>									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.320 <sup>a</sup>	0.102	0.062	0.532	0.102	2.524	7	155	0.017
a. Predictors: (Constant):									
<ul style="list-style-type: none"> <li>- I feel that the security actions in my organisation are easy to perform</li> <li>- I feel that the security actions in my organisation are easy to understand</li> <li>- My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously</li> <li>- My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures</li> <li>- I can easily report any potential security issues or breaches that I may come across</li> <li>- I feel that the security actions in my organisation strike a good balance between security and usability</li> <li>- My organisation provides adequate support for employees to understand and perform effective security actions</li> </ul>									
b. Dependent Variable: Q14 MEAN									

Table 6.13: Model Summary of H1A with Q14's Mean Being the Dependent Variable

The model was statistically significant,  $F(7,155) = 2.524$ ,  $p = .017$ , and accounted for approximately 6.2% of the variance in Q14 mean scores (Adjusted  $R^2 = .062$ ). This indicates that the independent variables can explain approximately 10.2% of the variance in the dependent variable.

Coefficients <sup>a</sup>								
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics		
	B	Std. Error	Beta			Tolerance	VIF	
(Constant)	2.619	0.148		17.748	0.000			
I feel that the security actions in my organisation are easy to understand	0.035	0.081	0.072	0.436	0.663	0.214	4.670	
I feel that the security actions in my organisation are easy to perform	-0.037	0.078	-0.073	-0.473	0.637	0.245	4.082	
I feel that the security actions in my organisation strike a good balance between security and usability	-0.099	0.058	-0.201	-1.712	0.089	0.421	2.375	
I can easily report any potential security issues or breaches that I may come across	0.132	0.046	0.297	2.880	0.005	0.546	1.832	
My organisation provides adequate support for employees to understand and perform effective security actions	-0.032	0.059	-0.066	-0.552	0.582	0.405	2.468	
My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures	0.005	0.047	0.011	0.113	0.910	0.632	1.582	
My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously.	0.096	0.052	0.202	1.864	0.064	0.494	2.024	
a. Dependent Variable: Q14 MEAN								

Table 6.14: Correlation Coefficients (Dependent Variable: Q14 Mean)

- Only one item is a significant predictor of Q14: “I can easily report any potential security issues or breaches that I may come across” ( $\beta = 0.132$ ,  $p = 0.005$ ), meaning that the ease of reporting potential security issues was a significant positive predictor of the dependent variable.
- Also, “My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously” is close to significant ( $p = 0.064$ ), but other variables were not significant predictors of the dependent variable.

<b>H2A: A positive perception of usable security is negatively associated with the frequency of reported incidents of bypassing security measures</b>		
<b>Variables of Interest</b>	<b>Relevant Survey Questions</b>	<b>Analytical Approach(es)</b>
<b>Independent Variable:</b> Bypassing security measures, indicating bad behavior.	<b>(Q16)</b> To what extent do you agree or disagree with the following statements:  a. I feel that the security actions in my organization are easy to understand b. I feel that the security actions in my organization are easy to perform c. I feel that the security actions in my organization strike a good balance between security and usability d. I can easily report any potential security issues or breaches that I may come across e. My organization provides adequate support for employees to understand and perform effective security actions f. My organization has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures g. My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously	Nonparametric Test: Mann-Whitney U
<b>Dependent Variable:</b> A positive perception of usable security measures within the organizations	<b>(Q15)</b> Have you ever had to bypass a cybersecurity technology or procedures due to usability issues?	

Table 6.15: H2A Overview

In H2A, Q16 is a scale question, and Q15 is a nominal/categorical variable because the responses can be “Yes” or “No”, which does not make the hypothesis suitable for correlation. Q16’s Mean was tested for normality in order to determine the suitable choices for the test. The normality test is shown in Table 6.16.

<b>Tests of Normality</b>						
	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q16 MEAN	0.074	199	<b>0.009</b>	0.981	199	<b>0.009</b>
a. Lilliefors Significance Correction						

Table 6.16: H2A Normality Test

A Kolmogorov-Smirnov test and a Shapiro-Wilk test were conducted to assess the normality of the Q16 MEAN scores. The Kolmogorov-Smirnov test indicated that the distribution was significantly different from normal,  $D(199) = 0.074$ ,  $p = 0.009$ . Similarly, the Shapiro-Wilk test also suggested a significant deviation from normality,  $W(199) = 0.981$ ,  $p = 0.009$ . Therefore, the assumption of normality was violated. Ideally, parametric tests, such as t-tests for independent samples, should not be used (Vickers, 2005), and it is imperative to look for a suitable alternative for the t-test for independent samples (comparing the difference between the average score on Q16 of the two groups of people who said “Yes” or “No”). This necessitates the use of nonparametric tests (Gibbons, 1993). The nonparametric equivalent is the Mann-Whitney test (McKnight and Najab, 2010).

Hypothesis Test Summary			
	Null Hypothesis	Sig. <sup>a,b</sup>	Decision
1	The distribution of Q16 MEAN is the same across categories of Q15	0.093	Retain the null hypothesis.
2	The distribution of "I feel that the security actions in my organisation are easy to understand" is the same across categories of Q15	0.253	Retain the null hypothesis.
3	The distribution of "I feel that the security actions in my organisation are easy to perform" is the same across categories of Q15	0.169	Retain the null hypothesis.
4	The distribution of "I feel that the security actions in my organisation strike a good balance between security and usability" is the same across categories of Q15	<b>0.045</b>	<b>Reject the null hypothesis.</b>
5	The distribution of "I can easily report any potential security issues or breaches that I may come across" is the same across categories of Q15	0.326	Retain the null hypothesis.
6	The distribution of "My organisation provides adequate support for employees to understand and perform effective security actions" is the same across categories of Q15	<b>0.041</b>	<b>Reject the null hypothesis.</b>
7	The distribution of "My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures" is the same across categories of Q15	0.132	Retain the null hypothesis.
8	The distribution of "My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously" is the same across categories of Q15	0.078	Retain the null hypothesis.
a. The significance level is .050.			
b. Asymptotic significance is displayed.			

Table 6.17: H2A Test Summary

Looking at the average of the Q16 mean against Q15 ( $p = 0.093$ ), as illustrated in Table 6.17, one can observe that there is no significant difference between the "Yes" and "No" responses to Q15, indicating that the relationship is not statistically significant. However, examining the individual items of Q16 reveals two items with significant differences: "I feel that the security actions in my organization strike a good balance between security and usability" ( $p = 0.045$ ) and "My organization provides adequate support for employees to understand and perform effective security actions" ( $p = 0.041$ ). Figures 6.19 and 6.20 show the differences between the "Yes" and "No" responses for these two items.

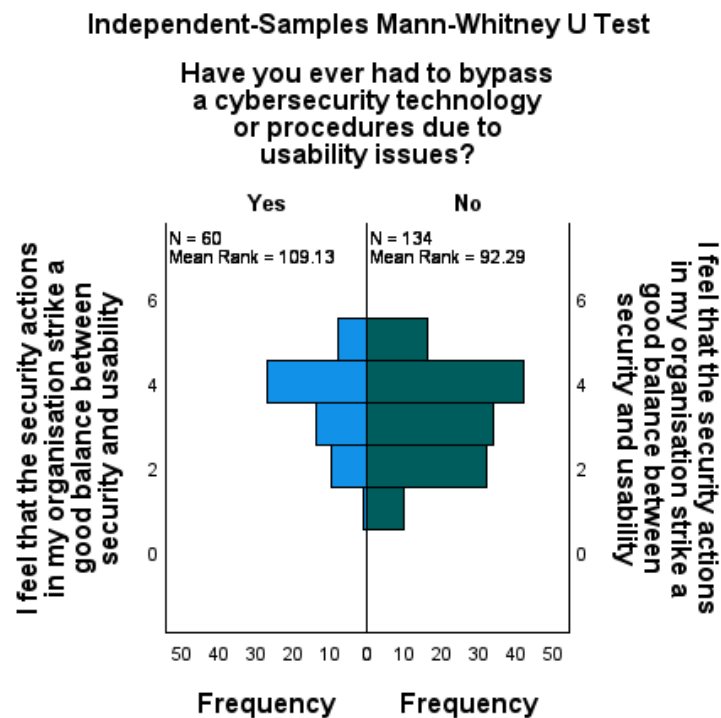


Figure 6.19: Difference between the Participants' "Yes" and "No" Participants Responses to the Security and Usability Balance Perspective

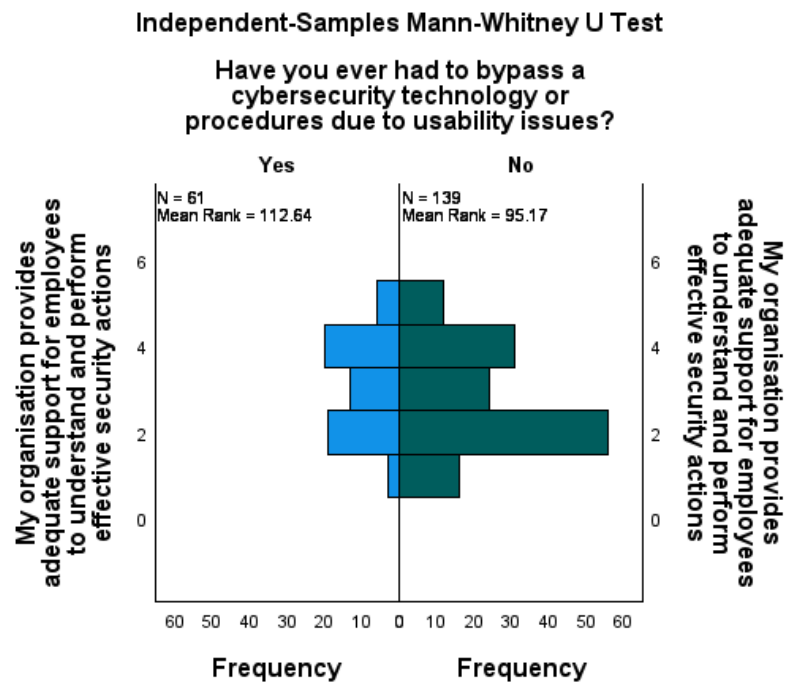


Figure 6.20: Difference between the Participants' "Yes" and "No" Participants Responses about the Organizational Support for Cybersecurity

The findings suggest that personal experiences with system inefficiencies are significantly related to the perceptions of usability and organizational support in cybersecurity measures. It is noted that participants who have bypassed cybersecurity protocols as a result of usability issues perceive a lesser balance between security and usability, as well as feeling less supported by their organizations. This indicates that increasing the usability of cybersecurity measures can reduce the necessity for employees to bypass them.



<b>H3<sub>A</sub>: Ease of understanding and performing security actions predicts users' confidence in complying with security requirements within organizations</b>		
<b>Variables of Interest</b>	<b>Relevant Survey Questions</b>	<b>Analytical Approach(es)</b>
<b>Independent Variables:</b> Perceived ease of understanding and performing security actions within the organization	(Q16) To what extent do you agree or disagree with the following statements:  a. I feel that the security actions in my organization are easy to understand b. I feel that the security actions in my organization are easy to perform	Multiple Linear Regression
<b>Dependent Variable:</b> Confidence in following cybersecurity requirements	(Q11) How confident are you in: b. Following cybersecurity requirements in your organization	

Table 6.18: H3<sub>A</sub> Overview

Regression analysis was utilized to determine how the perceived usability (ease of understanding and performing security actions) predicts confidence in following cybersecurity requirements. MLR allows for examining various factors and their combined and individual effects on user confidence. Furthermore, both the independent and dependent variables are on a continuous scale (e.g., Likert), which is appropriate for MLR {Field, 2013 #430}. Table 6.19 shows the model summary of Q16's mean being the independent variable and Q11 the dependent variable.

<b>Model Summary<sup>b</sup></b>									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.504 <sup>a</sup>	0.254	0.246	0.907	0.254	33.311	2	196	0.000
a. Predictors: (Constant), I feel that the security actions in my organisation are easy to perform, I feel that the security actions in my organisation are easy to understand									
b. Dependent Variable: Following cybersecurity requirements in your organisation									

Table 6.19: Model Summary of Q16's Mean Being the Independent Variable and Q11 the Dependent Variable

The regression model was statistically significant,  $F(2,196) = 33.311$ ,  $p < .001$ , explaining 25.4% of the variance in following cybersecurity requirements in the organization ( $R^2 = .254$ , Adjusted  $R^2 = .246$ ). Also, since H3<sub>A</sub> focuses on prediction, ANOVA supports the model's overall predictive power {Cedervik, 2005 #442}. The ANOVA summary in Table 6.20 demonstrates if the regression model is statistically

significant, i.e., whether the predictors (ease of understanding and implementing security measures) combined explain a substantial amount of variance in the dependent variable (user confidence).

ANOVA <sup>a</sup>						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	54.857	2	27.428	33.311	.000 <sup>b</sup>
	Residual	161.384	196	0.823		
	Total	216.241	198			
a. Dependent Variable: Following cybersecurity requirements in your organisation						
b. Predictors: (Constant), I feel that the security actions in my organisation are easy to perform, I feel that the security actions in my organisation are easy to understand						

Table 6.20: Summary of H3A's ANOVA Test

The regression model significantly predicted 'following cybersecurity requirements in the organization':  $F(2,196) = 33.311, p < .001$ . The total variance explained by the model was 25.4% ( $R^2 = .254$ ), with a residual sum of squares of 161.384.

Coefficients					
	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	0.754	0.198		3.810	0.000
I feel that the security actions in my organisation are easy to understand	0.187	0.112	0.202	1.665	0.098
I feel that the security actions in my organisation are easy to perform	0.301	0.115	0.319	2.623	0.009
Dependent Variable: Following cybersecurity requirements in your organisation					

Table 6.21: H3A's Correlation Coefficients (Dependent Variable: Cybersecurity Compliance)

The intercept, representing the baseline level of following cybersecurity requirements when both predictors are at zero, was significant,  $B = 0.754, t(196) = 3.810, p < .001$  as Table 6.12 illustrates. Perception of the ease of understanding security actions was not a significant predictor,  $B = 0.187, \beta = 0.202, t(196) = 1.665, p = 0.098$ . However,

perception of the ease of performing security actions was a significant predictor,  $B = 0.301$ ,  $\beta = 0.319$ ,  $t(196) = 2.623$ ,  $p = 0.009$

The key information we are interested in from running the test is the Adjusted  $R^2$  (i.e., the percentage of the variance in the dependent variable explained by the two independent variables), the standardized coefficients ( $\beta$ ), and the significance value from the ANOVA table. The regression results shows that these two independent variables explain 25% of the variance in the dependent variable. The model is statistically significant, indicating that it is much better than chance at predicting the values of the dependent variable. Individually, for "I feel that the security actions in my organization are easy to understand," the variable accounts for approximately 20% of a point on the dependent variable (confidence in following cybersecurity requirements). For "I feel that the security actions in my organization are easy to perform," going up one unit will give an increase of 0.31 units on the dependent variable (confidence in following cybersecurity requirements). It is worth noting that even though the first independent variable has a  $p$ -value of 0.098, the test is still considered significant because the regression assesses the model and the combined effect of the independent variables.

Overall, "Ease of performing security actions" is the significant predictor, indicating that employees are more likely to follow cybersecurity requirements when they can execute security measures easily. It is, therefore, imperative that security measures be designed in a usable manner in order to increase their adherence. Although "ease of understanding security actions" was not a significant predictor, it approached significance, suggesting that it may still play an important role. By promoting usable security practices, organizations can foster a more robust security culture by making compliance more accessible and intuitive to their employees.

<b>H4<sub>A</sub>: Ease of understanding and performing security actions is negatively associated with the frequency of reported security incidents</b>		
<b>Variables of Interest</b>	<b>Relevant Survey Questions</b>	<b>Analytical Approach(es)</b>
<b>Independent Variable:</b> Ease of understanding and performing security actions within the organization	<b>(Q16)</b> To what extent do you agree or disagree with the following statements:  a. I feel that the security actions in my organization are easy to understand b. I feel that the security actions in my organization are easy to perform	Logistic regression
<b>Dependent Variable:</b> Frequency of reported security incidents	<b>(Q17)</b> Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?	

Table 6.22: H4<sub>A</sub> Overview

Logistic regression was used due to the binary nature of the dependent variable (reported difficulties or not). Logistic regression is appropriate when predicting a binary outcome from a set of continuous or categorical predictor variables (Nick and Campbell, 2007).

<b>Classification Table<sup>a</sup></b>				
Observed		Predicted		
		Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?		Percentage Correct
		Yes	No	
Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?	Yes	0	51	0
	No	0	149	100
<b>Overall Percentage = 74.5</b>				
a. The cut value is .500				

Table 6.23: H4<sub>A</sub>'s Prediction Classification Table

The numbers in Table 6.23 the model correctly predicted the absence of reporting difficulties (i.e., when participants answered “No”) 100% of the time and failed to

predict the presence of reporting difficulties (i.e., when participants answered “Yes”), with an overall prediction success rate of 74.5% (i.e., three-quarters of the time).

Omnibus Tests of Model Coefficients				
		Chi-square	df	Sig.
Step 1	Step	7.722	2	<b>0.021</b>
	Block	7.722	2	<b>0.021</b>
	Model	7.722	2	<b>0.021</b>

Table 6.24: H4A's Model Coefficients

Table 6.24 shows that the model was statistically significant,  $\chi^2(2) = 7.722$ ,  $p = .021$ , indicating that the model was able to distinguish between respondents who reported difficulties in using cybersecurity technologies or following cybersecurity procedures and those who did not based on the predictors.

Variables in the Equation								
	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I. for	
							Lower	Upper
I feel that the security actions in my organisation are easy to understand	0.398	0.278	2.049	1	<b>0.152</b>	<b>1.489</b>	0.863	2.568
I feel that the security actions in my organisation are easy to perform	-0.706	0.289	5.962	1	<b>0.015</b>	<b>0.494</b>	0.280	0.870
Constant	2.122	0.546	15.095	1	<b>0.000</b>	<b>8.352</b>		
Variable(s) entered on step 1: I feel that the security actions in my organisation are easy to understand, I feel that the security actions in my organisation are easy to perform.								

Table 6.25: H4A's Variable in the Equation

Looking at the variables in the equation shown in Table 6.25, ease of understanding security actions was not a significant predictor of reporting difficulties,  $B = .398$ ,  $SE = .278$ ,  $Wald = 2.049$ ,  $p = .152$ ,  $Exp(B) = 1.489$ . However, ease of performing security actions was a significant predictor, indicating that greater ease of performance was associated with a lower likelihood of reporting difficulties,  $B = -.706$ ,  $SE = .289$ ,  $Wald = 5.962$ ,  $p = .015$ ,  $Exp(B) = .494$ . This suggests that for each unit increase in ease of performing security actions, the odds of reporting difficulties decrease by 50.6%. There is no strong evidence that understanding alone influences the reporting of

difficulties, as the regression coefficient for ease of understanding security actions is positive but not statistically significant. In contrast, the negative coefficient for ease of performing security actions indicates that improvements in making security measures easy to perform significantly reduce the likelihood of finding these measures complicated. This suggests that organizations should focus on enhancing the practical aspects of their security measures to reduce operational challenges.

<b>H5A: Organizational support and policies promoting the reporting of usable security issues positively influence employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches</b>		
<b>Variables of Interest</b>	<b>Relevant Survey Questions</b>	<b>Analytical Approach(es)</b>
<b>Independent Variable:</b> Perceived organizational support for reporting cybersecurity issues	<b>(Q16)</b> To what extent do you agree or disagree with the following statements:  f. My organization has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures  g. My organization takes staff feedback and concerns about cybersecurity technologies and procedures seriously	Multiple Linear Regression
<b>Dependent Variable:</b> Employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches	<b>(Q11)</b> How confident are you in:  c. Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace	

Table 6.26: H5A Overview

For H5A, a regression analysis is useful for determining the predictive relation between organizational support/policies (independent variable) and employee confidence in reporting vulnerabilities (dependent variable). It also allows us to quantify the strength and direction of this influence. Primarily, because both variables are evaluated on continuous or ordinal scales (e.g., Likert items), MLR is suited for determining the extent to which organisational support explains variance in employee confidence.

Model Summary <sup>b</sup>									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.348 <sup>a</sup>	0.121	0.111	1.147	0.121	11.738	2	170	0.000
a. Predictors: (Constant): - My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously - My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures									
b. Dependent Variable: Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace									

Table 6.27: H5A's Model Summary

A multiple regression analysis was performed and the test indicated that the model, as shown in Table 6.27 explains approximately 12.1% of the variance in employees' confidence in identifying and reporting cybersecurity issues ( $R^2 = .121$ , Adjusted  $R^2 = .111$ ). This model was statistically significant,  $F(2, 170) = 11.738$ ,  $p < .001$ .

ANOVA <sup>a</sup>						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.909	2	15.455	11.738	.000 <sup>b</sup>
	Residual	223.819	170	1.317		
	Total	254.728	172			
a. Dependent Variable: Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace						
a. Predictors: (Constant): - My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously - My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures						

Table 6.28: Summary of H5A's ANOVA Test

The summary of H5A's ANOVA test in Table 6.28 shows that the regression model significantly predicted employees' confidence in identifying and reporting cybersecurity vulnerabilities, explaining 12.1% of the variance ( $R^2 = .121$ , Adjusted  $R^2 = .111$ ). The regression sum of squares was 30.909, and the residual sum of squares was 223.819, with a total of 254.728.

Coefficients <sup>a</sup>						
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	
	B	Std. Error	Beta			
(Constant)	1.397	0.254		5.489	0.000	
1 My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures	0.181	0.090	0.168	2.020	0.045	
My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously	0.243	0.087	0.232	2.780	0.006	
a. Dependent Variable: Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace						

Table 6.29: H5A's Correlation Coefficients (Dependent Variable: Identifying and Reporting Cybersecurity Incidents)

H5A's correlation coefficients shown in Table 6.29 (dependent variable: "Identifying and reporting cybersecurity Incidents") demonstrates that the baseline confidence level when all predictors are zero was significant,  $B = 1.397$ ,  $p < .001$ . Looking at the results individually, organizational policies that promote reporting difficulties positively impacted confidence, with  $B = .181$ ,  $\beta = .168$ ,  $t(170) = 2.020$ ,  $p = .045$ . Similarly, organizational support for staff feedback and concerns also showed a significant prediction,  $B = .243$ ,  $\beta = .232$ ,  $t(170) = 2.780$ ,  $p = .006$ . As a result, both are statistically significant and are positive coefficients, meaning that both independent variables are significant predictors in their own right, and the model is significant overall. The findings imply that employees' confidence in their capacity to identify and report vulnerabilities in cybersecurity is greatly increased by organizational support for staff feedback as well as organizational rules that encourage reporting. This suggests that proactive organizational actions motivate workers and encourage compliance, increasing their alertness and response to cybersecurity threats. Organizations should further emphasize policies that encourage communications regarding cybersecurity issues and enhance support for staff feedback. As approved in the study, this will likely increase employee confidence and proactive behaviors in managing cybersecurity risks.



## 6.4 Chapter Summary

The findings from the quantitative analysis highlight several key insights into user interactions with cybersecurity within organizational settings. For instance, the majority of participants agreed that shared behaviors and beliefs about cybersecurity within their organizations create a sense of collective responsibility for maintaining cybersecurity practices. However, many participants reported frequent encounters with usability issues in cybersecurity technologies, which hinder adherence to security measures and negatively impact productivity in the workplace. In addition, drawing upon the results, there is a relationship between perceived usability and positive security behaviors, which suggests that enhancing the perceived balance between security and usability will reduce the tendency to bypass security measures. Furthermore, the data indicate that employees are more inclined to adhere to cybersecurity requirements when security measures are usable. The findings also suggest that organizations should facilitate employee communication regarding cybersecurity issues since these practices increase employee confidence and encourage proactive behaviors in managing cybersecurity risks. Continuing from these quantitative insights, the following section focuses on the qualitative findings, providing a deeper understanding of the relationship between usable security and security culture.

# **Chapter 7: Qualitative Analysis and Findings**

## 7.1 Introduction

This chapter presents the findings derived from the qualitative data analysis collected through the survey's open-ended responses and data collected through semi-structured interviews. This involved generating codes to find broader themes and investigating the interactions between codes by examining the data to detect potential linkages, which aided in discovering common themes and connections within the dataset as guided by Braun and Clarke (2006); Braun and Clarke (2021). As themes emerged, contestant topics were selected based on the initial codes, and the data was examined for additional information. Subsequently, the identified themes were refined by ensuring that they were accurate and that the data represented was in accordance with the research objectives. Subthemes have also been generated where appropriate, and some themes have been merged to improve conceptual clarity. The following sections detail the analysis process.

## 7.2 Findings from the Survey

This section provides results from the open-ended responses, including the themes and subthemes identified. Including subthemes in a study findings allow for a more detailed exploration of the themes (Pietkiewicz and Smith, 2014). The survey questions which form this part of the study are:

**Q12:** *“Please feel free to offer any additional thoughts or feedback that you feel would be relevant to your organization's security culture.”*

Q12 enables respondents to provide their views on organizational security culture.

**Q15a:** *“Have you ever had to bypass a cybersecurity technology or procedures due to usability issues? Please describe the situation briefly.”*

Q15a collects reported incidences of respondents bypassing cybersecurity technology or procedures due to usability issues.

**Q17:** *“Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organization? Please explain the nature of the difficulty you encountered.”*

Q17 allows respondents to report challenges encountered while using cybersecurity technologies or following procedures.

**Q18:** *“Please feel free to offer any additional thoughts or feedback that you feel would be relevant to the usability of cybersecurity in your organization.”*

Q18 allows general feedback on the usability of security measures within the participants’ workplace.

**Q20:** *“Please feel free to offer any additional thoughts or feedback relevant to the relationship between usable security and security culture.”*

Q20 provides the participants with a space to express their views on the relationship between usable security and security culture.

**Q21:** *“What would be the main drivers for you to follow cybersecurity best practices in your organization (please select all that apply)? If you selected Other, please specify.”*

Q21 explores what other factors motivate respondents’ adherence to cybersecurity practices.

**Q22:** *“What would prevent you from following cybersecurity best practices in your organization (please select all that apply). If you selected Other, please specify.”*

Q22 allows participants to provide potential barriers to following cyber practices other than the ones listed under the question.

**Q23:** *“Do you have suggestions for how the usability of cybersecurity could be further improved in your organization?”*

Q23 allows respondents to offer suggestions for improving the usability of cybersecurity in their organization with the aim of gathering practical recommendations for enhancing the overall security measures.

There are three main themes identified, each comprising subthemes. Themes 1 and 2 include two subthemes each, while Theme 3 include four subthemes:

### **Theme 1: Usability Challenges in Cybersecurity**

**Subtheme 1.1: Bypassing cybersecurity technology or procedures due to usability issues to complete tasks.** The study participants reported many situations where they had to bypass a cybersecurity measure due to usability issues. Most participants indicated that they had used a colleague's account to do a job-related task when they could not do it via their devices, among other approaches. Below are the comments from the study, which explain the situations where participants had to bypass cybersecurity measures:

- *“Asked others to use their access rights to do my job when my account was not available.”*
- *“We needed to get a client project out and my computer did not have the correct tool. So, I borrowed a colleague’s computer that did and their password.”*
- *“Due to an access error, my credentials did not work as they should to generate a report I needed urgently. I asked a colleague for his credentials in order to complete the actions.”*
- *“Asked other to carry out the task for me. Used other platform to carry out the task, however not reducing the security level. Carry out task "manually".”*
- *“I needed to teach certain concepts in cybersecurity and needed to find a way to show how it works, how to review and how to stop. Virtual machines off the network are used”*
- *“Install backdoor for remote access”*
- *“I had to send an attachment to my personal email so I can open it”*
- *“Sometimes removing my smart card from my computer when away from my desk (the cybersecurity requirement) puts the computer in an inaccessible state when I reinsert the card, causing me to have to reboot. Therefore, I don’t always take my card out and with me if I’m only stepping out of my office for a few minutes.”*

- *“I used personal email to transfer some data which I couldn’t using my company’s email.”*

**Subtheme 1.2: Difficulties encountered while using cybersecurity technologies or following cybersecurity procedures.** The study participants reported encountering many usability issues when dealing with cybersecurity. It is worth noting that some of these issues are related to technologies, and others are related to the procedures and processes that organizations employ to secure their systems. Identified issues include unclear instructions, difficulty understanding and remembering authentication methods, security technologies, such as firewalls blocking functionality, and inadequate support from the cybersecurity department for generally complex security measures.

**Authentication issues:**

- *“Most of the usability issues I encounter are related to authentication. Not all issues are being resolved yet, but I can understand that the security team has to implement and apply certain policies to ensure organisation security and to comply with regulations”*
- *“I had to disable 2FA in order to get an account to function properly”*
- *“I could not access my email as it was protected by two steps verification, and I did not have my phone at that particular time”*
- *“Used different method of MFA due to issues with other MFA methods”*
- *“Not being able to install programs, not being able to use MFA. Inconsistent guidelines and controls for passwords”*
- *“Accessibility failure due to complex authentication process”*
- *“We work with both our Office 365 accounts and client Office 365 accounts. This creates confusion about how to login.”*

**No clear policies for reporting security issues:**

- *“In my organisation It is not very clear what kinds of vulnerabilities users are responsible to report and to whom they need to report.”*

- *“It is very unclear how security incidents should be reported and what the internal security procedures are.”*
- *“I don't know how or if there is any channel to report security and usability issues in my organisation”*
- *“I know how and who to report cybersecurity incidents to - however, this is not always clear to other staff and students. Users should be made more aware of the processes involved”*

**External devices issues:**

- *“The USB ports don't work in my organisations' desktops, and I needed to download an important report that was stored in a USB, so I had to ask the responsible person from the cybersecurity team to give me access so I can download the report.”*
- *“Printer not working caused by Firewall.”*

**Other cybersecurity policies issues:**

Participants highlighted other cybersecurity issues which can be summarized as follows:

- Complex security procedures
- Restricted access to email
- Lack of flexibility in software approval
- Firewall restrictions on internet access
- System performance issues from security tools
- Disruptive updates

Below are the participant quotes that highlight the several cybersecurity-related issues that they faced in their organizations:

- *“I don't like complicated processes or language. Also, it's so annoying to read and follow long steps and then fail to solve the issue. Sometimes, these technologies ask you to read a long document to understand the threats that you may face and how to solve.”*

- *“Not able to open the attachment through the company email”*
- *“I have regularly required software that was not approved to finish my job. Now I 've been exempt from the policy”*
- *“Inability to browse external internet links (part of job) due to firewalls.”*
- *“Unable to use external sites, need to download needed software for classes”*
- *“Lately we were facing MS outlook hanging and jam issues that were caused by one of the cybersecurity applications and the fix solution took a long time to find”*
- *“Rebooting my computer due to updates is annoying as I have so many things open in my computer always.”*

## **Theme 2: Perceptions and Feedback on Usable Security and Security Culture**

**Subtheme 2.1: Views and Feedback on Usable Security.** Participants provided their views and feedback on the usable security in the organisation, indicating aspects which could make cybersecurity measures more usable or expressing general usable security views:

- *“Usable security measures should be considered from early stages of developing and implementing security measures”*
- *“Security has to be considered early on in the development process and it should be easy to use for everyone”*
- *“In my organisation the weight is in secure systems, usability comes a way after.”*
- *“What about Security by Design as part of this research and nudging?”*
- *“Using Wi-Fi in the workplace may cause breaches to our data, so it's not always secure. In addition, I find it easy to follow the cybersecurity requirements when I have a brief and easy language on my workplace's device “on the desktop screen”. ”*
- *“Stop password changing every 90 days.”*



- *“If you introduce very complex cybersecurity procedures, you need to provide support, knowledge, and training.”*
- *“No need to require complicated passwords or changing the password every couple of months. You may add a card swipe since every employee have one + keep the same pass unless there’s a reason to change.”*

**Subtheme 2.2: Feedback relevant to the relationship between usable security and security culture.** A number of participants provided feedback on the relationship between usable security and the security culture of the organization by emphasizing how user experience affects the organization's security practices. For example, they noted that employees are more likely to follow cybersecurity measures if these are made usable and seamlessly integrated into day-to-day workflows, meaning that more intuitive methods may encourage better security behavior. The following are some of the key comments from the survey:

- *“To have strong security culture, it’s important to consider usable security and make it clear and easy to understand”*
- *“Ensuring 'usable cybersecurity', and making controls and reporting processes as easy to use as possible, should encourage good cybersecurity habits and discourage workarounds - which could lead to a 'healthier' cybersecurity culture”*
- *“Culture is at the early stage, where policy is just on paper and awareness training is just about to get run for the first time”*

### **Theme 3: Recommendations for Improvement**

**Subtheme 3.1: Improving Reporting and Support.** Participants highlighted the importance of improving their organizations' reporting and support mechanisms. Their emphasis was on the importance of clear and efficient reporting processes for the purpose of addressing security issues as quickly and effectively as possible. There were also a number of suggestions for improving the usability of reporting tools and providing assistance with security concerns by the support staff. Some of the comments are as follows:

- *“There must be a dedicated system for reporting only IT security issues.”*
- *“Single sign on for various web services/pages. The services all have different logins and password requirements. For reporting, the IT department wants you to fill out a long form, which dissuades people from reporting. An easy way to report would help.”*
- *“Better way to report problems with more knowledgeable people to solve them”*
- *“I work in the cybersecurity department so I can’t really judge if we are providing the employees in my company with the required support, they need in terms of enabling them to report issues and addressing these issues although we are trying our best to meet their expectations while also complying with regulations”*

**Subtheme 3.2: Simplicity beats complexity.** There was a consensus among participants that cybersecurity measures must be simplified in order to improve the security culture of the organisation. This would involve creating a set of clear, easy-to-follow guidelines for employees to follow, besides finding ways to resolve current complex issues. Some of the key comments are as follows:

- *“I think it would be helpful if cybersecurity department can listen from employees about the security issues they face and try to resolve them or find alternatives that would allow employees complete their tasks without having issues that disrupt their work.”*
- *“Providing prompt support to ensure that employees have easy access to support personnel who can provide guidance/support. Also, it would be helpful to encourage employees to report security incidents and provide feedback on usability issues that they encounter.”*
- *“Use easy and accessible processing to contact the IT department or solve the issue immediately if we have online contact services.”*
- *“Being prepared is good, over-preparation is not necessarily good. Should give more permission to your employees. You hired them, you trust them!”*

- *“I suggest building a tech team consisting of senior expert in the it field (cybersecurity-server team-it support-network-system etc) to resolve complex issues together”*
- *“Make it simple, more will follow”*

**Subtheme 3.3: Consideration of the Human Aspect of the Stakeholders.** The comments below suggest that the study participants appreciate cybersecurity, but they need measures that consider them as humans in order to facilitate more adherence:

- *“While the move to the cloud is overall good, it needs more work. There needs to be a way to validate the identity of PERSON, note a person not a user or account, and grant that PERSON the rights and authorities they have. This should work across all cloud platforms.”*
- *“People often equate usability with user interfaces and user experiences. But the fundamental issue here is that security to date deals with accounts and user ids. Until we can make it work for a person, all the user interface and experience improvements will mean little.”*
- *“Often budgets are so tight that the cybersecurity methods adopted by an organisation are standalone systems and manual tasks rather than using an enterprise level comprehensive suite of tools that takes the work and responsibility off of the end user”*
- *“By collective understanding and agreement among all stakeholders”*
- *“Identifying me a person. All the items above are just covering up the underlying issue.”*

**Subtheme 3.4: Collaborative effort is needed.** The participants acknowledge the importance of collaborative efforts within the organization to enhance cybersecurity. In their view, addressing cybersecurity challenges cannot be the sole responsibility of IT; rather, it requires a collaborative effort from all levels of the organization. For instance, there seems to be a disconnect between the perceived usable security actions and end-user technical expertise, suggesting that fostering collaboration between technical and non-technical staff would help bridge this gap. Below are some key comments from the participants:

- *“Cybersecurity domain has been an important domain in my company in the last few years, at the beginning cybersecurity team was facing negative backlash from the IT team and the end users but after many workshops and advertisement about the importance of cybersecurity there has been some sort*

*of acceptance. I still think they need more collaboration with IT team to work as one force.”*

- *“Communicate to the worker any security decision made based on recent breach or threat. They always block things and never talked about it.”*
- *“Open channel with IT team. They update regularly but without informing the IT admins which causes some conflict and resistance”*
- *“There is often a disconnect between the perceived ease of usability of security actions and the technical know-how of the end user who is expected to actually use those actions.”*

**Subtheme 3.5: Continuous Education and Awareness.** This subtheme contains feedback from participants on their opinions of what the motivators other than those listed as part of the questionnaire (i.e., *finding cybersecurity actions easy to perform, management and leadership enforcement, complying with the national regulatory or corporate requirement, understanding the risks associated with not following the best practice, attending more cybersecurity training courses, attending more security awareness sessions*). As stated in the Quantitative Findings section, the most significant motivator for participants was *“finding cybersecurity actions easy to perform”* followed by *“management and leadership enforcement”*. However, other comments from participants include:

- *“The fear to be vulnerable or a victim to cyberattack”*
- *“In my first three months, there was a whole nine days of training, with three or four days dedicated to cybersecurity issues”*
- *“More focus on educating employees”*
- *“I’m a security awareness advocate and thought leader. It is my job to stay on top of recent developments and advocate for security culture”*
- *“Continuing cybersecurity training and raising awareness during the year and not only one time”*
- *“First of all, the cybersecurity best practices should exist, then we can talk about the drivers to follow them!”*

This subtheme captures the essence of the participants' comments, emphasizing the importance of ongoing training, awareness, and proactive measures to create a positive cybersecurity environment.

### 7.3 Findings from the Semi-structured Interviews

The semi-structured interviews performed as part of this research provide substantial insights into the impact of usability on cybersecurity measures across organizational contexts. The interviews were conducted with eight participants (four males and four females). Also, four of them are academics, three are industry professionals, and one is a PhD student with an industry background. Participants were based in South Africa, Saudi Arabia, Estonia, the United Kingdom, Armenia, Finland, Sweden, and the United States, offering a diverse perspective on cybersecurity across different cultures and regulatory contexts. Table 7.1 provides a summary of the interviews' participant demographics.

Participant ID	Gender	Age range	Highest Level of Education	Organization Size	Country
P1	Female	35-44	Doctoral	1000 or more	South Africa
P2	Female	35-44	Doctoral	1000 or more	Saudi Arabia
P3	Male	25-34	Master's	1000 or more	Estonia
P4	Male	25-34	Master's	1000 or more	United Kingdom
P5	Female	35-44	Master's	50-249	Armenia
P6	Male	25-34	Doctoral	1000 or more	Finland
P7	Female	35-44	Doctoral	1000 or more	Sweden
P8	Male	45-54	Bachelor's	1000 or more	United States

Table 7.1: Interviews Participant Demographics

A thematic analysis was conducted based on the interviews, which form part of the broader study to enable participants to express their thoughts more freely and help the effort to understand the interplay between usable security and organizational security culture. The following identified five themes highlight how each aspect contributes to the overall security culture.

#### Theme 1: Usability Impact on Security Behaviour

This theme revolves around users' behavior and their reactions to security measures. Often, usability issues determine whether security measures are effective (Fallatah, Furnell and He, 2023). Employees have different attitudes towards security measures in general depending on different factors, such as the urgency of completing the task

or the employee's background and level of security awareness. However, when these measures are not usable, even people with a high level of awareness will tend to do what is usable for them or bypass the measure altogether. When asked to elaborate on why P1 bypassed a complex authentication measure, she replied, "I'm fully aware that I shouldn't share my credentials and I shouldn't use anyone's credentials," but she has to get the job done. She reported, "It is a tricky one because I am fully aware. I teach these stuff and yet, in reality, I had to do it on occasion in order to get something working or something done." Many people understand and appreciate security, but complexity is "irritating", and it can be more frustrating for people who don't fully understand security and the reasoning behind its requirements. This can be applied to many situations, proving that some risky security habits are the result of unusable measures that users use to complete their tasks or avoid unnecessary frustrations.

Moreover, when asked about reporting incidents, most participants said that their organization's procedures are unclear on how users should report security incidents. P6 further said that if encountering a security incident or malicious activity, "I'll keep quiet because I am not willing to take the blame." On the contrary, participants acknowledged policies that positively changed employees' behaviors. For instance, when an email comes from outside the organization, external email warning banners are helpful for users to identify them. P1 asserted that "while this may not be considered highly usable security, it has had an impact because when they run phishing campaigns, and since including that, there has been a reduction in terms of people clicking on links and things like that. So, incorporating the banners when an email comes from outside the organization has changed people's behavior in terms of how many of them have actually clicked on links. They have just had that bit of an awareness, which has certainly been an improvement in terms of something basic that has just been included."

## **Theme 2: Usability Impact on Productivity**

This theme is concerned with the intersection of security practices and operational efficiency on a daily basis. Interviewing the study participants revealed key insights regarding usable security's impact on productivity. The implementation of security measures can often interfere with essential tasks, resulting in frustration among

employees and potential non-compliance with security. In order to increase workplace productivity, security must be designed in a way that supports rather than hinders it (Caputo et al., 2016; NCSC, 2018). P7 thinks that “the lack [of usability] can hinder employee's productivity” or, as stated by P8, unusable security is “a reduction in productivity”, and employees find it “time-consuming”. P6 provided an example: “On my organization's learning management system, I have to organize a quiz, and then I suddenly realized that I had changed my password. I have to enter the password again, which requires changing some of the security settings or approving some of the settings that have been done recently or enforced by the system...That is a clear deviation from the tasks that I intended to perform”. P1 complained that “systems are not supporting our jobs or what we should be doing.” Furthermore, P6 argues that “once we are scared [of security measures], there is a general common sense in the humans that if you have a feeling of scare or fear and you are not your 100%, you are not as productive as you should be because the feeling of fear has already overtaken some part of yourself.”

### **Theme 3: Training and Awareness**

An effective security culture is built on a foundation of aware users (Sherif, Furnell and Clarke, 2015). P5 described a real-life incident involving a hacked email account that repeatedly occurred in her workplace, and she felt that training and awareness, in addition to technology, could resolve this issue. Also, she stated, "It is likely that people from computer-related fields are more aware of the importance of security than people from other majors," indicating that users from departments other than information technology may require tailored training in order to ensure that all employees remain informed about the latest security threats regardless of their background. Additionally, she recommended that “a reward system be established for employees who take the initiative to protect their accounts.” P2 also has a similar experience in her organization, stating that “a colleague's hacked email led to inappropriate messages sent to the whole staff. Lack of awareness was evident.” She suggested that corporates should ensure all employees understand and can actively contribute to cybersecurity efforts, and it is necessary to provide comprehensive staff cybersecurity training that considers different educational backgrounds and cultural contexts. “As for the ease of performing cybersecurity actions, ideally, I'd like to see a



more friendly interface, easy processes, and training or support to make these even easier for everyone in the company to implement without any issues.”

#### **Theme 4: Regulations and Compliance**

Regulatory requirements play a significant role in driving security practices within organizations (Breaux and Antón, 2008). Many participants mentioned the specific regulations and their implementation within their working environments. Participants from Europe repeatedly referred to the GDPR, whereas P8, who is based in the United States, mentioned that “generally, North America has several regulatory requirements across different states, such as the California Consumer Privacy, HIPAA, and others. These can significantly influence security practices.” However, P8 highlighted that he is “not sure if they are considering usability but think that usability considerations should align with these regulations to make it easier for people and organization.” He added that “cybersecurity departments should also consider taking and gathering feedback from all users regarding their experiences and what they find hard to comply with.” Nonetheless, P7 asserted that sometimes organizations are “afraid to get fined”, and “when it comes to fines, they take everything seriously...Not because the user needs to be secure.” P6 believes that to comply with security, it has to be usable, but “usability things are not very well integrated because nobody bothers.”

#### **Theme 5: Geographical and Cultural Impact**

There is no doubt that culture has a profound influence on human beings as it shapes many of our perceptions and actions. In the study, participants provided insights into how their organizations' geographical location impacted how they perceive security and interact with it. P7 argued that people in Sweden and Scandinavian countries are naturally cautious and careful, which made it easier to instill security concepts, and P6 asserted that “in technologically advanced countries like Finland, people will be more concerned about their security”. Moreover, P3 stated, “I think here in Estonia, I am spoiled because they have to be able to collectively agree upon this, and it is a small population and all digital. They are able to agree upon common regulations to cater to all this stuff so that there is little discrepancy between different businesses. They have a communist, sort of, centralized strategy.” He also asserted that “They have three or four independent committees and probably more, where they actively go out to

organizations as part of the government duty and try to ensure two things: the regulations the companies have because our business here is online, and they try to get feedback and improve those things.” P3 elaborated, “The best-case study is the Estonian cybersecurity system because whatever aspect you want to do, or any kind of government or something like that, it's all hassle-free. Even the education system, if you want to log into the student system management, I basically go through the police portal, and it's like a heartbeat.” P3 thinks that the “motivation in Estonia might come from the proximity of Russia and Russian cyber threats,” and noted that “There's a lot of these hacker groups here. They [the government] make these relatively popular social events where people from all walks of life just show up, then they just do stuff together like that,” indicating social events related to cybersecurity in particular. P3 said the systems in Estonia make working simple. For example, “There is a system called smart ID. Whenever I have a work contract, employment contract, residence contract, or purchasing something online, I just need to know two PINs plus my social security number in order to access every service. I can basically sign a lease or rental agreement, open a company or have some business within 30 seconds.” In other geographical locations, P8 thinks that “there are many cultural norms, legal frameworks, etc that can influence the security in the US.” P2, who works in an organization in Saudi Arabia with employees from “India, Georgia, Jordan, the US and the UK,” believes that although the diversity of her organization’s work environment brings various perspectives which can enhance cybersecurity efforts, awareness is still needed as “some of them see security as very important, but some of them do not.” P5 thinks that in her country, “governmental levels manage cybersecurity well, but education institutions lack emphasis on cybersecurity.” P4, who worked in different geographical locations, including the Middle East and Europe, noted the difference in handling cybersecurity measures across the organizations he worked for and asserted that “cybersecurity procedures across organizations are different. Some of them are very clear, and they provide training. Some of them just say ‘be careful,’ but they don't take real practical measures to ensure that no cybersecurity issues will occur.”

Further, there are some challenges that might affect the usability of cybersecurity in certain places. For example, P1 stated, "There have been occasions where in South Africa, due to things like load shedding, we lose power for a bit. And when it comes

back, the system is not back completely, and then there are authentication issues." She added another challenge: "it is maybe not applicable to the entire South Africa or Africa, but certainly for our students coming into our institution, the majority of them come in without any kind of technology background." She explained that many students "may have used smartphones, but very few have been in any kind of formalized computing environment. Even in their schools, they would not have computer labs. So, we get a lot of first-year students coming in who first have to become digitally literate before you can even think about the security aspects. They are learning as they go." The different technological literacy backgrounds of the students present another layer of complexity. P1 described that they "have students who come in very comfortable with technology, and sometimes it is difficult to unlearn bad habits. Then, we have students who have had very little exposure to technology, and now everything they are doing is online. It is overwhelming for them when they first come to our university. They are just learning how to use PCs, keyboards, and mice." P1 concluded by highlighting the practical difficulties: "The usability factor to access what they need is challenging, and then there has got to be that security coming in as well, which I think is sometimes the hindrance."

### **General Recommendations:**

During the interviews, participants provided a number of recommendations that they think would enhance user experiences while interacting with cybersecurity in corporate settings. These recommendations include:

- *"There could be a really simple flowchart that people are made aware of"* (P1).
- *"To have a good security culture or strong security culture, they should consider how to make it [security] usable for the employee"* (P2).
- *"I think giving people an easy solution and a clear path to follow would go a long way, ultimately leading to culture or influencing culture"* (P1).
- *"So, trusting or engaging your users, knowing their needs, knowing their aptitudes, behaviors, education. Don't assume anything on behalf of the user that they will be able to implement the right thing or make the right decision"* (P3).

- *“If you can take away the burden as much as possible from the people, do what you can in the background, obviously filter what you can, protect what you can, raise some awareness where you can, try and make things more usable and make things more secure” (P1).*
- *“By establishing knowledge and resources for employees regarding security measures and by making the system easily accessible for employees to find information related to cybersecurity policies, they are more likely to comply and have a strong security culture” (P2).*
- *“Make that security seamless” (P1).*

Participants pointed out the importance of usability to establish a robust cybersecurity culture. They promoted the use of simple measures such as flowcharts, unambiguous instructions, and easily available materials to assist staff in accessing and adhering to security procedures. Several expressed that compliance and security culture may be greatly enhanced by engaging users, exploring their capabilities, and reducing the workload associated with security activities. The recommendations obtained from the interviews offer practical insight that, in the participants' opinion, will meet user expectations and make security usable, which will substantially enhance compliance and the overall security posture.

## **7.4 Chapter Summary**

The qualitative analysis indicates that study participants strongly believe that the usability of security measures influences their adherence to security practices. Additionally, participants' perceptions of the impact of cybersecurity measures on their productivity reflected instances in which the measures either facilitated or hindered their productivity. Also, the study participants highlighted issues related to management support, indicating the degree of support provided for cybersecurity initiatives and how that can facilitate compliance. Participants also discussed the effectiveness of existing training and awareness programs in promoting cybersecurity knowledge and behavior and identifying areas for improvement. It was also discussed how participants from different geographic locations or cultural backgrounds perceived cybersecurity practices within their organizations.

# **Chapter 8: Developing a Usability-focused Security Culture Framework**

## 8.1 Introduction

This chapter discusses how the quantitative results align with and complement the qualitative themes and identifies patterns and relationships to ultimately address the study objectives. It also discusses how the combined findings contribute to understanding the influence of usable security on security culture. Sections 8.2 and 8.3 provide insights of study's key findings before section 8.5 discusses the issues identified and their proposed solutions. This led to introducing a usability-focused security culture framework that aims to help organizations reduce usability barriers that may impede their efforts toward a strong security culture.

## 8.2 Insights from the Quantitative Findings

### 8.2.1 Survey Findings

- **Cybersecurity Competence Confidence:** While the study respondents report a high foundational knowledge and compliance confidence, there is a clear indication that additional focus is needed on identifying and reporting vulnerabilities.
- **Usability Challenges in Cybersecurity:** The majority of participants reported encountering usability issues.
- **Response of Unusable Cybersecurity Likelihood:** The majority of respondents indicated that they would seek assistance from their colleagues when faced with challenging cybersecurity tasks. Nonetheless, 57% of participants expressed a high probability of finding a way around the action, 23% indicated that they would ignore security measures in order to complete broader tasks, and 28% of respondents indicated they would likely or very likely stop the task.
- **Bypassing Cybersecurity Measures:** One-third of participants admitted bypassing cybersecurity measures because of usability issues.
- **Agreement on the Usability of Cybersecurity Measures:** A significant portion of participants feel that security actions are neither easy to understand nor easy to perform, and they feel that there is no balance between usability and security measures in their organizations. Also, the findings showed that

while mechanisms for reporting security incidents may already be in place, they could be improved in terms of accessibility or communication.

- **Reporting and Resolution of Cybersecurity Issues:** There is a significant gap between how issues are reported and how they are resolved. A quarter of participants have reported cybersecurity concerns. The large number of respondents who do not report issues is concerning as it may indicate issues that are not being reported, which could result in unresolved security vulnerabilities. Even when issues are reported, a tiny fraction of respondents feel that they have been resolved satisfactorily.
- **Impact of Usable Cybersecurity on Organisational Culture:** There is a strong consensus among participants that usable cybersecurity has a positive impact on organizational security culture. The vast majority of respondents (89% combined strongly agree and agree) believe that usable cybersecurity would encourage them to make sensible decisions while adhering to security protocols. Also, 83% of respondents reported that they are more likely to report security issues if cybersecurity is made easier to use.
- **Cybersecurity Best Practice Motivators:** Most participants indicated that finding cybersecurity actions that are easy to perform is their top motivator.
- **Cybersecurity Practice Adherence Barriers:** The majority of participants believe that the complexity of cybersecurity measures and their lack of convenience are the main barriers.

### 8.2.2 Hypotheses Testing

*H1A: There will be a positive correlation between users' perception of usable security measures and their behavior towards unusable security measures within the organization.*

The correlation test showed a positive correlation between users' perception of usable security measures and their behavior towards unusable security measures, meaning there is evidence that higher perceptions of usability are associated with more positive security behaviors, which is consistent with the previous research. Also, by delving further into the variable details, the correlations suggest that when employees perceive usable security measures, they tend to comply strictly with these measures. However,

no significant correlation was found between perceiving usable security measures and the tendency to seek help from colleagues when encountering security difficulties.

*H2A: A positive perception of usable security is negatively associated with the frequency of reported incidents of bypassing security measures.*

The correlation is not statistically significant. However, examining the individual items of the independent variable revealed two items with significant differences: "I feel that the security actions in my organization strike a good balance between security and usability" and "My organization provides adequate support for employees to understand and perform effective security actions". The findings suggest that participants who have bypassed cybersecurity protocols as a result of usability issues perceive a lesser balance between security and usability, as well as feeling less supported by their organizations.

*H3A: Ease of understanding and performing security actions predicts users' confidence in complying with security requirements within organizations.*

The "Ease of performing security actions" was the significant predictor, indicating that employees are more likely to follow cybersecurity requirements when they can execute security measures easily. This suggests that promoting usable security practices can cultivate a positive security culture by making compliance more accessible and intuitive.

*H4A: Ease of understanding and performing security actions is negatively associated with the frequency of reported security incidents.*

There is no strong evidence that ease of understanding security actions alone affects users' decisions to report unusable security measures, but the study confirms that making security measures easy to perform in organizations significantly reduces the likelihood of finding these measures complicated by users, suggesting that organizations should focus on enhancing the practical aspects of their security measures to reduce operational challenges.

*H5A: Organizational support and policies promoting the reporting of usable security issues positively influence employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches.*



The findings indicate that organizational support for staff feedback and rules to promote reporting usable security issues increase employee confidence in identifying and reporting cybersecurity vulnerabilities. It means that proactive organizational actions motivate and encourage workers to respond to cybersecurity threats. Organizations should promote policies that encourage communication about cybersecurity issues to increase employee's confidence and proactive behavior in managing cybersecurity risks.

## 8.3 Insights from Qualitative Findings

### 8.3.1 Open-ended Responses

Themes	Subthemes
<b>Theme 1</b> - Usability Challenges in Cybersecurity	<b>Subtheme 1.1</b> - Bypassing cybersecurity technology or procedures due to usability issues to complete tasks <b>Subtheme 1.2</b> - Difficulties encountered while using cybersecurity technologies or following cybersecurity procedures, including: <ul style="list-style-type: none"> <li>• <i>Authentication issues.</i></li> <li>• <i>No clear policies for reporting security issues</i></li> <li>• <i>External devices issues</i></li> <li>• <i>Cybersecurity policies issues</i></li> </ul>
<b>Theme 2</b> - Perceptions and Feedback on Usable Security and Security Culture	<b>Subtheme 2.1</b> - Views and Feedback on Usable Security <b>Subtheme 2.2</b> - Feedback relevant to the relationship between usable security and security culture
<b>Theme 3</b> - Recommendations for Improvement	<b>Subtheme 3.1</b> - Improving Reporting and Support <b>Subtheme 3.2</b> - Simplicity beats complexity <b>Subtheme 3.3</b> - Consideration of the Human Aspect of the Stakeholders <b>Subtheme 3.4</b> - Collaborative effort is needed <b>Subtheme 3.5</b> - Continuous Education and Awareness

Table 8.1: Identified Themes and Subthemes of the Open-Ended Responses

### **8.3.2 Semi-structure Interviews**

#### **Theme 1 - Usability Impact on Security Behavior**

The theme focuses on user behavior and security measures. A security measure's effectiveness depends on its usability. Employees perceive security measures differently depending on a number of factors, including urgency, background, and level of security awareness. Even people with a high level of awareness will disregard these measures if they are not usable. Users often use unusable measures to avoid frustration or complete their tasks. Most participants said their organization's procedures for reporting security incidents are unclear. However, they acknowledged that there are good policies that have positively changed employee behavior.

#### **Theme 2 - Usability Impact on Productivity**

This theme focuses on how security practices intersect with operational efficiency on a daily basis. Implementing security measures can often interfere with essential tasks, which can lead to employee frustration and non-compliance. Workplace security must be designed to support employee productivity rather than hinder it.

#### **Theme 3 - Training and Awareness**

Effective security cultures are built on the foundation of informed users. In order to ensure that all employees remain informed about the latest security threats and can prevent those, tailored training is required for employees considering different educational backgrounds and cultural contexts in order to ensure they understand and can contribute to cybersecurity efforts. Also, there should be a reward system for employees who take the initiative to protect their organization's information systems.

#### **Theme 4 - Regulations and Compliance**

Regulations play a significant role in driving security practices within organizations. The current regulations should, however, ensure that the usability aspect is taken into account to make it easier for individuals and organizations to comply. It is also imperative to include a method of collecting feedback from all stakeholders regarding their experiences and what they find difficult to adhere to.

### **Theme 5 - Geographical and Cultural Impact**

An organization's geographical location affects employee perceptions of security and how they interact with it. Many cultural norms, legal frameworks, and other factors can affect security and how people respond to it. In addition, specific challenges might affect cybersecurity's usability in certain areas but may not apply elsewhere.

## **8.4 Overview of Issues Identified in Study Findings and Recommended Solutions**

As evidenced by the key findings, security barriers continue to hinder employees' cybersecurity compliance. The majority of employees (79%) seek assistance from colleagues when faced with unusable cybersecurity tasks instead of directly contacting the organization or seeking help from the responsible department. Also, the study demonstrates that while most employees attempt to work around security requirements by consulting their peers, 23% admit they will ignore them in order to complete their tasks, and 28% are likely to abandon the task altogether if security measures become a barrier. Considering this, it is apparent that usability issues must be addressed. This section organizes the study's main findings into categories, identifying the types of usable security issues encountered. Each of the categories is followed by a solution that addresses usability barriers.

### **1. Communication:**

- While many organizations have incident reporting mechanisms, communication approaches require enhancement.
- Only a quarter of employees report security incidents, and those who do often find the resolution unsatisfactory.
- There is a lack of a clear strategy for reporting usability issues with cybersecurity policies and security issues related to external devices (e.g., printers, hard drives, and flash drives).
- There is a lack of confidence and proactive behavior in managing cybersecurity risks among employees.

### **Solution: Effective Communication**

Establishing clear channels for effective communication is essential to ensure that employees' concerns are addressed promptly and resolved satisfactorily. It is equally important to keep all employees well-informed about security policies and best practices, ensuring that every action by the employees is aligned with the organization's security goals. Effective communication fosters understanding, collaboration, and trust within an organization (Aksoy, 2024). An organization's management has a significant role to play in developing effective communication, which in turn results in improved productivity (Sadia *et al.*, 2016) and increases employee confidence and proactive behavior.

### **2. Support:**

- Employees who bypass cybersecurity measures as a result of usability issues perceive a lesser balance between security and usability in their organizations, and they feel less supported by their organizations.
- Negative security behaviors may result when employees perceive the security measures provided by the organization as ineffective, unusable, or poorly supported.

### **Solution: Management Support**

Top management must play a central role in shaping and reinforcing the cybersecurity culture within an organization (Hu *et al.*, 2012; Sherif, Furnell and Clarke, 2015; Da Veiga, 2018; Ioannou, Stavrou and Bada, 2019; Da Veiga *et al.*, 2020; Evripidou *et al.*, 2022). A strong leadership commitment to certain practices or policies may lead employees to recognize their significance (Krajcsák, 2019). Conversely, if employees perceive that top management is unconcerned about a particular issue, they may disregard or overlook it despite its importance. The leadership of an organization must actively enforce and promote security initiatives in order to develop a robust security culture. This will ensure that all factors contributing to a secure environment are given a high priority. Employees should feel supported and valued when they report concerns or incidents. Employees must be confident that their feedback will be addressed sufficiently without fear of reprisals or shame. For example, a company where management visibly supports cybersecurity programs and fosters open communication

about risks is likely to experience higher employee engagement. In contrast, organizations with leadership that downplay security concerns may experience greater neglect, such as employees who fail to report suspicious activity or ignore security incidents.

### **3. Training and education:**

- Employees need training that specifically addresses their challenges, which include authentication difficulties, unclear reporting policies, problems with external devices, and issues with other cybersecurity policies.
- Employees feel that continuous training and education are essential to address security challenges while doing their work.

#### **Solution: Tailored Training**

Everyone can realize the value of training, regardless of their role or position within the organization. However, if training programs do not address the employees' specific needs, they may be a waste of time and resources for both the employee and the company as a whole. This can also lead to a decrease in employees' acceptance of cybersecurity training (Kävrestad, Fallatah and Furnell, 2023). Also, according to research, factors such as trust, apathy, regulatory control, and worry affect users' behavioral intention to adopt cybersecurity training (Fallatah, Kävrestad and Furnell, 2024). It is important that organizations take into account such factors when developing cybersecurity training programs. In general, organizations should adhere to best practices, which include delivering training programs at the right time and in the proper scope to maximize the benefits of training.

### **4. Organizational and regional culture:**

- An organization's geographical location affects employee perceptions of security and their interactions with it.
- Usable security measures positively impact organizational culture, providing a more accessible and intuitive way for employees to adhere to security policies.
- Study participants indicated that regulations play a significant role in developing security practices within their organizations.

### Solution: Cultural Aligned Strategies

A company's regional and organizational cultures impact its employees' behavior in adhering to cybersecurity measures by influencing their perception of the importance of cybersecurity and how it is integrated into their daily routines. Research has shown that norms have a significant impact on how individuals behave within an organization (Posey and Folger, 2020; Ameen *et al.*, 2021; Hofstede *et al.*, 2010). As an example, in regions where collective responsibility and compliance are cultural norms, people may be more likely to see cybersecurity requirements as essential and be willing to comply with them. Alternatively, in cultures where individual autonomy is prioritized or security is not taken seriously, strict measures may be viewed as obstacles that reduce motivation to adhere to them. Furthermore, an organizational culture emphasizing cybersecurity awareness and aligning cybersecurity practices with employees' workflows encourages compliance. Integrating security protocols into existing workflows will ensure that security protocols do not hinder productivity. Thus, organizations should facilitate an engaging, culturally appropriate environment that emphasizes the benefits of cybersecurity for individuals and organizations. Specifically, organizations can motivate their employees to adopt necessary cybersecurity measures by focusing on usability and aligning security practices with their cultural context and day-to-day activities.

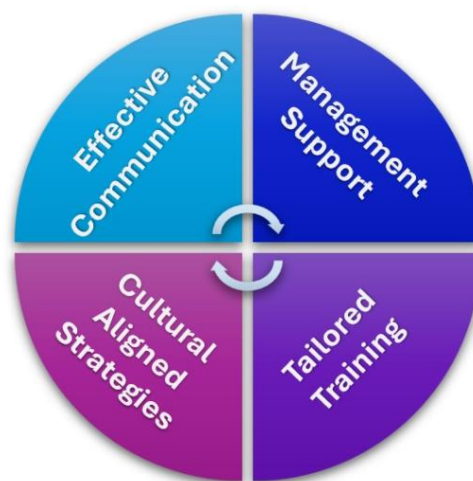


Figure 8.1: Mediating Strategies

There is a profound interconnectivity between these strategies when shaping an organization's cybersecurity posture. Effective communication helps to ensure that

security practices are clearly understood, while management support reinforces security's importance throughout the organization and facilitates factors that make security more usable. Providing employees with tailored training that meets their specific needs ensures that educational material is relevant, and integrating cultural factors into security strategies warrants that security strategies are applicable to the region and organization. As a result, the combination of these strategies creates an environment that fosters positive cybersecurity behaviors. A summary of the proposed solutions that will serve as mediating strategies is shown in Figure 8.1. Nonetheless, reinforcing these behaviors at the right time is still essential by implementing a real-time intervention method. One effective way to achieve that is through cybersecurity nudges. While the mediating strategies address the main issues identified in the study, cybersecurity nudges function as a supplementary method to provide users with a timely means to make the right security decisions, ultimately leading to a more robust security culture. Incorporating nudges into the study aligns with its focus on usability by addressing the human factor in cybersecurity.

### **Nudge as a Supporting Theory**

Nudge theory is derived from behavioral economics and is primarily applied to influence behavior. In general, a nudge (some studies refer to it as Choice Architecture) is a method that changes people's behavior without limiting their options or radically altering their incentives (Thaler and Sunstein, 2008). The nudge concept has been applied to many disciplines, including healthcare, education, business, and AI, to influence behavior (Ebert and Freibichler, 2017; Caris *et al.*, 2018; Möhlmann, 2021; Weijers, de Koning and Paas, 2021). In the context of the human aspect of cybersecurity, nudges can be used to guide people's choices and behaviors through positive reinforcement, ensuring that security measures are designed to steer employees toward secure behavior without restricting them. Cybersecurity nudges can significantly impact improving organizational security postures, and they are effective in various contexts, such as increasing security awareness, reducing operational risk, improving decision-making, and changing behavioral patterns (ISACA, 2021; Zimmermann and Renaud, 2021). For example, organizations can integrate password meters with hints (e.g., suggestions of using passphrases or password managers) to

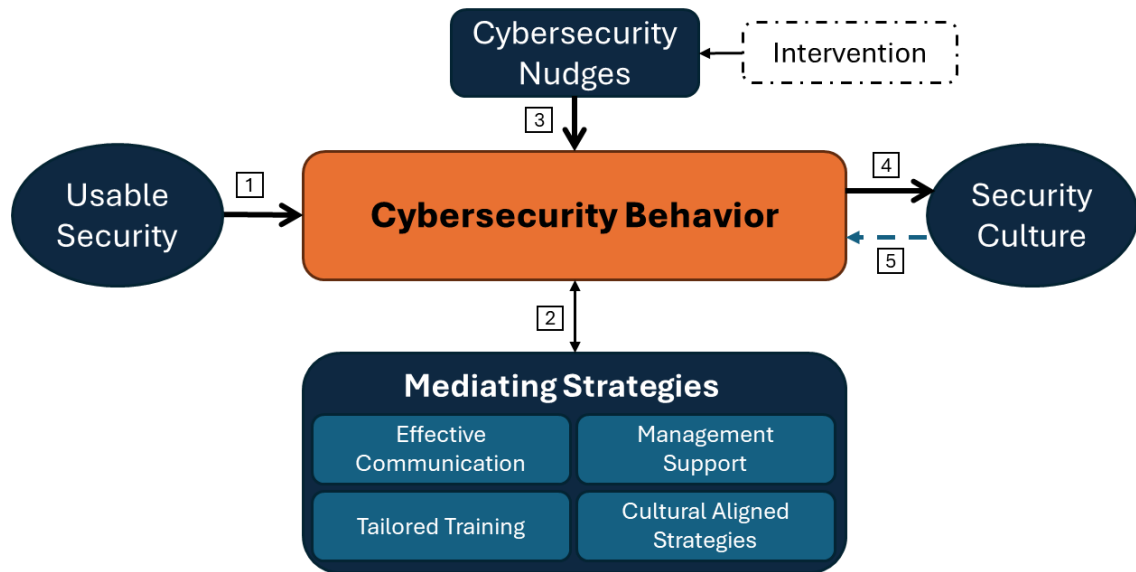
make passwords usable yet robust and provide immediate feedback that nudges employees toward selecting stronger passwords that are easy to remember.

## **8.5 Introducing a Usability-focused Security Culture Framework**

Security culture frameworks support in fostering a proactive cybersecurity mindset throughout organizations by focusing on employee awareness and shared responsibility. As mentioned in Chapter 2, core components of existing security culture studies often include factors such as policies, training activities, and communication and management support. Also, these frameworks aim to improve regulatory compliance, reduce human error, and integrate secure good behavior into regular routines. While the current approaches provide essential assistance for developing organizational security culture, there is a notable gap in their consideration of usable security, specifically, how usable security measures affect employee engagement and adherence to secure practices. This study proposes a framework that provides a structured method for organizations to strengthen their security culture through a human-centric lens. The framework presented in Figure 8.2 focuses on prioritizing usability and strategically integrating mediating strategies and security nudges introduced in the previous section (i.e., 8.4) to effectively influence employee behavior, leading to a strong security culture.

As established in Chapter 5, the study combines both quantitative and qualitative analysis to characterize this linkage between usable security and security culture. The quantitative analysis (e.g., statistical relationships between users' perceptions and security behaviors) was complemented by the qualitative analysis, which provided the study with contextual depth. The development of the proposed framework involved identifying the problem (i.e., the underrepresentation of usable security in existing security culture studies), synthesizing the components derived from the empirical study into a structured model, and further supporting it with cybersecurity nudges to encourage secure choices without being intrusive.



Figure 8.2: Usability-focused Security Culture Framework<sup>2</sup>

- Step 1** – The first step in operationalizing the framework focuses on usable security. The objective of this stage is to ensure usable security measures (i.e., usability concepts are utilized to enable cybersecurity concepts). In this step, usability must be prioritized to ensure that security mechanisms are intuitive for employees and easier to adopt in their day-to-day activities. Usable security has a direct and significant influence on cybersecurity behavior, meaning that regardless of their IT or security literacy, individuals in organizations are more likely to comply with security practices when they are easy to use and align with their regular workflows.
- Step 2** - Mediating strategies are an essential component of the framework. In this step, the strategies should not remain static; they should be continuously tailored and adapted to meet the organization's evolving needs and challenges. These strategies maintain a dynamic nature, ensuring employees are well-informed, supported, and trained to adhere to security best practices. There is a two-way relationship between mediating strategies and cybersecurity behavior; these strategies directly shape the actions of users, while feedback on employees' behavior can inform how these strategies are adjusted over time.

<sup>2</sup> Some aspects of the framework are refined following the evaluation stage and the final version of the diagram appears in Figure 9.1.

- **Step 3** - The introduction of security nudges is imperative to reinforcing secure behaviors. As the name implies, nudges are subtle prompts or reminders designed to assist in making secure decisions at critical moments without the feel of being intrusive. This step serves as a practical, real-time reinforcement that aligns employee behavior with cybersecurity requirements.
- **Step 4** - Upon implementing these steps successfully, employees are able to improve their cybersecurity behaviors and comply with security practices. Over time, these behaviors contribute to the development of an organizational security culture. In this context, cybersecurity should not be viewed as a set of isolated activities but rather as an integral part of daily operations.
- **Step 5** - Ultimately, security culture has a feedback effect on employees' cybersecurity behavior. When employees observe secure behavior embedded within the organizational culture, this collective adherence to security practices can reinforce their own cybersecurity actions and decisions.

To understand the flow of the framework, let us assume an optimal scenario with usable security. When security measures are effectively implemented as input, there is a smooth flow through the framework. The need for additional interventions or strategies diminishes as employees naturally exhibit secure behaviors. Still, the framework elements will be utilized to foster the process of developing a secure culture (e.g., sending reward nudges for compliance and gathering employees' feedback). On the other hand, if the initial input lacks usability, the components of the framework become actively engaged in enhancing user behavior, leading to reduced risks and an improved security culture. This process ultimately feeds back into the Usable Security element, alerting the organization to adjust the usability factor.

## 8.6 Framework Implementation Guidelines

To implement the framework, there should be an initial assessment in order to understand how people within the organization behave around security practices. This concept is also supported by research (ICAO, 2021; Pfadenhauer *et al.*, 2017; Nilsen and Bernhardsson, 2019) and also by some of the participants in the interview part of this study. For instance, P3, who has extensive experience in the cybersecurity industry, asserts that “the best course of action is to start with what people already

know and are familiar with.” That would also help determine the pain points and what kind of issues related to usability employees encounter. It is imperative to involve stakeholders early in the process to ensure alignment (Voinov and Bousquet, 2010; Silva *et al.*, 2019), and they acknowledge milestones to reinforce positive behavior among employees. A number of tools are available to evaluate the usability of organizational systems, including the System Usability Scale (SUS) (Brooke, 1996), which is the most widely used measure of users' perception of usability and is likely to continue to be so for some time to come (Lewis, 2018) and Google's HEART Framework (Rodden, Hutchinson and Fu, 2010), which measures user satisfaction, task success rates, and overall system efficiency. The HCI community has widely adopted such tools to identify usability issues and provide recommendations for improving users' experience. Next, it is recommended to refer to steps 1-4 to define clear objectives and develop a targeted action plan considering the assessment results in the initial phase. The final step is to implement the plan, and this is where the framework elements begin to engage actively.

After executing the plan, any wins, whether big or small, should be acknowledged to reinforce positive actions and sustain compliance. Various studies assert this value of acknowledging wins within organizations (Stajkovic and Luthans, 2003; Pinder, 2014; Kotter, Akhtar and Gupta, 2021). Moreover, the implementation plan involves ongoing feedback and reviews to maintain progress and identify any areas that require improvement. This study recommends the following approach for feedback and improvement process:

1. Obtain employee feedback through appropriate channels (e.g., surveys, feedback forms, anonymous suggestion boxes) in order to gain insight into the usability of security measures.
2. Adjust and review measures as necessary:
  - Review security measures periodically based on feedback or changing emerging cybersecurity threats.
  - Maintain the usability of security tools and make iterative improvements as necessary.
3. Security Culture Review:

- Conduct an annual security culture assessment to evaluate the progress against the initial objectives. This can be achieved by employing relevant existing tools and platforms, which (at the time of writing) would include but not be limited to those offered by providers such as KnowBe4, CybSafe, and the International Civil Aviation Organization.
- Adjust objectives and the action plan based on the results of the review.

Figure 3 summarizes the framework implementation process.

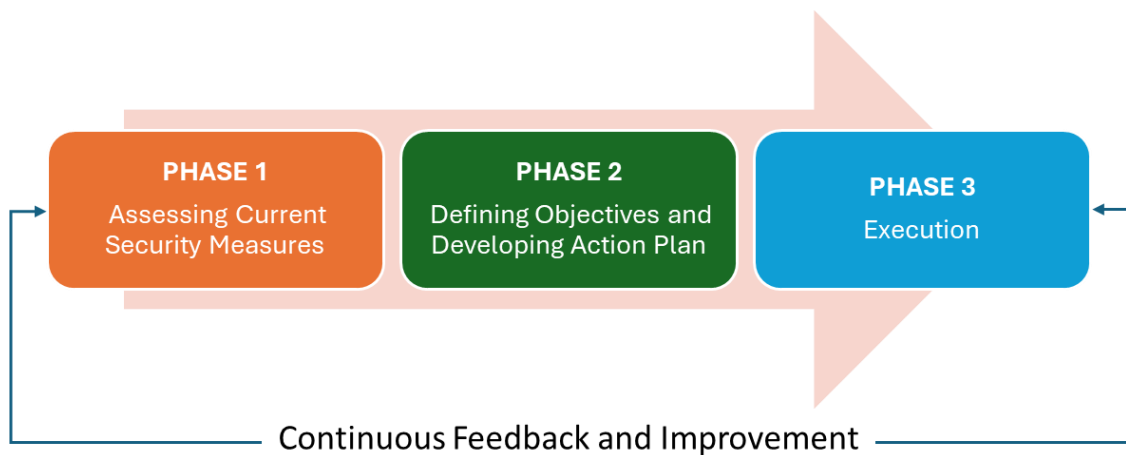


Figure 8.3: Framework implementation Phases

## 8.7 Case Study Application

ABC, a company with 500 employees across North America, Europe, and the Middle East, deals with sensitive client data, which makes robust cybersecurity essential. While ABC has implemented standard security policies, it has experienced various security incidents due to human errors. The company aimed to develop a strong security culture and decided to employ the framework to enhance cybersecurity behavior and embed security awareness into its organizational culture. ABC specifically targeted challenges related to complex password policies and cumbersome authentication processes that were identified as critical barriers to employee compliance. This case study describes the process ABC followed, the actions taken, and the results achieved, illustrating how the framework results in usable security measures, leading to better cybersecurity behaviors and a more resilient security culture.

### **Phase 1 - Assessing current security measures**

ABC identified key stakeholders from the IT, HR, security, and department heads before starting the assessment process. All parties were brought together to discuss the importance of fostering a security culture and to gain their agreement. Consequently, a steering committee was formed within the organization to oversee implementation. Next, the Cybersecurity Department at ABC conducted an extensive assessment of the existing security measures with the aim of finding where usability is embedding employees' compliance with cybersecurity. The assessment identified two significant challenges faced by employees:

- Employees experienced problems with frequent password changes and complex passwords. This resulted in many people writing down their passwords or using one easily guessable password to access all their accounts, which increased security risks.
- Employees appreciate that MFA increased security but perceived it as time-consuming and frustrating, particularly as they had to manually enter authentication codes during busy workdays.

### **Phase 2 - Defining Objectives and Developing Action Plan**

The results of the assessment led the company to define objectives that guide implementing targeted changes to improve the usability of security measures while maintaining security. Examples include improving adherence to password policies, increasing MFA adaption, and reducing workarounds instances.

### **Phase 3 - Execution**

The execution of the plan marks the start of implementing the framework. The following steps were taken:

#### **Step 1:**

ABC decided to change the password policy and simplify MFA by introducing the following:

- Passphrases
- Extended expiration periods of passwords

- Biometric-based authentication

The plan was presented to the steering committee for approval and to ensure alignment with organizational needs. Employees were instructed to create memorable yet strong passphrases (e.g., “*PalmTreesOnTheBeachH2025*”), and the company extended its 90-day password policy to 365 days. Also, instead of typing a six-digit code, employees use a fingerprint scan to authenticate.

### **Step 2:**

ABC shared tips about passphrase creation and secure behavior via email and digital signage in a company-wide campaign. In addition, the company sought feedback and suggestions regarding addressing peers’ risky behaviors during any authentication process. ABC’s top management participated in security awareness events, sending a clear message about the crucial role of authentication management. For instance, the CEO and senior executives attended workshops and led discussions on the necessity of personal responsibility in maintaining security policies. Members of top management shared their stories about usability issues that led to human errors and how they reported them. It conveyed the idea that security measures can pose hurdles to everyone in the organization, and everyone should be aware of how to deal with them. Furthermore, the Finance and Human Resources departments were identified as high-risk, as most authentication issues and complaints come from these two departments. Therefore, they received specialized, hands-on training tailored to their specific requirements. ABC’s global workforce also had access to a variety of multilingual resources. The company used culturally appropriate graphics and storytelling methods during training sessions in regions where verbal communication is more prevalent than written communication.

### **Step 3:**

ABC has developed a number of security nudges to alert employees only at critical moments, ensuring that key actions are taken without creating alert fatigue. In particular, suggestions appeared when employees were required to create or update passwords, advising them to select strong passphrases. In order to ensure that the nudges were practical and respectful, they were customized in accordance with

regional communication styles. In some regions, nudges are provided more informally and conversationally, while in others, the tone is more formal. Below is an example of how employees were nudged:



Hey Mike,  
Did you know your fingerprint is more secure than your pet's birthday?!  
Your account is ultra-safe when you use biometrics (like your fingerprints or face scan). No guessing required!  
It's also faster than typing in a code, so you get to what matter most - your work!  
Give your fingerprint a high-five next time you log in and experience top-notch security!

### **Step 4:**

Since ABC invested in developing more usable authentication methods, employees could interact with security protocols more comfortably and consistently. The new measures were easily adopted by employees, which resulted in a change in their behavior (for example, no sticky notes with passwords written down). As a result of this shift in behavior, security practices became seamless across the organization. This has been a key factor in developing the organization's security culture.

### **Step 5:**

The efforts of ABC to embed usable authentication methods and promote secure behavior eventually generated a feedback effect, strengthening the security culture of the organization. As employees observed their colleagues consistently following security practices, a shared norm developed over time. Individuals who deviated from these practices were viewed as outliers, making non-compliance socially undesirable. Besides formal policies, behavioral expectations of peers strengthened employees' commitment to cybersecurity. Over time, compliance became second nature, and deviations were rare, thus sustaining the organization's overall security culture.

### **Acknowledging Wins and Reinforcement:**

As a result of implementing usable security, employees' cybersecurity behaviors were significantly improved within the organization. The observed outcomes include:

- An increase in compliance:  
Passphrases and simplified MFA led to a 30% reduction in password reset requests, indicating greater compliance with password management policies. Also, there was a reduction in time spent on authentication by over 50%.
- Reduction of workarounds:  
By improving usability, Employees were less likely to bypass security protocols, such as writing down passwords. Consequently, employees were able to follow security procedures without feeling overwhelmed.

Individuals or teams demonstrating proactive security behavior were recognized with “Cyber Star” recognition or other rewards.



## **8.8 Chapter Summary**

This chapter provided insights from the quantitative and qualitative findings leading to the introduction of the USCF. The chapter detailed the framework development process and the practical approach to implement it within organizational settings. The framework incorporates essential elements that work together to impact user behavior and, consequently, the organization's overall security culture. These elements focus on employing mediating strategies, which prioritize effective communication, managerial assistance, tailored training initiatives, and cultural considerations. Equally important, the framework recommends incorporating security nudges to help employees make secure decisions at key moments. These insights offer a foundation for understanding how the USCF can be leveraged for strategic benefit. The framework evaluation is discussed in the following chapter.

# **Chapter 9: Framework Evaluation**

## 9.1 Introduction

Validating the framework introduced in Chapter 8 is crucial to ensure its practical utility and relevance. There are various potential approaches for validation in this context. Common examples include empirical tests, expert reviews, pilot testing, and participant feedback. Many studies recommend combining different approaches to enhance the quality and reliability of the study findings (Davis, 1992; Stevens *et al.*, 2018; Cho and MacArthur, 2010). This study combined participant feedback with expert review in order to offer a holistic view and robust evaluation process. While participants' feedback ensures the framework is relevant to end-users, expert reviews provide insights into real-world practice, ensuring that the framework aligns with the broader practices in cybersecurity and the impact of its usability. In addition, usable security and security culture intersect many aspects, including behavioral and organizational dimensions; therefore, combining feedback from experts and the study participants captures this diversity. The participants' educational background and experts' expertise add strength and enhance the credibility of the study output. With this in mind, the following sections illustrate the USCF evaluation process.

## 9.2 Evaluators Recruitment

The participants from the original study who completed both the survey and the interview ( $n = 8$ ) and who serve as end-users of the framework were contacted to determine their willingness to take part in the evaluation process. This was ten to twelve months after their involvement, depending on when their original interviews occurred, though all were approached simultaneously for the evaluation stage. An email was sent, and six participants expressed interest in reviewing the framework and examining its relevance to their organizations' contexts. Additionally, a human-centered cybersecurity group, maintained by the NIST Human-Centered Technologies Group with expert members in the field, was invited to participate in the evaluation process. The purpose of inviting the experts was to obtain additional feedback from a second independent group that had not previously been exposed to the project but was considered collectively to have strong backgrounds in cybersecurity usability and culture. Ten experts responded, expressing their interest in reviewing the framework. The experts were informed that, in the earlier phases of the study, surveys and

interviews had been conducted to inform the framework's design and that this final evaluation process would ensure the framework's relevance and effectiveness. Additionally, since the experts were not part of the study from the outset, basic demographic information was collected to better understand their backgrounds and perspectives. This included gender, age range, highest level of education, organization size, and country. However, only three experts submitted complete feedback, bringing the total number of evaluators to nine: six from the earlier stages and three experts who joined at this final stage. Table 9.1 below illustrates the demographics of the original contributors and additional experts.

Unique ID	Original Identifier	Gender	Age Range	Highest Level of Education	Organization Size	Country
E1	P2	Female	35-44	Doctoral	1000 or more	Saudi Arabia
E2	P3	Male	25-34	Master's	1000 or more	Estonia
E3	P4	Male	25-34	Master's	1000 or more	United Kingdom
E4	P5	Female	35-44	Master's	50-249	Armenia
E5	P6	Male	25-34	Doctoral	1000 or more	Finland
E6	P7	Female	35-44	Doctoral	1000 or more	Sweden
E7	N/A	Female	35-44	Master's	1000 or more	United States
E8	N/A	Male	35-44	Master's	Less than 50	United Kingdom
E9	N/A	Male	52	Bachelor's	50-249	United States

Table 9.1: Participant Demographics for the Validation Process

Evaluators from the early stages of the study who completed the survey and interview were initially identified as P2, P3, P4, P5, P6, and P7. For clarity and consistency during the evaluation phase, these evaluators were assigned a new unique identifier (E1–E6) while their original identifiers (P2–P7) were noted for reference. The three experts who participated solely in the validation process later were assigned unique identifiers E7, E8, and E9.

## 9.3 The Evaluation Process

A folder was shared with both groups of participants to facilitate the evaluation process. The folder contained two resources:

- **Framework Documentation:** This document introduced the framework, included a diagram of the framework and its components, and outlined its steps and phases. Each step was accompanied by a brief explanation of its purpose and activities. Also, a visual representation of the implementation phases was included to aid comprehension.
- **Explanatory Video:** A 10:32-minute narrated slideshow with subtitles to explain the framework concept. The video covers the following topics:
  - Introduction (00:35 min): outlining the purpose of the video and the framework briefly.
  - Framework Concept (3:15 min): explaining the core concept of the framework and its principles.
  - Implementation Phases (1:55 min): providing an overview of the phases involved in implementing the framework.
  - Case Study (4:26 min): illustrating the practical application of the framework by providing a real-world example.
  - Conclusion (1:01 min): providing a summary of the key points and highlighting the framework's value.

The evaluators accessed the shared materials using a University of Nottingham OneDrive link. The evaluators were asked to provide general feedback, specifically regarding the practical value of the framework for organizations and any areas they believed required clarification or improvement.

## 9.4 Analysis and Reflection on the Evaluators' Feedback

The feedback received from the evaluators provides perspectives on the strengths and areas for improvement of the framework. Please refer to the full version of the evaluators' feedback in Appendix IV. In their remarks, evaluators highlighted the framework's potential to fill critical gaps in cybersecurity practices by adopting a human-centered approach. A particular emphasis on usability and behavior-driven strategies was noted, as reflected in comments such as "The framework ensures that cybersecurity measures are both effective and user-friendly, addressing concerns raised during interviews about usability challenges" (E1). However, evaluators also pointed out areas of development. The following themes categorize evaluators' input into key concepts that guide further development and validations. The themes were identified through thematic analysis. The following subsections outline the themes and the responses.

### 9.4.1 Theme 1: Alignment with Key Issues and Practical Value

Evaluators recognized that the framework focuses on usability, mediating strategies, and behavior-driven interventions that align well with human-centered concepts, and this approach is essential for fostering a strong security culture. A practical benefit of the framework is its ability to bridge the gap between technical measures and employee engagement by simplifying security measures and tailoring them to users' and organizations' needs. However, there was some feedback that questioned whether some of the concepts in the framework, such as usability and simplicity leading to compliance, were adequately supported by evidence. Evaluators believe that this needs to incorporate supporting data from studies to prove the framework's impact. Other comments recommend highlighting the practical value of the framework. Examples of evaluators comments include:

- *"The framework emphasizes user-centric design, highlighting the importance of tailoring security applications to user preferences and behaviors."* (E1)
- *"Its actionable approach to fostering a strong security culture could bridge the gap between technical measures and employee adoption."* (E4)
- *"What measurable benefits, such as reduced incidents or cost savings, can organizations expect?"* (E9)

**Response:** The importance of usability in driving user engagement is supported by several HCI studies, as discussed in Chapter 4. However, there is a notable gap in research directly linking the usability of cybersecurity applications to user compliance and its broader impact on security culture, which is a gap this study aims to address. Also, while the primary measurable benefit of the framework is strengthening security culture, this improvement is expected to influence aspects such as reducing training time and costs, minimizing damage from security incidents, and fostering more effective adoption of security practices. Further quantifiable metrics, such as incident reduction rates or cost savings, might be explored to prove its practical value when the framework is applied in practice, which was not possible given the timeframe of the research.

### 9.4.2 Theme 2: Clarity and Presentation

Some evaluators emphasized the need for more specific examples and case studies to make the framework more applicable and actionable. Also, the need for detailed guidance on conducting initial assessments, implementing mediating strategies, and measuring progress was highlighted. Additionally, two evaluators noted that the framework's visual presentation needs clear explanations for the design elements. The comments on this theme include:

- *“It is hard to guess what happens and how from the diagrams.” (E6)*
- *“I’m unclear about the main difference between effective communication and tailored training.” (E4)*
- *“I was expecting a bit more detail in the framework” (E3)*

**Response:** Since some evaluators commented on the overall visualization of the framework (e.g., questions regarding shapes and confusion surrounding the dotted box labeled "interventions"), the visual design of the framework has consequently been enhanced to ensure that the shapes, boxes, and colors convey specific meanings. Further, the box labeled "interventions" has been removed to avoid any further confusion. Figure 9.1 presents the resulting refined version of the framework. Also, the case studies in the following subsections can add more clarity.

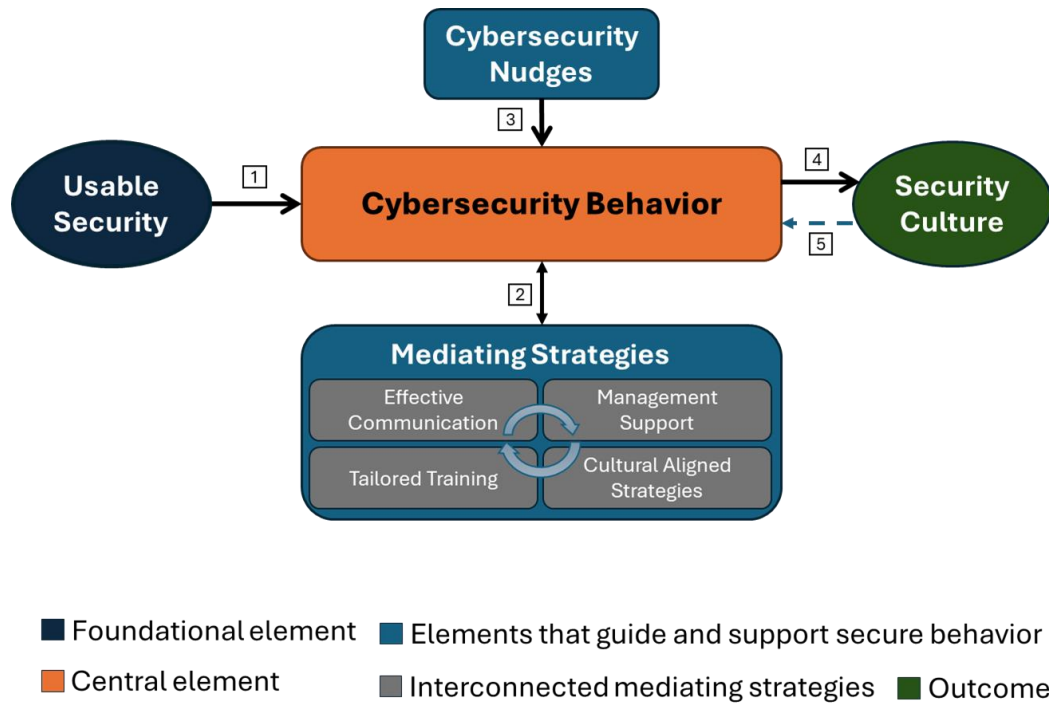


Figure 9.1: Usability-focused Security Culture Framework

### 9.4.3 Theme 3: Scalability and Integration

The importance of scalability and adaptability was highlighted in the evaluators' feedback as being critical to the framework's relevance across different organization sizes and sectors. For example, one expert noted the significance of tailoring the framework for small and medium-sized enterprises (SMEs) due to the unique challenges they may face when applying the framework. Moreover, the adaptability of the framework to different organizational cultures and evolving cybersecurity threats was acknowledged, but additional guidance is needed. In addition, another comment recommends the integration with existing frameworks, such as NIST CSF or CIS Controls, to enhance adoption. Evaluators believe that positioning the framework as complementary to the established standards could encourage its implementation by organizations already committed to other approaches rather than replacing existing ones. Below are examples of the evaluators' input to this theme:

- “How well does it work in different-sized enterprises? SMEs might need extra help scaling the phases.” (E2)
- “How will new hires pick up the security practices compared to senior staff?” (E2)



- *“Positioning this framework as complementary to existing standards could ease adoption.” (E9)*
- *“The framework’s commitment to ongoing feedback and adaptability ensures it can remain relevant and effective.” (E9)*

**Response:** The adaptability of the framework ensures that it can be applied in various organizational contexts. SMEs can utilize the framework by focusing on cost-effective tools and strategies, such as open-source security platforms and streamlined assessments. On the other hand, larger organizations can leverage advanced analytics or automation to tailor interventions to specific users or departments. As an example, multinational corporations may utilize behavioral analytics to detect anomalies in employees behavior and implement targeted training sessions or nudges to enhance the situation. In addition, evaluators pointed out that the framework should align with the existing cybersecurity framework. The following three case studies help understand the framework's scalability and alignment with the existing frameworks.

### **Case Studies**

As a method of addressing some of the points raised by evaluators, this section presents three case studies. The case studies outline the mechanism for applying the framework from multiple perspectives, including the security controls that employees are expected to utilize, the threats that they are intended to prevent, and the assets they are responsible for protecting. The resulting organizational culture that emerges as a result of applying the framework will also be explained.

**WID Organization****Industry:** Finance**Employ count:** 50K**Case Study 1****Description/Challenge:**

The organization operates across Europe, North America, and the Middle East and adheres to NIST CSF, ISO, and CIS controls. The organization has a remote working policy and allows Bring Your Own Device (BYOD) practice, which adds to the challenges of ensuring compliance with security measures. Employees had difficulty adhering to password management policies despite following robust frameworks due to their complexity, which resulted in repeated credential-related breaches. As a result, the organization had to balance compliance with these controls with addressing usability issues that discouraged adoption.

**Objectives:**

The primary objective was to align the USCF with existing controls (NIST CSF, ISO, and CIS) in an effort to increase employee compliance with security measures and simplify security procedures without compromising compliance, especially in remote working and BYOD environments.

**Method(s) to Achieve the Objectives:**

Based on an initial assessment using the SUS and surveys, the organization discovered that employees reuse passwords due to complex policies, struggled with confusing BYOD guidelines, and encountered problems with remote access. As part of Step 1 of the framework, the company introduced an integrated password manager with single sign-on (SSO) to address usability issues and simplified guidelines for BYOD. As part of Step 2, the organization utilized mediating strategies, such as clear communication and tailored training for remote working policies targeting employees who work remotely. In step 3, security nudges were deployed to offer employees timely guidance without overwhelming them, such as automatic password reminders and alerts when suspicious links are posted. By implementing these measures, cybersecurity behaviors were improved, password reuse was reduced, and secure procedures were adhered to more consistently. Employees were recognized for small achievements to reinforce positive engagement. In Step 5, an embedded security culture is developed that is supported by regular reviews and feedback loops that facilitate the maintenance of momentum and relevance.

**Results:**

The implementation of the USCF improved alignment with existing controls (e.g., complementing the existing NIST Protect and Identify functions) while also addressing the human aspect of security processes. Credential-related breaches decreased by 35%, and employee satisfaction with security tools improved by 40%. BYOD compliance increased by 45%, ensuring consistent standards across personal and corporate devices. Employees become active participants in maintaining compliance, even in remote and flexible work environments, given that the security processes are intuitive and manageable. In turn, this created a more human-centric, robust security culture that balanced usability and security needs. After six months, integrating usability-focused

strategies improved user engagement and compliance rates, especially concerning pain points in remote/BYOD environments.

**NottsTele**

**Industry:** ICT

**Employ count:** 150

## Case Study 2

### Description/Challenge:

An Information & Communication SME based in Nottingham was frequently targeted by ransomware and phishing attacks. There was confusion around software patching responsibilities and adoption of multi-factor authentication (MFA) among employees. The limited resources of the small organization made handling these threats more difficult.

### Objectives:

A key objective was to simplify the implementation of the Essential Eight strategies and to ensure that employees understood their role in mitigating security threats, in particular phishing attacks and ransomware attacks.

### Method(s) to Achieve the Objectives:

Based on employee interviews and observations, a preliminary assessment revealed that employees felt MFA was overly complicated, resulting in long login delays and frustration. In addition, many users failed to update critical software patches due to unclear instructions on when and how to do so. The organization redesigned its MFA process by implementing a one-click tool that significantly reduced the time spent on authentication. The training sessions addressed common misconceptions about updates and provided concise guidelines regarding patching schedules and procedures. During team meetings, management and leadership stressed the importance of timely patching and helped desk support to address any onboarding hurdles. In order to further boost compliance, Security Nudge introduced creative and humorous interventions. For instance, employees were reminded of upcoming patch deadlines with playful graphics and humorous one-liners. The nudges reinforced the usability-centered measures and cultivated security habits by making critical security tasks more engaging. The employees' collective behavior shaped the company's culture, and every individual felt the responsibility of protecting the company.

### Results:

Employee behavior has been positively influenced by usability improvements and engaging nudges. The adoption rate of MFA increased by 60%, while the patching completion rate improved by 50%. In response to security threats, employees reported feeling more confident and proactive. As a result of this behavioral shift, the company was able to cultivate a proactive security culture, facilitating consistency and responsible behavior throughout the organization by making controls easier to use.

despite limited resources. Efforts centered on user understanding showed early improvements in awareness and reporting behaviors within a few months. Behavior change was observed in nine months.

**University X**
**Industry:** Education

**Employ count:** 20K

**Case Study 3**
**Description/Challenge:**

A large university with international students, faculty, and staff required a robust security strategy to protect sensitive research data, personal information, and IT infrastructure. The university faced challenges resulting from the users' diverse cultural and professional backgrounds.

**Objectives:**

The main objective was to secure critical assets by improving secure access controls, which ensure encryption of sensitive data and foster a positive security culture across the university environment.

**Method(s) to Achieve the Objectives:**

The initial assessment revealed inconsistent use of encryption for research files and student records, besides challenges in communicating security policies across the diverse university community. Guided by the Mediating Strategies, the university began by crafting clear security policies and updates to ensure that faculty, staff, and students received information in a format they could easily understand. The university offered role-specific training sessions to address the varying needs and pressures. In parallel, security nudges help users adopt secure behaviors without overwhelming them. For example, lighthearted emails were sent out with campus mascots and links to quick videos labeled "Encryption Week."

**Results:**

As a result of improved communication and tailored interventions, encryption compliance rates increased by 50%. Also, management created a sense of accountability, reinforcing the importance of secure behavior. Consequently, faculty, staff, and students adhered to security practices consistently, which led to a positive security culture. This enabled individuals to protect critical assets proactively while maintaining academic and operational efficiency. Shifting toward a robust security culture across the organization required sustained efforts. The improvements in the university security culture became apparent within the third quarter after applying the USCF.

#### **9.4.4 General Reflection**

The feedback indicates that the framework is recognized for its ability to address usability challenges in cybersecurity and emphasize user-centric practices to positively influence security culture. However, the feedback emphasizes the importance of explicitly communicating the framework components and processes and aligning them with existing cybersecurity frameworks or controls. It is important to note that evaluators were intentionally provided with a simplified version of the details that explains the framework, along with an accompanying video, to ensure accessibility and encourage engagement. A highly detailed version might overwhelm evaluators and discourage participation. Many of the issues raised in the feedback have already been addressed in the full version, which provides detailed explanations of the framework and its implementation phases.

### **9.5 Chapter Summary**

This chapter outlined the validation process of the framework. It began with a description of the evaluator recruitment process, followed by an analysis of their feedback along with the responses. These were categorized into three key themes: the practical value of the framework, the clarity of its presentation, and the framework's scalability and integration. Additionally, three case studies were included, each focusing on a specific aspect: how the framework assists users in managing security processes, helps them address threats, and supports asset protection.

The validation of the framework was achieved through feedback from two groups of evaluators: the original study participants, who provided insights via surveys and interviews, and a group of experts in the fields of usable security and security culture.

# **Chapter 10:**

# **Conclusions**

## 10.1 Summary of Research Achievements and Contributions

This study focused upon usable cybersecurity as an enabler for fostering a robust security culture. The influence of usable security on security culture has remained largely unexplored. Therefore, the primary aim of this project was to examine how cybersecurity usability influences security culture in organizations. The main contribution was achieved through addressing the objectives originally identified in Chapter 1. The achievements in relation to each of these are listed below:

- **To examine prior studies and authoritative sources on usability, usable security, and security culture to define usable security and identify the key influencing factors of security culture.**

A comprehensive review was conducted to identify the factors influencing usability and security culture. Although several factors have been discussed in the literature, the direct influence of usable security on security culture has not been explicitly investigated in prior work. Users' awareness and the training programs provided by organizations to enhance this awareness and knowledge are frequently discussed as key factors in shaping organizational security culture. The study highlights the importance of these elements and further explores cybersecurity training and user acceptance as critical aspects of fostering a robust security culture. However, a gap in the literature regarding comprehensive analysis of user acceptance of cybersecurity training was identified. To address this gap, a review of existing research on user acceptance of cybersecurity training from a socio-technical perspective was conducted. The review revealed that most existing research focuses primarily on the nature of training interventions themselves, with limited attention to user acceptance. User perception of cybersecurity training is critical for its adoption, emphasizing the importance of integrating usable materials into daily routines to foster positive user perception. Design practices, such as user-centric design, can enhance the effectiveness of training programs.

Moreover, the study highlights the importance of tailoring training programs to specific user groups to maximize their impact. To address the lack of comprehensive literature on user acceptance of cybersecurity training, the

study explored the application of factors from the TAM in this context. This exploration led to the introduction of the CTAM. The CTAM offers a framework for understanding and enhancing user acceptance of cybersecurity training, which contributes to the broader objective of fostering a robust security culture within organizations.

Additionally, a review of usability definitions from both IT/HCI and cybersecurity perspectives was carried out. It was concluded that the representation of usability in the literature is more consistent than that of usable security. The cybersecurity community is gradually adopting concepts that the HCI field has long understood. Due to the lack of consistency in the definition and representation of usable security, this study established a working definition aimed at supporting the cybersecurity community's efforts to capture the practical meaning of usable security. Also, through examining the different aspects identified in the literature, a framework of usable security is established as one key result of assessing usability and usable security studies.

- **To characterize the relationship between usable security and security culture by framing relevant study variables and assessing whether usable security positively influence security culture. This will be achieved through quantitative and qualitative means to produce validated findings that demonstrate the nature of this relationship.**

An empirical study using a mixed-methods approach was conducted, involving a review of previous work and data collection through surveys and interviews. Hypotheses were developed to provide clear direction, expectations, and predictions about the relationships between the variables under investigation. The quantitative and qualitative findings analysis revealed a significant influence of usable security on organizational security culture. Organizations can strengthen their security posture by addressing the gaps between employees' perceptions and actual security practices while fostering a culture that values and supports secure behavior.

The study integrated quantitative and qualitative data to understand how usable security measures influence security culture. Statistical analysis and hypothesis



testing offer a basis for understanding trends and general attitudes, while a qualitative perspective offers valuable context into perceptions and experiences, facilitating a deeper understanding of concepts that cannot be expressed through numbers. The results of quantitative studies indicate that the usability of security measures is strongly associated with compliance behaviors. Employees adhere to security measures more often when they find them easy to understand and perform. These findings are further supported by qualitative insights that reveal specific cases of employees adhering to usable security measures or bypassing security measures due to usability issues, including complex authentication methods, difficulties using external devices, and unclear policies. Also, qualitative data revealed instances in which security protocols impeded the completion of tasks, leading to alternatives such as using a colleague's account or disregarding them altogether. A third of participants admitted to bypassing security measures as a result of these challenges. This indicates that the balance between security and usability in current security practices is not yet optimal, resulting in potential vulnerabilities.

Moreover, an analysis of the quantitative data reveals that there is a significant gap in the reporting and resolution of security incidents, with many incidents either going unreported or unresolved. This observation was reflected in the qualitative responses in which participants expressed frustration over unclear reporting processes and inadequate resolution outcomes. The qualitative data clarifies this perspective, as it provides specific examples of these challenges and suggests that a more accessible and understandable reporting mechanism is needed. Employees' feedback highlights the need for improved organizational support and communication from all levels, including higher management, which would encourage a more proactive and consistent security culture. The findings also support many studies' observations of the importance of management support and policy enforcement, pointing out that leadership has a critical role to play in cultivating a robust security culture (Sherif and Furnell, 2015; Tolah, Furnell and Papadaki, 2021; Harun et al., 2021). For example, top management and leadership in organizations must enforce usable security policies that promote good behaviors. They must also encourage

offering targeted training and resources and applying mechanisms that help simplify and streamline their organizations' communication processes. Furthermore, a large majority of survey respondents believed that simplifying cybersecurity would facilitate sensible security decisions and ensure adherence to protocols. Qualitatively, respondents discussed the need to integrate security measures seamlessly into daily workflows, which will have a positive impact on increasing work productivity.

In addition, integrating quantitative and qualitative findings reveals evidence that regulatory frameworks, such as GDPR in Europe and some specific privacy laws in the U.S., including HIPAA and the California Consumer Privacy Act, drive security practices primarily through compliance rather than a user-centric approach. Participants highlighted that although these regulations mandate strict adherence, integrating usability could further enhance compliance, reflecting the need to align security measures more closely with user needs. It is also imperative to note that geographical and cultural contexts significantly influence security perceptions and practices. According to the study findings, the inherent caution in Scandinavian cultures and the strong governmental support for usable security in Estonia demonstrate how local cultures and policies can foster a positive security culture. Nevertheless, challenges arise in regions with diverse cultural backgrounds or where the population does not possess a high degree of technological literacy, making it difficult to apply security practices. Most importantly, the findings highlight organizations' need for clear, accessible cybersecurity guidelines. Cybersecurity processes must be simplified using appropriate tools and resources that make security practices meet the needs and capabilities of actual users. With the aid of these tools, organizations will be able to develop a security culture that values both compliance and user experience.

The interpretation of the findings contributed to the development of a framework that promotes a positive security culture by integrating usable security principles with essential practices.

- **To design and evaluate a framework that leverages usable security and related factors to identify usability improvements that enhance security behaviors and promote a positive security culture. The framework's effectiveness and relevance will be measured through stakeholder engagement to ensure its practicality and alignment with organizational needs and security practices.**

A significant outcome of this research is a framework designed to promote a positive security culture through the integration of usable security and other essential elements. This framework enables organizations to overcome usability barriers that could otherwise impede the development of a robust security culture. The framework ensures more user-friendly and effective cybersecurity systems by designing cybersecurity measures with human factors in mind and aligning security goals with usability objectives. The first step in operationalizing this framework involves assessing the usability of existing security measures. Simultaneously, mediating strategies should be developed, including incorporating security nudges. Incorporating nudges into the framework extends its scope to offer practical interventions that support and amplify the mediating strategies. With this holistic approach, individuals improve cybersecurity behavior, embedding security awareness into organizational culture. In turn, a strong security culture can influence individual behavior, creating a feedback loop where group behavior positively reinforces individual actions. Ultimately, the interplay between the framework's elements is critical to shaping effective security practices within organizations.

After achieving these objectives, the framework was evaluated by participants who contributed during the early stages of the study and experts in the fields of cybersecurity usability and security culture. It is important to reemphasize that the USCF is designed to improve organizational security cultures through a human-centric approach that focuses on influencing cybersecurity behavior as a fundamental pillar to then influence security culture. The usability

principles are at the core of the framework, ensuring that security measures and tools are intuitive. The concept of usable security is operationalized by principles explained in Chapter 4. Putting an emphasis on usability ensures that security measures are aligned with employee workflows rather than hindering them.

The mediating strategies, which are an integral part of the framework, are intended to be dynamic and adaptable in order to address the specific usability challenges. For instance, communication strategies should prioritize clarity and simplicity, presenting security policies and procedures in accessible language and supplemented by visual aids such as infographics. Similarly, it is necessary to use tailored approaches; for example, the IT department may benefit from advanced security simulations, while the customer-facing teams may require practical training on how to secure client data. To ensure that these strategies remain relevant and effective over time, organizations must incorporate regular feedback from employees. For example, an employee or a department may suggest that quarterly feedback sessions are more convenient than annual reviews since they allow for quicker adjustments to security measures.

In terms of using security nudges, organizations are able to reinforce secure behaviors in real-time without being intrusive. A nudge may be a reminder to update passwords, a dashboard alert that tracks individual compliance scores, or a reminder to double-check email addresses before sending sensitive information. It is specifically practical when employees are guided toward secure decisions during critical moments, such as when they are approving financial transactions or accessing sensitive information.

As for the implementation phases, it is crucial to conduct an initial assessment of the security tools in order to understand how employees interact with them and identify usability issues. Usability testing can be used to validate the effectiveness of new tools before they are fully implemented or existing ones to identify usability issues. Also, during this phase, various methods are utilized to gather information about employee behaviors, pain points, and experiences. A number of tools can be used to conduct this assessment,

including the SUS or the HEART Framework. In addition to usability testing sessions, observation methods can also be used to observe employees as they carry out security-related tasks, including logging into systems, for example, or identifying phishing emails. It is also possible to identify recurring challenges by reviewing security incident logs and employee feedback from prior training programs. For example, an employee who has difficulty remembering complex passwords may require solutions such as password managers or simple passphrase policies. Utilizing these tools and methods, one can generate actionable insights regarding usability barriers during the assessment phase.

## **10.2 Limitations of the research**

This study included an examination of the research landscape through a review of prior research. While the research has focused on identifying the most relevant studies, future research could further enhance these findings by undertaking a more extensive exploration of related literature to broaden the scope of understanding in this area.

Additionally, the number of participants (203 for the survey and 8 for the interview) represents a small sample size, especially for the interview aspect. Obtaining a larger and more diverse sample would have been ideal; however, the research was constrained by needing to select interviewees from within the original survey sample group. This approach ensured continuity and the inclusion of participants already familiar with the nature of the research. Also, some valuable information might have been missed from the open-ended responses and interview data, although efforts were made to carefully analyze the data, including involving a second rater to enhance the credibility of the analysis.

The respondent group also skewed towards the younger and more educated individuals, which limits representativeness. This demographic likely reflects a "best-case" sample, as these individuals regularly use technology. If this group encountered challenges, it suggests potential difficulties for others, who are less familiar with technology. Moreover, most participants were from large organizations in Europe and the Middle East. A more varied dataset from different organizational sizes and diverse geographical locations would enhance the representation of participants.

Finally, when validating the framework, evaluators were intentionally provided with a simplified version of the framework details, accompanied by an explanatory video. This approach aimed to ensure accessibility and encourage participation. However, while this was meant to facilitate engagement, it may have omitted some concepts. Many issues raised during the feedback process had already been addressed in the full, detailed version of the framework, which includes explanations of the framework and implementation phases. Also, the framework's development and theoretical foundation have been examined, but its practical application in real-world settings was not feasible due to the short timeframe of the study, and it remains to be explored.

### **10.3 Directions for Future Work**

Future research should continue to identify emerging factors influencing user engagement. This would facilitate designing and implementing more effective cybersecurity measures, ultimately enhancing compliance and contributing to a more robust organizational security culture. Similarly, further exploration is needed into organizations' challenges in embedding security into daily behaviors, particularly in addressing usability to achieve a sustainable security culture. This is increasingly important given the growing importance of human-centered approaches in cybersecurity and the potential impact of this study's findings.

Notably, understanding these behavioral patterns would enable the development of targeted approaches or solutions to address most of the bad security behaviors. Additionally, the effects of mediating strategies and cybersecurity nudge interventions, as discussed in this study, warrant further investigation to determine what works best in corporate environments. A practical application of the framework would also be helpful for future work in order to enable the framework to be further refined and its impact to be measured in an organizational setting.

Moreover, the increasing interest in human-AI interaction for enhanced security presents an opportunity for future research. AI could be a valuable addition by automating key elements of functionality based on a prior understanding of user preferences and behaviors and augmenting the existing cybersecurity efforts. By integrating AI, organizations could further enhance their ability to create usable cybersecurity solutions that align with human workflows and promote a strong security

culture. This could simplify the user experience by reducing the need for explicit security-related interactions and decisions, therefore minimizing user fatigue and errors.

## **10.4 The Importance of Security Culture and Usable Security**

Security culture is an essential concept for enhancing organizational resilience to cybersecurity risks. Security culture extends beyond relying solely on technological solutions; it fosters an environment where cybersecurity is a shared responsibility. This study focused on usable security as a key enabler for developing a strong security culture. The research explored the representation of usability, usable security, and security culture in studies, which helped in refining the understanding of usable security and characterizing its relationship with security culture. This resulted in the design of a framework that leverages the influence of usability to foster a positive security culture.

Usable security needs to be embedded from the outset. Systems designed with usability in mind, considering human abilities such as memory capacity, attention span, and cognitive limitations, are more effective at encouraging secure behaviors. Many security issues are not merely due to a lack of awareness but rather to the failure to design systems that accommodate human factors. Usability empowers security by reducing complexity and enabling users to engage seamlessly with secure systems.

Ultimately, organizations need to shift away from viewing humans as the "weakest link" in cybersecurity. Instead, the focus should be on empowering users to practice positive security behaviors through systems and strategies that support, rather than hinder, their efforts. Usable security fosters a supportive security culture and helps organizations achieve more resilient cybersecurity.

# References

- Abawajy, J. (2014) 'User preference of cyber security awareness delivery methods', *Behaviour & information technology*, 33(3), pp. 237-248.
- Abran, A., Khelifi, A., Suryn, W. and Seffah, A. (2003) 'Usability meanings and interpretations in ISO standards', *Software quality journal*, 11(4), pp. 325-338.
- Acharya, A. S., Prakash, A., Saxena, P. and Nigam, A. (2013) 'Sampling: Why and how of it', *Indian journal of medical specialties*, 4(2), pp. 330-333.
- Aksoy, C. (2024) 'BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS', *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), pp. 96-110.
- Al Natheer, M., Chan, T. and Nelson, K. 'Understanding and measuring information security culture'. *Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS)*: University of Science (Vietnam)/AIS Electronic Library (AISeL), 1-15.
- Al Sabbagh, B. and Kowalski, S. 'Developing social metrics for security modeling the security culture of it workers individuals (case study)'. *The 5th International Conference on Communications, Computers and Applications (MIC-CCA2012)*: IEEE, 112-118.
- Aladawy, D., Beckers, K. and Pape, S. 'PERSUADED: fighting social engineering attacks with a serious game'. *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15*: Springer, 103-118.
- Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues', *Future internet*, 11(3), pp. 73.
- Alfawaz, S., Nelson, K. and Mohannak, K. 'Information security culture: a behaviour compliance conceptual framework'. *Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security [Conferences in Research and Practice in Information Technology, Volume 105]*: Australian Computer Society, 51-60.
- Alhalafi, N. and Veeraraghavan, P. (2023) 'Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model', *Smart Cities*, 6(3), pp. 1523-1544.
- AlHogail, A. (2015) 'Design and validation of information security culture framework', *Computers in human behavior*, 49, pp. 567-575.
- AlHogail, A. and Mirza, A. 'Information security culture: a definition and a literature review'. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*: IEEE, 1-7.
- AlHogail, A. and Mirza, A. 'A proposal of an organizational information security culture framework'. *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014*: IEEE, 243-250.
- AlHogail, A. and Mirza, A. 'Organizational information security culture assessment'. *Proceedings of the International Conference on Security and Management (SAM)*: The Steering Committee of The World Congress in Computer Science, Computer ..., 286.
- AlKalbani, A., Deng, H. and Kam, B. (2015) 'Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure'.



- Alnatheer, M. and Nelson, K. (2009) 'Proposed framework for understanding information security culture and practices in the Saudi context'.
- Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J. and Choudrie, J. (2021) 'Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce', *Computers in Human Behavior*, 114, pp. 106531.
- ANSI (2022) *Ergonomics Of Human-System Interaction - Part 11: Usability: Definitions And Concepts*. Available at: [https://webstore.ansi.org/standards/iso/iso9241112018?\\_ga=2.3299568.111955288.1644355252-1926938011.1644355252](https://webstore.ansi.org/standards/iso/iso9241112018?_ga=2.3299568.111955288.1644355252-1926938011.1644355252).
- Bada, M. (2022) 'Stakeholder Analysis: Motives, Needs, and Drivers for Cybersecurity Awareness Training in Modern Work Environments', *AwareGO*.
- Bada, M., Sasse, A. M. and Nurse, J. R. (2019) 'Cyber security awareness campaigns: Why do they fail to change behaviour?', *arXiv preprint arXiv:1901.02672*.
- Baxter, G. and Sommerville, I. (2011) 'Socio-technical systems: From design methods to systems engineering', *Interacting with computers*, 23(1), pp. 4-17.
- BDA (2010) *What is dyslexia?:* British Dyslexia Association (BDA). Available at: <https://www.bdadyslexia.org.uk/dyslexia/about-dyslexia/what-is-dyslexia#:~:text=Dyslexia%20is%20a%20learning%20difficulty,memory%20and%20verbal%20processing%20speed>. (Accessed: 13/5/2024).
- Bélanger, F., Maier, J. and Maier, M. (2022) 'A longitudinal study on improving employee information protective knowledge and behaviors', *Computers & Security*, 116, pp. 102641.
- Bello, A. and Maurushat, A. 'Technical and behavioural training and awareness solutions for mitigating ransomware attacks'. *Applied Informatics and Cybernetics in Intelligent Systems: Proceedings of the 9th Computer Science On-line Conference 2020, Volume 3 9*: Springer, 164-176.
- Bevan, N., Kirakowskib, J. and Maissela, J. 'What is usability'. *Proceedings of the 4th International Conference on HCI*: Citeseer.
- Bevan, N. and Macleod, M. (1994) 'Usability measurement in context', *Behaviour & information technology*, 13(1-2), pp. 132-145.
- Bonett, D. G. and Wright, T. A. (2015) 'Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning', *Journal of organizational behavior*, 36(1), pp. 3-15.
- Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative research in psychology*, 3(2), pp. 77-101.
- Braun, V. and Clarke, V. (2021) 'Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches', *Counselling and psychotherapy research*, 21(1), pp. 37-47.
- Braun, V. and Clarke, V. (2022) 'Conceptual and design thinking for thematic analysis', *Qualitative psychology*, 9(1), pp. 3.
- Breaux, T. and Antón, A. (2008) 'Analyzing regulatory rules for privacy and security requirements', *IEEE transactions on software engineering*, 34(1), pp. 5-20.
- Brewerton, P. M. and Millward, L. J. (2001) *Organizational research methods: A guide for students and researchers*. Sage.

Brooke, J. (1996) 'SUS-A quick and dirty usability scale', *Usability evaluation in industry*, 189(194), pp. 4-7.

Bryan Foltz, C., Schwager, P. H. and Anderson, J. E. (2008) 'Why users (fail to) read computer usage policies', *Industrial Management & Data Systems*, 108(6), pp. 701-712.

BSI (2022) *Ergonomics of human-system interaction - Usability: Definitions and concepts*. Available at: <https://shop.bsigroup.com/products/ergonomics-of-human-system-interaction-usability-definitions-and-concepts/tracked-changes>.

Caputo, D. D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J. and Deng, L. (2016) 'Barriers to usable security? Three organizational case studies', *IEEE Security & Privacy*, 14(5), pp. 22-32.

Caris, M. G., Labuschagne, H. A., Dekker, M., Kramer, M. H., van Agtmael, M. A. and Vandenbroucke-Grauls, C. M. (2018) 'Nudging to improve hand hygiene', *Journal of Hospital Infection*, 98(4), pp. 352-358.

Carpenter, P. and Roer, K. (2022) *The Security Culture Playbook. An executive guide to reducing risk and developing your human defense layer*: Wiley.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2015) 'Impacts of comprehensive information security programs on information security culture', *Journal of Computer Information Systems*, 55(3), pp. 11-19.

Cho, K. and MacArthur, C. (2010) 'Student revision with peer and expert reviewing', *Learning and instruction*, 20(4), pp. 328-338.

Chowdhury, N. H., Adam, M. T. and Teubner, T. (2023) 'Rushed to crack—On the perceived effectiveness of cybersecurity measures for secure behaviour under time pressure', *Behaviour & Information Technology*, 42(10), pp. 1568-1589.

Constantine, L. L. and Lockwood, L. A. (1999) *Software for use: a practical guide to the models and methods of usage-centered design*. Pearson Education.

CPNI (2021) *Security Culture*: Centre for the Protection of National Infrastructure. Available at: <https://www.cpni.gov.uk/security-culture> (Accessed: 1/09 2022).

Cruz, R. M. (2022) 'Teleworking and Cyber security in the Higher Education Institutions, Dominican Republic Case'.

Cullinane, I., Huang, C., Sharkey, T. and Moussavi, S. (2015) 'Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging', *Journal of Computing Sciences in Colleges*, 30(6), pp. 75-81.

CybeSafe (2024) *Human risk management is...official!* Available at: <https://www.cybsafe.com/value/forresters-pronounces-security-awareness-official-now-what/#:~:text=At%20CybSafe%2C%20we%20define%20HRM,the%20realization%20of%20digital%20opportunities.%E2%80%9D> (Accessed: 13/11 2024).

D'Arcy, J. and Greene, G. (2014) 'Security culture and the employment relationship as drivers of employees' security compliance', *Information Management & Computer Security*.

Da Veiga, A. (2016a) 'Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study', *Information & Computer Security*.

Da Veiga, A. 'A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument'. *2016 SAI computing conference (SAI)*: IEEE, 1006-1015.

- Da Veiga, A. (2018) 'An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture', *Information & Computer Security*.
- Da Veiga, A., Astakhova, L. V., Botha, A. and Herselman, M. (2020) 'Defining organisational information security culture—Perspectives from academia and industry', *Computers & Security*, 92, pp. 101713.
- Da Veiga, A. and Eloff, J. H. (2010) 'A framework and assessment instrument for information security culture', *Computers & security*, 29(2), pp. 196-207.
- Da Veiga, A. and Martins, N. (2017) 'Defining and identifying dominant information security cultures and subcultures', *Computers & Security*, 70, pp. 72-94.
- Dahabiyeh, L. (2021) 'Factors affecting organizational adoption and acceptance of computer-based security awareness training tools', *Information & Computer Security*, 29(5), pp. 836-849.
- Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017) 'Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace', *Computers in Human Behavior*, 67, pp. 196-206.
- Davies, J. *Word Cloud Generator*. Available at: <https://www.jasondavies.com/wordcloud/> (Accessed: 25/05 2022).
- Davis, F. D. (1985) *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Massachusetts Institute of Technology.
- Davis, L. L. (1992) 'Instrument review: Getting the most from a panel of experts', *Applied nursing research*, 5(4), pp. 194-197.
- DeCoster, J. and Claypool, H. (2004) 'Data analysis in SPSS'.
- Dhillon, G. (2007) *Principles of information systems security: Texts and cases*. John Wiley & Sons Incorporated.
- Dillman, D. A. (2011) *Mail and Internet surveys: The tailored design method--2007 Update with new Internet, visual, and mixed-mode guide*. John Wiley & Sons.
- Eason, K. D. (1989) *Information technology and organisational change*. CRC Press.
- Ebert, P. and Freibichler, W. (2017) 'Nudge management: applying behavioural science to increase knowledge worker productivity', *Journal of organization Design*, 6(1), pp. 1-6.
- EC, E. C. (2022) *Usability*. Internal Market, Industry, Entrepreneurship and SMEs: European Commission. Available at: [https://ec.europa.eu/growth/sectors/tourism/business-portal/usability\\_en](https://ec.europa.eu/growth/sectors/tourism/business-portal/usability_en) (Accessed: 17/02 2022).
- Edwards, M. (2018) *Exploring Human-Computer Interaction*. hp.com: HP TECH TAKES. Available at: <https://www.hp.com/us-en/shop/tech-takes/exploring-human-computer-interaction> (Accessed: 15/02 2022).
- Emerson, R. W. (2021) 'Convenience sampling revisited: Embracing its limitations through thoughtful study design', *Journal of Visual Impairment & Blindness*, 115(1), pp. 76-77.
- ENISA (2017) 'Cyber Security Culture in Organisations', *European Union Agency For Network and Information Security*.

- Evripidou, S., Ani, U., Watson, J. D. M. and Hailes, S. (2022) 'Security Culture in Industrial Control Systems Organisations: A literature review', *HAISA*.
- Fallatah, W., Furnell, S. and He, Y. 'Refining the Understanding of Usable Security'. *International Conference on Human-Computer Interaction*: Springer, 49-67.
- Fallatah, W., Kävrestad, J. and Furnell, S. (2024) 'Establishing a Model for the User Acceptance of Cybersecurity Training', *Future Internet*, 16(8), pp. 294.
- Field, A. 2013. *Discovering statistics using IBM SPSS statistics*. sage.
- Forbes (2020) *The Human Element Of Cybersecurity*. Available at: <https://www.forbes.com/councils/forbestechcouncil/2020/01/24/the-human-element-of-cybersecurity/>.
- Forrester (2024) *The Future Is Now: Introducing Human Risk Management*. Available at: <https://www.forrester.com/blogs/the-future-is-now-introducing-human-risk-management/> (Accessed: 13/11 2024).
- Furnell, S., Esmael, R., Yang, W. and Li, N. (2018) 'Enhancing security behaviour by supporting the user', *Computers & Security*, 75, pp. 1-9.
- Furnell, S. and Rajendran, A. (2012) 'Understanding the influences on information security behaviour', *Computer Fraud & Security*, 2012(3), pp. 12-15.
- Gadzma, W. A., Jatau Isaac Katuka, Yusuf Gambo, Aliyu M Abali, and Muhammed Joda Usman (2014) 'Evaluation of Employees Awareness and Usage of Information Security Policy in Organizations of Developing Countries: A Study of Federal Inland Revenue Service, Nigeria', *Journal of Theoretical & Applied Information Technology*, 67(2).
- Garfinkel, S. and Spafford, G. (1991) *Web security, privacy & commerce*. " O'Reilly Media, Inc."
- Gartner (2024) *CISO Foundations: Build a Culture of Security Consciousness — Introducing the Gartner PIPE Framework*. Available at: [https://www.gartner.com/en/doc/773138-ciso-foundations-build-a-culture-of-security-consciousness-introducing-the-gartner-pipe-framework?utm\\_content=315302548&utm\\_medium=social&utm\\_source=linkedin&hss\\_channel=lcp-10551016](https://www.gartner.com/en/doc/773138-ciso-foundations-build-a-culture-of-security-consciousness-introducing-the-gartner-pipe-framework?utm_content=315302548&utm_medium=social&utm_source=linkedin&hss_channel=lcp-10551016) (Accessed: 13/11 2024).
- Georgiadou, A., Mouzakitis, S. and Askounis, D. (2021) 'Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis', *arXiv preprint arXiv:2102.03000*.
- Georgiadou, A., Mouzakitis, S. and Askounis, D. (2022) 'Working from home during COVID-19 crisis: a cyber security culture assessment survey', *Security Journal*, 35(2), pp. 486-505.
- Ghasemi, A. and Zahediasl, S. (2012) 'Normality tests for statistical analysis: a guide for non-statisticians', *International journal of endocrinology and metabolism*, 10(2), pp. 486.
- Gibbons, J. D. (1993) *Nonparametric statistics: An introduction*. Sage.
- Gokul, C., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V. and Lodha, S. 'Phishy-a serious game to train enterprise users on phishing awareness'. *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts*, 169-181.
- Gould, J. D. and Lewis, C. (1985) 'Designing for usability: key principles and what designers think', *Communications of the ACM*, 28(3), pp. 300-311.
- Guest, G., MacQueen, K. M. and Namey, E. E. (2012) 'Introduction to applied thematic analysis', *Applied thematic analysis*, 3(20), pp. 1-21.

Guo, K. H., Yuan, Y., Archer, N. P. and Connelly, C. E. (2011) 'Understanding nonmalicious security violations in the workplace: A composite behavior model', *Journal of management information systems*, 28(2), pp. 203-236.

Haney, J. M. and Lutters, W. G. " ' It's {Scary... It's} {Confusing... It's} Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security'. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 411-425.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020) 'Riskio: A serious game for cyber security awareness and education', *Computers & Security*, 95, pp. 101827.

Hassan, N. H. and Ismail, Z. (2012) 'A conceptual model for investigating factors influencing information security culture in healthcare environment', *Procedia-Social and Behavioral Sciences*, 65, pp. 1007-1012.

Hassan, N. H., Maarop, N., Ismail, Z. and Abidin, W. Z. 'Information security culture in health informatics environment: A qualitative approach'.

HFES, H. F. a. E. S. (2021) *Human Readiness Level Scale in the System*

Development Process. Available at: [https://www.hfes.org/Portals/0/Documents/DRAFT%20HFES%20ANSI%20HRL%20Standard%2012\\_2021.pdf?ver=2021-01-06-142004-860&timestamp=1609964482681](https://www.hfes.org/Portals/0/Documents/DRAFT%20HFES%20ANSI%20HRL%20Standard%2012_2021.pdf?ver=2021-01-06-142004-860&timestamp=1609964482681).

HHS and GSA (2004) *U.S. Dept. of Health and Human Services. The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. Washington: U.S. Government Printing Office, 2006.* Usability.gov. Available at: <https://www.usability.gov/what-and-why/usability-evaluation.html> (Accessed: 31/01 2022).

Hof, H.-J. (2015) 'User-centric IT security-how to design usable security mechanisms', *arXiv preprint arXiv:1506.07167*.

Hofstede, G., Garibaldi de Hilal, A. V., Malvezzi, S., Tanure, B. and Vinken, H. (2010) 'Comparing regional cultures within a country: Lessons from Brazil', *Journal of Cross-Cultural Psychology*, 41(3), pp. 336-352.

Holzinger, A. (2005) 'Usability engineering methods for software developers', *Communications of the ACM*, 48(1), pp. 71-74.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012) 'Managing employee compliance with information security policies: The critical role of top management and organizational culture', *Decision Sciences*, 43(4), pp. 615-660.

IBM (2008) *USER EXPERIENCE. Usability.* Available at: [https://www-03.ibm.com/services/ca/en/mobility/offerings\\_userexperience\\_usability.html#:~:text=Usability%20is%20the%20discipline%20of,error%20tolerant%2C%20and%20subjectively%20pleasing](https://www-03.ibm.com/services/ca/en/mobility/offerings_userexperience_usability.html#:~:text=Usability%20is%20the%20discipline%20of,error%20tolerant%2C%20and%20subjectively%20pleasing).

ICAO (2021) *Self assessment questionnaire.* Available at: <https://www.icao.int/Security/Security-Culture/ICAO%20SC%20Resources/Forms/AllItems.aspx>.

IEC, I. E. C. (2018) *Usability: The International Electrotechnical Commission.* Available at: <https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=871-01-08> (Accessed: 15/02 2022).

IEEE (1990) *IEEE Standard Glossary of Software Engineering Terminology: IEEE Std 610.12-1990*, vol., no., pp.1-84, . Available at: <https://ieeexplore.ieee.org/document/159342/definitions#definitions> (Accessed: 02/02 2022).

IEEE (2022) *Usability and Accessibility: IEEE Brand Experience*. Available at: <https://brand-experience.ieee.org/guidelines/digital/style-guide/usability-and-accessibility/> (Accessed: 02/02 2022).

Interaction Design Foundation (2022) *Usability*: [intaction-design.org](https://www.interaction-design.org/literature/topics/usability#:~:text=Usability%20is%20a%20measure%20of,deliverable%E2%80%94to%20ensure%20maximum%20usability.). Available at: <https://www.interaction-design.org/literature/topics/usability#:~:text=Usability%20is%20a%20measure%20of,deliverable%E2%80%94to%20ensure%20maximum%20usability.> (Accessed: 11/02 2022).

Ioannou, M., Stavrou, E. and Bada, M. 'Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination'. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*: IEEE, 1-4.

ISACA (2021) *Nudging Our Way to Successful Information Security Awareness*. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-1/nudging-our-way-to-successful-information-security-awareness> (Accessed: 8/10 2024).

ISO (2018) *Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. Available at: <https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en> (Accessed: 01/01 2022).

Jesson, J., Lacey, F. M. and Matheson, L. (2011) 'Doing your literature review: Traditional and systematic techniques'.

Jin, G., Tu, M., Kim, T.-H., Heffron, J. and White, J. 'Game based cybersecurity training for high school students'. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 68-73.

JISC (2024) *What is "Respondent progress"?: JICS Online surveys (formerly BOS)*. Available at: <https://www.onlinesurveys.ac.uk/help-support/what-is-respondent-progress/>.

Johnston, J., Eloff, J. H. and Labuschagne, L. (2003) 'Security and human computer interfaces', *Computers & Security*, 22(8), pp. 675-684.

Jordan, P. W., Thomas, B., McClelland, I. L. and Weerdmeester, B. (1996) *Usability evaluation in industry*. CRC Press.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A. and Van Bruggen, D. (2014) 'An exploratory investigation of message-person congruence in information security awareness campaigns', *Computers & security*, 43, pp. 64-76.

Kallio, H., Pietilä, A. M., Johnson, M. and Kangasniemi, M. (2016) 'Systematic methodological review: developing a framework for a qualitative semi-structured interview guide', *Journal of advanced nursing*, 72(12), pp. 2954-2965.

Kävrestad, J., Fallatah, W. and Furnell, S. 'Cybersecurity training acceptance: A literature review'. *International symposium on human aspects of information security and assurance*: Springer, 53-63.

Kävrestad, J., Furnell, S. and Nohlberg, M. 'What parts of usable security are most important to users?'. *IFIP World Conference on Information Security Education*: Springer, 126-139.

Kävrestad, J., Gellerstedt, M., Nohlberg, M. and Rambusch, J. 'Survey of users' willingness to adopt and pay for cybersecurity training'. *International Symposium on Human Aspects of Information Security and Assurance*: Springer, 14-23.

Kirchherr, J. and Charles, K. (2018) 'Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia', *PloS one*, 13(8), pp. e0201710.



Kletenik, D., Butbul, A., Chan, D., Kwok, D. and LaSpina, M. (2021) 'Game on: teaching cybersecurity to novices through the use of a serious game', *Journal of Computing Sciences in Colleges*, 36(8), pp. 11-21.

KnowBe4 (2020) *What Is the Security Culture Survey (SCS)?* Available at: <https://support.knowbe4.com/hc/en-us/articles/360037393134-What-Is-the-Security-Culture-Survey-SCS-> (Accessed: 01/08 2022).

Kotter, J. P., Akhtar, V. and Gupta, G. (2021) *Change: How organizations achieve hard-to-imagine results in uncertain and volatile times*. John Wiley & Sons.

Kraemer, S. and Carayon, P. (2007) 'Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists', *Applied ergonomics*, 38(2), pp. 143-154.

Krajcsák, Z. (2019) 'Leadership strategies for enhancing employee commitment in TQM', *Journal of Management Development*, 38(6), pp. 455-463.

Krug, S. (2000) *Don't make me think!: a common sense approach to Web usability*. Pearson Education India.

Kvale, S. and Brinkmann, S. (2009) *Interviews: Learning the craft of qualitative research interviewing*. sage.

Lee, Y., Kozar, K. A. and Larsen, K. R. (2003) 'The technology acceptance model: Past, present, and future', *Communications of the Association for information systems*, 12(1), pp. 50.

Lewis, J. R. (2018) 'The system usability scale: past, present, and future', *International Journal of Human-Computer Interaction*, 34(7), pp. 577-590.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', *International Journal of Information Management*, 45, pp. 13-24.

Lopes, I. and Oliveira, P. (2014) 'Understanding information security culture: a survey in small and medium sized enterprises', *New Perspectives in Information Systems and Technologies, Volume 1*: Springer, pp. 277-286.

Lui, S. M. and Hui, W. 'The effects of knowledge on security technology adoption: Results from a quasi-experiment'. *The 5th International Conference on New Trends in Information Science and Service Science*: IEEE, 328-333.

Ma, S., Zhang, S., Li, G. and Wu, Y. (2019) 'Exploring information security education on social media use: Perspective of uses and gratifications theory', *Aslib Journal of Information Management*, 71(5), pp. 618-636.

Mahfuth, A., Yussof, S., Baker, A. A. and Ali, N. a. 'A systematic literature review: Information security culture'. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*: IEEE, 1-6.

Malcolmson, J. 'What is security culture? Does it differ in content from general organisational culture?'. *43rd Annual 2009 international Carnahan conference on security technology*: IEEE, 361-366.

Marotta, A. and Pearlson, K. (2019) 'A culture of cybersecurity at Banca Popolare di Sondrio'.

Martins, A. and Elofe, J. (2002) 'Information security culture', *Security in the information society*: Springer, pp. 203-214.

- McCrohan, K. F., Engel, K. and Harvey, J. W. (2010) 'Influence of awareness and training on cyber security', *Journal of internet Commerce*, 9(1), pp. 23-41.
- McKnight, P. E. and Najab, J. (2010) 'Mann-Whitney U Test', *The Corsini encyclopedia of psychology*, pp. 1-1.
- Meline, T. (2006) 'Selecting studies for systemic review: Inclusion and exclusion criteria', *Contemporary issues in communication science and disorders*, 33(Spring), pp. 21-27.
- Microsoft (2019) *Usability in Software Design*. Available at: <https://docs.microsoft.com/en-us/windows/win32/appuistart/usability-in-software-design#defining-usability> (Accessed: 16/02 2022).
- Möhlmann, M. (2021) 'Algorithmic nudges don't have to be unethical', *Harvard Business Review*, 22, pp. 1-7.
- Mokwetli, M. and Zuva, T. 'Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa'. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*: IEEE, 1-7.
- Moustafa, A. A., Bello, A. and Maurushat, A. (2021) 'The role of user behaviour in improving cyber security management', *Frontiers in Psychology*, 12, pp. 561011.
- Mumford, E. (2006) 'The story of socio-technical design: Reflections on its successes, failures and potential', *Information systems journal*, 16(4), pp. 317-342.
- Naderifar, M., Goli, H. and Ghaljaie, F. (2017) 'Snowball sampling: A purposeful method of sampling in qualitative research', *Strides in development of medical education*, 14(3).
- Nævestad, T.-O., Meyer, S. F. and Honerud, J. H. (2018) 'Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security', *Safety and Reliability—Safe Societies in a Changing World*, pp. 3021-3029.
- Nasir, A., Arshah, A. R. and Hamid, M. R. (2019) 'A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions', *Information Security Journal: A Global Perspective*, 28(3), pp. 55-80.
- National Academies Press (1999) *Importance and Use of Scientific and Technical Databases A Question of Balance: Private Rights and the Public Interest in Scientific and Technical Databases*. Washington, DC: National Academies of Sciences, Engineering, and Medicine. (Accessed: 16/08/2024).
- NCSC (2018) 'Security and usability: you CAN have it all!', *This blog post explains how making security more usable can help to make an organisation more secure*. in *Written by Emma W, Head of Advice & Guidance for small & medium sized organisations, self employed & sole traders, and large organisations* [Online]. Available at: <https://www.ncsc.gov.uk/blog-post/security-and-usability--you-can-have-it-all-> 2024].
- Neisse, R., Hernández-Ramos, J. L., Matheu-Garcia, S. N., Baldini, G., Skarmeta, A., Siris, V., Lagutin, D. and Nikander, P. (2020) 'An interledger blockchain platform for cross-border management of cybersecurity information', *IEEE Internet Computing*, 24(3), pp. 19-29.
- Nel, F. and Drevin, L. (2019) 'Key elements of an information security culture in organisations', *Information & Computer Security*.
- Ng, B.-Y., Kankanhalli, A. and Xu, Y. C. (2009) 'Studying users' computer security behavior: A health belief perspective', *Decision Support Systems*, 46(4), pp. 815-825.



- NHS (2022) *Short-sightedness (myopia)*. Available at: <https://www.nhs.uk/conditions/short-sightedness/> (Accessed: 13/5/2024).
- Nick, T. G. and Campbell, K. M. (2007) 'Logistic regression', *Topics in biostatistics*, pp. 273-301.
- Nickerson, R. S. (2000) 'Null hypothesis significance testing: a review of an old and continuing controversy', *Psychological methods*, 5(2), pp. 241.
- Nielsen, J. (1993) *Usability engineering*. Morgan Kaufmann.
- Nielsen, J. (2012) *Usability 101: Introduction to Usability*: Nielsen Norman Group. Available at: <https://www.nngroup.com/articles/usability-101-introduction-to-usability/> (Accessed: 15/01 2022).
- NIH (2017) *Stuttering*: National Institutes of Health. Available at: <https://www.nidcd.nih.gov/health/stuttering> (Accessed: 13/5/2024).
- Nilsen, P. and Bernhardsson, S. (2019) 'Context matters in implementation science: a scoping review of determinant frameworks that describe contextual determinants for implementation outcomes', *BMC health services research*, 19, pp. 1-21.
- Nowell, L. S., Norris, J. M., White, D. E. and Moules, N. J. (2017) 'Thematic analysis: Striving to meet the trustworthiness criteria', *International journal of qualitative methods*, 16(1), pp. 1609406917733847.
- Nurse, J., Creese, S., Goldsmith, M. and Lamberts, K. (2011) 'Guidelines for usable cybersecurity: Past and present', *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*.
- NVivo (2024) *About NVivo*. Available at: <https://help-nv.qsrinternational.com/20/win/Content/about-nvivo/about-nvivo.htm> (Accessed: 21/1/2024).
- OECD (2023) *Population with tertiary education*. Available at: <https://data.oecd.org/eduatt/population-with-tertiary-education.htm> (2024).
- Offor, P. and Tejay, G. (2014) 'Information systems security training in organizations: andragogical perspective'.
- Padayachee, K. (2012) 'Taxonomy of compliant information security behavior', *Computers & Security*, 31(5), pp. 673-680.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A. and Brennan, S. E. (2021) 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *Bmj*, 372.
- Paré, G. and Kitsiou, S. (2017) 'Methods for literature reviews', *Handbook of eHealth evaluation: An evidence-based approach [Internet]*: University of Victoria.
- Parker, C., Scott, S. and Geddes, A. (2019) 'Snowball sampling', *SAGE research methods foundations*.
- Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010) *Human factors and information security: individual, culture and security environment*.
- Petersen, R. D. and Valdez, A. (2005) 'Using snowball-based methods in hidden populations to generate a randomized community sample of gang-affiliated adolescents', *Youth violence and juvenile justice*, 3(2), pp. 151-167.
- Pfadenhauer, L. M., Gerhardus, A., Mozygemba, K., Lysdahl, K. B., Booth, A., Hofmann, B., Wahlster, P., Polus, S., Burns, J. and Brereton, L. (2017) 'Making sense of complexity in context and

implementation: the Context and Implementation of Complex Interventions (CICI) framework', *Implementation science*, 12, pp. 1-17.

Pietkiewicz, I. and Smith, J. A. (2014) 'A practical guide to using interpretative phenomenological analysis in qualitative research psychology', *Psychological journal*, 20(1), pp. 7-14.

Pinder, C. C. (2014) *Work motivation in organizational behavior*. psychology press.

Pinsonneault, A. and Kraemer, K. (1993) 'Survey research methodology in management information systems: an assessment', *Journal of management information systems*, 10(2), pp. 75-105.

Posey, C. and Folger, R. (2020) 'An exploratory examination of organizational insiders' descriptive and normative perceptions of cyber-relevant rights and responsibilities', *Computers & Security*, 99, pp. 102038.

Potgieter, M., Marais, C. and Gerber, M. 'Fostering content relevant information security awareness through browser extensions'. *Information Assurance and Security Education and Training: 8th IFIP WG 11.8 World Conference on Information Security Education, WISE 8, Auckland, New Zealand, July 8-10, 2013, Proceedings, WISE 7, Lucerne Switzerland, June 9-10, 2011, and WISE 6, Bento Gonçalves, RS, Brazil, July 27-31, 2009, Revised Selected Papers 8*: Springer, 58-67.

Preece, J. (1993) *A guide to usability: Human factors in computing*. Addison-Wesley Longman Publishing Co., Inc.

Quesenbery, W. 'Dimensions of usability: Defining the conversation, driving the process'. *UPA 2003 Conference*, 23-27.

Quesenbery, W. (2004) 'Balancing the 5Es of usability', *Cutter IT Journal*, 17(2), pp. 4-11.

Quesenbery, W. (2006) 'Using the 5Es to understand users', Available in *WQUsability website in <http://www.wqusability.com/articles/getting-started.html>*.

Reeves, A., Calic, D. and Delfabbro, P. (2021) "'Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training', *Computers & security*, 106, pp. 102281.

Rhee, H.-S., Kim, C. and Ryu, Y. U. (2009) 'Self-efficacy in information security: Its influence on end users' information security practice behavior', *Computers & security*, 28(8), pp. 816-826.

Rodden, K., Hutchinson, H. and Fu, X. 'Measuring the user experience on a large scale: user-centered metrics for web applications'. *Proceedings of the SIGCHI conference on human factors in computing systems*, 2395-2398.

Roer, K. (2014) *How to build and maintain security culture*. Available at: <https://roer.com/how-to-build-and-maintain-security-culture-4619472db508>.

Roer, K., Petrić, G., Eriksen, A.-C., Paglia, J., Ulimoen, T., Huisman, J., Smothers, R. L. and Carpenter, P. (2022) *The Security Culture Report 2022: KnowB4 Research*. Available at: [https://www.knowbe4.com/hubfs/2022-Security-Culture-Report-Research\\_EN-US.pdf?hsCtaTracking=8b6558de-f36f-4dbe-abc6-60c5c06ccdd0%7Cdd079e6a-b308-4e89-8588-9ab09e45c452](https://www.knowbe4.com/hubfs/2022-Security-Culture-Report-Research_EN-US.pdf?hsCtaTracking=8b6558de-f36f-4dbe-abc6-60c5c06ccdd0%7Cdd079e6a-b308-4e89-8588-9ab09e45c452).

Ross, S. J. (2011) *Creating a Culture of Security*. In: *ISACA*.

Rouder, J., Saucier, O., Kinder, R. and Jans, M. (2021) 'What to do with all those open-ended responses? Data visualization techniques for survey researchers', *Survey Practice*.

- Ruhwanya, Z. and Ophoff, J. 'Information security culture assessment of small and medium-sized enterprises in Tanzania'. *International Conference on Social Implications of Computers in Developing Countries*: Springer, 776-788.
- Sadia, A., Salleh, B. M., Kadir, Z. A. and Sanif, S. (2016) 'The relationship between organizational communication and employees productivity with new dimensions of effective communication flow', *Journal of business and social review in emerging economies*, 2(2), pp. 93-100.
- Sah, L. K., Singh, D. R. and Sah, R. K. (2020) 'Conducting qualitative interviews using virtual communication tools amid COVID-19 pandemic: A learning opportunity for future research', *JNMA: Journal of the Nepal Medical Association*, 58(232), pp. 1103.
- Saltzer, J. H. and Schroeder, M. D. (1975) 'A proteção de informação em sistemas de computador', *Proceedings of the IEEE*, 63(9), pp. 1278-1308.
- Sarkis-Onofre, R., Catalá-López, F., Aromataris, E. and Lockwood, C. (2021) 'How to properly use the PRISMA Statement', *Systematic Reviews*, 10, pp. 1-3.
- Schlienger, T. and Teufel, S. 'Analyzing information security culture: increased trust by an appropriate information security culture'. *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*: IEEE, 405-409.
- Schober, P., Boer, C. and Schwarte, L. A. (2018) 'Correlation coefficients: appropriate use and interpretation', *Anesthesia & analgesia*, 126(5), pp. 1763-1768.
- Schoonenboom, J. and Johnson, R. B. (2017) 'How to construct a mixed methods research design', *Kolner Zeitschrift für Soziologie und Sozialpsychologie*, 69(Suppl 2), pp. 107.
- Schumacher, R. M., Lowry, S. Z. and Schumacher, R. M. (2010) *NIST guide to the processes approach for improving the usability of electronic health records*. US Department of Commerce, National Institute of Standards and Technology.
- Shackel, B. (2009) 'Usability–Context, framework, definition, design and evaluation', *Interacting with computers*, 21(5-6), pp. 339-346.
- Sharp, H., Rogers, Y. and Preece, J. (2019) 'Interaction design : beyond human-computer interaction / [Helen] Sharp, [Yvonne] Rogers, [Jennifer] Preece'.
- Shen, L. W., Mammi, H. K. and Din, M. M. 'Cyber security awareness game (CSAG) for secondary school students'. *2021 International Conference on Data Science and Its Applications (ICoDSA)*: IEEE, 48-53.
- Sherif, E., Furnell, S. and Clarke, N. (2015) "'An identification of variables influencing the establishment of information security culture.'", *International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham*, pp. (pp. 436-448).
- Shillair, R. 'Talking about online safety: a qualitative study exploring the cybersecurity learning process of online labor market workers'. *Proceedings of the 34th ACM International Conference on the Design of Communication*, 1-9.
- Shneiderman, B. and Plaisant, C. (2010) *Designing the user interface: Strategies for effective human-computer interaction*. Pearson Education India.
- Shukla, S. S., Tiwari, M., Lokhande, A. C., Tiwari, T., Singh, R. and Beri, A. 'A Comparative Study of Cyber Security Awareness, Competence and Behavior'. *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*: IEEE, 1704-1709.

Sibley, M. H., Mitchell, J. T. and Becker, S. P. (2016) 'Method of adult diagnosis influences estimated persistence of childhood ADHD: a systematic review of longitudinal studies', *The Lancet Psychiatry*, 3(12), pp. 1157-1165.

Silic, M. and Lowry, P. B. (2020) 'Using design-science based gamification to improve organizational security training and compliance', *Journal of management information systems*, 37(1), pp. 129-161.

Silva, L. M. d., Bitencourt, C. C., Faccin, K. and Iakovleva, T. (2019) 'The role of stakeholders in the context of responsible innovation: A meta-synthesis', *Sustainability*, 11(6), pp. 1766.

Sinkowitz-Cochran, R. L. (2013) 'Survey design: To ask or not to ask? That is the question...', *Clinical Infectious Diseases*, 56(8), pp. 1159-1164.

Stajkovic, A. D. and Luthans, F. (2003) 'Behavioral management and task performance in organizations: conceptual background, meta-analysis, and test of alternative models', *Personnel psychology*, 56(1), pp. 155-194.

Stevens, S., Read, J., Baines, R., Chatterjee, A. and Archer, J. (2018) 'Validation of multisource feedback in assessing medical performance: a systematic review', *Journal of Continuing Education in the Health Professions*, 38(4), pp. 262-268.

Stockett, J. 'Dr. InfoSec: how to teach your community to stop worrying and love 2-factor authentication'. *Proceedings of the 2018 ACM SIGUCCS Annual Conference*, 21-23.

Talib, S., Clarke, N. L. and Furnell, S. M. 'An analysis of information security awareness within home and work environments'. *2010 International Conference on Availability, Reliability and Security*: IEEE, 196-203.

Tang, M., Li, M. g. and Zhang, T. (2015) 'The impacts of organizational culture on information security culture: a case study', *Information technology and management*, 17(2), pp. 179-186.

Terry, G., Hayfield, N., Clarke, V. and Braun, V. (2017) 'Thematic analysis', *The SAGE handbook of qualitative research in psychology*, 2(17-37), pp. 25.

Thaler, R. and Sunstein, C. 'Nudge: Improving decisions about health, wealth and happiness'. *Amsterdam Law Forum; HeinOnline: Online*: HeinOnline, 89.

The World Economic Forum (2022) *How user experience and behavioural science can guide smart cybersecurity*. Available at: <https://www.weforum.org/stories/2022/11/how-user-experience-and-behavioural-science-can-guide-smart-cybersecurity/#:~:text=Cyber%20attacks%20are%20on%20the,engineering%20techniques%20get%20more%20sophisticated>.

Theofanos, M. (2020) 'Is Usable Security an Oxymoron?', NIST Computer Security Resource Center (CSRC). Computer (Long Beach, Calif.), *IEEE*, 53(2), pp. 71-74.

Thomson, K.-L., Von Solms, R. and Louw, L. (2006) 'Cultivating an organizational information security culture', *Computer fraud & security*, 2006(10), pp. 7-11.

Timans, R., Wouters, P. and Heilbron, J. (2019) 'Mixed methods research: what it is and what it could be', *Theory and Society*, 48, pp. 193-216.

Tolah, A., Furnell, S. and Papadaki, M. (2021) 'An empirical analysis of the information security culture key factors framework', *Computers & Security*, 108, pp. 102354.

U.S Department of Homeland Security (2009) 'A Roadmap for Cybersecurity Research', *Homeland Security*, pp. 90.

Uchendu, B., Nurse, J. R., Bada, M. and Furnell, S. (2021) 'Developing a cyber security culture: Current practices and future needs', *Computers & Security*, 109, pp. 102387.

Usability Professionals Association (2010) *What is Usability?: Usability Body of Knowledge*. Available at: <https://www.usabilitybok.org/what-is-usability> (Accessed: 17/02 2022).

Usability.gov (2022) *Glossary: Usability*. Available at: <https://www.usability.gov/what-and-why/glossary/u/index.html> (Accessed: 15/02 2022).

Vaismoradi, M., Jones, J., Turunen, H. and Snelgrove, S. (2016) 'Theme development in qualitative content analysis and thematic analysis'.

Vaismoradi, M. and Snelgrove, S. (2019) 'Theme in qualitative content analysis and thematic analysis'.

Valerio, M. A., Rodriguez, N., Winkler, P., Lopez, J., Dennison, M., Liang, Y. and Turner, B. J. (2016) 'Comparing two sampling methods to engage hard-to-reach communities in research priority setting', *BMC medical research methodology*, 16, pp. 1-11.

Venkatesh, V. and Bala, H. (2008) 'Technology acceptance model 3 and a research agenda on interventions', *Decision sciences*, 39(2), pp. 273-315.

Venkatesh, V. and Davis, F. D. (2000) 'A theoretical extension of the technology acceptance model: Four longitudinal field studies', *Management science*, 46(2), pp. 186-204.

Verizon (2022) *2022 Data Breach Investigations Report*. Available at: <https://www.verizon.com/business/resources/reports/dbir/> (Accessed: 10/07 2022).

Verizon (2024) *2024 Data Breach Investigations Report*. Available at: <https://www.verizon.com/business/en-gb/resources/reports/dbir/>.

Vickers, A. J. (2005) 'Parametric versus non-parametric statistics in the analysis of randomized trials with non-normally distributed data', *BMC medical research methodology*, 5, pp. 1-12.

Voinov, A. and Bousquet, F. (2010) 'Modelling with stakeholders', *Environmental modelling & software*, 25(11), pp. 1268-1281.

Wash, R. and Cooper, M. M. 'Who provides phishing training? facts, stories, and people like me'. *Proceedings of the 2018 chi conference on human factors in computing systems*, 1-12.

Weichbroth, P. (2020) 'Usability of mobile applications: a systematic literature study', *IEEE Access*, 8, pp. 55563-55577.

Weijers, R. J., de Koning, B. B. and Paas, F. (2021) 'Nudging in education: From theory towards guidelines for successful implementation', *European Journal of Psychology of Education*, 36, pp. 883-902.

Wen, Z. A., Lin, Z., Chen, R. and Andersen, E. 'What. hack: engaging anti-phishing training through a role-playing phishing simulation game'. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-12.

Whitten, A. and Tygar, J. D. 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0'. *USENIX security symposium*, 169-184.

Wiley, A., McCormac, A. and Calic, D. (2020) 'More than the individual: Examining the relationship between culture and Information Security Awareness', *Computers & Security*, 88, pp. 101640.

Yasin, A., Liu, L., Li, T., Fatima, R. and Jianmin, W. (2019) 'Improving software security awareness using a serious game', *IET Software*, 13(2), pp. 159-169.

Yee, K.-P. 'User interaction design for secure systems'. *International Conference on Information and Communications Security*: Springer, 278-290.

Zimmermann, V. and Renaud, K. (2021) 'The nudge puzzle: matching nudge interventions to cybersecurity decisions', *ACM Transactions on Computer-Human Interaction (TOCHI)*, 28(1), pp. 1-45.

Zimmermann, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M. and Ebert, N. (2024) 'Human-Centered Cybersecurity Revisited: From Enemies to Partners', *Communications of the ACM*, 67(11), pp. 72-81.

Zurko, M. E. and Simon, R. T. 'User-centered security'. *Proceedings of the 1996 workshop on New security paradigms*, 27-33.

# Appendices

## Appendix I: Ethical Approval

**School of Computer Science**

**Research Ethics Committee (CS REC)**



### **Ethics application for research that involves human participants or collects data directly from human participants**

This form should be used if the research involves human participants or processes personal data that are obtained directly from participants. For example, if data is collected through interview or someone's involvement in an experiment.

If you are not sure what personal data is or what processing personal data means, see *READ ME (does my research require ethics approval?)*

Sections A and B of this form must be completed and approved **\*before\*** potential participants are approached to take part in the research.

**Sections A and B should be completed by the researcher. Complete all sections. Edit italicised text only. Do NOT modify this form prior to ethics review.**

**Section B should be provided to participants in the research.** It may be modified (e.g., non-applicable sub-sections deleted or reformatted) after the application has been approved.

If the research requires different categories or groups of participants to engage in different activities, complete a separate copy of Section B for each category or group.

The principal investigator or supervisor should sign-off this ethics application and submit the completed form to [cs-ethicsadmin@cs.nott.ac.uk](mailto:cs-ethicsadmin@cs.nott.ac.uk).

The principal investigator or supervisor is responsible for ensuring the application has been completed correctly and providing feedback to the researcher if it is required. Principal investigators or supervisors must have completed ethics training.

A data management plan (DMP) should be put in place by the researcher and be reviewed and approved by the supervisor or PI \*before\* submission of the ethics application.<sup>3</sup>

If your application is a modification of an existing submission, or a new submission having only minor modifications to one previously approved, see Section A4.

## **Section A. Information to be provided to the Research Ethics Committee, along with Section B**

<b>1. The applicant</b>	
Applicant's name	Wesam Fallatah
Applicant's role	Student (20205841)
UoN email address	wesam.fallatah@nottingham.ac.uk
Module / course details	N/A
Supervisor/PI's name	Prof. Steven Furnell Dr Ying He
Supervisor/PI's email address	<a href="mailto:steven.furnell@nottingham.ac.uk">steven.furnell@nottingham.ac.uk</a> <a href="mailto:ying.he@nottingham.ac.uk">ying.he@nottingham.ac.uk</a>
Clinical advisor's name	N/A
Clinical advisor's email address	N/A

<b>2. The project</b>	
Project title	The Influence of Usable Security on Security Culture

---

<sup>3</sup> See the Data Management Plan (DMP) form and guidance.



Proposed start date	ASAP
Date and version of application	11 January 2023
Type of application	First submission
Application ID (if known) <sup>4</sup>	

<b>3. Change log</b>
N/A

<b>4. Modifications and related applications</b>
N/A

<b>5. Research ethics checklist (part one)</b>	
<b>Answer all questions:</b>	<b>Yes/No</b>
a) Does the study involve participants who are unable to give informed consent (e.g., children, people with learning disabilities or dementia, prisoners, your own students)?	No
b) Will the study involve participants who are particularly vulnerable? <sup>5</sup>	No

---

<sup>4</sup> An ethics application is usually allocated an ID by the CS REC *after* initial submission.

<sup>5</sup> A vulnerable person is defined as someone “who is or may be in need of community care services by reason of mental or other disability, age or illness; and who is or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation” (Department of Health *No Secrets: Guidance on Protecting Vulnerable Adults in Care*, 2000)

c) Will it be necessary for participants to take part in the study without their knowledge and consent at the time (e.g., covert observation of people in non-public places)?	No
d) Will it be necessary for participants to be kept in ignorance, misled or deceived at any point in the study (e.g., if revealing the full aims of the project during the consent process would undermine the research)?	No
e) Will the study involve the discussion of sensitive topics (including but not limited to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, health or participant's sex life or sexual orientation)?	No
f) Will participants be asked to discuss anything or partake in any activity that they may find embarrassing or traumatic?	No
g) Is it likely that the study will cause offence to participants for reasons of ethnicity, religion, gender, sexual orientation or culture?	No
h) Are drugs, placebos or other substances (e.g., food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive or potentially harmful procedures of any kind?	No
i) Is pain or more than mild discomfort likely to result from the study?	No
j) Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?	No
k) Will the study involve prolonged or repetitive testing for each participant?	No
l) Will financial inducement (other than reasonable expenses and compensation for time) be offered to participants?	No

m) Will the study involve the recruitment of patients, staff, tissue sample, records or other data through the NHS or involve NHS sites and other property?	No
n) Does the research pose any risks to the researchers, participants, culture, the environment, and/or the reputation of those involved in the research or the reputation of university?	No
<b>5. Research ethics checklist (part two)</b>	
<b>Answer all questions:</b>	<b>Yes/No/NA</b>
a) For research conducted in public, non-governmental and private organisations and institutions (such as schools, charities, companies and offices), will approval be gained in advance from the appropriate authorities?	Yes
b) If the research uses human participants, personal data or the use of biological material, will explicit consent be gained?	Yes
c) Will participants be informed of their right to withdraw from the study at any time, without giving explanation?	Yes
d) If data is being collected, will this data be anonymised before publication or sharing?	Yes
e) Will participants be assured of the confidentiality of any data?	Yes
f) Will all data be stored in accordance with the Data Protection Act?	Yes
g) Will participants be informed about who will have access to the data?	Yes
h) If quotations from participants will be used, will participants be asked for consent?	Yes
i) If audio-visual media (voice recording, video, photographs etc) will be used, will participants be asked for consent?	Yes

j) If digital media (e.g., computer records, http traffic, location logs) will be used, will participants be asked for consent?	NA
k) If the research involves contact with children, will appropriate safeguards be in place (e.g., supervision, DBS checks) if required?	NA
l) If research data itself is to be published, shared or reused (e.g., alongside a publication or in an archive), will participants be asked for consent?	Yes

If you have answered “no” to all questions in part 1 and “yes” or “NA” to all applicable questions in part two of the research ethics checklist, your research is deemed to involve **minimal risk** and you may go to Section A7.

If you have answered “yes” to any of the questions in part 1 or “no” to any applicable questions in part 2 of the research ethics checklist, the research is deemed to involve **more than minimal risk**. Please explain overleaf (Section A6) why this is necessary and how you plan to deal with the ethical issues raised.

6. Research involving more than minimal risk	
N/A	
7. Data processing	
<b>Data subjects</b>	Adult users who use IT devices within the context of their workplace
<b>Data to be collected</b>	Demographic information about the participants (age group, gender, education, accessibility to technology, role in the organisation, sector of work, the geographical region in which the organisation is located, and the size of the organisation). Contact details of the participants will be collected if they are willing to participate in the project’s next phase (interviews). However, this contact information will be separated from the individual responses during the analysis of the data collected

	in the survey and will not be used as a basis for identifying data from participants in the interview phase.
<b>How data will be collected</b>	<p>The survey will be conducted using the Jisc Online Survey (JOS) platform, which is a GDPR complaint.</p> <p>Participants who show interest in taking part in the interviews phase will be contacted by email and interviewed via Microsoft Teams. The interview sessions will be recorded for review and analysis purposes. A consent form concerning the recording of sessions will be distributed to participants prior to the sessions; if they decline, notes will be taken instead.</p>
<b>Pre-processing of data</b>	<p><b>i. Pre-processing procedure(s)</b></p> <p>Interviews discussions will be recorded using the transcription application embedded in Microsoft Teams or using the University of Nottingham's automated transcription service (<a href="https://www.nottingham.ac.uk/dts/researcher/applications-and-tools/automated-transcription.aspx">https://www.nottingham.ac.uk/dts/researcher/applications-and-tools/automated-transcription.aspx</a>)</p> <p><b>ii. Anonymisation / pseudonymisation applied</b></p> <p>The interview transcripts will be stored on the OneDrive server of the University of Nottingham. The transcripts will be made anonymous, utilising a method of unique number identification. Any identifying information from both the survey and the interview will be removed/anonymised.</p>
<b>Data analysis</b>	The survey responses will be analysed using the Statistical Package for Social Science (SPSS), while the interview data will be analysed through thematic analysis.
<b>Data sharing</b>	<p>The data assets will be shared with the project's supervisors, Prof. Steven Furnell and Dr Ying He.</p> <p>The resulting outputs will be written down within the project's thesis.</p>
<b>Data storage</b>	<p>Data assets:</p> <ul style="list-style-type: none"> <li>• Survey Results</li> <li>• Interview Recordings</li> </ul>

	Stored on: OneDrive at the University of Nottingham Owner: Wesam Fallatah
--	--

<b>8. Participant recruitment</b>	
<b>a) How participants will be recruited</b>	
It is anticipated to recruit (n=250) participants for the survey and up to (n=30) participants for the interviews. Potential participants will be reached via email or social media platforms (e.g., LinkedIn, Twitter, and Telegram) to complete the survey and via emails to take part in the interview sessions.	
<b>b) Incentives</b>	
N/A	
<b>c) Compensation</b>	
N/A	

<b>9. Further information</b>
<p>The survey will be piloted before conducting the actual data collection.</p> <p>The drafted structure of the survey is as follows:</p> <ul style="list-style-type: none"> <li>• Demographic information about the participants and their workplace</li> <li>• Questions about security culture in the organisation</li> <li>• Questions about the usability of cybersecurity</li> <li>• Questions about usable security and security culture</li> <li>• Questions to measure security culture influential factors</li> </ul> <p>The interview sessions will explore similar issues, but the specifics of the interview plan will be determined at a later point, in response to the survey findings.</p>

<b>10. Applicant declaration</b>	
<b>Please confirm each of the following statements:</b>	<b>Yes/No</b>

The research is <b>minimal risk</b>	Yes
The data management plan (DMP) form has been completed	Yes
Applicant	Wesam Fallatah
Date	06 January 2022

11. Supervisor/PI declaration	
Please confirm each of the following statements:	Yes/No
I have completed ethics training	Yes
The proposed research complies with the UoN Code of Research Conduct and Research Ethics	Yes
<p>I have reviewed and approve the DMP</p> <p><i>The supervisor/PI must refer the DMP to CS REC for approval if the answer is NO to Sections 6.2, 7.4, 7.5 or 8.2. If the applicant and the PI are the same, the DMP should be submitted with this application for review by CS REC.</i></p>	Yes
Supervisor/PI	Prof. Steven Furnell
Date	Enter date application submitted to <a href="mailto:cs-ethicsadmin@cs.nott.ac.uk">cs-ethicsadmin@cs.nott.ac.uk</a>

## **Section B. Information to be provided to research participants**

**PROJECT TITLE:** The Influence of Usable Security on Security Culture

<b>1. The research</b>
<b>a) Aims and objectives of the research</b>
<p>This project aims to determine the influence of the usability of cybersecurity technologies and processes upon security culture in organisations. The project will also identify in what ways usable security can help organisations maintain good security culture and offer a practical contribution that organisations can rely on to enhance the general security culture. We are interested in gathering your insights about using security and how the usability affects your behaviour while using cybersecurity technologies or following cybersecurity procedures. The insights from an initial survey will be used to inform follow-on interviews and then ultimately to determine areas that may promote positive security culture.</p>
<b>b) Funder information</b>
<p>The work is being conducted as part of a PhD project conducted at the University of Nottingham, and funded by the Saudi Arabian Cultural Bureau (SACB)</p>
<b>c) Governance</b>
<p>This research has been approved by the School of Computer Science Research Ethics Committee (CS REC), ethics application ID <b>CS-2022-R32</b></p>
<b>2. Taking part in the research</b>



This research will be conducted in two phases. You can choose to participate in either Phase 1 only, or both Phases 1 and 2.

In Phase 1, you are asked to complete a survey to understand your perceptions of the usability of cybersecurity and its impact on your organisation. The survey also asks questions about security culture to understand your perceptions of factors that influence the overall security culture in your organisation. The researchers will analyse the data from Phase 1 to understand how different aspects affect security culture in organisations.

Phase 2 of the research will involve a follow-up interview. This phase aims to review the findings from the data collection and gain a deeper understanding of your behaviours and attitudes towards the usability of security in your workplace.

To participate in this research, you must be 18 years or older and a regular IT user in the context of your workplace.

### **3. Risks of participation**

#### **a) Risks**

There are always risks of compromise associated with online data storage platforms. However, the nature of the study and the collected data indicate that you will not experience any substantial impacts from this risk.

The data collection does not intend to collect any sensitive information about you or your organisation.

Although you might choose to provide your contact information as part of the Phase 1 activity, it will only be used to invite you to join in Phase 2.

#### **b) Mitigation of risks**

See section 5 for the measures we put in place to mitigate the risk of unauthorised access.

### **4. Purpose of data processing**

#### **a) Data collected**

<p>We collect the following categories of data during your participation in the research:</p> <p>Age group, gender, education, accessibility to technology, role in the organisation, sector of work, the geographical region in which the organisation is located, the size of the organisation, and contact email address.</p>
<p><b>b) Specific purposes for which the data are processed</b></p>
<p>Contact details will only be used to invite you to participate in the phase 2 interview.</p> <p>Anonymised versions of all other data collected during the research will be:</p> <ul style="list-style-type: none"> <li>• Analysed to meet the aims and objectives described in Section 1.</li> <li>• Reviewed and discussed in research meetings between members of the research team.</li> </ul> <p>Anonymous quotations of comments made by participants may be used in scientific works, including presentations, reports and publications stored in databases and posted online and in marketing materials that promote the research and its findings.</p>
<p><b>c) Automated decision-making and profiling</b></p>
<p>N/A</p>
<p><b>d) Legal basis for processing your data</b></p>
<p>We collect personal data under the terms of the University of Nottingham's Royal Charter and in our capacity as a teaching and research body to advance education and learning. We thus process your data on the legal basis that our research is in the public interest, we have legitimate interests and / or that you consent to data processing in freely and voluntarily participating in our research activities.</p>

<p><b>5. Storage and retention of your data</b></p>
<p><b>a) Data protection measures</b></p>
<p>We put the following organisational and / or technical safeguards in place to protect your data and your identity to the best of our ability:</p> <p>i) All data stored digitally will be encrypted and password protected</p>
<p><b>b) Retention period</b></p>

Data protection law allows us to retain personal data for an indefinite period and use it in future for public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of technical and organisational measures that safeguard your data, your legal rights and your freedoms. These safeguards include the storage measures described above to protect your data against unauthorised access, and de-identification (anonymisation or pseudonymisation) of your data wherever possible and practicable. Data that identifies or could identify you will not be made public without your consent. You have the right to request data to be erased according to the principles of the UK GDPR (art. 17). Once made public, (anonymous) collected data can no longer be withdrawn.

## **6. Third party recipients, services and data transfers**

### **a) Project partners**

Your data will not be shared with others

### **b) Third-party services**

N/A

### **c) Data transfers**

N/A

## **7. Your legal rights**

### **Data protection rights (Data Protection Act 2018)**

You have the right:

- To be informed about the collection and use of personal data (as per this document).
- To access and receive a copy of your personal data, and other supplementary information, on request.
- To object to and restrict data processing if you think we are not complying with data protection law, and to rectify inaccuracies.
- To be forgotten, i.e., to have your personal data erased.
- To data portability and to obtain your data in an accessible and machine-readable format if appropriate, or to transfer your data to another organisation if technically feasible.
- To complain to about the way we process your personal data to our ethics committee ([cs-ethicsadmin@cs.nott.ac.uk](mailto:cs-ethicsadmin@cs.nott.ac.uk)), our Data Protection Officer

([dpo@nottingham.ac.uk](mailto:dpo@nottingham.ac.uk)) or the Information Commissioner's Office (<https://ico.org.uk/make-a-complaint>).\*

## 8. Your ethical rights

### a) Right to withdraw

You have the right to withdraw from the research at any time without explanation. You also have the right to request that your data be deleted if you do withdraw.

### b) Handling of 'mixed' data

In Phase 2 the data will be collected by means of recording the interview sessions and it cannot be deleted unless requested. Any data involving you will be redacted accordingly wherever possible, with the exception of scientific works produced prior to your notification of withdrawal.

### c) Withdrawal procedure

If you wish to withdraw, please notify Wesam Fallatah ([Wesam.fallatah@nottingham.ac.uk](mailto:Wesam.fallatah@nottingham.ac.uk))

If you do not receive confirmation of withdrawal from the research, please email [cs-ethicsadmin@cs.nott.ac.uk](mailto:cs-ethicsadmin@cs.nott.ac.uk)

## 9. Consent to participate

### a) I consent to participate in the research and my signature or mark confirms the following:

- understand that your participation is voluntary
- understand the aims and objectives of the research
- understand what the research requires you to do
- accept the risks of participation
- understand what data will be collected and the purposes for which the data will be used
- understand safeguards will be put in place to protect your data and your legal rights

*Signature or mark:*

\* Our DPO's postal address is Data Protection Officer, Legal Services, A5 Trent Building, University of Nottingham, University Park, Nottingham NG7 2RD.

<ul style="list-style-type: none"> <li>• understand that you will not be identified unless the use of identifiable data has been requested</li> <li>• understand that you can withdraw at any time without explanation</li> <li>• understand that once you have completed the study and submitted your answers, it will not be technically possible to withdraw the data</li> </ul>	
<b>b) Opt out.</b> I do not consent to use of my visual image in scientific works or materials that promote the research and its results	Signature or mark:
Name of participant(s)	
Date	
Witness  <i>If participant(s) cannot sign</i>	<i>In signing I confirm the participant(s) named above have been fully informed about the research, have been able to ask questions, and consent freely.</i>

## Appendix II: Survey



University of  
**Nottingham**  
UK | CHINA | MALAYSIA

# The Influence of Usable Security on Security Culture Survey

---

Welcome to our study

### Information Sheet

This study aims to determine the potential influence of the usability of cybersecurity technologies and processes on organisational security culture. We are interested in gathering your insights based upon your own experiences of dealing with cybersecurity and how usability affects your behaviour while doing so.

This research will be conducted in two phases:

- In Phase 1, you are asked to complete this survey to help us understand your perceptions of the usability of cybersecurity and its impact on your organisation.
- Phase 2 of the research will involve a follow-up interview. This phase aims to help us understand users' behaviours and attitudes towards the usability of security in your workplace.

You can choose to participate in either Phase 1 only, by just filling in this questionnaire, or both Phases, by filling in this questionnaire and providing your contact details at the end so that we can contact you to arrange an interview.

Participating in the survey involves the use of an online data storage platform, but the collection process does not seek to gather any sensitive information about you or your organisation and so the risk is minimal. We will store the data collected, which is anonymised, on the OneDrive server of the University of Nottingham. If you choose to provide your contact information during Phase 1, it will solely be used to invite you to join Phase 2. The overall insights from both Phases will be used to help identify areas that

may promote positive security culture.

Also, to help understand the key terms used in this survey, we would like to provide some brief definitions for your reference:

- **Cybersecurity usability issues** are difficulties that users encounter while using security-related tools or systems. These can include issues such as lengthy security procedures that hinder productivity, confusing user interfaces, or difficulty remembering how to do things (e.g. complex passwords).
- **Cybersecurity actions** refer to user actions to safeguard systems and data, such as performing regular software updates, strong passwords, data backup, and identifying suspicious emails or messages.
- **Cybersecurity technologies** include tools, software, and hardware solutions such as firewalls, antivirus software, and encryption mechanisms that protect systems, networks, and data.
- **Cybersecurity procedures** include documented processes and guidelines that help address security risks and maintain a proactive security posture. This includes elements such as access control policies and security training and awareness sessions.

This study has been approved by the University of Nottingham's School of Computer Science Ethics Committee. The reference number for this approval is **CS-2022-R32**.

Wesam Fallatah

Wesam.Fallatah@nottingham.ac.uk

## Consent to participate

As a participant in this study, you should...

- understand that your participation is voluntary
- understand the aims and objectives of the research
- understand what the research requires you to do
- accept the risks of participation
- understand what data will be collected and the purposes for which the data will be used
- understand safeguards will be put in place to protect your data and your legal rights
- understand that you will not be identified unless the use of identifiable data has been requested

2 / 20

- understand that you can withdraw at any time without explanation
- understand that once you have completed the study and submitted your answers, it will not be technically possible to withdraw the data

1. By clicking below, I confirm that I have read the above and consent to participate \*  
*Required*

☐ Yes

3 / 20



## General information

### About you

2. What is your age?

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65 or above

3. What gender do you identify as?

- ☐ Male
- ☐ Female
- ☐ Prefer not to say
- ☐ Other

3.a. If you selected Other, please specify:

4. Highest level of education completed:

- ☐ High school or less

- ☐ College/Diploma
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctoral degree
- ☐ Professional degree
- ☐ Other

4.a. If you selected Other, please specify:

5. Do you have any disabilities that impact your ability to use technology?

- ☐ Yes
- ☐ No
- ☐ Prefer not to say

5.a. Please specify:

6. What is your role/position in your organisation?

- ☐ Director / Executive / C-level role
- ☐ Managerial role (including supervisory and middle management)
- ☐ Operational role (including admin assistants, analysts, specialists, and technicians)
- ☐ Other

6.a. If you selected Other, please specify:

6.b. Please select what applies to you from the following:

- ☐ I work in the cybersecurity department
- ☐ I work in the IT department, including the cybersecurity team if applicable
- ☐ I work in a department other than the cybersecurity or IT department
- ☐ Other

6.b.i. If you selected Other, please specify:

### About your organisation

7. What is the primary industry of your organisation?

- ☐ Healthcare and social assistance
- ☐ Information technology and communication
- ☐ Energy supply
- ☐ Water supply, waste management, and remediation services
- ☐ Education
- ☐ Finance and insurance
- ☐ Construction
- ☐ Manufacturing
- ☐ Agriculture
- ☐ Transportation
- ☐ Real estate/rental and leasing

- ☐ Arts, entertainment, and recreation
- ☐ Accommodation or food services
- ☐ Public administration
- ☐ Other

7.a. If you selected Other, please specify:

8. What is the geographic region of your organisation?

- ☐ North America
- ☐ South America
- ☐ Europe (including UK)
- ☐ Asia
- ☐ Middle East
- ☐ Africa
- ☐ Australia/Oceania
- ☐ Other

8.a. If you selected Other, please specify:

9. What is the size of your organisation (number of employees)?

- ☐ Less than 50
- ☐ 50-249

- ☐ 250-499
- ☐ 500-999
- ☐ 1000 or more

## Security culture in the organisation

10. To what extent do you agree that shared attitudes, behaviours, and beliefs about cybersecurity within your organisation promote shared responsibility for maintaining cybersecurity?

- ☐ Strongly agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly disagree
- ☐ Don't know / unable to answer

11. How confident are you in

	Very confident	Confident	Neutral	Unconfident	Very unconfident	Don't know / unable to comment
Your understanding of cybersecurity principles and best practices	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Following cybersecurity requirements in your organisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace



12. Please feel free to offer any additional thoughts or feedback that you feel would be relevant to your organisation's security culture. *Optional*

## Usability of cybersecurity

13. How often do you encounter usability issues while using cybersecurity technologies or following cybersecurity procedures in your organisation?

- ☐ Very often
- ☐ Often
- ☐ Occasionally
- ☐ Rarely
- ☐ Never

14. How likely would you do the following if you found a cybersecurity action difficult to perform

	Very likely	Likely	Neutral	Unlikely	Very unlikely	Don't know / unable to comment
Ignore it to complete my wider task	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Stop the task as I can't complete the action	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Try my best to perform the action and complete the task	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Find my own ways around the action	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Complain/report to the responsible person or team (e.g., my supervisor, the IT department, or the cybersecurity team)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Seek help from my colleagues



15. Have you ever had to bypass a cybersecurity technology or procedures due to usability issues?

☐ Yes

☐ No

15.a. Please describe the situation briefly:

Your answer should be no more than 1000 characters long.

16. To what extent do you agree or disagree with the following statements:

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Don't know / unable to comment
I feel that the security actions in my organisation are easy to understand	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I feel that the security actions in my organisation are easy to perform	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

I feel that the security actions in my organisation strike a good balance between security and usability	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I can easily report any potential security issues or breaches that I may come across	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organisation provides adequate support for employees to understand and perform effective security actions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17. Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?

- ☐ Yes
- ☐ No

13 / 20

17.a. Please explain the nature of the difficulty you encountered:

Your answer should be no more than 1000 characters long.

17.b. Have the difficulties been resolved to your satisfaction?

☐ Yes

☐ No

18. Please feel free to offer any additional thoughts or feedback that you feel would be relevant to the usability of cybersecurity in your organisation. *Optional*

## Usable security and security culture

19. To what extent do you agree or disagree with the following statements:

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Don't know / unable to comment
Usable cybersecurity would encourage me to take sensible decisions while following cybersecurity requirements put in place	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Usable cybersecurity would contribute to increased compliance with cybersecurity policies among my colleagues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The emphasis on following easy-to-use cybersecurity will make me more likely to report potential cybersecurity issues	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The usability of cybersecurity will improve users' security behaviours in the organisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The emphasis on the usability of cybersecurity will contribute to a stronger sense of responsibility for maintaining the security in my organisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

20. Please feel free to offer any additional thoughts or feedback relevant to the relationship between usable security and security culture. *Optional*

## Measuring factors influencing security culture

21. What would be the main drivers for you to follow cybersecurity best practices in your organisation (please select all that apply)?

- ☐ Finding cybersecurity actions easy to perform
- ☐ Management and leadership enforcement
- ☐ Complying with the national regulatory or corporate requirement
- ☐ Understanding the risks associated with not following the best practices
- ☐ Attending more cybersecurity training courses
- ☐ Attending more security awareness sessions
- ☐ Other

21.a. If you selected Other, please specify:

22. What would prevent you from following cybersecurity best practices in your organisation (please select all that apply).

- ☐ Lack of convenience and the complexity of performing cybersecurity actions
- ☐ Lack of management and leadership support to comply with cybersecurity requirements
- ☐ Lack of cybersecurity training
- ☐ Lack of raising awareness for cybersecurity
- ☐ I think cybersecurity issues are the cybersecurity department's job. They should deal with them
- ☐ I cannot adopt the same security requirements in my own device as I do on the organisation's devices
- ☐ Nothing would

17 / 20

☐ Other

22.a. If you selected Other, please specify:

23. Do you have suggestions for how the usability of cybersecurity could be further improved in your organisation?

☐ Yes

☐ No

23.a. Please provide your suggestion(s) here:

24. Please feel free to offer any additional thoughts or feedback relevant to factors influencing security culture. *Optional*

## Invitation to the 2nd part of the study

25. We are interested in following up to get further insights. If you would be willing to be contacted for an interview that would last ~20 minutes to discuss areas that may promote positive security culture in organisations, please type your email in the box below. If you are not interested, please feel free to click finish to end this survey. *Optional*



## Thank you for taking part in the study!

Your contribution is valuable and appreciated.

If you have concerns or if you would like to view a summary of the results of this study, please email Wesam Fallatah at [Wesam.Fallatah@nottingham.ac.uk](mailto:Wesam.Fallatah@nottingham.ac.uk)

---

## **Appendix III: Interview Plan**

### **1. Interview Structure:**

The planned duration for each interview is approximately 20 minutes.

The interview questions are built upon the participants' responses from the initial questionnaire to allow for more elaboration. In addition, the following questions were brought to the conversations:

- a) Do you feel that cybersecurity usability issues affect your overall productivity and effectiveness in carrying out your day-to-day tasks?
- b) Can you tell me if there are any specific cybersecurity actions or processes that you find more challenging than others due to issues related to usability? How would you suggest improving them?
- c) Does management and leadership support affect the implementation of usable security measures? What actions have been taken or could be taken in this regard?
- d) What strategies can be employed to effectively balance usability and cybersecurity measures in your organisation?
- e) Do you believe the usability of cybersecurity measures impacts your ability (or your colleagues') to comply with security expectations or good practices?
- f) Can you share an example from your organization where the usability of cybersecurity has positively or negatively impacted security culture?
- g) Considering your organisation's geographical location, are there cultural or regional factors influencing security culture and the usability of cybersecurity? How can these factors be considered in improving security practices?

### **2. Recruitment and Scheduling:**

Participants were enabled to choose their preferred date and time for the interview through a scheduling calendar service. An initial email was sent to participants who showed interest in taking part in the interview phase. The email provided an overview of the study's purpose, the importance of their contribution, and a brief explanation of the interview process.

The email was as follows:

**Subject:** Invitation to Participate in the Second Phase of “The Influence of Usable Security on Security Culture” Study: Semi-Structured Interview

Dear Participant,

I hope this email finds you well. We sincerely appreciate your participation in the study’s first phase, where you completed the questionnaire. Your input has been invaluable, and we appreciate your continued involvement in the second part of our research. This phase will involve a one-on-one interview that will provide us with a deeper understanding of whether usability positively or negatively affects user behaviour and the wider security culture in your organisation.

The interview is expected to last around 20 minutes and will be conducted via Microsoft Teams. Building upon your responses from the initial questionnaire, the interview will offer an opportunity for more elaboration on your perspectives. Additionally, we will discuss related questions to gain a better view of the topic.

By indicating your availability through this [link](#), you are giving your consent to participate in the interview phase. Your confidentiality is of utmost importance to us, and rest assured that your responses will be anonymised and handled in accordance with the University of Nottingham’s ethical considerations.

Thank you once again for your commitment to our research. We eagerly await the opportunity to engage in discussions with you.

Best regards,

Wesam Fallatah  
PhD Candidate at the University of Nottingham  
Wesam.Fallatah@nottingham.ac.uk

### 3. Follow-Up and Gratitude:

A thank-you email also was sent to participants after the interview, expressing appreciation for their time and insights. Also, if a participant requires any relevant updates about the study’s progress and outcomes, a separate email was sent with the required information.

## **Appendix IV: Feedback for the validation process**

### **E1:**

I reviewed the framework. Well done :)

My answer for three questions:

- 1- The framework presented in the search results aligns with key issues and insights about the usability of cybersecurity shared during interviews. It emphasises user-centric design, highlighting the importance of tailoring security application to user preferences and behaviours through personalisation and adaptive awareness and training programs. This framework ensures that cybersecurity measures are both effective and user-friendly, addressing concerns raised during interviews about usability challenges.
  - 2- No. The framework is clear and well designed. The developed framework not only addresses current usability challenges but also can be adapted to future needs and technological advancements.
  - 3- I believe that the framework holds significant practical value for organisations by providing a structured approach to managing cybersecurity risks. It helps organisations identify, assess, and prioritise cybersecurity risks. The framework can be adaptable to organisations of all sizes and sectors. It aids in achieving compliance with regulatory requirements and reducing potential legal risks. It facilitates communication about cybersecurity risks across different organisational levels, fostering a unified understanding of security risk and governance.
- 

### **E2:**

The Usability-focused Framework for Security Culture uses a human-centered approach to improve enterprise cybersecurity culture:

It focuses on usability, adaptive mediation strategies, and real-time reinforcement with the help of security ‘nudges’.

It packages best practices in an actionable format, progressing sensibly. The framework could deliver results in reinforcing bottom-up organizational security culture by addressing behaviors at the individual employee level.

#### **Comments:**

1. The ‘initial assessment of how people behave around security practices’ may need more detailed guidance and examples on how to spot pain points and usability issues.
  - adding more examples and visuals could make it easier for organizations to understand and adopt the framework.
2. It looks like a flexible security culture framework, but a selection of practical examples backed with case studies would improve it and make it more relatable or generalizable since organizations can be quite diverse.

3. How well does it work in different-sized enterprises? Depending on the organization's size, for example, SMEs might need extra help scaling the phases.
4. Metrics that keep track of security performance, for example, (fewer) phishing incidents, employee experience (frustrations, ease of use etc), or (better) compliance ratings, could help measure the impact of introducing the framework as part of an organization's security policy (measurable impact statements).
  - Visuals (flowcharts etc) could help deliver the metrics
  - Guidance on making use of emerging technologies and metrics safely (ie, including behavioral analytics in the framework of a particular organization)
    - 'micro-monitoring leads to macro-level inefficiencies' (be pragmatic and consider employee freedom + unit costs)
5. A list of strategies for addressing unique/special needs for employee roles (user profiling) with some examples might go a long way to make the framework more complete.
  - Consider timed (ie. quarterly) feedback sessions to try and future-proof security culture but also to keep security measures compatible with day-to-day functions (ie a new security measure causes issues, but staff dont know - the feedback could help here?)
  - How will new hires pick up the security practices compared to senior staff? Guidance on onboarding new hires into established security practices would be helpful to consider, in particular, keeping in mind their learning curve compared to that of senior staff

***Does the framework reflect the key issues and insights you shared during the interview about the usability of cybersecurity?***

I barely remember the interview - it was a long time ago. I tried to review it as a layman anyway.

But, the framework does address issues and insights about usability in cybersecurity by prioritizing intuitive, user-friendly practices, adaptive strategies, and real-time reinforcement. It seems well aligned with human-centered principles in general.

***Are there any areas in the framework that you believe should be clarified or improved?***

I broke down the areas for improvement in the comment section above.

In summary, areas for improvement include providing more detailed guidance for the initial assessment phase, incorporating practical examples or case studies to improve relatability, and ensuring scalability across diverse organizational sizes.

Metrics to measure impact, supporting visuals of metrics, and strategies for addressing unique employee roles will help elevate the practical value of the framework by helping to reduce the cognitive load on staff trying to adopt the framework.

***In your opinion, what is the practical value of this framework for organizations?***

Its actionable approach to fostering a strong security culture.

Putting individual behaviors in the spotlight while keeping usability in mind could bridge the gap between technical measures and employee adoption (provided employees are okay with the approaches). It could be a valuable tool for organizations who want to improve their (cyber)security practices

### **E3:**

#### **Does the framework reflect the key issues and insights shared during the interview about the usability of cybersecurity?**

Overall, I think the framework does a good job of addressing the main usability issues. Focusing on usability as a first step shows an understanding that people are more likely to follow security measures if they're simple (though that's a big assumption honestly --->> even if it's "more likely" --->> I'd say it's still an assumption! So I'd say since you're basing a strategy on this assumption, I'd suggest being cautious or maybe even backing it up somehow! I'd know how but maybe that's for you to figure out 😊 maybe with psychology/human behaviour studies showing that people are more compliant when tasks are simple? It'd add sort of evidence-based angle/justifications to this assumption. This might not be from cybersecurity literature but that's fine, it could be an interesting argument to build on!

#### **Are there any areas in the framework that you think should be clarified or improved?**

It's unclear to me what "adapting" would look like in practice? Seems highly dependent on company culture? Also on the idea of adjustments based on feedback, maybe consider including specific settings/scenarios of how mediating strategies could be tweaked based on feedback? Or how organisations could measure if an adjustment actually makes things easier or more secure? Are you planning to run any simulations or sensitivity analysis to explore this? Maybe think about referencing reinforcement learning (a big area in ML) where feedback loops between ML-based agents and human input create strong systems. There's a lot of research on RL that might offer you some sort of evidence-backed methods for feedback strategy/mechanism/loop! Maybe an automatic RL-based feedback loop could be a reasonable/practical/inexpensive way of doing it? I really don't know :)

Also, "non-intrusive" can mean different things to different people/users depending on the organisation's culture? So it might be worth clarifying! Should organisations think of "non-intrusive" in a way that fits their specific culture? Or how might they approach this?

#### **In your opinion, what is the practical value of this framework for organisations?**

If I were a manager looking at applying this framework, the first thing I'd say is that these strategies/steps/phases are already happening within the company? So what's the new about your framework? What would make me interested in implementing it? Also, how would you measure progress and make necessary adjustments? Seeing an increase in password compliance doesn't really mean the company's security is strong! It's tricky to claim that "secure behaviour has become the norm" without defining what "the norm" is in this context? If I were you, I'd be extra careful with the wording here.

Final comments: if I were reviewing this study, I'd want to know how this framework stacks up against others in the literature? What are the limitations of other frameworks? Are they mostly theoretical? Or have any been implemented with evidence-based results?

Also, I was expecting a bit more detail in the framework, the current version feels quite broad/generic/ maybe even intuitive to many. I'm not an expert in your field, but it seems like there's room to make it more specific here and there!

How will you validate this framework? I'm not sure I fully understand how the ABC case study covers every part of the framework. Are you planning on running some simulations or anything that would test different scenarios? How will you ensure it's generalisable? I do not know much about your data but your study participants, including me, might not cover the whole spectrum? Especially if you've got a lot of participants from niche areas like academia (academics/PhD students are really different from the general population, so we're highly unlikely to represent a normal distribution! If that's the case, then your samples are skewed

towards academics (or any other group), it could introduce sampling bias and skewness, which of course limiting generalisability, as the distribution of security behaviours may not reflect the mean/variance/normal distribution you'd expect in a broader workforce. That's something to think of/acknowledge/discuss somewhere in your study.

---

**E4:**

1. Does the framework reflect the key issues and insights you shared during the interview about the usability of cybersecurity?

Yes, the framework effectively captures the importance of usability in enhancing cybersecurity practices. The inclusion of usable security as the first step aligns closely with the concerns regarding employee adoption and ease of use. The focus on security nudges and mediating strategies also reflects a human-centric approach, addressing the need for practical, real-time guidance and tailored strategies that adapt to organizational needs.

2. Are there any areas in the framework that you believe should be clarified or improved?
  - Feedback Integration: Ensure employee feedback is clearly acted upon and visibly incorporated into updates to security measures.
  - Mediating Strategies: Provide specific examples or case studies showing how these strategies adapt to meet changing organizational needs.
  - Assessment Tools: Include examples of tools for the annual security culture review to help organizations measure and track progress effectively.
3. What is the practical value of this framework for organizations?

The framework's practical value lies in its structured approach, which emphasizes both usability and continuous improvement. This ensures that organizations can:

- Foster an employee-friendly environment that encourages compliance with cybersecurity practices.
  - Continuously adapt to evolving cybersecurity threats by maintaining a dynamic and responsive security culture.
  - Minimize resistance to security measures by making them intuitive and user-focused. The framework is not just theoretical but also applicable to real-world organizational contexts.
- 

**E5:**

1. Does the framework reflect the key issues and insights you shared during the interview about the usability of cybersecurity?

Sorry, that I do not remember exactly what we discussed, but as far as I remember I think it does reflect the key issues in a satisfactory manner.

2. Are there any areas in the framework that you believe should be clarified or improved?

In the Framework document you stated: *“The framework presented in Figure 6.2 focuses on prioritizing usability and strategically integrating mediating strategies and security nudges to effectively influence employee behavior, leading to a strong security culture.”* I do not understand how the framework- as you asserted- prioritize usability. I mean it is not shown in the framework and I might think that security nudges might have priority.

It might seem like I'm focusing on the nitty-gritty details, but as someone interested in modeling, I'm curious about the reason for choosing different shapes in your framework. For example, you use oval shapes for Usable Security and Security Culture, but rectangular shapes for Mediating Strategy and Security Nudges.

3. In your opinion, what is the practical value of this framework for organizations?

I agree that your framework could have practical value for organizations specially where you show the mutual impact of information security culture and information security behaviour on each other. However, I can't fully discuss its potential since I don't have access to a complete explanation of the framework. For example, under "mediating strategies," I'm unclear about the main difference between effective communication and tailored training. If by effective communication you mean information security policies, tailoring them could also influence employee training and even facilitate tailored training.

Additionally, management support seems crucial for both effective communication and tailored training. It might be worth considering whether management support should be presented as an overarching concept in the framework to highlight its impact on all parts of this component or, I may have misunderstood its role entirely.

---

#### **E6:**

1. Does the framework reflect the key issues and insights you shared during the interview about the usability of cybersecurity?

I'm not sure, as I could not understand how the framework operates. The document refers to some framework in Figure 6.2, however there is no Figure 6.2 in the document. I kept wondering if the framework is Figure 1 or 2, and if its Figure 1 it's based on some preconceived notions. The first step is usable security, what do you mean by usable security? how do you achieve that? it's the real big challenge. Another question is how nudges are different from intervention strategies.

Figure 2 again is a black box and it is hard to guess what happens and how. the propositions make sense but how you achieve that is a real question.

2. Are there any areas in the framework that you believe should be clarified or improved? Please refer to the comments above, the areas of improvement have been identified.

3. In your opinion, what is the practical value of this framework for organizations? With a lack of clarity on operation, NO.

#### **E7**

##### **Here is my feedback about the framework:**

- I appreciate that the materials and video that you have created make the framework simple to understand and easy to follow. I think overall, the framework provides good high level guidance for an organization to implement practices to improve their security culture.
- For step 1: usable security - I recognize the importance for this being the first step, my only concern is the existing adoption of usable security within the cyber security



field. I still have a lot of colleagues in cyber who I keep in touch with and they are either not aware of or have an interest in human-centered security. I think it would be good to expand on what is usable security and why it is important. It would also be good to include resources on how usable security can be applied.

- For the implementation phase - I think it would be useful to have a baseline for the assessment. What should the assessment look like? Can you provide an example? What topics should be covered? How should the assessment be conducted? I think people need an understanding of what is a good or bad result for the assessment. Maybe providing examples like looking at metrics and/or violations that point to a weak security culture (ex. password violation frequency, etc). Just some pointers to help them get started and build their own assessment. Or an assessment template that they can use and implement for their organization.
- Similarly for phase 2 it would be good to see examples of what objectives and action plans could look like. What do they cover? What tools does an organization need to implement these different phases?

Overall, I think your framework is strong, it just needs more tools to help people understand how they can implement it.

---

## **E8**

1) You mention in the video / document that this is aimed at employees, are employees distinct from the leadership team or is this applicable to everyone? It is really difficult to drive a culture if those at the top demonstrate conflicting attitudes, in my experience.

2) I'd suggest trying to work with an organisation's HR / culture team to see how you can align your framework with what they're doing. I think security culture would have a greater impact if it formed part of the organisation's wider strategy. You've made some mention of it here, I just wanted to highlight my thoughts / support for this topic!

3) It may be worth mentioning the types of things that should / could be monitored throughout the three phases

---

## **E9**

### **Feedback on the Usability-Focused Security Culture Framework**

#### **Strengths**

##### **Human-Centered Focus:**

The emphasis on usability and behavior-driven strategies is a useful addition to cybersecurity practices, addressing gaps in existing frameworks that often overlook user experience. This aligns well with a growing recognition that security culture must work with people, not just technology.

##### **Behavioral Interventions:**

Integrating concepts like security nudges and mediating strategies offers actionable insights to guide user behavior toward secure practices without being disruptive of their work or

overly intrusive. These elements reflect a more nuanced understanding (at least more nuanced than CIS or NIST) of how habits form within organizations.

### **Iterative Improvements:**

The framework's commitment to ongoing feedback and adaptability ensures it can remain relevant and effective as organizational needs and threat landscapes evolve.

### **Concerns and Opportunities**

#### **Demonstrating the Problem:**

For this framework to resonate with organizational leaders, especially CISOs or security program managers, it needs to clearly articulate the shortcomings of existing security measures. Where and why are human-centered failures occurring? Presenting data or evidence (e.g., metrics on breaches caused by usability issues, case studies highlighting user frustrations) would underscore the urgency of adopting a new approach.

#### **Compelling Value Proposition:**

To compete with established frameworks like CIS Controls or NIST CSF, this framework must demonstrate measurable benefits. What security outcomes—such as reduced incidents, improved compliance rates, or cost savings—can organizations expect when they address human-centered challenges? Concrete data supporting these claims will be critical.

#### **Integration with Existing Frameworks:**

Many organizations are already committed to established frameworks. Positioning this framework as complementary to existing standards, rather than a replacement, could ease adoption. For example, how can it enhance the implementation of CIS Controls or NIST CSF by improving user engagement and compliance?

### **Suggested Improvements**

#### **Data-Driven Evidence:**

Include metrics or research findings showing how usability challenges in current security measures lead to real-world failures (e.g., breaches, noncompliance). Then, quantify how a human-centered approach has successfully addressed these issues in pilot studies or case studies.

#### **Actionable Tools:**

Provide templates, examples, and quick-start guides to help organizations easily implement the framework. This would demonstrate practicality and reduce barriers to adoption.

#### **Alignment with Business Goals:**

Emphasize how improving usability and security culture can align with broader organizational objectives, such as reducing incidents, improving performance and safeguarding reputation. This framing might appeal more to decision-makers.

## **Conclusion**

The "Usability-Focused Security Culture Framework" introduces important concepts that highlight the role of human behavior in cybersecurity. However, for leaders to adopt it instead of—or alongside—established frameworks, it must provide compelling evidence of the failings of current approaches, demonstrate measurable improvements, and position itself as a practical, complementary solution. Strengthening these areas will ensure the framework's impact and adoption in real-world contexts.

## Appendix V: Posters & Flyers

- Poster during HAISA conference 2023



**University of Nottingham**  
UK | CHINA | MALAYSIA

# The Influence of Usable Security on Security Culture

**Wesam Fallatah, Steven Furnell and Ying He**  
School of Computer Science, University of Nottingham

### Project Objectives

Investigating the impact of usable security and its influence upon healthy organizational security culture

- Refining the understanding of usable security
- Characterizing the linkage between usable security and security culture
- Identifying where usable security can promote a positive security culture and providing practical insights that organizations can use to enhance their position



### Usable Security Framework



### Data Collection

- Two stages of data collection:
  1. a questionnaire to understand users' perceptions of cybersecurity usability and its impact on their organization
  2. follow-up interview to understand users' behaviors and attitudes towards security usability in the workplace
- Participants can choose to participate in Phase 1 only or both phases

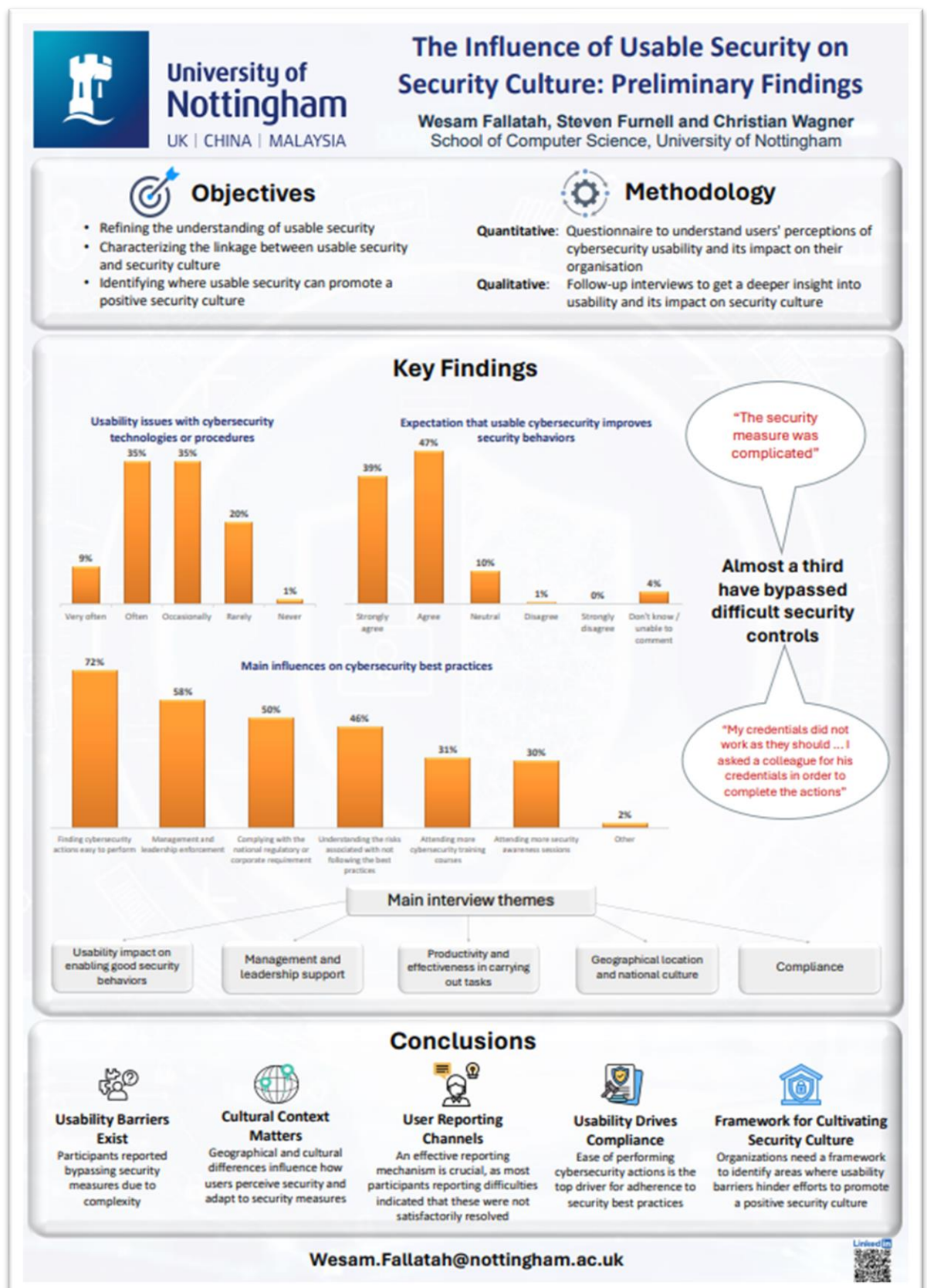


### Interested in being involved?

Please scan the QR Code, take a flyer, or email  
[Wesam.Fallatah@nottingham.ac.uk](mailto:Wesam.Fallatah@nottingham.ac.uk)


- [illegible]

- Poster during RISCs Annual Conference 2024






- Poster during Step into Cyber events 2024




University of Nottingham  
UK | CHINA | MALAYSIA




## The Influence of Usable Security on Cyber Security Culture

Cybersecurity extends beyond technical measures; it involves understanding **human behaviour**, motivations, and vulnerabilities while interacting with digital technologies




Why do we study human aspects of cybersecurity?



- Reduce human errors and vulnerabilities
- Increase awareness and adoption of security practices
- Strengthen organizational resilience against cyber threats
- Cultivate a cybersecurity-conscious society (security culture)

Usability



Security

**Usable Security**

Focuses on designing systems that prioritize users and their experience without compromising security

Complex Password

"F@7b8p2#wXr\$9Lm!"


Passphrase

"likeMyCatNamedCyber!"

Which is easier to memorize and type (i.e., more usable)?

Usable security enhances user experience and encourages adoption of secure practices, thus shaping a culture

[Wesam.Fallatah@nottingham.ac.uk](mailto:Wesam.Fallatah@nottingham.ac.uk)



- **Poster for the East Midlands Cyber Security Communities of Support 2024**

