

**DEVELOPMENT OF A NIST CYBERSECURITY FRAMEWORK-BASED
USABLE SECURITY COMMUNITY PROFILE: INTEGRATING USER
EXPERIENCE INTO ORGANIZATIONAL CYBERSECURITY PRACTICES**

A Dissertation Presented for the
Doctor of Philosophy
Degree
The University of Tennessee, Knoxville

Shreenandan Rajarathnam

December 2025

Copyright © 2025 by Shreenandan Rajarathnam

All rights reserved.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my advisor & dissertation chair, Professor Vandana Singh, for her unwavering guidance, mentorship, and support from day one. Her insights, encouragement, and patience have been instrumental throughout every stage of this research journey. I would also like to thank my committee members: Professor Devendra Potnis, Professor Laura Miller, and Professor Doowon Kim, for their insightful feedback, engaging discussions, and steady support throughout this process.

I extend my sincere appreciation to my former colleagues, clients, and professional connections who graciously participated in the surveys and interviews, and to all who helped share my study within their professional network. This work would not have been possible without their generous contributions of time and perspective.

To my family: my mother Dr. Uma Rajarathnam, my wife Allegra Signorino, my father Dr. Rajarathnam Nallusamy, and my brother Shivanandan Rajarathnam, and our beloved animal companions Midnight, Misha, and Smokey - thank you for your endless love, patience, and encouragement. Your presence and support, in every form, made this achievement possible.

Lastly, I would like to thank Dr. Abebe Rorissa, the UTK SIS Director, the UTK CCI leadership, and Ms. Margaret Taylor and the administrative team for their continued support and for creating an environment that made this work possible.

ABSTRACT

This dissertation develops a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v2.0-based Community Profile for the field of Usable Security, with a focus on integrating User Experience (UX) considerations into organizational cybersecurity practices. Organizations continue to face persistent UX challenges with cybersecurity tools & platforms, policies & standards, and role-specific training initiatives, which can undermine the effectiveness of security measures and practitioner adoption.

The study was guided by three (3) main Research Questions: **RQ1:** What are the standard elements of a NIST CSF Community Profile?; **RQ2:** What are the UX challenges faced by Cybersecurity/IT teams in an organization?; **RQ3:** What are the UX elements that are critical for organizations from a Usable Security standpoint, and how can they be integrated into a NIST CSF Community Profile?

To address these questions, the research employed a mixed-methods design across four (4) phases. Phase I involved developing a generalizable template for NIST CSF Community Profiles (**Appendix E**) based on available examples. Building on a pilot study (Phase II, **Appendix F**), Phase III involved a structured online survey of 110 cybersecurity professionals across the US, exploring their experiences with tools & platforms, policies & standards, and training. Phase IV consisted of follow-up interviews with 26 practitioners, which provided deeper insight into recurring cybersecurity UX

issues. Thematic analysis of survey and interview data identified key challenges such as complexity, integration gaps, policy readability and update cycles, training fatigue, and so forth. Drawing on these findings, this dissertation presents the first NIST CSF v2.0-based Usable Security Community Profile. The Profile outlines practitioner-reported issues, actionable recommendations, and informative references drawn from both scholarly research and industry guidance. Expert reviews with four (4) practitioners were used to validate the priorities and recommendations.

The study makes contributions on three (3) levels: theoretically, by addressing a gap in usable security research and situating UX within a widely adopted cybersecurity framework; methodologically, by documenting a replicable process for developing CSF-based Community Profiles; and practically, by delivering a Profile that organizations can adapt to improve the UX of their cybersecurity tools, policies, and training programs.

Keywords: Usable Security, NIST Cybersecurity Framework (CSF) v2.0, User Experience (UX), Organizational Cybersecurity, Community Profile

TABLE OF CONTENTS

Chapter One Introduction and General Information.....	1
Introduction.....	1
Problem Statement & Study Objective	2
Significance of the Study	3
Theoretical Framework.....	5
NIST CSF	5
Definitions of Key Terms	8
Cybersecurity	8
User Experience (UX).....	8
Usability	9
Chapter Two Literature Review.....	12
Overview.....	12
Scope, Gaps, and Contributions of Prior Literature.....	12
SLR Methodology.....	15
Data Collection	15
Inclusion & Exclusion Criteria	16
Screening / Filtering Process	18
Data Analysis	21
SLR Results and Discussion	22
Overview and Current Research Landscape	22

Prevalent Themes in Cybersecurity & UX Research.....	25
Gaps in Current Literature and Potential Future Research Opportunities	35
Chapter Three Materials and Methods.....	37
Overview.....	37
Research Questions (RQs)	37
RQs and Sub-RQs	37
RQs Breakdown & High-level Approach	40
Phase III: Surveys	45
Approach.....	45
Study Population and Criteria	45
Instruments & Procedures.....	47
Analysis.....	48
Phase IV: Interviews	48
Approach.....	48
Study Population and Criteria	49
Instruments & Procedures.....	50
Analysis.....	51
Post-Phase IV Analysis, Expert Review and Iteration.....	54
Approach.....	54
Community Profile Elements and Integration of Practitioner Insights.....	55
Expert Review.....	56
Iteration	57

Timeline and Budget.....	58
Timeline	58
Budget & Funding Source	60
Ethical Considerations	60
Approach.....	60
Chapter Four Results and Discussion	62
Overview	62
(Sub-RQ2c) Theme 1: Tools & Platforms	63
Procurement & Integration (Tools & Platforms Sub-theme 1).....	64
Consolidation vs. Best-of-Breed (Tools & Platforms Sub-theme 2)	73
Adoption & Usage	75
Usability	77
Training & Vendor Support	84
UX Challenges	85
Workflow Efficiency (Tools & Platforms Sub-theme 3).....	88
Performance & Reliability (Tools & Platforms Sub-theme 4)	96
UI Quality & Impact of Changes (Tools & Platforms Sub-theme 5)	97
Documentation, Learnability, and Onboarding (Tools & Platforms Sub-theme 6)	100
Feedback Loops & Issue Tracking (Tools & Platforms Sub-theme 7).....	102
Balancing Strong Security with Operational Realities (Tools & Platforms Sub-theme 8)	104
(Sub-RQ2d) Theme 2: Policies & Standards	106

Accessibility & Centralization (Policies & Standards Sub-theme 1)	107
Clarity & Understandability (Policies & Standards Sub-theme 2)	114
Guidance & Support	116
Challenges.....	117
Compliance & Framework Alignment (Policies & Standards Sub-theme 3)	119
Feedback, Enforceability, and Escalation (Policies & Standards Sub-theme 4)	123
(Sub-RQ2e) Theme 3: Training & Awareness	125
Availability	126
Cadence & Frequency (Training & Awareness Sub-theme 1)	131
Role-Specific Training Approach (Training & Awareness Sub-theme 2).....	134
Effective Training Sources (Training & Awareness Sub-theme 3)	136
Challenges (Training & Awareness Sub-theme 4)	137
Summary of Key Findings	143
Chapter Five NIST CSF-Based Usable Security Community Profile	148
Overview.....	148
Community Profile Structure & Components.....	148
NIST CSF 2.0 Core Categories and Outcomes.....	149
Relevant Artifacts	151
Issues - from Data Analysis	151
Priority & Rationale.....	152
Recommendations & Considerations.....	153
Informative References	154

Chapter Six Conclusions and Recommendations	168
Overview	168
Applying the Usable Security Community Profile	169
Contributions of the Study	170
Theoretical Contributions	170
Methodological Contributions	171
Practical Contributions.....	172
Limitations and Future Directions	173
Limitations	173
Future Research Directions.....	175
References.....	177
Appendices.....	188
Appendix A: Invitation Letter.....	188
IRB Application Details.....	188
Disclaimer	188
Draft Initial Invitation Email	188
Draft Follow-up Email.....	191
Appendix B: Draft Survey Instrument.....	193
IRB Application Details.....	193
Disclaimer	193
Default Question Block (in Qualtrics)	193
Demographics Info Block (in Qualtrics).....	194

Roles & Responsibilities Block (in Qualtrics).....	195
Cybersecurity UX Part I (Tools & Platforms) Block (in Qualtrics)	196
Cybersecurity UX Part II (Policies & Standards) Block (in Qualtrics)	199
Cybersecurity UX Part III (People & Training) Block (in Qualtrics)	201
Interview Interest Block (in Qualtrics)	202
Appendix C: Informed Consent Form	204
IRB Application Details.....	204
Disclaimer	204
Informed Consent Verbiage.....	204
Appendix D: Draft Interview Questions	211
IRB Application Details.....	211
Disclaimer	211
Opening statement example (after introductions).....	211
Roles & Responsibilities.....	212
Cybersecurity UX Part I (Tools & Platforms)	212
Cybersecurity UX Part II (Policies & Standards)	213
Cybersecurity UX Part III (People & Training)	213
Interest in Providing Feedback for the Usable Security Community Profile)	214
Appendix E: NIST CSF (v1.1) Profile Template.....	215
Overview	215
Approach & Outcome	215
Study Significance	217

Appendix F: Pilot Phase Summary	221
Overview	221
Introduction and Context	221
Pilot Study Methodology	222
Results Summary	224
Tools & Platforms	224
Policies & Standards	226
Training & Awareness	226
Practitioner Feedback & Study Instruments' Refinement	227
Pilot Study Conclusion	228
Appendix G: Codebook	229
Overview	229
Vita.....	255

LIST OF TABLES

Table 2.1. First round screening / filtering outcome - screening based on TI, AB, and AK fields. Adapted from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	19
Table 2.2. Second round screening / filtering outcome - screening based on manual review of full-text (PDF) articles. Adapted from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	21
Table 2.3. Distribution of records by publication type, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	23
Table 2.4. Top five (5) journals in the convergence of cybersecurity and UX research, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	23
Table 2.5. Top five (5) journals in the convergence of cybersecurity and UX research, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	24
Table 2.6. Top 10 words from the NVivo Word Frequency Analysis, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	28

Table 2.7. Top 20 themes from the NVivo Thematic Analysis with auto-coding, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajaratnam & Singh, 2024).	30
Table 3.1. High-level overview of the author / student’s broader research efforts.....	40
Table 3.2. Expert review panel comprising selected follow-up interview participants, presented with their roles and anonymized position and organizational information, in accordance with the established selection criteria.	57
Table 3.3. PhD dissertation activities, milestones, status, and timeline.....	58
Table 4.1. Sub-themes and excerpts from the overarching Tools & Platforms theme that were derived from the thematic analysis of the follow-up interview data.....	65
Table 4.2. Cybersecurity tools & platforms cited by multiple survey participants among their top two most used in their work, along with brief descriptions based on publicly available information, the number of participants who mentioned each tool/platform, and the relevant NIST CSF (v2.0) Category mappings as determined by the researcher.	78
Table 4.3. Reported challenges related to the most-used and second most-used cybersecurity tools & platforms at work, based on participants’ responses to the open-ended (text-input) survey question.	89
Table 4.4. Sub-themes and excerpts from the overarching Policies & Standards theme that were derived from the thematic analysis of the follow-up interview data.....	108

Table 4.5. Reported challenges related to organizations’ cybersecurity policies & standards, based on participants’ responses to the open-ended (text-input) survey question.	120
Table 4.6. Sub-themes and excerpts from the overarching Training & Awareness theme that were derived from the thematic analysis of the follow-up interview data.....	127
Table 4.7. Reported challenges related to role-specific cybersecurity training & awareness initiatives, based on participants’ responses to the open-ended (text-input) survey question.	141
Table 5.1. NIST CSF-based Community Profile for Usable Security, based on available templates and guidance (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024; Rajarathnam & Singh, 2023).	155
Table 6.1. Common elements included (“√”) or not included (“X”) in the published examples of NIST CSF v1.1 Profiles. Reproduced from Rajarathnam & Singh (2023), IEEE Security & Privacy Symposium Poster: “A Template for Developing NIST CSF Profiles”.	218
Table 6.2. Cybersecurity Tools & Platforms’ Usability & UX Challenges. Adapted from Rajarathnam & Singh (2025), IEEE Cyber Awareness and Research Symposium paper: “Assessing the Cybersecurity User Experience (UX) in an Organizational Context”.	225
Table 6.3. Cybersecurity Policies & Standards’ Usability & UX Challenges. Adapted from Rajarathnam & Singh (2025), IEEE Cyber Awareness and Research	

Symposium paper: “Assessing the Cybersecurity User Experience (UX) in an Organizational Context”.	227
--	-----

Table 6.4. Codebook: Themes, sub-Themes, and qualitative codes with definitions and illustrative coded excerpts (example quotes, verbatim) from follow-up interviews	230
---	-----

LIST OF FIGURES

Figure 1.1. NIST CSF Core structure. Reproduced from the NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024).....	9
Figure 1.2. NIST CSF Core Functions. Reproduced from the NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024).....	10
Figure 1.3. NIST CSF Core Functions & Categories. Reproduced from the NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024)	11
Figure 2.1. Identification, filtering / screening, and inclusion of documents / records obtained during data collection - adapted from the PRISMA Diagram template (PRISMA, n.d.), reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).....	20
Figure 2.2. Temporal distribution of articles in the dataset, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).....	25
Figure 2.3. Geographic distribution of articles - specifically, top 10 publisher countries in the dataset, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).....	26
Figure 2.4. Word Frequency Analysis Tree Map from NVivo. Round 1: Analysis of title (TI) & abstract (AB) fields, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	27

Figure 2.5. Word Frequency Analysis Tree Map from NVivo. Round 2: Analysis of title (TI), abstract (AB), and author keywords (AK) fields, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).....	27
Figure 2.6. Word Frequency Analysis Tree Map from NVivo. Round 3: Analysis of the full-text articles (PDFs), reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).	28
Figure 3.1. Mapping of the RQs to the research design and artifacts	44
Figure 4.1. Thematic map illustrating the themes and sub-themes identified through thematic analysis of the interview data (Braun & Clarke, 2006; Goyanes et al., 2025).	63
Figure 4.2. Charts showing survey responses to questions asking participants whether they're involved in the cybersecurity tools & platforms procurement (left), and their level of involvement in the procurement process (right).	72
Figure 4.3. Chart showing survey responses to the question asking participants whether they use any cybersecurity tools & platforms as part of their work.	77
Figure 4.4. Chart showing survey responses to the question asking participants to select all applicable aspects of usability for the cybersecurity tools & platforms that they use most frequently as part of their work.....	83

Figure 4.5. Chart showing survey responses to the question asking participants how the perceived benefits of the cybersecurity tools & platforms they use most frequently compare with their actual benefits in practice, in terms of usability.	84
Figure 4.6. Chart showing survey responses to the question asking participants whether their organization provided or mandated formal training on how to use cybersecurity tools & platforms effectively.	85
Figure 4.7. Chart showing survey responses to the question asking participants whether they experienced challenges in using cybersecurity tools & platforms most frequently used as part of participants’ work.....	86
Figure 4.8. Charts showing survey responses to questions asking participants whether their organizations have specific cybersecurity policies & standards (left), and whether those cybersecurity policies & standards are easily accessible (right).	112
Figure 4.9. Charts showing survey responses to the question asking participants whether their organizations’ cybersecurity policies & standards are understandable.	114
Figure 4.10. Charts showing survey responses to the question whether they received any training or guidance on these cybersecurity policies & standards from their organizations.	116
Figure 4.11. Chart showing survey responses to the question asking participants whether they face any challenges in following or implementing their organizations’ cybersecurity policies & standards.	118
Figure 4.12. Charts showing survey responses to questions asking participants whether they believe that their organizations prioritize cybersecurity education, awareness,	

and training for their employees (left), and whether they receive role-specific cybersecurity 131

Figure 4.13. Chart displaying survey responses to the question about how frequently participants receive role-specific cybersecurity education & training from their organization..... 132

Figure 4.14. Chart showing survey responses to the question asking participants whether they encountered any challenges specific to cybersecurity education, awareness, and training. 138

Figure 6.1. Proposed template for a Framework Profile based on NIST CSF v1.1, developed using common elements identified across published Framework Profile examples. Reproduced from Rajarathnam & Singh (2023), IEEE Security & Privacy Symposium Poster: “A Template for Developing NIST CSF Profiles”. 220

CHAPTER ONE

INTRODUCTION AND GENERAL INFORMATION

Introduction

Although there is no universally accepted formal definition, Usable Security is a nearly three-decade-old and evolving field that focuses on applied problems and interactions of Cybersecurity and User Experience (UX) & Usability fields (Theofanos, 2020). The United States Department of Homeland Security (DHS) emphasized the significance of Usable Security in their 2009 Roadmap for Cybersecurity Research, stating, “In the absence of usable security, there is ultimately no effective security” (U.S. Department of Homeland Security (DHS), 2009).

The tension between usability and cybersecurity is a well-recognized challenge, renowned cybersecurity expert Bruce Schneier points out, even CEOs often struggle to balance these seemingly competing priorities (ServiceNow, 2021). Traditional cybersecurity frameworks and tools often emphasize robustness of security measures at the expense of user-friendliness, leading to friction between security governance and everyday operational needs. This tension is particularly evident in organizations where cybersecurity teams must balance the implementation and enforcement of security protocols with the usage of these systems by non-technical staff. UX & usability focus on ease of use, accessibility, and so forth, while cybersecurity emphasizes stringent protection measures. Usable Security aims to create a balance by designing security

solutions and processes that are not only effective but also easy-to-use, thus minimizing errors, reducing frustration, and enhancing overall security posture.

Problem Statement & Study Objective

While various cybersecurity frameworks and guidance documents exist, including the widely adopted National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (National Institute of Standards and Technology (NIST), 2024) for general guidance, as well as domain-specific NIST CSF-based Community Profiles for industry sectors such as manufacturing and election infrastructure, and use cases like ransomware mitigation (NIST National Cybersecurity Center for Excellence (NCCoE), n.d.), there remains a notable gap in implementation guidance specifically tailored to the Usable Security field. *Chapter 2 (Literature Review)* of this dissertation study further details this gap and explores emerging trends, themes, and patterns in the convergence of the Cybersecurity and UX fields.

The objective of this study is to develop a NIST CSF-based Usable Security Community Profile to provide organizations with practical guidance on incorporating UX and usability considerations into their cybersecurity practices. This study examines the UX challenges that organizations face when implementing and managing cybersecurity tools & platforms, policies & standards, and training initiatives. By gathering and analyzing data from cybersecurity professionals across various industries, the study creates a comprehensive Community Profile that balances cybersecurity needs with UX

requirements. Recommendations drawn from this research have been integrated into a Community Profile based on the generalizable template that the author presented at the 2023 IEEE Security & Privacy (IEEE S&P) Symposium (Rajarithnam & Singh, 2023), as well as the recent template published by NIST (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024; Rajarithnam & Singh, 2023).

The Research Questions (RQs) guiding this dissertation study, along with the corresponding methodological approach, are detailed in *Chapter 3 (Materials and Methods)*. The results of data collection and analysis are presented in *Chapter 4 (Results and Discussion)*. The baseline recommendations for organizations to improve the UX of their cybersecurity tools and platforms, policies and standards, and training are provided in the form of the NIST CSF Usable Security Community Profile in *Chapter 5 (NIST CSF-Based Usable Security Community Profile)*. And lastly, the study significance, study limitations, and next steps & future directions are presented in *Chapter 6 (Conclusion and Recommendations)*.

Significance of the Study

The significance of this study lies in addressing a key gap at the intersection of cybersecurity and User Experience (UX), that is, the absence of discussions on widely adopted standards and frameworks for Usable Security, as explained in *Chapter 2*. Although several NIST Cybersecurity Framework (CSF) Community Profiles exist for domains such as manufacturing, election infrastructure, and ransomware mitigation

(NIST NCCoE, n.d.), none focus on usable security. This study develops the first CSF-based Community Profile centered on UX, providing a structured way to integrate human-centered concerns into organizational cybersecurity practices.

The significance of this work also lies in its timing. With the release of NIST CSF v2.0 in 2024, which introduced the new Govern (GV) Function and other updates, organizations require early guidance for applying the framework. By mapping practitioner-reported UX challenges to CSF v2.0 Categories, this study produces a Profile that reflects both updated standards and the realities of organizational practice.

The study is relevant to both academics and practitioners. For scholars, it serves as a reference model. By documenting the NIST CSF-based Community Profile development process in a transparent, replicable manner, using available templates and guidance, real-world organizational data, a pilot study, and expert validation, it provides an approach that others can replicate or adapt, supporting the broader advancement of human-centered cybersecurity guidance across contexts, as well as the future development of NIST CSF-based Community Profiles by scholars for other fields. For practitioners, it identifies recurring cybersecurity UX challenges, such as tool complexity, policy accessibility, training fatigue, etc., and provides actionable recommendations for addressing them.

Theoretical Framework

This study is based on the NIST CSF (National Institute of Standards and Technology (NIST), 2024), one of the most widely adopted frameworks for managing and improving an organization's cybersecurity risks (Tenable, 2016). The NIST CSF's structure, including the Framework Core and Profiles, is key to shaping the study's theoretical approach. A detailed overview of the NIST CSF and its relevant components, such as Community Profiles, is outlined below.

NIST CSF

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (National Institute of Standards and Technology (NIST), 2024) serves as a comprehensive and widely adopted framework for organizations seeking to harmonize their cybersecurity strategies and practices with their business objectives. Although initially developed to safeguard critical infrastructure security in the United States (US), it has since gained widespread adoption by a diverse range of organizations nationwide. In a 2016 survey (Tenable, 2016) that sought to assess the adoption of security frameworks among over 300 security professionals from various sectors within the US, approximately 70% of respondents identified the NIST CSF as an industry best practice.

The NIST CSF includes three (3) major components, as shown below:

1. **CSF Core:** The Framework Core is a set of cybersecurity activities and outcomes that are common across critical sectors. The most recent iteration, NIST CSF v2.0 is structured hierarchically into three (3) levels, as depicted in **Figure 1.1**, which is reproduced from NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024):
 - a. **Functions:** At the highest level, the Framework defines six (6) essential cybersecurity Functions, namely Govern (GV), Identify (ID), Detect (DE), Protect (PR), Respond (RS), and Recover (RC), as shown in **Figure 1.2** below, reproduced from NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024). These Functions represent the fundamental cybersecurity processes that organizations must implement to effectively manage cybersecurity risks.
 - b. **Categories:** Each Function is further broken down into categories, which are groups of related cybersecurity outcomes. E.g., "Asset Management (ID.AM)" is one of the Categories under the Identify (ID) Function. In total, the NIST CSF v2.0 comprises 22 Categories distributed across the six (6) Functions, as depicted in **Figure 1.3**, reproduced from NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024).
 - c. **Sub-categories:** The Sub-categories provide more granular outcomes of technical and management cybersecurity activities that support the broader Categories. E.g., "ID.AM-01: - Inventories of hardware managed by the organization are maintained" is a Sub-category under the Asset

Management (ID.AM) Category within the Identify (ID) Function. There are 100+ Sub-categories across the 22 Categories.

2. **Organizational & Community Profiles:** Previous iterations of the NIST CSF, such as version 1.1 (National Institute of Standards and Technology (NIST), 2018), identified "Profiles" as one of the key components, where they functioned as customizable baselines that addressed common cybersecurity outcomes for particular sectors or contexts. These are now known as "Community Profiles" in the latest iteration, NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024) and are designed to address shared cybersecurity goals across multiple organizations in a specific industry or sector. In this structure, individual organizations can develop target Profiles based on a Community Profile, allowing them to align their cybersecurity efforts with industry best practices. In NIST CSF v2.0, "Organizational Profiles" remain as a tool for describing an organization's current and target cybersecurity postures in terms of the CSF Core. Unlike Community Profiles, Organizational Profiles are typically developed internally and are not publicly shared (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024). These profiles help organizations tailor their approach to cybersecurity by aligning it with their unique operational and risk management contexts.
3. **Implementation Tiers:** The NIST CSF also introduces "Implementation Tiers", which describe the degree of formality and rigor of an organization's cybersecurity risk governance and management practices. There are four (4)

Tiers: “Partial (Tier 1)”, “Risk Informed (Tier 2)”, “Repeatable (Tier 3)”, and “Adaptive (Tier 4)”. The four (4) Tiers provide a pathway for organizations to improve their cybersecurity maturity over time.

Definitions of Key Terms

Cybersecurity

According to the U.S. Cybersecurity & Infrastructure Security Agency (CISA) (Cybersecurity and Infrastructure Security Agency (CISA), 2021), Cybersecurity is defined as “the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information”. This definition plays a key role in establishing the inclusion criteria for the literature review, specifically outlined in *Chapter 2 (Literature Review)* of this study.

User Experience (UX)

Digital.gov (U.S. General Services Administration (GSA), 2024) (formerly Usability.gov (Assistant Secretary for Public Affairs, 2013)), maintained by the U.S. General Services Administration (GSA) Technology Transformation Service defines UX as “A broad term for several disciplines that study the effect of design on the ease of use and level of satisfaction with a product, site or system.” This definition plays a key role in establishing the inclusion criteria for the literature review, specifically outlined in *Chapter 2 (Literature Review)* of this study.

Usability

Usability, a subset of UX, is defined as “How effectively, efficiently, and satisfactorily a user can interact with a user interface” by the Digital.gov (U.S. General Services Administration (GSA), 2024) (formerly Usability.gov (Assistant Secretary for Public Affairs, 2013)). This definition plays a key role in establishing the inclusion criteria for the literature review, specifically outlined in *Chapter 2 (Literature Review)* of this study.

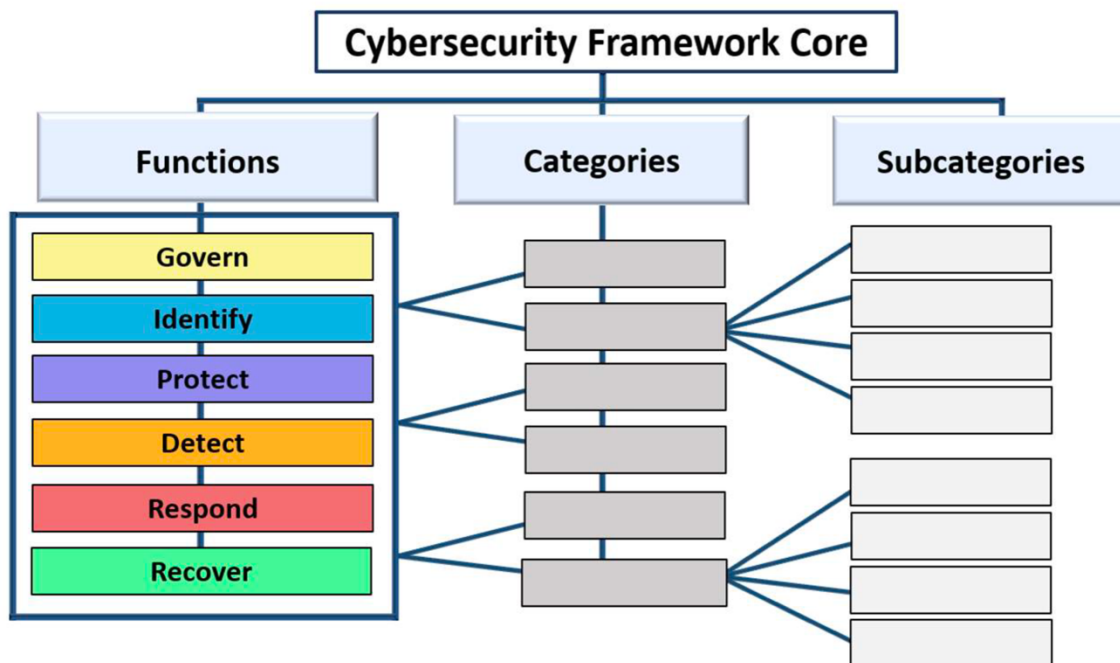


Figure 1.1. NIST CSF Core structure. Reproduced from the NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024)



Figure 1.2. NIST CSF Core Functions. Reproduced from the NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024)

Function	Category	Category Identifier
<u>Govern (GV)</u>	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
<u>Identify (ID)</u>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<u>Protect (PR)</u>	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
<u>Detect (DE)</u>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<u>Respond (RS)</u>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<u>Recover (RC)</u>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Figure 1.3. NIST CSF Core Functions & Categories. Reproduced from the NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024)

CHAPTER TWO

LITERATURE REVIEW

Overview

Prior to defining the objectives and research questions for this dissertation, a Systematic Literature Review (SLR) was undertaken to examine the convergence of the Cybersecurity and User Experience (UX) fields over a period of five (5) years (2018 - 2022). The primary aim of this review was to assess the current body of literature in the convergence of these domains, identify key themes and patterns, and highlight potential gaps. The results of this literature review were presented at the 4th Institute of Electrical and Electronics Engineers (IEEE) Cyber Awareness and Research Symposium (CARS), in October 2024 (Rajarithnam & Singh, 2024), and are detailed in the following sections of this chapter.

Scope, Gaps, and Contributions of Prior Literature

While prior literature reviews had examined the intersection of Cybersecurity and UX and/or usability, a few limitations persisted across many of these studies. Common limitations included narrow search strategies, such as restricting queries to author keywords, and small sample sizes, often analyzing fewer than 100 articles (Di Nocera et al., 2023; Garfinkel & Lipford, 2014; Grobler et al., 2021; Lennartsson et al., 2021; Reuter et al., 2022). Others had focused on specific subdomains within cybersecurity, such as software engineering and system interfaces (Distler et al., 2021; Nwokedi et al., n.d.), thereby limiting the generalizability of their findings. To address these gaps, this

SLR employed broader search parameters, including titles, topics, abstracts, and author keywords, and analyzed a larger dataset of over 1000 articles that encompassed the broader landscape of cybersecurity and UX, rather than focusing on specific contexts only. Detailed explanations of the gaps in previous literature are outlined below.

Reuter et al. (Reuter et al., 2022) provided a detailed historical overview of Usable Security field, tracing its emergence in the 1990s, with significant milestones such as the first workshop pairing user studies with security analyses at the Association for Computing Machinery (ACM) Conference on Human Factors in Computing Systems (CHI) in 2003 and the establishment of the Symposium on Usable Privacy and Security (SOUPS) conference in 2005. However, their study primarily emphasized the transparency and tailor-ability of user interventions and did not position itself as a systematic literature review. Similarly, the book titled “Usable Security: History, Themes, and Challenges” (Garfinkel & Lipford, 2014) offered an extensive overview of literature from workshops such as ACM CHI and SOUPS, and databases like IEEE and ACM libraries. However, the book acknowledged the potential for relevant literature beyond these sources. Furthermore, its publication over a decade ago means it does not capture more recent advancements in the field.

Other studies that positioned themselves as literature reviews, such as Lennartsson et al. (2021) and Grobler et al. (2021), were constrained by limited search criteria, resulting in datasets of only 70 and 78 articles, respectively. The former focused

on the usability of security solutions over a five-year period, but had narrow search criteria which considered titles and keywords only, while the latter surveyed user-centered cybersecurity over a larger time-frame, specifically from 2005 to 2019, but considered a small dataset in its analysis due to the specificity in its keywords as part of its search query. Di Nocera et al.'s systematic review (2023) covered publications from 2005 to 2022, and used broad search terms like “Usable” and “Usability” in combination with cybersecurity-related terms. While comparable to this dissertation's literature review in its scope, Nocera's study also analyzed a small dataset comprising of only 55 articles, as it had limited its search to the author keywords field.

Other research studies in prior literature on cybersecurity and usability/UX had limited their scope by focusing on a specific subsections or contexts of cybersecurity, such as software engineering & system interfaces (Nwokedi et al., n.d.), or risk representation by researchers (Distler et al., 2021).

In contrast, the SLR as part of this dissertation utilized broader search parameters, extending beyond titles and keywords, and analyzed a much larger dataset. Therefore, this SLR provided a more holistic view of the current state of research in the convergence of Cybersecurity and UX fields.

SLR Methodology

The methodology for the Systematic Literature Review (SLR) portion of this dissertation was adapted based on recommendations from multiple sources. This included general guidance from frameworks and sources like the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Page et al., 2021) and Nightingale's (2009) recommendations for Systematic Literature Reviews (SLR), along with Computer Science-specific guidance from sources such as Silva and Neiva (2016).

Data Collection

The Web of Science (WOS) Core Collection, one of the world's leading citation databases, was selected as the primary database for data collection due to its comprehensive coverage of peer-reviewed journals and conference proceedings. As of the time of search, WOS included over 92 million records, spanning more than 22,000 peer-reviewed journals and 308,000 conferences (Clarivate, n.d.). WOS also indexes key sources such as IEEE Xplore and the ACM Digital Library, which are frequently cited in prior studies on Cybersecurity and UX. An advanced search was conducted on October 12, 2022, using the following parameters:

- **Search terms:** (“cyber\$security” OR “security”) AND (“user\$experience” OR “usability” OR “UX”)
 - The wildcard operator \$ denoted zero (0) or one (1) character, and was used to capture variations such as “cybersecurity,” “cyber-security,” and “cyber security”.

- **Fields searched:** Title (TI), Abstract (AB), Author Keywords (AK), and Topic (TS)
- **Publication years:** 2018 - 2022 (five-year span)
- **Publication language:** English only
- **Search query link:** Available upon request

The search yielded 1,860 records, which were exported as a Microsoft Excel spreadsheet (full record option) for screening and analysis. Each record included metadata such as title, abstract, authors' information (name, institutional affiliation, email address, etc.), source, author keywords, and so forth.

Inclusion & Exclusion Criteria

To ensure relevance and accessibility, the following inclusion criteria were applied during the screening or dataset filtering process to keep relevant documents / records in the dataset:

1. **Cybersecurity Relevance:** The document / record must pertain to cybersecurity, as defined in *Chapter 1 (Definition of Key Terms)* section) using the U.S. Cybersecurity and Infrastructure Security Agency (CISA) definition.
2. **UX / Usability Relevance:** The document must address User Experience (UX) or usability, as defined in *Chapter 1 (Definition of Key Terms)* section) based on the U.S. General Services Administration (GSA) Technology Transformation Services definitions.

3. **Accessibility:** The full text document must be accessible through open access or the library system of the author's institutional affiliation, namely the University of Tennessee, Knoxville (UTK) library system, which includes databases such as IEEE Xplore and the ACM Digital Library (UTK Library, n.d.).

The exclusion criteria used to remove documents from the dataset during the screening process were the inverse of the aforementioned inclusion criteria, as follows:

1. **Lack of Cybersecurity Relevance:** The document is not related to cybersecurity per CISA definition outlined in *Chapter 1 (Definition of Key Terms)* section)
2. **Lack of UX / Usability Relevance:** The document is not related to UX or Usability per U.S. GSA definition outlined in *Chapter 1 (Definition of Key Terms)* section)
3. **Inaccessibility:** The article can not be accessed via open access or the UTK library system

Please note: The SLR also made a clear distinction between usability and User Experience (UX), as outlined in *Chapter 1 (Definition of Key Terms)* section). Usability focuses on how easily and effectively users can interact with a system to accomplish their goals, emphasizing practical factors such as efficiency, effectiveness, and satisfaction. It ensures that users are able to navigate the system, perform tasks, and achieve desired outcomes with minimal effort and errors (Nielsen, 2012). In contrast, UX takes a broader approach, encompassing not only usability but also users' emotions, beliefs, preferences,

perceptions, responses, and behaviors during their interaction with a system (Bevan, 2009). The SLR explored the convergence of cybersecurity and UX, which inherently included the subset usability. This broader perspective was incorporated into the research questions of the published SLR (Rajarathnam & Singh, 2024), as well as throughout the data collection process and the inclusion & exclusion criteria outlined above for the data filtering / screening process.

Screening / Filtering Process

The initial dataset of 1860 records underwent a two-stage screening process, following recommendations from PRISMA (Page et al., 2021) and Nightingale (2009), as follows:

1. **First Round:** Manual review of titles (TI), abstracts (AB), and author keywords (AK) fields in the Microsoft Excel spreadsheet obtained from WOS during the data collection process. The 1,860 records were categorized into three (3) categories; “Keep,” “Unsure,” or “Remove” based on the aforementioned *Inclusion & Exclusion Criteria*, as recommended by Silva and Neiva (2016). Breakdown records into these three (3) categories, along with number & percentage of records are outlined in **Table 2.1**.
2. **Second Round:** Full-text review of “Unsure” records to classify them as “Keep” or “Remove” records, and the verification of “Keep” records to ensure that they were accessible based on the aforementioned *Inclusion & Exclusion Criteria*. Articles were accessed via links provided in the spreadsheet obtained from WOS,

or through manual searches on Google. It is worth noting that some initially retained records (i.e., labeled “Keep” in the first round) were reclassified as “Remove” due to the inaccessibility exclusion criterion. Final counts are summarized in **Table 2.2**.

A PRISMA-style flow diagram, **Figure 2.1**, adapted from the PRISMA diagram template and guidelines (Page et al., 2021; PRISMA, n.d.) illustrates the overall screening process.

Table 2.1. First round screening / filtering outcome - screening based on TI, AB, and AK fields. Adapted from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

First Round Screening Outcomes and Descriptions	# of Records (% of Records) per Category
Keep: This category includes documents / records that met the <i>Inclusion & Exclusion Criteria</i> and were advanced to the subsequent stages of screening / filtering and data analysis.	433 (23.28%)
Remove: This category includes records that were removed from the subsequent stages of screening / filtering and data analysis based on the <i>Inclusion & Exclusion Criteria</i> .	450 (24.19%)
Unsure: This category includes records wherein assessment of Titles (TI), Abstracts (AB), and Author Keywords (AK) fields were not sufficient to determine whether or not they met the <i>Inclusion & Exclusion Criteria</i> , therefore were subjected to additional screening.	977 (52.23%)
Total:	1860 (100%)
Please note: This table provides the counts & percentages of records per category based on the first round of screening / filtering only. Examples of detailed rationale for exclusion (records labeled “Remove”) and ambiguity (records labeled “Unsure”) are included in the paper presented at the 2024 IEEE CARS (Rajarithnam & Singh, 2024).	

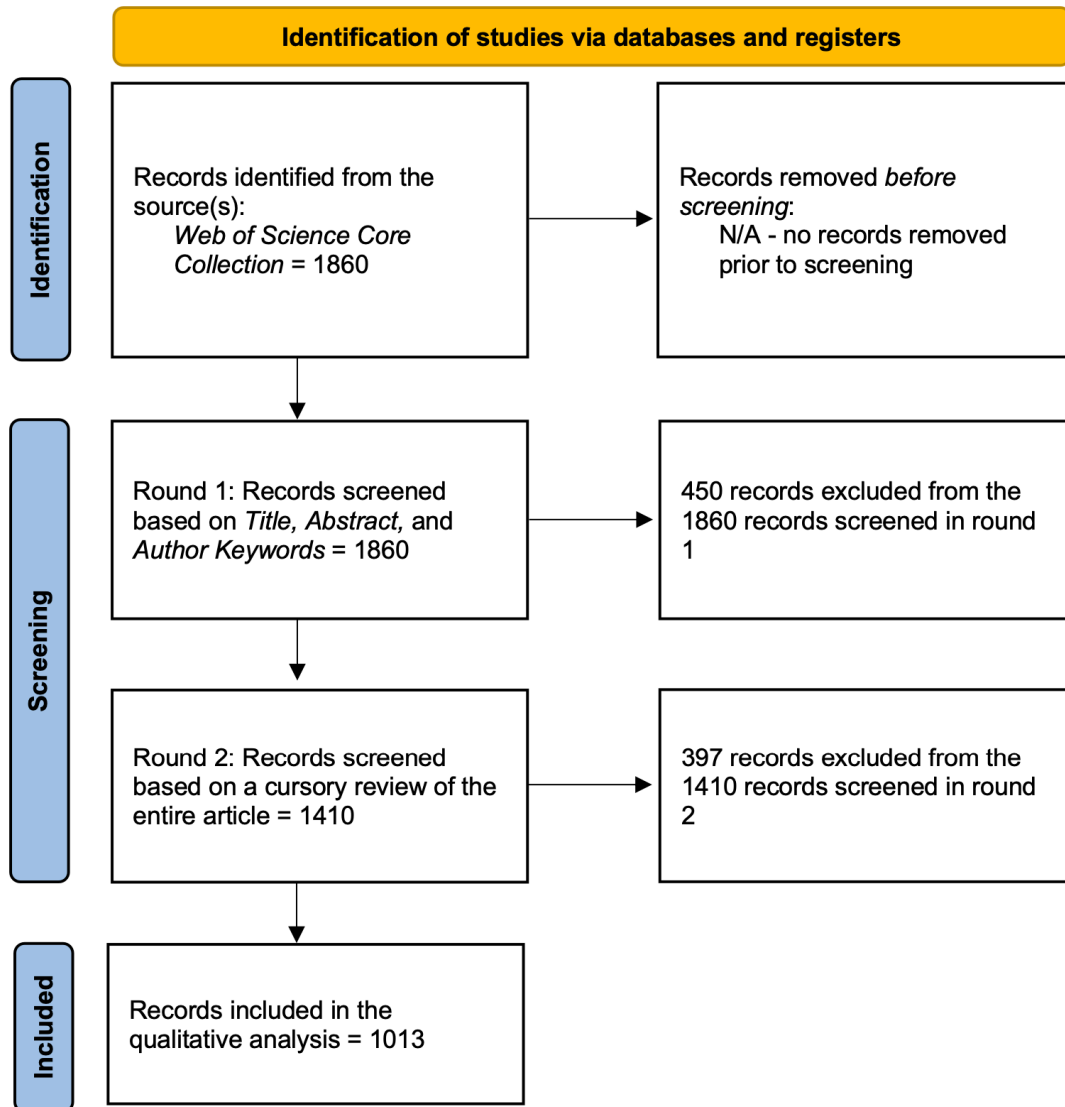


Figure 2.1. Identification, filtering / screening, and inclusion of documents / records obtained during data collection - adapted from the PRISMA Diagram template (PRISMA, n.d.), reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

Table 2.2. Second round screening / filtering outcome - screening based on manual review of full-text (PDF) articles. Adapted from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

Final Screening Outcome & Description	# of Records (% of Records) per Category
Keep: This category includes records that met the <i>Inclusion & Exclusion Criteria</i> and were advanced to the data analysis phase.	1013 (54.46%)
Remove: This category includes records that were removed from the data analysis phase based on the <i>Inclusion & Exclusion Criteria</i> .	847 (45.54%)
Total:	1860 (100%)

Data Analysis

Following screening, the final dataset comprising of 1013 documents was analyzed to assess the state of research at the convergence of Cybersecurity and UX. The analysis included:

- **Count Analysis & Descriptive Statistics:** The distribution of articles by publication type, publication year, the top 10 countries by the number of published articles, and the top five (5) conferences & journals. Microsoft Excel Pivot Tables were used to organize and visualize the data.
- **Word Frequency Analysis:** Three (3) rounds of word frequency analysis were performed using NVivo, a Computer-Assisted Qualitative Data Analysis Software (CAQDAS) tool by Lumivero (Dhakal, 2022; Lumivero, n.d.). The first round focused solely on the titles and abstracts of the articles in the dataset. In the second round, the scope was expanded to include author keywords alongside titles and abstracts. The third round consisted of a manual review of the full-text articles, retrieved as PDFs from their respective sources, as listed in the Excel

document obtained from the Web of Science platform from the SLR data collection. For each round, NVivo was used to generate tree maps based on the word frequency results, which were then analyzed in conjunction with the thematic analysis.

- **Thematic Analysis:** Thematic analysis was conducted using NVivo's auto-coding feature, focusing on the top 20 themes identified. Each theme was examined in detail by exploring the associated qualitative codes, reviewing relevant coded excerpts from the articles, and identifying patterns across the dataset.

SLR Results and Discussion

Following two (2) rounds of data filtering / screening, the final dataset comprising of 1013 documents related to the convergence of Cybersecurity and UX fields was analyzed using the aforementioned methods. The findings are presented below, encompassing multiple analytical dimensions to offer a comprehensive understanding of the Cybersecurity & UX research landscape.

Overview and Current Research Landscape

As shown in **Table 2.3**, the majority of research addressing the convergence of Cybersecurity and User Experience (UX) fields is published in scholarly journals (59.33%), followed by a substantial share presented at academic and professional conferences (40.57%). Only a small fraction appears in books (0.1%). This distribution

suggests that journals serve as the primary venue for in-depth, peer-reviewed studies, while conferences play a critical role in introducing emerging ideas and fostering real-time scholarly discourse.

Table 2.3. Distribution of records by publication type, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

Publication Type	# of Publications (% of Publications)
Journal (J)	601 (59.33%)
Conference (C)	411 (40.57%)
Book (B)	1 (0.1%)

Table 2.4 & Table 2.5 highlight the five (5) most frequently cited journals and conferences respectively, identified through publication count analysis. IEEE Access journal and the ACM CHI conference emerge as leading platforms for research in this domain. Other notable journals include Computers & Security and JMIR mHealth and uHealth, while key conferences include SOUPS and ACM CCS. These findings highlight the influential role of IEEE, ACM, and USENIX-affiliated venues in fostering research and interdisciplinary collaboration in Cybersecurity and UX.

Table 2.4. Top five (5) journals in the convergence of cybersecurity and UX research, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

#	Top Five (5) Journals	# of Publications
1	Institute of Electrical and Electronics Engineers (IEEE) Access	37
2	Computers & Security	26
3	Journal of Medical Internet Research (JMIR) mHealth and uHealth	22

Table 2.4. Continued

#	Top Five (5) Journals	# of Publications
4	International Journal of Advanced Computer Science and Applications (IJACSA)	15
5	Journal of Medical Internet Research (JMIR)	14 (tied)
	IEEE Transactions on Dependable and Secure Computing (TDSC)	14 (tied)

Table 2.5. Top five (5) journals in the convergence of cybersecurity and UX research, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

#	Top Five (5) Conferences	# of Publications
1	Association for Computing Machinery (ACM) Conference on Human Factors in Computing Systems (CHI)	21
2	Symposium on Usable Privacy and Security (SOUPS)	17
3	ACM Computing Classification System (CCS)	13
4	Human Computer Interaction (HCI) International	12
5	USENIX, The Advanced Computing Systems Association	5

Figure 2.2 presents the temporal distribution of publications, revealing a consistent scholarly output over time. A slight dip in 2020 likely reflects disruptions caused by the COVID-19 pandemic. It is important to note that data collection for the SLR concluded in October 2022, and therefore, more recent publications may not be fully represented, or represented as unspecified / early-access. Nonetheless, the upward trend observed in 2022 indicates sustained interest and the potential for continued growth in cybersecurity & UX research.

Geographical distribution was assessed through count analysis based on publisher countries, including the USA, Canada, China, India, and so forth. **Figure 2.3** showcases the top 10 contributing countries, with North America and Europe, especially the US,

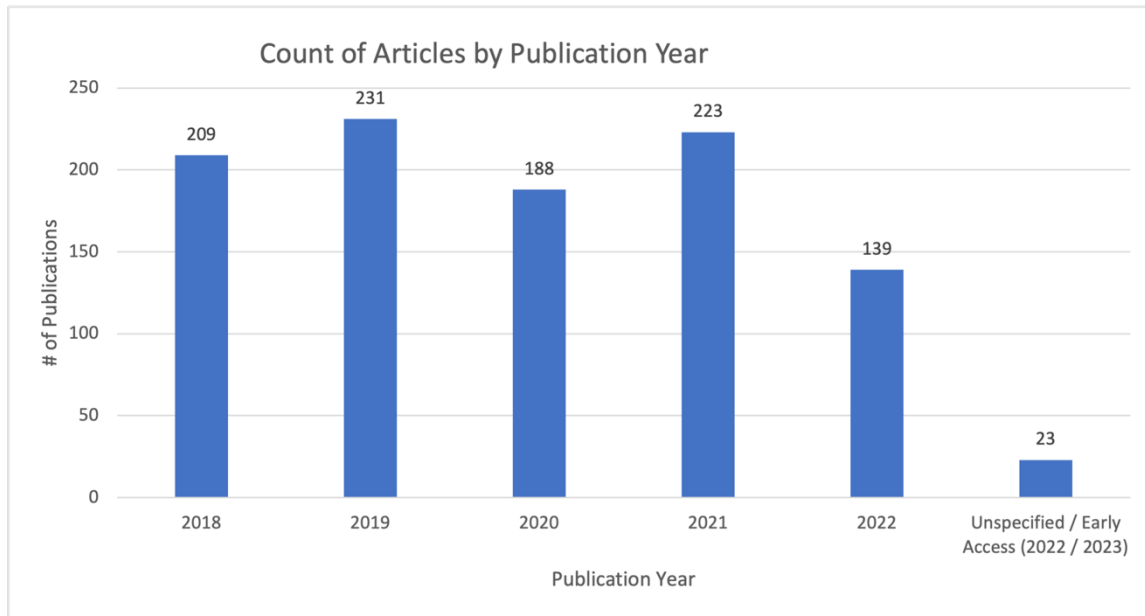


Figure 2.2. Temporal distribution of articles in the dataset, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

which leads with 534 publications, standing out. The international diversity in the geographic distribution reflects the influence of cultural and regional contexts on research priorities and highlights the importance of global perspectives in shaping future studies and fostering cross-border collaboration.

Prevalent Themes in Cybersecurity & UX Research

As outlined in the *Data Analysis* subsection, three (3) rounds of word frequency analysis were conducted using NVivo. The first round focused on the titles and abstracts of all 1013 records, the second round expanded the scope to include author-provided keywords, and the third round involved a detailed review of the full-text PDFs of the articles. **Figure 2.4**, **Figure 2.5**, and **Figure 2.6** shows the word frequency analysis tree

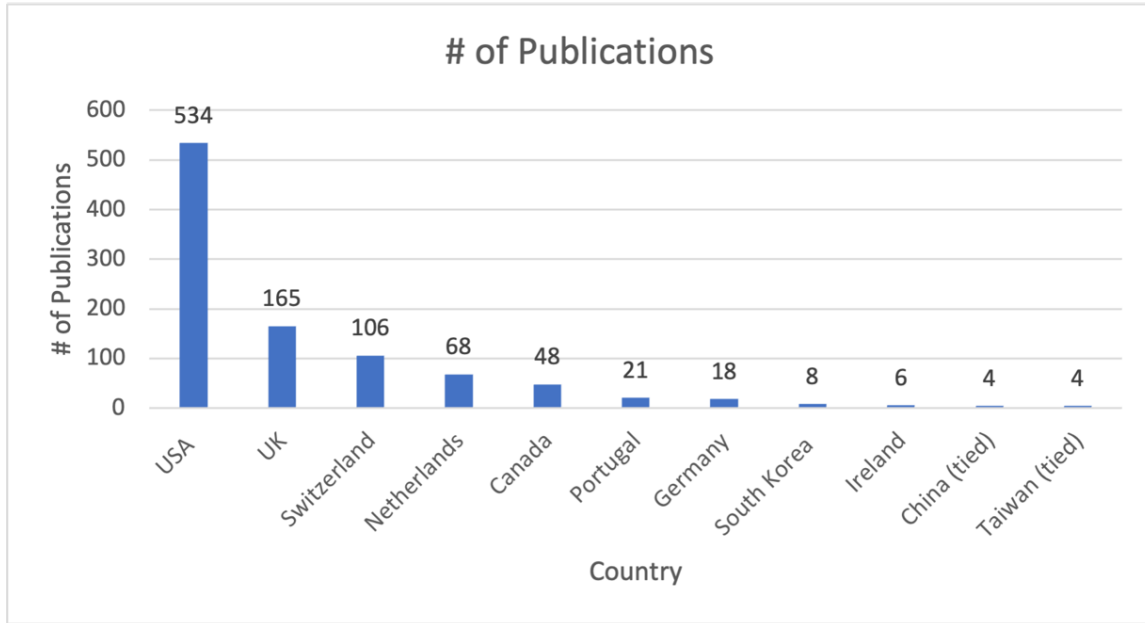


Figure 2.3. Geographic distribution of articles - specifically, top 10 publisher countries in the dataset, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajaratnam & Singh, 2024).

maps produced in NVivo for each of the three (3) rounds. The top 10 words remained largely consistent across all three rounds, with only minor shifts in ranking.

Table 2.6 presents the top 10 most frequent words identified in the third round, along with excerpts from representative documents in the dataset. In each round, the top 100 words were analyzed, with a minimum word length of three (3) characters. Stemmed word matching was applied to capture lexical variations (e.g., “walk” included “walking”).

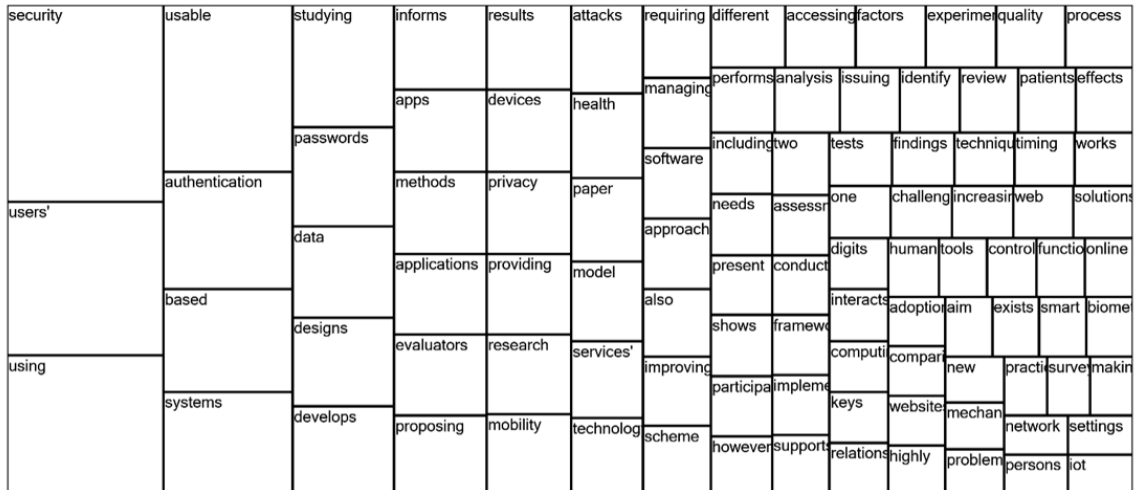


Figure 2.4. Word Frequency Analysis Tree Map from NVivo. Round 1: Analysis of title (TI) & abstract (AB) fields, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).

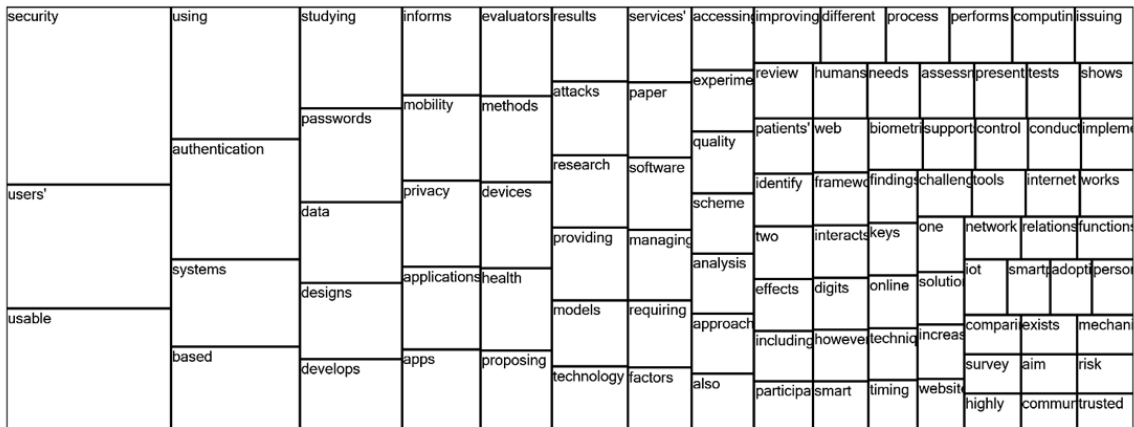


Figure 2.5. Word Frequency Analysis Tree Map from NVivo. Round 2: Analysis of title (TI), abstract (AB), and author keywords (AK) fields, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarathnam & Singh, 2024).

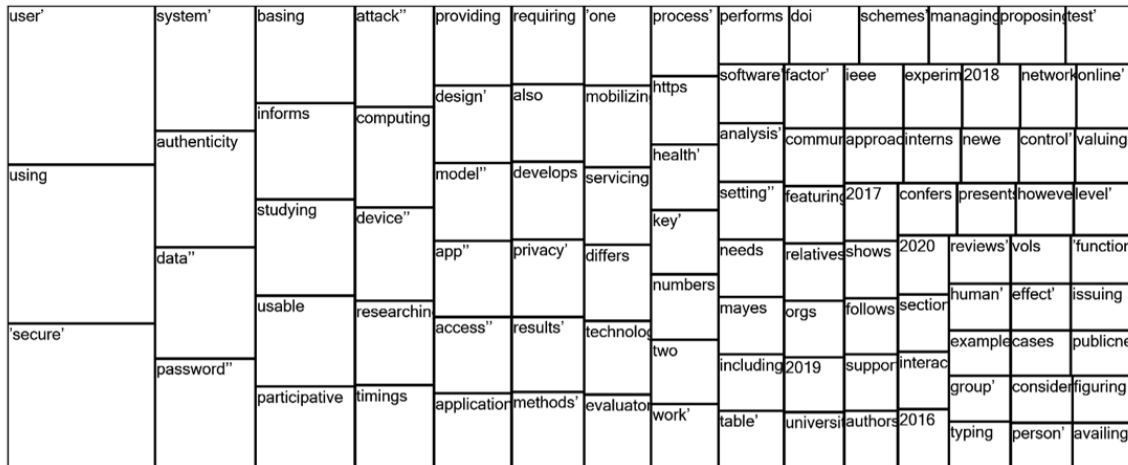


Figure 2.6. Word Frequency Analysis Tree Map from NVivo. Round 3: Analysis of the full-text articles (PDFs), reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

Table 2.6. Top 10 words from the NVivo Word Frequency Analysis, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

Word	Count (Weighted %)	Similar Words	Examples of Usage (in the Articles) w. References
user'	6813 (1.03%)	user's acceptance, users' goals, users' credentials, users' attitude, users' behavior, users' evaluations, etc.	"...in turn, leads to a user-friendly and scalable solution. Moreover..." (Lim et al., 2020)
using	6749 (1.02%)	use, used, useful, usefulness, etc.	"...deployed our prototype for a use case using real-world medical..." (Lim et al., 2020)
'secure'	6169 (0.93%)	securable, security, securing, securely, secured, etc.	"...Finding other means to evaluate security systems is vital to be..." (Mathis, 2021)
system'	3619 (0.55%)	systems, systemic, systematically, etc.	"...in where we evaluated the system's usability and observation resistance through..." (Mathis, 2021)

Table 2.6. Continued

Word	Count (Weighted %)	Similar Words	Examples of Usage (in the Articles) w. References
authenticity	3319 (0.50%)	authentication, authenticated, authenticates, authenticator, authenticity, authentically, etc.	<i>“Passwords are an often unavoidable authentication mechanism, despite the availability of...”</i> (Seiler-Hwang et al., 2019)
data”	3204 (0.48%)	Data, data’, data”	<i>“...study Questionnaire to gather demographic data and information about their previous...”</i> (Seiler-Hwang et al., 2019)
password”	3128 (0.47%)	passwords, password@2019, etc.	<i>“...also had allowed an alphanumeric password for disk encryption.”</i> (Wolf et al., 2019)
basing	2819 (0.42%)	base, based, bases, basing	<i>“...use. As facial and voice-based authentication also gain acceptance by...”</i> (Wolf et al., 2019)
informs	2771 (0.42%)	information, information’s security, informativeness, informant, informally, etc.	<i>“...of communications, and safeguards sensitive information. Given the need for cryptography...”</i> (Haney et al., 2018)
Studying	2770 (0.42%)	studies, study, studying, studied, etc.	<i>“...is the first in-depth study to explore cryptographic development practices...”</i> (Haney et al., 2018)
Note: The excerpts provided above are not exhaustive and are for reference only.			

Table 2.7 presents the 20 most frequent themes identified through the thematic analysis using NVivo’s auto-coding. Each theme is accompanied by sample qualitative codes, reference counts, and excerpts from relevant documents in the dataset. Thematic analysis revealed “User” and “Security” as the most dominant themes, aligning with the advanced search keywords and inclusion criteria described in the *SLR Methodology*

section. Themes such as “authentication,” “password,” and “key” appeared prominently in both the word frequency and thematic analyses, indicating that Identity and Access Management (IAM) is a central focus in research at the intersection of cybersecurity and UX. Similarly, terms like “data,” “system,” “application,” and “device” were significant in the thematic analysis, with “data” and “system” also ranking highly in the word frequency results, highlighting Data and Systems Security as another key domain. Words such as “study,” “research,” and “method” were frequently observed but are likely reflective of general academic language rather than specific thematic content.

It is important to note that word frequency and auto-coded thematic analyses serve as exploratory tools and should not be considered substitutes for comprehensive qualitative analysis conducted by multiple experienced coders. Nonetheless, these methods offer valuable initial insights into dominant themes and areas of focus within the cybersecurity and UX research landscape, providing a foundation for deeper investigation into these complex and evolving topics.

Table 2.7. Top 20 themes from the NVivo Thematic Analysis with auto-coding, reproduced from the SLR paper presented at the 2024 IEEE Cyber Awareness and Research Symposium (CARS) (Rajarithnam & Singh, 2024).

Auto-coded Themes	# of Files (References)	Example Codes	Examples of Usage, Code (Article Reference)
User	1004 (10411)	User authentication, end users, user satisfaction, personal use, user interfaces, etc.	<i>“Traditional passwords are used widely for authenticating users nowadays, but other alternatives also are available such as biometric systems, smart cards, and so on.”</i> User

Table 2.7. Continued

Auto-coded Themes	# of Files (References)	Example Codes	Examples of Usage, Code (Article Reference)
			authentication (Khodadadi et al., 2021)
Security	915 (8013)	Information security, security issues, network security, secure storage, etc.	<i>“From a usability aspect, traditional passwords have some drawbacks, and these issues directly address security issues.”</i> Security issues (Khodadadi et al., 2021)
System	898 (5394)	System design, software systems, Android Operating System, authentication system, system administrator, etc.	<i>“From the system designer perspective, Senarath et al. (2019) proposed a model that could be used by system developers to measure the privacy risk perceived by users when they disclose data into software systems.”</i> Software systems (Grobler et al., 2021)
Data	874 (6738)	Data collection, personal data, sensitive data, data encryption, medical data, etc.	<i>“In terms of data security and data protection, patients can also check the My Kanta service to see where their healthcare data have been processed and shared.”</i> Data security (Kuusisto et al., 2023)
Information	846 (4187)	Information security, demographic information, biometric information, confidential information, credit card information, etc.	<i>“5.2.1 Intelligent Objects Although smart phones add value and context to human centric interaction, these interfaces are not obvious to users and can be used to extract private information in a stealthy way.”</i> Private information (Grobler et al., 2021)
Process	828 (3095)	Authentication process, login process, data processing, natural	<i>“Authentication processes occur between the service user, or payer, and the bank, between the merchant, or</i>

Table 2.7. Continued

Auto-coded Themes	# of Files (References)	Example Codes	Examples of Usage, Code (Article Reference)
		language processing, etc.	<i>receiver, and the bank, and between the payer and the receiver.</i> ” Authentication process (Alshamsi & Andras, 2019)
Study	743 (3256)	Previous studies, case study, empirical study, usability study, study participants, etc.	<i>“The objective of this study is to carry out a user study, which not only provides deep insight into how users perceive the usability and security of Bitcoin, but also indicates the level of user interaction with the newly emerged decentralized anonymous digital currency system.”</i> User study (Alshamsi & Andras, 2019)
Time	718 (2412)	Average time, multiple times, response time, authentication time, time constraints, etc.	<i>“The concept of ‘user experience’ in this scientific domain has been de- fined in consideration of several factors, including usability, functionality, response time and response to errors.”</i> Response time (Talal et al., 2019)
Usability	697 (2977)	Usability issues, usability study, usable security, usability testing, poor usability, etc.	<i>“The proposed scheme was performed as a prototype and a usability evaluation towards the proposed scheme was conducted to measure its usability and practicality as the alternative user authentication scheme.”</i> Usability evaluation (Khodadadi et al., 2021)
Research	669 (2447)	Future research, research team, academic research, research	<i>“RQ3: What are the characteristics of VR that can augment current research paradigms to evaluate usable</i>

Table 2.7. Continued

Auto-coded Themes	# of Files (References)	Example Codes	Examples of Usage, Code (Article Reference)
		methodology, research gaps, etc.	<i>security prototypes?</i> ” Current research (Mathis, 2021)
Model	619 (2669)	Threat model, mental models, technology acceptance model, authentication model, learning model, etc.	<i>“Also, in many cases, as the complaint by participant P38 above reflects, the PMs do not meet the expectations or mental models of the users.”</i> Mental models (Seiler-Hwang et al., 2019)
Application	554 (2037)	Mobile applications, web applications, application layer, application programming interface, etc.	<i>“We designed our survey based on the PACMAD [23] model, a tool specifically oriented to evaluate the usability of mobile applications.”</i> Mobile applications (Seiler-Hwang et al., 2019)
Device	548 (2694)	Mobile device, medical devices, computing devices, IoT devices, smart home devices, etc.	<i>“One major drawback of the algorithm was that it did not support dynamic addition of nodes and medical devices which rendered the model ineffective in realworld environments.”</i> Medical devices (Sharma et al., 2021)
Authentication	522 (5624)	Authentication process, user authentication, biometric authentication, multi-factor authentication, etc.	<i>“User perceptions of security and usability of singlefactor and two-factor authentication in automated telephone banking.”</i> Two-factor authentication (Grobler et al., 2021)
Services	498 (2166)	Online services, healthcare services, cloud-based services, service delivery, social services, etc.	<i>“For example, many healthcare services such as diagnosing cardio rate, measuring blood pressure, or detecting fever can be performed at users’ end to eliminate prior appointments or personal visits to health</i>

Table 2.7. Continued

Auto-coded Themes	# of Files (References)	Example Codes	Examples of Usage, Code (Article Reference)
			<i>units.</i> ” Healthcare services (Aljedaani et al., 2021)
Method	444 (1705)	Authentication method, existing methods, qualitative methods, data collection methods, research methods, etc.	<i>“The limitations of usability include issues such as taking more time to log in, passwords being too difficult to recall after a period of time, and the authentication method being too complicated for users without proper education and practice.”</i> Authentication method (Sun et al., 2018)
Password	399 (4599)	Graphical passwords, complex passwords, password strength, password managers, one-time password, etc.	<i>“Those users who could not choose secure and strong passwords made the authentication process insecure and gave opportunities to attackers to gain access to the passwords [2-3].”</i> Strong password (Khodadadi et al., 2021)
Key	336 (1335)	Private key, public key, key management, key exchange, key concerns, etc.	<i>“The server also generates a public key (g, gy), which is given to all clients.”</i> Public key (Lim et al., 2020)
Attacks	330 (1944)	Brute force attacks, malicious attacks, attacker model, phishing attacks, social engineering attacks, etc.	<i>“For example, a lack of encryption to protect transmitted passwords, storage of clear text passwords in server databases and little protection of passwords from brute force attacks were common amongst the websites surveyed.”</i> Brute force attacks (Grobler et al., 2021)
Design	314 (1139)	Study design, system design, interface design, industrial designers, human-	<i>“For example, a lack of encryption to protect transmitted passwords, storage of clear text</i>

Table 2.7. Continued

Auto-coded Themes	# of Files (References)	Example Codes	Examples of Usage, Code (Article Reference)
		centered design, etc.	<i>passwords in server databases and little protection of passwords from brute force attacks were common amongst the websites surveyed.</i> ” System design (Grobler et al., 2021)
Note: The examples and excerpts provided above are not exhaustive and are for reference purposes only.			

Gaps in Current Literature and Potential Future Research Opportunities

To identify gaps in the existing literature, the dataset, study constraints, qualitative codes, and themes derived from the word frequency and thematic analyses were carefully reviewed.

One notable limitation in prior studies is the restricted scope and small sample sizes, often resulting from narrow search criteria. As discussed in the *Scope, Gaps, and Contributions of Prior Literature* subsection, earlier reviews frequently relied solely on author keywords or focused on datasets with fewer than 100 articles (Di Nocera et al., 2023; Garfinkel & Lipford, 2014; Grobler et al., 2021; Lennartsson et al., 2021; Reuter et al., 2022). Some also concentrated on specific subfields within cybersecurity, such as software engineering (Distler et al., 2021; Nwokedi et al., n.d.). This SLR aimed to address these limitations by broadening the search parameters to include multiple fields - title, topic, abstract, and author keywords, and analyzing a substantially larger dataset of 1013 articles. Despite these improvements, some gaps persist. For instance, while the

dataset includes documents that mention both UX and Cybersecurity, some may treat them as separate topics rather than discussing their convergence. This could introduce content that is less relevant to the intended focus. Future research could refine filtering criteria to better target studies that explicitly address Usable Security, following the approach taken in earlier focused reviews.

Another significant gap is the limited discussion of standards or frameworks specifically tailored to Usable Security. This observation aligns with findings from other literature reviews (Di Nocera et al., 2023). Existing frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provide Community Profiles, that is, implementation guidance for specific sectors or technologies but do not offer specific guidance on Usable Security (NIST, 2024; NIST National Cybersecurity Center for Excellence (NCCoE), n.d.). The subsequent chapters of this dissertation study aim to address this gap by exploring the development of a dedicated NIST CSF-based Usable Security Community Profile or implementation guidance, building on existing templates and methodologies (NIST, 2024; Pascoe et al., 2024; Rajarathnam & Singh, 2023), which would fill a critical gap in the field of Usable Security.

CHAPTER THREE

MATERIALS AND METHODS

Overview

To address the identified gap in the literature concerning the convergence of cybersecurity and UX fields, specifically, the lack of standards or frameworks tailored to Usable Security (Di Nocera et al., 2023; Rajarathnam & Singh, 2024), as discussed in *Chapter 2 (Literature Review)*, a set of overarching research objectives, Research Questions (RQs), and Sub-Research Questions (Sub-RQs) were developed. This chapter presents these research objectives and RQs, along with the methodological approach employed to investigate these questions, including details on sampling strategies, data collection and analysis procedures. The main objective of this research is to develop a NIST CSF Community Profile for Usable Security, that is, a customizable baseline that addresses common cybersecurity outcomes from the NIST CSF for a particular sector or context, in this case, for the Usable Security domain. Specifically, this NIST CSF-based Usable Security Community Profile will help organizations improve the UX of their cybersecurity tools & platforms, policies & standards, and training initiatives.

Research Questions (RQs)

RQs and Sub-RQs

To guide the development of the NIST CSF-based Usable Security Community Profile, this dissertation study is driven by three (3) primary research questions (RQs), each with multiple sub-questions as outlined below:

Phase I: Template Development

RQ1: What are the standard elements of a NIST CSF Community Profile?

- Research Objective: To develop a standardized template for a NIST CSF Community Profile based on published examples, which will serve as the foundation for the subsequent development of the NIST CSF Usable Security Community Profile.

Sub-RQ1a: What are the common elements among the NIST CSF Profiles examples?

Sub-RQ1b: What are the key differences among the NIST CSF Profiles examples?

RQ2: What are the UX challenges faced by Cybersecurity/IT teams in an organization?

- Research Objective: To identify the critical elements that should be included in the NIST CSF Profile, ensuring it accurately addresses the UX challenges faced by Cybersecurity teams, and by extension, IT teams, within corporate environments.

Phase II: Pilot Study

Sub-RQ2a: What are the UX challenges faced by organizations when using their cybersecurity tools & platforms, policies & standards, and practices?

Sub-RQ2b: What are the potential challenges of implementing a framework for assessing Cybersecurity UX in an organizational setting?

Phases III & IV: Dissertation Study (using Surveys & Interviews)

Sub-RQ2c: What are the UX challenges that Cybersecurity/IT teams in an organization face when implementing or operating their cybersecurity tools & platforms?

Sub-RQ2d: What are the UX challenges that Cybersecurity/IT teams in an organization face when implementing and/or managing their internal policies & standards?

Sub-RQ2e: What are the UX challenges that Cybersecurity/IT employees face when they are assigned tool or role-specific training?

RQ3: What are the UX elements that are critical for organizations from a Usable Security standpoint, and how can they be integrated into a NIST CSF Community Profile?

- Research Objective: To collect data about critical Usable Security elements for different types of organizations, verify the results from RQ2, and develop the Community Profile for Usable Security domain using the standardized template from RQ1

Sub-RQ3a: What UX principles are most critical for inclusion in a cybersecurity framework?

Sub-RQ3b: Which NIST CSF Core components (such as Functions and Categories) are relevant to or impacted by Usable Security considerations?

Sub-RQ3c: What are the UX challenges that organizations face when developing or maintaining their tool or role-specific training?

RQs Breakdown & High-level Approach

Table 3.1 below outlines the breakdown of the Research Questions (RQs) to provide a clearer understanding of the scope of this proposed dissertation study.

Table 3.1. High-level overview of the author / student’s broader research efforts

Research Questions (RQs)	Research Stage	Status, Timeline, and Outcomes
N/A - Precursor to the proposed dissertation study	Pre-phase I Systematic Literature Review (SLR) of Cybersecurity & UX	Status: Completed (pre-PhD proposal defense) Timeline: Aug 2022 - May 2024 (Fall 2022 - Spring 2024) Outcome: Paper presented at IEEE Cyber Awareness and Research Symposium 2024 (Rajarithnam & Singh, 2024)
RQ1	Phase I Developing a standardized template for creating NIST CSF Community Profiles	Status: Completed (pre-PhD proposal defense) Timeline: Aug 2022 - May 2023 (Fall 2022 - Spring 2023) Outcome: Poster presented at IEEE Symposium on Security and Privacy (S&P) 2023 (Rajarithnam & Singh, 2023)
RQ2 Sub-RQ2a Sub-RQ2b	Phase II Pilot Study to explore the feasibility of implementing a framework to assess an organization’s Cybersecurity UX	Status: Completed (pre-PhD proposal defense) Timeline: Aug 2023 - May 2024 (Fall 2023 - Spring 2024) Outcome: Paper accepted to be presented at IEEE Cyber

Table 3.1. Continued

Research Questions (RQs)	Research Stage	Status, Timeline, and Outcomes
		Awareness and Research Symposium 2025 (Rajarithnam & Singh, 2025)
RQ2 Sub-RQ2c Sub-RQ2d Sub-RQ2e	Phase III Refining the pilot study's survey instrument and expanding the research across multiple organizations	Status: Completed (current dissertation study) Timeline: Aug 2024 - Aug 2025 (Fall 2024 - Summer 2025) Outcome: PhD dissertation
RQ2 Sub-RQ2c Sub-RQ2d Sub-RQ2e	Phase IV Refining the interview process and extending the study to include multiple organizations	Status: Completed (current dissertation study) Timeline: Aug 2024 - Aug 2025 (Fall 2024 - Summer 2025) Outcome: PhD dissertation
RQ3 Sub-RQ3a Sub-RQ3b Sub-RQ3c	Post-phase IV Synthesizing study results, developing a NIST CSF-based Usable Security Community Profile, and Expert Review	Status: Completed (current dissertation study) Timeline: Aug 2024 - Dec 2025 (Fall 2024 - Fall 2025) Outcome: PhD dissertation
Note: Grayed-out rows indicate research stages completed during the first two (2) years of the student's broader research efforts, prior to the PhD dissertation proposal defense, conducted under their advisor's supervision. These stages are outside the scope of this dissertation and are provided for context.		

The first research question (**RQ1**) laid the groundwork for this dissertation study. It involved conducting a document analysis of 14 Community Profiles (formerly referred to as Profiles) published by NIST (National Institute of Standards and Technology (NIST), 2021) based on the NIST CSF v1.1 (National Institute of Standards and Technology, 2018), which spanned various industries, technologies, and use cases, including manufacturing, election infrastructure, and ransomware mitigation, among others. The analysis identified common elements and key differences across these Profiles, leading to the development of a standardized template for creating Community

Profiles based on the NIST CSF v1.1, the previous iteration of the framework. This template was as a poster at the IEEE Symposium on Security and Privacy (S&P) 2023 (Rajarathnam & Singh, 2023). Additional details are included in **Appendix E**.

Concurrently, NIST released a Community Profile template (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024) with the latest iteration, NIST CSF v2.0 (National Institute of Standards and Technology (NIST), 2024), which further emphasized the significance of this study phase.

The second research question (**RQ2**) involves both a completed IRB-approved pilot study (ID: UTK IRB-23-07689-XM) (Rajarathnam & Singh, 2025) and this dissertation study. The pilot study tested the feasibility of assessing cybersecurity UX within a single organization in Tennessee, USA. Additional details are included in **Appendix F**. This dissertation study expanded the scope of the pilot study by gathering data from multiple organizations across diverse sizes and sectors in the US to develop generalizable, industry-wide recommendations. **RQ2** is divided into five (5) sub-questions, two (2) of which were answered (Sub-RQ2a & 2b) in the pilot study (**Appendix F**), and the remaining three (3) are addressed in this dissertation study. These sub-questions aim to systematically investigate different aspects of organizational Cybersecurity UX: Sub-RQ2c focuses on cybersecurity tools & platforms, Sub-RQ2d on policies & standards, and Sub-RQ2e on role-specific cybersecurity training initiatives. This segmentation enabled a focused data collection and analysis.

The third research question (**RQ3**) links the UX challenges identified through RQ2 with the standardized NIST CSF Community Profile template from **RQ1** (Rajarathnam & Singh, 2023) (**Appendix E**), as well as NIST's newly released version (NIST, 2024; Pascoe et al., 2024). Sub-RQ3a explores how UX principles align with organizations' cybersecurity goals and business/mission objectives, while Sub-RQ3b maps Usable Security considerations to NIST CSF Core components. Sub-RQ3c helped guide the development of the Usable Security NIST CSF Community Profile based on corporate data and includes the viewpoints and feedback of relevant stakeholders and industry leaders.

To address the research questions and objectives, this dissertation study adopts a mixed-methods research design, specifically using an explanatory sequential approach (Creswell, 2014; Fetters et al., 2013; Sandelowski, 2000). In the third phase, broad, generalizable data was collected through surveys to assess the current state of cybersecurity UX across tools & platforms, policies & standards, and training within organizations. In the fourth phase, follow-up interviews (individual and/or group) were conducted with a subset of survey participants. The sequential approach ensured that the follow-up qualitative research was targeted and relevant, focusing on the most important issues or patterns identified in the survey data.

This dissertation study builds upon findings from the previously IRB-approved pilot study (ID: UTK IRB-23-07689-XM) (Rajarathnam & Singh, 2025), which explored

the feasibility of implementing a framework to assess an organization’s cybersecurity UX in a real-world setting (phase II, **Appendix F**). The survey instruments and interview questions used in this study are adapted from the pilot study, incorporating lessons learned and participant feedback. Following the analysis of both the survey and follow-up interview data, recommendations and general guidance were formulated into a NIST CSF-based Community Profile. This draft profile was then presented to or shared with experts, including survey and interview participants to gather feedback and refine the Community Profile based on their expert input. **Figure 3.1** demonstrates the relationship between questions, research design, and relevant artifacts.

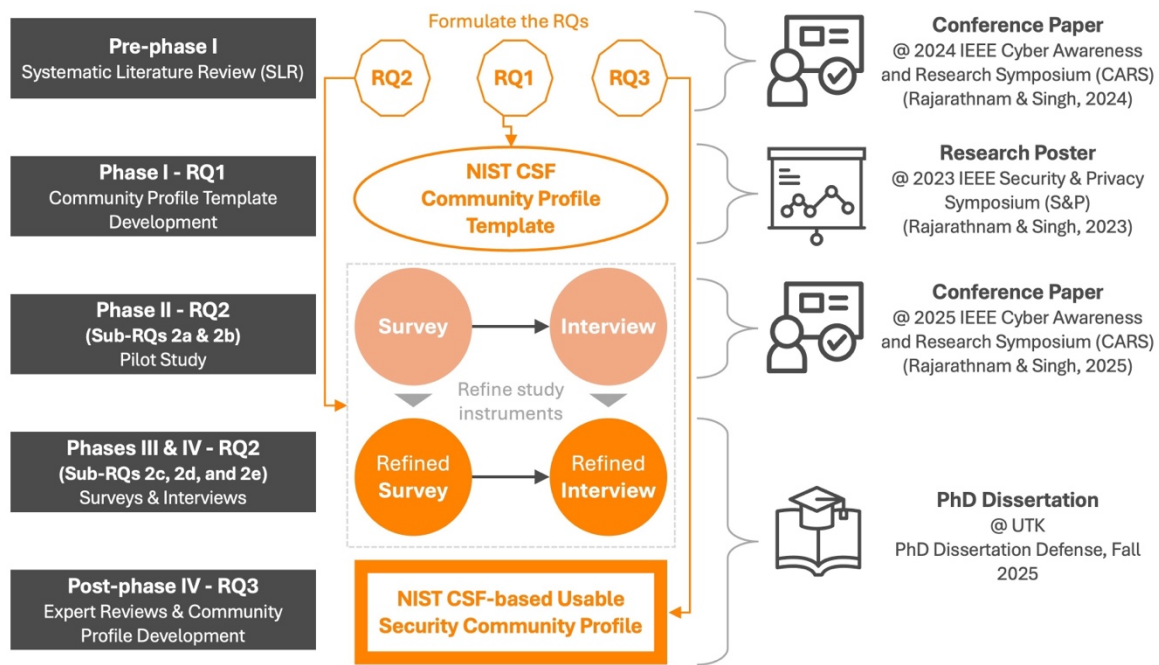


Figure 3.1. Mapping of the RQs to the research design and artifacts

Phase III: Surveys

Approach

In order to reach a broad and diverse set of participants, online surveys were utilized in the third phase of the project, with Qualtrics serving as the platform for data collection. This approach predominantly gathered quantitative data. The survey aimed to identify key issues, trends, and patterns from a large sample of employees, with the quantitative data enabling statistical analysis to assess the significance of observed patterns. This analysis helped provide a clear picture of where the main issues lie (Creswell, 2014; Fetters et al., 2013).

Additionally, survey participants had the option to volunteer for follow-up interviews. The survey focused on addressing the second research question, outlined below for reference.

RQ2: What are the UX challenges faced by Cybersecurity/IT teams in an organization?

Study Population and Criteria

A total of 110 survey responses were collected for this dissertation, representing multiple organizations across the US. Of these, 82 were complete responses and 28 were partial. Survey respondents came from a diverse range of industries, including Information Technology (IT), healthcare, financial services, education, and so forth.

Survey data collection was conducted virtually, and follow-up interviews were carried out through a combination of virtual and in-person methods, depending on participant availability and preference.

The achieved sample size aligns with research best practices (Babbie, 2020; Fowler, 2013; Regmi et al., 2016). While initial estimates were based on the U.S. cybersecurity workforce of approximately 1.34 million professionals (National Center for Science and Engineering Statistics, 2024), with a 95% confidence interval and a 5% margin of error, the final number of 110 participants is consistent with the specialized and niche nature of the cybersecurity field. In addition, 26 participants took part in follow-up interviews, which provided deeper qualitative insights and helped uncover perspectives not fully captured in the survey data.

A stratified purposive/judgmental sampling approach was used to identify participants, with strata based on organizational roles within cybersecurity (e.g., executives, managers, technical staff, etc.). Recruitment occurred through pre-established connections, professional networks, and word-of-mouth referrals, supplemented by email invitations. This approach ensured representation across industries and organizations of varying sizes, from small start-ups to large corporations.

Instruments & Procedures

A structured survey questionnaire was administered online using Qualtrics, one of the leading online survey platforms. Qualtrics is compliant with the university's IRB requirements for securely collecting and storing data, including Personally Identifiable Information (PII), by providing encryption during transit, at rest, and in backups (OIT UTK, n.d.).

The questionnaire was administered online during fall 2024, spring 2025, and summer 2025 (September 2024 - July 2025) using Qualtrics. Participants received an email invitation containing a link to the questionnaire, along with a brief explanation of the study's purpose and instructions for completing the questionnaire. The questionnaire started with a section or question for Informed Consent before navigating to the remaining questions. The email invitation is included in **Appendix A**.

The survey questionnaire (**Appendix B**) included a combination of open-ended and closed-ended questions to assess employees' familiarity with cybersecurity tools & platforms, policies & standards, education, awareness, and training, as well as the UX challenges they encounter. The questionnaire also gathered demographic information and details regarding participants' organizational roles and responsibilities. The survey questions are largely adapted from a previously approved pilot study (ID: UTK IRB-23-07689-XM, **Appendix F**) (Rajarithnam & Singh, 2025), and the full instrument is divided into 3 sections, totaling 32 items. On average, the survey was designed to take

under 12 minutes to complete, as research has shown that surveys exceeding 12 minutes often experience higher dropout rates (Qualtrics Support, n.d.). The survey questionnaire follows research best practices such as using straightforward questions, avoiding double-barreled questions or double negation statements, ensuring that the survey is optimized for viewing on mobile devices, and so forth (Babbie, 2020; Fowler, 2013; Qualtrics Support, n.d.; Sanders et al., 2021). The survey questionnaire is included in **Appendix B**.

Analysis

The survey data collected through the questionnaire were analyzed using descriptive statistics, such as means and standard deviations. Microsoft Excel pivot tables and charts were employed for data analysis and visualization. In addition, word frequency analysis using NVivo was conducted for selected survey questions related to cybersecurity tools & platforms. Responses to open-ended or text-input questions (e.g., those addressing challenges with cybersecurity tools and platforms) were manually analyzed to identify key themes and to inform the design of the follow-up interviews.

Phase IV: Interviews

Approach

The subsequent qualitative phase (interviews) delved deeper into the specific issues and patterns identified in the third phase, aiming to understand the underlying reasons behind these trends (Creswell, 2014; Fetters et al., 2013; Sandelowski, 2000). This phase provided deeper insights into the survey data by allowing participants to

expand on their experiences and offer suggestions helping in the development of the NIST CSF Community Profile for Usable Security.

The follow-up interview questions were tailored to participants' roles and experiences, based on the survey data. For example, if a participant was involved in cybersecurity tools and platforms procurement, follow-up questions addressed procurement criteria and whether UX considerations were included. Conversely, if procurement was not part of their role, interviews focused on other areas such as day-to-day tool usage. Moreover, any unexpected trends or findings in the survey data were further explored and clarified during the interviews (Creswell, 2014; Fetters et al., 2013; Sandelowski, 2000).

The follow-up interviews were conducted either individually or in small groups, depending on participants' availability. They took place in person at mutually convenient locations or online via Zoom (or a suitable alternative), based on participants' preferences, ensuring that participation is accessible and convenient.

Study Population and Criteria

For the fourth phase, 26 participants from the survey pool were interviewed, either individually or in groups. These participants will be chosen through stratified purposeful sampling, aiming to provide deeper insights into the themes and issues identified during the survey analysis. The same strata used in the survey phase, based on

organizational roles, guided participant selection to ensure a well-rounded understanding of the UX challenges across different roles within cybersecurity. \$50 gift cards were offered as incentives to encourage participation in the follow-up interviews.

Instruments & Procedures

For the fourth phase, 26 participants from the survey pool were interviewed, either individually or in groups. The interviews were conducted in spring 2025 and summer 2025 (January 2025 - July 2025), either in-person at a mutually convenient location (e.g., participant's office) or online using UTK's Zoom video conferencing software and were recorded with the participants' permission.

Each interview lasted approximately 30-60 minutes. UTK's Zoom software was used for the recording and Microsoft Word Online and/or Zoom were used for transcription (for both; online and/or in-person). If requested by participants, suitable alternate UTK video conferencing software such as Microsoft Teams or Google Meet were used, depending on the participants' corporate policies and preferences. The interviews were conducted either individually or in a group setting, with participants encouraged to invite collaborators or team members, preferably those who also participated in the survey. This flexible approach was guided by the availability and convenience of the participants, ensuring a diverse and comprehensive discussion. For the interviews, participants were informed about the study's purpose and procedures, and

their consent was obtained either prior to or at the time of their participation. The informed consent form, based on the UTK IRB template (UTK IRB, n.d.), is included in **Appendix C**. The interview questions have also been largely adapted from a previously IRB-approved pilot study (ID: UTK IRB-23-07689-XM) (Rajarithnam & Singh, 2025), and draft list of questions included in **Appendix D**.

A \$50 gift card for Amazon, Target, or another suitable vendor was offered as an incentive to encourage participation in the interviews. Details regarding funding for the gift cards are outlined in the Budget sub-section below.

Analysis

The interview data were analyzed using thematic analysis (Braun & Clarke, 2006) and subsequently compared with insights from the survey questionnaire to enable triangulation and enrich the analytical depth.

During the pilot phase (**Appendix F**), NVivo auto-coding and thematic analysis was employed for the analysis of the interview data (Dhakal, 2022; Lumivvero, n.d.). However, for this dissertation study, generative Artificial Intelligence (AI) was integrated into the analysis process because of its advantages over traditional Computer-Assisted Qualitative Data Analysis Software (CAQDAS). For instance, recent studies indicate that tools such as ChatGPT can support thematic analysis by (i) improving efficiency in handling large volumes of qualitative data, (ii) reducing variability and individual coder

bias during the early stages of coding, (iii) facilitating the identification of latent themes and connections not immediately visible through manual analysis, and (iv) enhancing the transparency and reproducibility of coding protocols (Goyanes et al, 2025).

Although Microsoft Copilot was originally proposed to be used in the dissertation plan based on availability through institutional licensing, ChatGPT (GPT-5, Plus subscription) was used as the suitable alternative due to Microsoft Copilot's session limits that restricted continuity in the analysis process.

The protocol for AI-assisted interview data analysis developed by Goyanes et al. (2025) was followed. This protocol is itself based on Braun and Clarke's (2006) six-step framework for thematic analysis but tailored to the use of generative AI. The prompts from the online appendix and protocol provided by Goyanes et al. (2025) were adapted to the needs of this study. For example, prompts relating to convergences and divergences across participants were excluded, as these were less relevant to the research focus of this dissertation study. Another notable adaptation concerned prompt engineering efforts: explicit instructions were added to the prompts requesting verbatim quotations only. This was necessary because initial exploratory analysis on earlier models (GPT-4o / GPT-4.5, free subscription) occasionally presented paraphrased content as direct quotations, which risked compromising the integrity of the qualitative data. The adapted steps undertaken in this dissertation were as follows:

- Data preparation: Interview transcripts were manually transcribed, anonymized, and formatted with clear headings, labels, and identifiers before being uploaded to ChatGPT. To accommodate file upload limitations, transcripts (PDF files) were uploaded one at a time, with follow-up prompts confirming successful file upload.
- Defining the analysis process: Structured prompts were designed to guide ChatGPT in identifying recurring and overarching themes across the dataset.
- Chatbot interaction: ChatGPT was asked to summarize each theme individually, provide representative quotes, and categorize them into relevant subtopics. Additional prompts were used to extract keywords and categorize responses.
- Iterative process: Follow-up prompts were employed to clarify and expand emerging themes. Detailed thematic analyses were requested for each theme, supplemented by tables summarizing themes, sub-themes, associated keywords, and illustrative excerpts. Outputs were then manually reviewed, with sub-themes consolidated or reorganized based on the researcher's judgement. For instance, more than 45 sub-themes or topics across 8 main themes were initially produced by ChatGPT; these were then manually consolidated into 18 sub-themes organized under 3 main themes to achieve clarity and cohesion.
- Review and validation: AI-generated outputs were validated against NVivo auto-coding and thematic analysis results. Transcripts were also manually revisited to confirm the accuracy and contextual relevance of the quotes in the AI-generated output.

- Analysis and interpretation: The final stage involved the researcher's synthesis of ChatGPT outputs with interpretive insight, producing a coherent account of the key UX issues and themes related to cybersecurity tools & platforms, policies & standards, and role-specific training initiatives.

The themes, sub-themes, and quotes from the thematic analysis of the interview data were compared with the insights from the survey data analysis to triangulate findings and enhance analytical depth.

Post-Phase IV Analysis, Expert Review and Iteration

Approach

Drawing on the findings from **Phase III (survey)** and **Phase IV (interview)** data analysis, a NIST CSF Usable Security Community Profile was developed, presented in *Chapter 5* of this dissertation. This Profile was developed using templates based on NIST's official Community Profile template (NIST, 2024; Pascoe et al., 2024) and the earlier template published by the author (Rajaratnam & Singh, 2023).

The NIST CSF Usable Security Community Profile development and expert review focused on addressing the third research question, outlined below for reference.

RQ3: What are the UX elements that are critical for organizations from a Usable Security standpoint, and how can they be integrated into a NIST CSF Community Profile?

Community Profile Elements and Integration of Practitioner Insights

The NIST CSF Usable Security Community Profile articulated key business and mission objectives from a usable security perspective and mapped the major themes identified during the survey and follow-up interview data analysis to relevant *Functions* and *Categories* of the NIST CSF (v2.0) Core. Issues and recommendations raised by practitioners in follow-up interviews were integrated into the Profile, ensuring that the proposed framework reflected professional practice. In addition, the *Priority* and *Rationale* elements of the template were grounded in recurring themes from the follow-up interviews, highlighting how they influenced the UX of cybersecurity tools & platforms, policies & standards, and role-specific training initiatives in organizational contexts. The Profile also incorporated *Informative References* from authoritative sources, including the Human-Centered Cybersecurity projects developed by the NIST Information Technology Laboratory Computer Security Resource Center, supplemented by relevant scholarly literature in the field of Usable Security. The Profile also incorporated *Informative References* from sources such the Human-Centered Cybersecurity projects developed by the NIST Information Technology Laboratory Computer Security Resource Center, alongside relevant scholarly sources in Usable Security, to ensure alignment with both practice and research.

Expert Review

To validate and refine the draft Community Profile, an expert review was conducted. Experts were drawn from **Phase III** interview participants according to the following defined selection criteria:

- **Experience:** a minimum of 5 years for professional-level participants, and typically 7–10 years or more for managerial and executive participants. This level of experience ensured that reviewers possessed a mature understanding of cybersecurity standards, frameworks, and their practical application within organizational contexts, as well as an informed perspectives on the usability and UX considerations that arise when implementing such frameworks in practice.
- **Roles:** spanning professional, managerial, and executive functions, including product management, consulting leadership, and senior technical roles.
- **Engagement:** direct involvement in critical cybersecurity functions such as tools & platforms procurement, leading client engagements, cybersecurity policies & standards development, and so forth.
- **Willingness:** expressed readiness to provide further feedback during interviews.

Table 3.2 presents the follow-up interview participants selected for the expert review panel, together with their roles and anonymized information regarding position and organization. The selection process was conducted with oversight from the dissertation committee to ensure methodological rigor. Communications with the expert reviewers were facilitated through email correspondence.

Feedback from the expert review contributed directly to the refinement of the issues and recommendations presented in the NIST CSF-based Usable Security Community Profile (please refer to *Chapter 5*). The expert reviewers also suggested additional resources to include as Informative References, strengthening the practical utility of the Community Profile for practitioners. Moreover, they provided insightful guidance on translating the research outcomes into real-world applications, both within organizational cybersecurity programs and in the researcher’s professional trajectory. Lastly, reviewers also words of encouragement, affirming the relevance and potential impact of integrating usability and UX considerations into the NIST CSF context.

Table 3.2. Expert review panel comprising selected follow-up interview participants, presented with their roles and anonymized position and organizational information, in accordance with the established selection criteria.

Participant #	Role	Position & Organization (Anonymized)
Participant 5	Managerial	Director, Big 4 Accounting Firm, Cybersecurity Consulting Practice
Participant 8	Managerial	Director (Sr. Manager at time of interview), Big 4 Accounting Firm, Cybersecurity Consulting Practice
Participant 10	Managerial	Product Manager, Hospital & Healthcare Organization (~10,000+ employees)
Participant 26	Executive	Managing Partner, IT Services & Consulting Company (2–10 employees)

Iteration

Expert feedback was systematically integrated into the Profile. Reviewers emphasized the importance of clarifying how UX-focused themes were mapped to NIST

CSF (v2.0) Core Functions & Categories, refining the Priority and Rationale sections for practical applicability, and ensuring balance between Informative References from relevant industry sources and scholarly literature in Usable Security. Through this iterative process, the Profile was refined to ensure both theoretical grounding and validation by seasoned practitioners, enhancing its utility as a community-driven resource for integrating UX & usability into cybersecurity governance frameworks.

Timeline and Budget

Timeline

The timeline for the dissertation is shown in **Table 3.3**, along with the list of key activities, milestones, and status.

Table 3.3. PhD dissertation activities, milestones, status, and timeline.

Timeframe	Key Activities, Milestones, and Status
September 2024	- Proposal internal review with the committee chair (status: completed) - IRB application and documents preparation (status: completed)
October 2024	- PhD proposal submission to the committee (status: completed, 10/07/2024) - PhD proposal defense (status: completed, 10/21/2024) - Funding application (UTK Graduate Student Research Awards) submission (status: completed) - Presented the Systematic Literature Review (SLR) findings at the 2024 IEEE Cyber Awareness Research Symposium (CARS) (status: completed) (Rajarathnam & Singh, 2024)
November 2024	- IRB application submission and follow-ups, as needed (status: completed) - Funding (UTK Graduate Student Research Awards) approval (status: completed, 11/24/2025)
December 2024	IRB application follow-ups, as needed (status: completed)

Table 3.3. Continued

Timeframe	• Key Activities, Milestones, and Status
January 2025	• IRB approval (status: completed, 01/15/2025) • Started survey data collection (status: completed)
February 2025	• Continued survey data collection and follow-ups (status: completed) • Started survey data analysis (status: completed)
March 2025	• Continued survey data collection, follow-ups, and analysis (status: completed) • Began follow-up interview data collection (status: completed)
April 2025 - June 2025	• Continued survey data collection, follow-ups, and analysis (status: completed) • Continued follow-up interview data collection (status: completed) • Started follow-up interview data processing (e.g., transcript refinement) (status: completed)
July 2025 - August 2025	• Completed survey data analysis (status: completed) • Started follow-up interview data analysis (thematic analysis) (status: completed)
September 2025	• Continued refinement and iterating of follow-up interview data analysis (thematic analysis) (status: completed) • Dissertation draft write-up (status: completed) • Dissertation submission to the committee (status: completed, 10/21/2025) • Preliminary dissertation draft submission (status: completed, due 5:00 pm 09/25, via TRACE ¹ (UTK Graduate School, n.d.)) • Discuss initial findings & interpretation with the committee members (status: completed) • Reach out to Expert Review panel (status: completed)
October 2025	• Incorporate initial findings & interpretation feedback from committee (status: completed) • Continue reaching out to Expert Review panel (status: completed) • Dissertation defense (status: completed, scheduled for 11/04, due 11/07) • Present the Pilot Study findings at the 2025 IEEE Cyber Awareness Research Symposium (CARS) (status: completed, accepted) • Incorporate PhD dissertation feedback (status: completed, via TRACE)
November 2025	• Final PhD dissertation acceptance (status: completed, due

Table 3.3. Continued

Timeframe	Key Activities, Milestones, and Status
	5:00 pm 11/21, via TRACE ² (UTK Graduate School, n.d.)) • (Optional) Synthesize the research findings and submit them for publication as a journal article (status: future work)
Notes: ¹ Backup deadline (Early-Spring, Spring registration not required): 12/08 (UTK Graduate School, n.d.) ² Backup deadline (Early-Spring, Spring registration not required): 01/16 (2026) (UTK Graduate School, n.d.) Specific font colors - green , gray, blue , orange , and red are used to represent distinct statuses: completed , not started or not applicable, future work , in progress , and delayed , respectively.	

Budget & Funding Source

The approved budget for this dissertation study allocated funds to support participant incentives, with a maximum of 30 interview participants. Incentives were provided in the form of \$50 gift cards per participant, yielding a total approved budget of \$1500. Ultimately, 26 participants were recruited and compensated, resulting in a total expenditure of \$1300. Funding for the project was awarded through the University of Tennessee, Knoxville (UTK) Graduate School’s Graduate Student Research Awards (GSRA) program. This support ensured the provision of incentives necessary for participant recruitment, thereby facilitating successful completion of the interview phase (study **phase IV**).

Ethical Considerations

Approach

The proposed study adheres to the ethical principles of informed consent,

confidentiality, and anonymity. Participants were informed of the study's purpose and procedures, and their consent was sought prior to or at the time of their participation. This research study solely focuses on assessing an organization's cybersecurity User Experience (UX) and does not involve the collection of identifiable biospecimens. In terms of identifiable information, any secondary data used was carefully anonymized to ensure the confidentiality and privacy of participants. Strict data de-identification protocols were implemented to remove any Personally Identifiable Information (PII), safeguarding the anonymity of individuals throughout the data analysis and reporting processes. The study was approved by the University of Tennessee, Knoxville (UTK) Institutional Review Board (IRB) (ID: UTK IRB-24-08536-XM). Furthermore, the study also complies with any Non-Disclosure Agreement (NDA) requirements mandated by the participants' organizations.

CHAPTER FOUR

RESULTS AND DISCUSSION

Overview

This chapter presents the findings and interpretive discussion derived from the analysis of survey responses, follow-up interviews, and the researcher's analytical reflections. This chapter constitutes **Phase III & IV: Dissertation Study (using Surveys & Interviews)** of the dissertation study and addresses Sub-RQs 2c, 2d, and 2e under **RQ2: What are the UX challenges faced by Cybersecurity/IT teams in an organization?** Sub-RQs 2a and 2b are addressed in the **Phase II: Pilot Study**, detailed in **Appendix F**. The results & discussion are organized thematically, guided by the structure of the thematic analysis (Braun & Clarke, 2006; Goyanes et al., 2025) of the follow-up interview data. **Figure 4.1** introduces the high-level thematic map, which outlines the three (3) main themes and their associated sub-themes. These three (3) themes, namely *Tools & Platforms*, *Policies & Standards*, and *Training & Awareness*, form the backbone of the chapter's organization. Each theme is explored in its own section, with sub-sections dedicated to the corresponding sub-themes that emerged from the data analysis. To provide clarity and context, each of the three (3) main section begin with a segment of the thematic analysis table, which includes the high-level sub-themes and illustrative quotes or excerpts from the follow-up interviews, offering insight into how each theme emerged and was interpreted. The codebook, including qualitative codes and their definitions, is provided in **Appendix G** for reference. The results and discussion presented in this chapter serve as the foundation for the issues and recommendations

synthesized into a NIST Cybersecurity Framework (CSF)-based Usable Security Community Profile in *Chapter 5*, which aims to provide actionable guidance to practitioners.

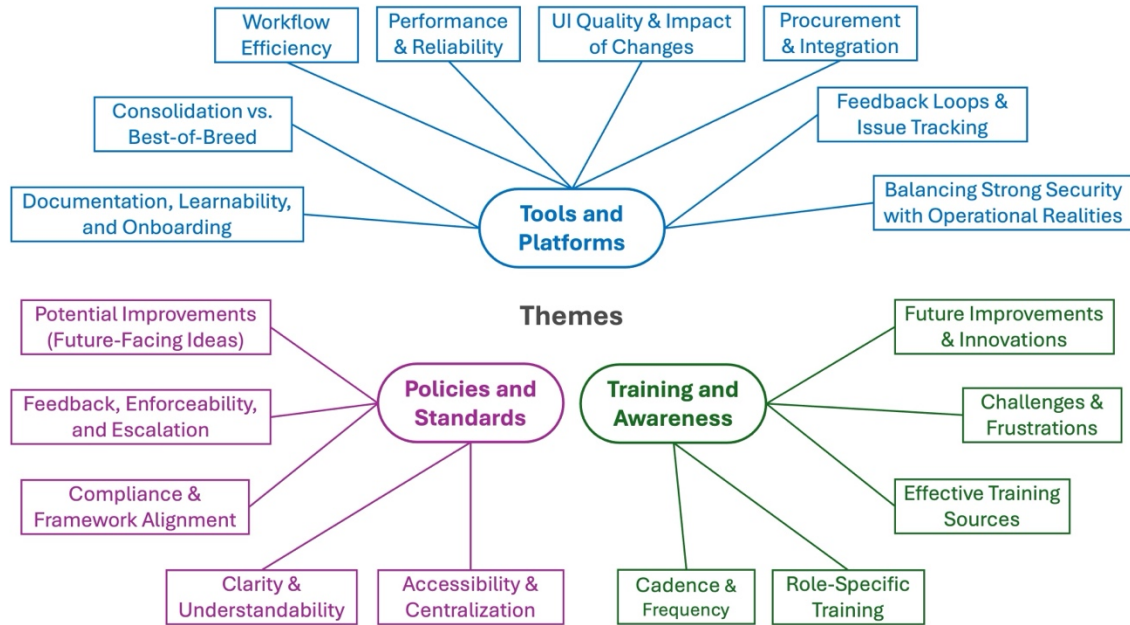


Figure 4.1. Thematic map illustrating the themes and sub-themes identified through thematic analysis of the interview data (Braun & Clarke, 2006; Goyanes et al., 2025).

(Sub-RQ2c) Theme 1: Tools & Platforms

Sub-RQ2c: What are the UX challenges that Cybersecurity/IT teams in an organization face when implementing or operating their cybersecurity tools & platforms?

This section addresses sub-RQ2c outlined above based on the data analysis of surveys and follow-up interviews. The sub-themes and illustrative excerpts from the interviews for the *Tools & Platforms* theme are presented in **Table 4.1**. The codebook,

including qualitative codes and their definitions, is provided in **Appendix G** for reference. The eight (8) interrelated sub-themes, namely *Procurement & Integration*, *Consolidation vs. Best-of-Breed*, *Workflow Efficiency*, *Performance & Reliability*, *UI Quality & Impact of Changes*, *Documentation*, *Learnability*, and *Onboarding*, *Feedback Loops & Issue Tracking*, and *Balancing Strong Security with Operational Realities* provide the analytic structure for the following subsections, where the survey results are integrated with qualitative insights from follow-up interviews, prior literature, the researcher's analysis and interpretive discussion.

Procurement & Integration (Tools & Platforms Sub-theme 1)

Survey findings suggest varied levels of involvement in the cybersecurity tools and platforms procurement process. Among those who responded to the question asking participants whether they are involved in the cybersecurity tools & platforms procurement, 49.51% indicated “yes” that they were involved, 14.56% said “maybe,” and 35.92% reported “no,” as shown in **Figure 4.2 (left)**. The extent of involvement varied: 32.31% respondents reported high involvement (e.g., leading the procurement process), 52.31% reported moderate involvement (e.g., participating in vendor evaluations), 12.31% reported minimal involvement (e.g., occasional feedback), while 3.08% said no involvement and 1.54% reported “not sure / not applicable,” as shown in **Figure 4.2 (right)**.

The follow-up interviews provided further insight into the procurement drivers.

Table 4.1. Sub-themes and excerpts from the overarching Tools & Platforms theme that were derived from the thematic analysis of the follow-up interview data.

Theme: Tools & Platforms	
Sub-theme	Example Quotes / Excerpts
Procurement & Integration	<i>“So yes, UX would be one of the options. One of the criteria, but it's not an important one. Always detections, all those things comes first.” (Participant 01)</i> <i>“Yeah, the criteria I've used in my security career, all spanning all the places I worked at, has been that threefold: 1. Making sure that complying with whatever regulations or laws are in place... HIPAA and... PCI and state of Tennessee requirements... The second criteria was... any obligations the company had... either in providing services for someone or requesting a third party provided service on our behalf to make sure that those obligations were met... And then finally... the safeguards that are appropriate to defend whatever the organization that was to make sure that it met those needs as well.” (Participant 26)</i> <i>“One of the things that we do with security tools, not so much here, but in any of the other places I've worked, is that we go with the function. What's the function we're trying to protect? How does it work? And then we work backwards from there. I don't think user experience is ever the first consideration. Sometimes, it's not considered at all, depending on how exclusive the tool is.” (Participant 15)</i> <i>“So, I think from a like core requirements perspective people will ask - do you have customizable dashboards? How flexible is the solution? Can you integrate with other solutions? And that's like more of a product capability perspective, but then how easy is it to integrate becomes like a UX thing. Like, can I go integrate with ServiceNow, or can I integrate with a third-party SIEM solution?” (Participant 09)</i> <i>“So, let's say we have X, Y, Z requirements, right?... solution A has two of the three criteria, solution B has one of the three, solution 3 has three of three. Obviously the choice would be solution 3 right based on POC perspective. But there are other nuances such as price, feasibility, you know, stakeholder management, where stakeholders would say this in this one platform has more roadmap options down the road.” (Participant 22)</i>
Consolidation vs. Best-of-Breed	<i>“CrowdStrike to me still the number one EDR tool that's out there – servers, workstations, it's just the best. However, Microsoft has Defender, they have a competitor to that, at you know, where it maybe it's not as pretty. Maybe it's not as well funded. Maybe it's not quite there on a comparison of capabilities. But the usability when I have one screen or one console... when I can stay in one place.” (Participant 26)</i>

Table 4.1. Continued

Theme: Tools & Platforms	
Sub-theme	Example Quotes / Excerpts
	<i>“Microsoft Defender - I'd say it's just as relevant because Defender provides the Endpoint Detection and Response, but it also provides e-mail security capabilities, so that you don't have to bring in CrowdStrike and ProofPoint. You can kind of just have Defender be slapped across multiple security functions, and it all has the same management console.” (Participant 11)</i> <i>“I primarily am responsible for Intune and then use Sentinel and Defender also. One thing is... not completely, but at least Microsoft tries to stay consistent across the different products. So, at least you're not totally learning a new UI moving from one to the other. Now, they could be more consistent for sure, but that is one thing that's helpful.” (Participant 18)</i> <i>“Maybe when it comes time to renew my license, if it costs more money to have a duplicate product... they want to keep me all in Microsoft things, Intune for Mobile Device Management, EntraID for Active Directory in the clouds, and all the things that they have in label to keep people kind of in that ecosystem...” (Participant 26)</i> <i>“There is a big obviously cost component... can this new vendor do this new capability, and also, replace my other three capabilities so that I'm not spending a lot of money and I don't have a lot of complexity...?” (Participant 09)</i>
Workflow Efficiency	<i>“...when you have like a Defender incident and then sends it over to Sentinel, a lot of the data that comes over isn't necessarily enough to work the incident, and you end up switching platforms and you move off a Sentinel and to the Defender for Endpoint when working an incident. I just find that really annoying because I feel like to a certain extent that kind of ruins the whole point of the SIEM.” (Participant 17)</i> <i>“How many clicks. How many times do I have to click before I get to what I'm looking for, and ideally the fewer clicks, the better... copy-pasting is a big part of my life... having direct links... open up in a new tab... limiting the number of clicks and the number of times I have to open a new window and copy-paste something... makes a big difference.” (Participant 23)</i> <i>“Even something simple as just accessing your Sentinel environments, we have to click through the same filters and buttons and do the same 5 steps every single time just to look at, for instance, that are assigned to us for today and there's no way to bookmark the page, no way to save that search query. No way, no way to do that stuff.” (Participant 14)</i>

Table 4.1. Continued

Theme: Tools & Platforms	
Sub-theme	Example Quotes / Excerpts
	<i>“So, I guess I'll give an example from like the DLP space with, you know... you know Purview... if the customer is having, experiencing you know, a large amount of false positives for however... how their data is structured on some of these data elements, Microsoft doesn't give you the ability to customize those out-of-the-box policies. So, it requires them then to go through and manually recreate and then tweak from there, without necessarily the visibility into some of the initial configuration that Microsoft had on the those sensitivity or sensitive data elements. So, they... they have to go from the ground up rather than, you know, the ability to kind of customize, and you know, an existing data element or policy that that the vendor has... has configured.” (Participant 05)</i> <i>“...what can I then do to make sure that people who are paid to look in a SOC monitor, SOC wall, look at the alerts, look at the things that happening, and make sure that they have the training and support they need so that they can reduce the time, from the time and alarm goes off... how quickly can I shorten the gap that they can recognize and respond to something?” (Participant 26)</i>
Performance & Reliability	<i>“So, you know, making sure the tools are fast, as fast as possible ... anything I can run a search on that does it quickly minimal number of clicks, minimal number of times that I have to go from one window to another. That all makes a big difference...” (Participant 23)</i> <i>“Basically everything that you can do in a console in a tool, you should be able to do it in API also. And if they had sufficient documentation on that, on their APIs, on the types of error codes you can receive, and... common troubleshooting things.” (Participant 21)</i> <i>“As a developer I've only pushed up a small change. But I'm having to wait 30 odd minutes and then after that I get like a timeout on the job or something. And again, there's no... none of my changes have been scanned and at that point if I force merge, I'm introducing a new vulnerability, potentially, which was missed.” (Participant 02)</i> <i>“Yeah, but with that, again, we've seen teams, you know, getting frustrated with certain tools because of the fact that there is no enough context there, you know... You know, some of them doesn't take like a risk-based approach to give them some priority on what needs to be worked on.” (Participant 06)</i> <i>“I do have this problem all the time, specifically with CyberArk, like when you're calling API's they're... they have very generic errors and they... like it will say unauthorized. Sometimes it'll even say unauthorized, and</i>

Table 4.1. Continued

Theme: Tools & Platforms	
Sub-theme	Example Quotes / Excerpts
	<i>that's not even what the error really is. And there's like a lot of with, like CyberArk especially, there's a lot of different reasons you can be unauthorized... like there's a lot of different authentication components there.”</i> (Participant 21)
UI Quality & Impact of Changes	<i>“I'd say the one thing with Microsoft Defender is that it seems like they do a lot of updates, and they're constantly, you know, working on that platform... once updates are shared and maybe the... the web page changes a little bit or some of the... the UX pieces changed, it seems like our teams were having to spend, you know, a... two to three days to really get caught up to speed, whereas with CrowdStrike it seems like things stayed the same, but the underlying technologies were being refreshed.”</i> (Participant 11) <i>“From a dashboarding perspective and an ability to customize your dashboards and generate executive reporting... how can I understand that my environment is safe?”</i> (Participant 09) <i>“...the issue was that on this UI, when you have 50 SaaS application, let's say you have... not every customer will buy 50 applications. But like think about it, if you have 50 applications, you can't put all the information in on the UI to show all the apps, right? It has to be... It has to be visible, but at the same time, it has to be like a drop-down or something on those lines which... which makes sense, because your page will be lengthy.”</i> (Participant 01) <i>“Usability comes in a little bit in terms of like integration or ease of... kind of connecting various platforms or log sources into certain areas... they're all going for that like single pane of glass view. So, if solutions aren't necessarily providing the ability to get data out, that kind of negatively impacts what the... at least they'll phrase as usability...”</i> (Participant 05) <i>“Is it clear, in a... dashboard... typically you know, red is bad typically, green is good... to be able to very quickly... see what's where's my to-dos... start at that high level. And then from there drill into what I need.”</i> (Participant 26)
Documentation, Learnability, and Onboarding	<i>“...these PDFs are like 200 pages long and you like no one has time to, like, read so many pages...”</i> (Participant 25) <i>“So, what we have done is like we have made like bite-size... bite-size videos. Once you onboard like a platform, you'll get these bite-size videos to just go through the user journey and it makes it easier for... for customers to... versus like just clicking through some links.”</i> (Participant 01)

Table 4.1. Continued

Theme: Tools & Platforms	
Sub-theme	Example Quotes / Excerpts
	<i>“One of the things that we added recently and has been received pretty well is: within every page in the in the product, there's a small help icon, and if you will learn something more about that specific page, you can click on that help icon and it will just pull up the documentation for it.” (Participant 02)</i> <i>“So, what we would do is like we'd have to develop a Build Book or Run Book to say, hey, when we are going to develop a virtual machine, if it's a server, a Windows Server or Linux Server, here are some of the options that will be presented to you and we'll document what they mean within like a formal procedural / build book.” (Participant 11)</i> <i>“...I once spent like half an hour in Splunk documentation trying to figure out how to do something that somebody did and I didn't know how they did it and so I hit the documentations. And after about 30 to 45 minutes, I'm like, I'm just going to give up and ask because I have no idea how they did that, and it turned out it was one incredibly simple thing that they did and I just didn't realize there was this tiny little button on the screen that they could click on.” (Participant 23)</i>
Feedback Loops & Issue Tracking	<i>“But like a lot of organizations formally we'll create a ticket using Jira in our case, so that it's documented and the engineers have something that they can then assign themselves to and work on to try to fix the problem.” (Participant 23)</i> <i>“Even like in theory, the documentation, what tells you how it's supposed to work - doesn't always translate to reality of what it's like. It might be out of date documentation, or it might not apply to your environments, or they don't just touch on what you're looking at, and they're like, oh, just call our support rep.” (Participant 14)</i> <i>“But what I like to see and with several clients I work with, they'll have regular touchpoints in with the vendor, whether it's CrowdStrike, whether it's Microsoft, or its Tenable, or whatever the vendor is... maybe on a Splunk, maybe on a monthly, maybe on a quarterly basis to... under NDA, under the support contracts thats in place, a vendor let me share my screen, what am I missing?” (Participant 26)</i> <i>“...what actually happens is it becomes a Teams chat to a manager... It's kind of like if there's a Slack channel or something, a little less formal, and there's not a formal paper trail.” (Participant 11)</i> <i>“...the challenge, the way we work around with that is very... it's thorough documentation. We call it a playbook. So, every time we have to do something, we go back to the playbook and look where it is because</i>

Table 4.1. Continued

Theme: Tools & Platforms	
Sub-theme	Example Quotes / Excerpts
	<i>we can't really change the tool, right? So unfortunately, if we could then, reorganize the tool.</i> ” (Participant 08)
Balancing Strong Security with Operational Realities	<i>“...when I'm implementing Okta mostly for my customers... we always tell customers to at least sign out all the users from the identity provider session once a day, which is, once in eight hours... But, depending on the customer that I'm working with, mostly I have seen for healthcare customers, they are absolutely not okay with this... say practitioners or their nurses are using their websites... if there is an emergency scenario and a person can die within seconds, but then if you just... if you just tell them that, hey, well you, you just have to do an username validation, authentication, etcetera, that would take somebody's life.”</i> (Participant 24) <i>“...one of the biggest, I think difficulties is... is just that, navigating that legacy environment... we work for a healthcare organization and a lot of times if it works, you don't touch it.”</i> (Participant 10) <i>“They purchase like every solution under the sun just to say they have it, and don't do any... or shouldn't say don't, but do limited work to kind of figure out what they truly need in their organization. So, a lot of things end up being shelfware, used for like a specific... specific use case, and they end up kind of inflating their cyber budget to pay for all these solutions, when they can get away with probably half of the... half of the solutions in their environment. That happens all over the place.”</i> (Participant 05) <i>“...think about when companies are in the cloud when they have products and services in the cloud, do they still need to pay for their network scanning license? Whether it's Tenable Nessus or Rapid7 or Qualys - when they're strong configuration monitoring in the cloud environments, do I still need to like, say with the Wiz, or with an Orca type of a product, do I still need to go in and do my scans with a scanning tool that, you can make a case for it, does a lot of those things already.”</i> (Participant 26) <i>“...if you cannot tell your users to sign out once in eight hours, at least try to do that once in maybe two days or three days.”</i> (Participant 24)
Note: The example quotes/excerpts shown above are not exhaustive and are limited to a maximum of five (5) per sub-theme for convenience and clarity. A complete list of excerpts obtained from the thematic analysis is available upon request.	

A recurring theme was that decisions were dominated by cybersecurity effectiveness and risk reduction, regulatory and legal compliance, cost, vendor reputation, and third-party and contractual obligations. As one participant summarized:

“Yeah, the criteria I've used in my security career, all spanning all the places I worked at, has been that threefold: 1. Making sure that complying with whatever regulations or laws are in place... HIPAA and... PCI and state of Tennessee requirements... The second criteria was... any obligations the company had... either in providing services for someone or requesting a third party provided service on our behalf to make sure that those obligations were met... And then finally... the safeguards that are appropriate to defend whatever the organization that was to make sure that it met those needs as well.” (Participant 26)

While UX and usability were occasionally mentioned, it was rarely decisive. When UX was considered at all, it was often evaluated informally during vendor demonstrations or Proofs of Concept (POC), rather than being embedded as a formal metric or core criterion in the procurement process. Dashboards that clearly conveyed status (e.g., “red is bad, green is good”) and allowed quick drill-down were appreciated but not prioritized over security efficacy or compliance. As one participant described:

“So yes, UX would be one of the options. One of the criteria, but it's not an important one. Always detections, all those things comes first.” (Participant 01)

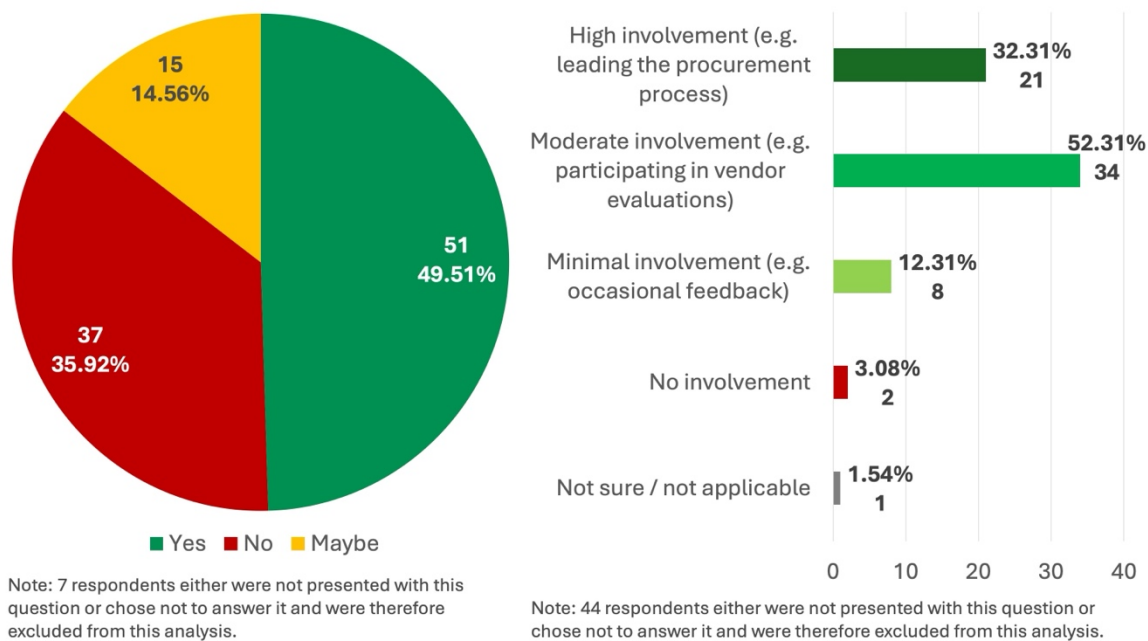


Figure 4.2. Charts showing survey responses to questions asking participants whether they're involved in the cybersecurity tools & platforms procurement (left), and their level of involvement in the procurement process (right).

Beyond compliance and security, procurement decisions were also influenced by budget constraints, licensing negotiations, and ecosystem lock-in. Participants described scenarios where vendor consolidation was favored to reduce governance overhead or eliminate duplicative tools. Long-term contracts often limited flexibility, even when usability concerns emerged post-deployment.

While the Systematic Literature Review (SLR, see *Chapter 2*) highlighted several studies that examined the UX/usability of cybersecurity tools & platforms in general, and design-stage considerations for improving tools' usability (Reuter et al., 2022; Grobler et al., 2021; Garfinkel & Lipford, 2014), there remains a notable gap in published research

regarding how usability and UX considerations are, or aren't factored into the procurement process for these tools & platforms. This gap points to the need for more formalized approaches that treat UX as a deliberate procurement criterion rather than an informal or secondary concern. The data-driven recommendations outlined in the NIST CSF-based Usable Security Community Profile (see *Chapter 5*) are intended to help address this specific shortcoming. Among the various Tools & Platforms sub-themes, this one represents a supplementary UX sub-theme, as the challenges identified here influence UX indirectly, through procurement decisions that determine which tools and design philosophies reach practitioners.

Consolidation vs. Best-of-Breed (Tools & Platforms Sub-theme 2)

A prominent sub-theme emerging from the follow-up interview data analysis was the strategic tension between adopting integrated platform suites (e.g., Microsoft suite) versus selecting best-of-breed tools (e.g., CrowdStrike for Endpoint Detection and Response (EDR)). Best-of-breed tools refer to specialized solutions that excel in a particular function or domain, often chosen for their superior capabilities compared to broader, integrated offerings. Participants consistently weighed the trade-offs between integration and operational simplicity on one hand, and technical depth and capabilities on the other.

Many organizations leaned toward consolidation, favoring platform approaches that offered a unified console, reduced complexity, and offered licensing advantages.

Microsoft's ecosystem was frequently cited as a preferred choice, not necessarily for superior technical capabilities, but for its bundling across enterprise agreements and ease of integration across the existing tools. As one participant explained:

“CrowdStrike to me still the number one EDR tool that's out there – servers, workstations, it's just the best. However, Microsoft has Defender, they have a competitor to that, at you know, where it maybe it's not as pretty. Maybe it's not as well funded. Maybe it's not quite there on a comparison of capabilities. But the usability when I have one screen or one console... when I can stay in one place.”
(Participant 26)

Despite acknowledging that best-of-breed tools often provided superior functionality and user interfaces, participants described how ecosystem lock-in, license renewal pressures, and cost-saving opportunities often tipped cybersecurity tools & platforms procurement decisions toward consolidated stacks. This was especially true when a single platform could replace multiple tools and reduce governance and operational overhead:

“Microsoft Defender - I'd say it's just as relevant because Defender provides the Endpoint Detection and Response, but it also provides e-mail security capabilities, so that you don't have to bring in CrowdStrike and ProofPoint. You

can kind of just have Defender be slapped across multiple security functions, and it all has the same management console.” (Participant 11)

This perspective broadens the discussion of cybersecurity UX beyond the design and interface level to include the UX of procurement and integration decisions. In doing so, it highlights that cybersecurity UX is not limited to how tools are designed, but also to how they are selected, bundled, and embedded within broader enterprise ecosystems, a dimension largely absent in the current literature. This is a core UX sub-theme that reflects challenges and implications at the ecosystem level, where integration simplicity and unified interfaces directly influence user workflows.

Adoption & Usage

Survey results indicated that 81.37% of participants who responded to the question asking participants whether they use any cybersecurity tools & platforms as part of their work said “yes”, while 6.86% said “maybe,” and 11.76% reported “no”, as shown in **Figure 4.3**. Follow-up survey questions asked participants to mention cybersecurity tools & platforms they used as part of their work, along with the most and second-most used tools.

In follow-up survey questions, participants were asked to list the cybersecurity tools & platforms they use, as well as to identify their most and second-most frequently used ones. Responses revealed a wide spectrum; 100+ unique tools and platforms were

listed, ranging from specific tools (e.g., Splunk, Wiz.io, Okta, etc.) to product suites (e.g., Microsoft suite, including tools like Microsoft Defender, Purview, etc.) and broader tool categories (e.g., Security Information and Event Management (SIEM), scanning solutions, Endpoint Detection and Response (EDR), etc.). Among the “most used” and “second-most used” responses, participants cited 60+ distinct tools, suites, or categories, reflecting the heterogeneity of organizational cybersecurity tool ecosystems. This diverse set of tools and platforms lays the groundwork for tailored recommendations presented in the NIST CSF-based Usable Security Community Profile (see *Chapter 5*) that align suggestions for improving UX with specific tools or types of tools. **Table 4.2** provides a more structured summary of the 25 tools & platforms identified by multiple participants as most frequently used in their work. To contextualize these findings, **Table 4.2** includes, alongside the name and frequency of each tool (or product suite), a brief description based on publicly available information, as well as a mapping to relevant NIST CSF v2.0 categories, as assessed by the researcher. This mapping not only organizes the survey data but also serves as a bridge to the qualitative findings from the follow-up interviews, where participants elaborated on usability challenges and pain points. By linking tool adoption & usage patterns to NIST CSF categories, reported usability issues, and recommendations, this analysis provides a foundation for the development of the NIST CSF-based Community Profile for Usable Security, which is presented in the next chapter, *Chapter 5 NIST CSF-based Usable Security Community Profile*.

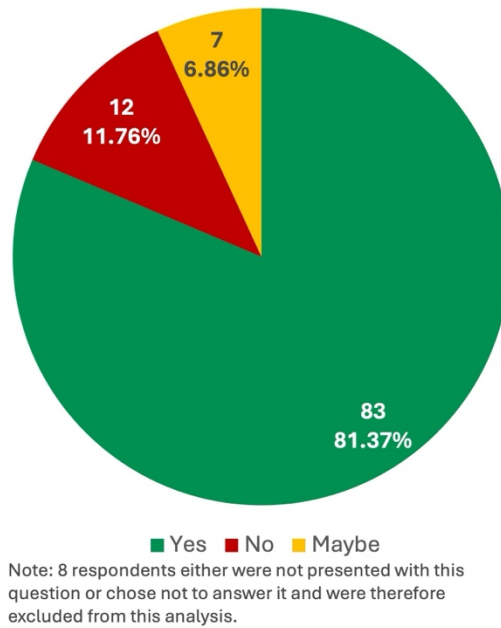


Figure 4.3. Chart showing survey responses to the question asking participants whether they use any cybersecurity tools & platforms as part of their work.

Usability

Survey participants were asked to identify the specific aspects of usability (Nielsen, 2012) that were applicable to the cybersecurity tools & platforms they use most frequently as part of their work. As shown in **Figure 4.4**, Efficiency (i.e., the efficiency in performing the desired task) and Memorability (i.e., being able to remember enough to use it effectively after initial use) were tied with each receiving 41 responses from those who responded to the relevant survey question. Satisfaction (the overall pleasantness of the design and user experience), followed with 32 responses. Meanwhile, Errors (i.e., low frequency and severity of errors, as well as ease of recovery from them) and Learnability (i.e., being easy to learn) were tied at 25 responses each. This distribution suggests that all aspects of usability are considered important by practitioners, despite minor variability

Table 4.2. Cybersecurity tools & platforms cited by multiple survey participants among their top two most used in their work, along with brief descriptions based on publicly available information, the number of participants who mentioned each tool/platform, and the relevant NIST CSF (v2.0) Category mappings as determined by the researcher.

Frequently Used Cybersecurity Tools & Platforms	Brief Description	# of Mentions (as Top 2 Most Used Tools & Platforms)	Relevant NIST CSF (v2.0) Categories
Wiz.io	Cloud-Native Application Protection Platform (CNAPP) offering security across cloud environments.	8	ID.AM (Asset Management), DE.CM (Security Continuous Monitoring), RS.AN (Incident Analysis), PR.DS (Data Security)
Splunk	Security Information and Event Management (SIEM) & data analytics platform for log management, threat detection, and incident response.	8	DE.CM (Security Continuous Monitoring), RS.AN (Incident Analysis), DE.AE (Adverse Event Analysis)
Microsoft Defender	Endpoint Detection & Response (EDR) platform that provides malware protection, threat detection, and automated response.	8	PR.DS (Data Security), RS.MI (Incident Mitigation), RS.AN (Incident Analysis), DE.AE (Anomalies & Events)
Microsoft Suite	Includes tools like Purview, Defender, etc. for identity, compliance, and threat management.	6	ID.IM (Asset Management), DE.CM (Security Continuous Monitoring), PR.AA (Identity Management, Authentication, and Access Control), RS.MI (Incident Mitigation), among others *
ServiceNow	IT service management and security operations platform for workflow automation, ticketing, and	5	GV.GV (Governance), GV.RM (Risk Management), PR.AA

Table 4.2. Continued

Frequently Used Cybersecurity Tools & Platforms	Brief Description	# of Mentions (as Top 2 Most Used Tools & Platforms)	Relevant NIST CSF (v2.0) Categories
	incident management.		(Identity Management, Authentication, and Access Control), ID.RA (Risk Assessment)
SailPoint	Identity Governance and Administration (IGA) solution for managing user access rights.	5	PR.AA (Identity Management, Authentication, and Access Control), ID.AM (Asset Management)
Snyk	Developer-focused security platform for identifying and fixing vulnerabilities in code, containers, and open source dependencies.	5	PR.PS (Platform Security), ID.RA (Risk Assessment)
CrowdStrike	Cloud-native Endpoint Detection and Response (EDR) platform with threat intelligence.	5	PR.DS (Data Security), RS.MI (Incident Mitigation), RS.AN (Incident Analysis), DE.AE (Anomalies & Events)
Microsoft Sentinel	Cloud-native SIEM and Security Orchestration, Automation, and Response (SOAR) solution for intelligent security analytics and threat response.	4	DE.CM (Security Continuous Monitoring), RS.AN (Incident Analysis), RS.CO (Incident Response Reporting and Communication), DE.AE (Adverse Event Analysis)
Palo Alto	Network and cloud security suite (firewalls, threat prevention, etc.) for perimeter and application-layer defense.	4	PR.IR (Technology Infrastructure Resilience), PR.PS (Platform Security), DE.CM (Security Continuous

Table 4.2. Continued

Frequently Used Cybersecurity Tools & Platforms	Brief Description	# of Mentions (as Top 2 Most Used Tools & Platforms)	Relevant NIST CSF (v2.0) Categories
			Monitoring)
Archer	Governance, Risk, and Compliance (GRC) platform that supports assessments and reporting.	3	GV.RM (Risk Management Strategy), GV.GV (Governance), ID.RA (Risk Assessment), RC.IM (Improvements)
Azure Security tools through the Azure Portal (e.g., Azure PIM, Azure Policy, etc.)	Microsoft Azure-native tools for Privileged Identity Management (PIM), policy enforcement, compliance, and so forth.	3	PR.AA (Identity Management, Authentication, and Access Control), PR.PS (Platform Security), GV.PO (Policy), among others *
Kali Linux	Linux distribution with Penetration Testing (Pen-testing) and ethical hacking tools.	3	DE.CM (Security Continuous Monitoring), ID.RA (Risk Assessment), PR.IR (Technology Infrastructure Resilience)
CyberArk	Privileged Access Management (PAM) platform for securing administrator accounts and credentials.	2	PR.AA (Identity Management, Authentication, and Access Control), ID.AM (Asset Management)
Okta	Identity and Access Management (IAM) solution with Single Sign On (SSO) and Multi-Factor Authentication (MFA)	2	PR.AA (Identity Management, Authentication, and Access Control), ID.AM (Asset Management)
Microsoft Purview	Data Loss Prevention (DLP) tool for data classification, discovery, and management.	2	PR.DS (Data Security), ID.AM (Asset Management), GV.RM

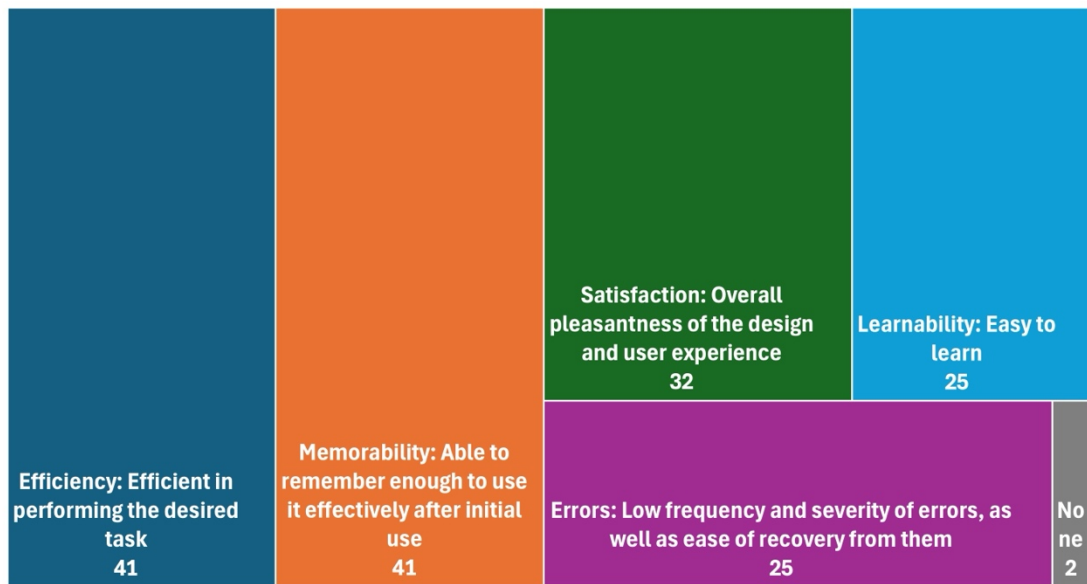
Table 4.2. Continued

Frequently Used Cybersecurity Tools & Platforms	Brief Description	# of Mentions (as Top 2 Most Used Tools & Platforms)	Relevant NIST CSF (v2.0) Categories
			(Risk Management Strategy)
BurpSuite Pro	Web application security testing tool allowing penetration testing, fuzzing, vulnerability scanning, etc..	2	PR.PS (Platform Security), PR.IR (Technology Infrastructure Resilience), ID.RA (Risk Assessment), DE.CM (Security Continuous Monitoring)
Prisma by Palo Alto	Cloud-Native Application Protection Platform (CNAPP) covering Cloud Security Posture Management (CSPM).	2	ID.AM (Asset Management), DE.CM (Security Continuous Monitoring), RS.AN (Analysis), PR.DS (Data Security)
ForgeRock	Identity and Access Management (IAM) solution that supports identity lifecycle, federation, etc.	2	PR.AA (Identity Management, Authentication, and Access Control), ID.AM (Asset Management)
VirusTotal	Online service for analyzing files and URLs for malware and suspicious content using multiple antivirus engines.	2	DE.CM (Security Continuous Monitoring), RS.AN (Incident Analysis), ID.RA (Risk Assessment)
Sonar	Static code analysis tool for identifying vulnerabilities and enforcing secure coding practices.	2	PR.PS (Platform Security), ID.RA (Risk Assessment)
Tenable	Vulnerability management platform for continuous scanning, monitoring, and reporting.	2	DE.CM (Security Continuous Monitoring), ID.RA (Risk Assessment), PR.PS (Platform

Table 4.2. Continued

Frequently Used Cybersecurity Tools & Platforms	Brief Description	# of Mentions (as Top 2 Most Used Tools & Platforms)	Relevant NIST CSF (v2.0) Categories
			Security)
Qualys	Cloud-based vulnerability management, compliance, and web application scanning tool.	2	DE.CM (Security Continuous Monitoring), ID.RA (Risk Assessment), PR.PS (Platform Security)
Proofpoint	Email security, Data Loss Prevention (DLP), and threat intelligence platform.	2	PR.DS (Data Security), ID.AM (Asset Management), DE.CM (Security Continuous Monitoring), RS.AN (Incident Analysis)
Microsoft Entra ID	IAM platform (formerly Azure AD) for secure authentication, authorization, SSO, and role-based access.	2	PR.AA (Identity Management, Authentication, and Access Control), ID.AM (Asset Management)
Microsoft Defender for Cloud Apps	Cloud Access Security Broker (CASB) for monitoring cloud applications, enforcing policies, and detecting threats.	2	DE.CM (Security Continuous Monitoring), PR.DS (Data Security), ID.AM (Asset Management), RS.AN (Incident Analysis)
*Refers to a suite of cybersecurity tools and platforms rather than individual products. As such, the mapped <i>Relevant NIST CSF (v2.0) Categories</i> may include additional relevant categories not listed here.			

in the scope for improvement, which reinforces the idea that in organizational cybersecurity contexts, usability encompasses more than just initial ease of use; it includes long-term operational fluency and the ability to re-engage with tools effectively.

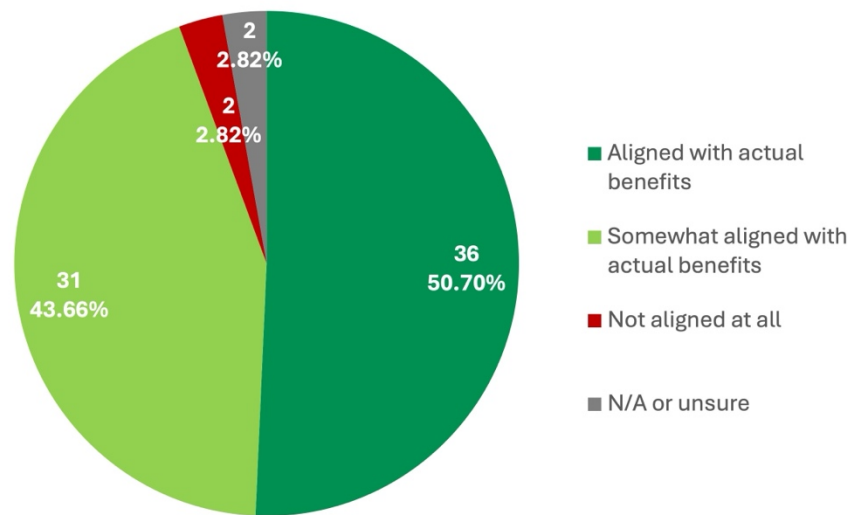


Note: 39 respondents either were not presented with this question or chose not to answer it and were therefore excluded from this analysis.

Figure 4.4. Chart showing survey responses to the question asking participants to select all applicable aspects of usability for the cybersecurity tools & platforms that they use most frequently as part of their work.

In addition to usability dimensions, participants were asked how the perceived benefits of their most-used cybersecurity tools & platforms compared with their actual benefits in practice. As shown in **Figure 4.5**, over 90% of participants who responded to the relevant survey question reported that the perceived and actual benefits were either aligned or somewhat aligned. Fewer than 3% indicated a misalignment between perceived benefits and real-world benefits. On the surface, while this high level of

alignment suggests that cybersecurity professionals generally have realistic expectations of their tools and platforms, it may also reflect a broader trend in which usability and UX expectations are modest or underdeveloped, indicating that practitioners may not anticipate high UX from cybersecurity tools & platforms, and instead focus on functionality and reliability. This theme is further explored in the qualitative findings.



Note: 39 respondents either were not presented with this question or chose not to answer it and were therefore excluded from this analysis.

Figure 4.5. Chart showing survey responses to the question asking participants how the perceived benefits of the cybersecurity tools & platforms they use most frequently compare with their actual benefits in practice, in terms of usability.

Training & Vendor Support

Survey data suggested that 67.61% of respondents reported “yes” to the question asking whether their organization provided or mandated formal training on how to use cybersecurity tools & platforms effectively, 5.63% said “maybe,” while 26.76% reported

“no”, as shown in **Figure 4.6**. While this reflects broad coverage, the fact that over a quarter of respondents reported not receiving formal training is a significant finding, highlighting potential gaps in organizational support for effective tools & platforms usage. Follow-up interviews revealed patterns, themes, and areas for improvement, as discussed in the *Documentation, Learnability and Onboarding*, and *Feedback Loops & Issue Tracking* subsections.

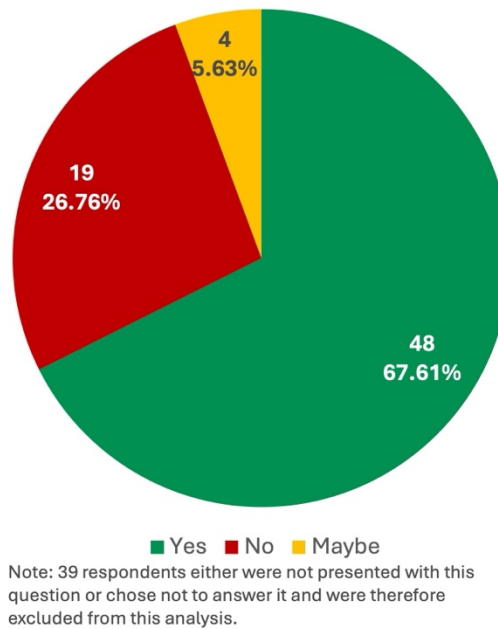


Figure 4.6. Chart showing survey responses to the question asking participants whether their organization provided or mandated formal training on how to use cybersecurity tools & platforms effectively.

UX Challenges

Survey responses indicated that 63.38% of the participants who answered the relevant question asking whether they experienced any challenges in using cybersecurity

tools & platforms they use most frequently as part of their work said “yes”, while 4.23% said “maybe”, and 32.39% said “no”, as shown in **Figure 4.7**.

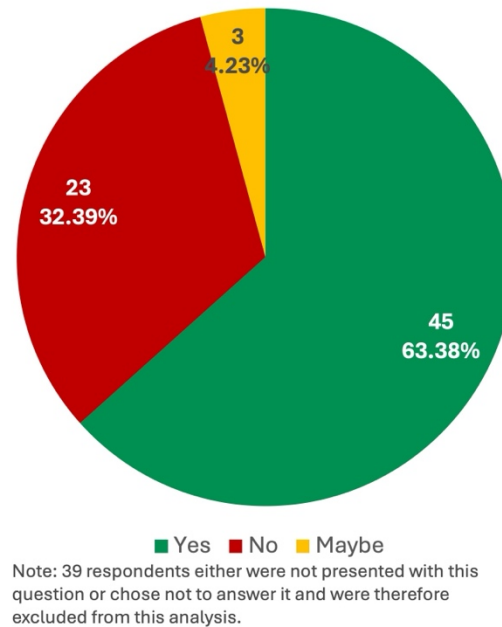


Figure 4.7. Chart showing survey responses to the question asking participants whether they experienced challenges in using cybersecurity tools & platforms most frequently used as part of participants’ work.

Taken together, nearly two-thirds of respondents experienced difficulties. **Table 4.3** outlines the challenges related to organizations’ cybersecurity tools & platforms, based on participants’ responses to the open-ended (text-input) follow-up survey question. The key takeaways are as follows:

- Usability and steep learning curves were cited by multiple respondents across SIEMs, network security, and EDR tools such as Splunk, Palo Alto, and

CrowdStrike, with practitioners describing non-intuitive interfaces, confusing layouts, and difficult navigation.

- Documentation and support gaps were noted across IAM and application security tools including CyberArk, Microsoft Intune, BurpSuite, among others, where incomplete or outdated vendor guidance left practitioners troubleshooting largely on their own.
- Alert fatigue, false positives, and noisy data were especially associated with SIEMs and vulnerability scanning tools like Splunk, Prisma Cloud, VirusTotal, etc., undermining confidence and creating operational inefficiencies.
- Frequent updates and UI changes were a recurring challenge with tools in the Microsoft ecosystem (e.g., Defender, Sentinel, Intune, Purview, Azure AD), as well as Wiz and Tenable. These changes often disrupted workflows, requiring practitioners to relearn interfaces and adapt to evolving functionality.
- Integration and interoperability challenges were common, particularly among SIEMs, GRC platforms, and cloud security tools. Examples include Splunk-ServiceNow and ServiceNow-Azure AD, where integration complexity sometimes impacted operational efficiency and required workarounds.

While survey responses provided a high-level view of commonly used cybersecurity tools & platforms challenges, the follow-up interviews revealed that these challenges can be categorized into the following interconnected sub-themes based on the type of tool and the nature of the challenge: *Workflow Efficiency, Performance &*

Reliability, UI Quality & Impact of Changes, Documentation, Learnability, and Onboarding, Feedback Loops & Issue Tracking, and Balancing Strong Security with Operational Realities. These sub-themes are discussed in detail as individual sub-sections below.

Workflow Efficiency (Tools & Platforms Sub-theme 3)

Across multiple interviews, participants consistently emphasized the importance of streamlining workflows within cybersecurity platforms to support high-volume investigative, monitoring, and reporting tasks. A key concern was the excessive number of clicks and repetitive manual actions, often referred to as “glue work”, such as copying and pasting data between systems or reapplying the same filters during routine tasks. While individually minor, these inefficiencies were seen as cumulative burdens that significantly impacted productivity when repeated hundreds of times per day.

Practitioners called for features that reduce friction and cognitive switching, including auto-hyperlinking indicators, deep linking to relevant data, and the ability to open items in new tabs. The absence of state persistence, where cybersecurity tools & platforms forget user preferences or filters upon refresh was a frequent source of frustration, as one participant explained:

“How many clicks. How many times do I have to click before I get to what I'm looking for, and ideally the fewer clicks, the better... copy-pasting is a big part of

Table 4.3. Reported challenges related to the most-used and second most-used cybersecurity tools & platforms at work, based on participants' responses to the open-ended (text-input) survey question.

Challenges Faced with Frequently Used Cybersecurity Tools and Platforms	Most Used Tool / Platform	2nd Most Used Tool / Platform
UX can be tough, performance and scalability can also be inconsistent	Palo Alto Networks Data Security Products	N/A
Changes to UI with respect to the velocity with which the product features are introduced.	Wiz.io	Microsoft Defender
Integrations with other tools/applications	Splunk (currently)	SailPoint
Tooling has become more rigid in what they allow users to do in an effort to make the tools more user friendly, this can make it more difficult as a "power user" to do more advanced actions	Purview	MDCA
Errors are not descriptive, insufficient documentation	CyberArk	Microsoft Entra ID
Products are continually being improved and new releases every other month.	Tenable, Tanium, Wiz, Palo, Google, Microsoft, servicenow, etc.	Microsoft
Citrix NetScaler has a challenging interface that is difficult to understand how it operates and where to find the configurations you need. It has deeply nested configurations that are far from intuitive, and even if you've been there before, very hard to remember where th configuration was the second time around	Citrix NetScaler Web Application Firewall (WAF)	Azure Security tools through the Azure Portal (e.g., Azure PIM, Azure Policy, etc.)
The tools I use are integrated in my development workflow. When I create a merge request for a new code change, CI jobs are triggered that scan for code vulnerabilities. Challenges I faced include jobs not failing due to error/timeout scenarios (unrelated to my changes), false positives and alert fatigue.	Prisma Cloud	Git Guardian
Initial access and navigation challenges with the tool	GRC	Scanning solution
There is a learning curve for all the tools, they don't always play well with each	GRC platform	Mimecast

Table 4.3. Continued

Challenges Faced with Frequently Used Cybersecurity Tools and Platforms	Most Used Tool / Platform	2nd Most Used Tool / Platform
other either.		
Not intuitive	SSE	SOAR
Gathering data consistently across cybersecurity tools, especially post mergers and acquisition.	To my work personally, data aggregation and data visualization tools are most related to my day to day activities.	N/A
Reliability and performance	Wiz	Snyk
Integrating with a hybrid and legacy environment.	ServiceNow	Splunk
The interfaces are absolutely non-intuitive.	Splunk	Palo Alto
Learning curve using the API, limitations of the API, false positives from the data, poor data quality from endpoints reporting to the platform resulting in poor data outputs, depth limitations on tool functionality such as not being able to show the logic for their outputs	Mandiant	Microsoft Defender
Cost, feature licensing	CrowdStrike	Palo Alto
Microsoft changes the locations and steps needed to make changes to security settings often which can be confusing, it requires more time to learn the changes.	Azure/M365	CIS
Varies from product to product	IAM products	Firewalls
Tribal knowledge is sometimes required to effectively use tools	Logrhythm	Kali Linux
Learning more advanced techniques to get past the initial usability of the platform	Splunk	VirusTotal
While current tools provide valuable insights and capabilities, they often fall short in addressing the full scope of challenges we face. Many solutions are either too broad, lacking the specificity needed for nuanced applications, or too rigid, failing to adapt to evolving threats and environments. Additionally, interoperability remains a persistent issue, as different platforms and systems frequently struggle to	Native GCP tools	Expel

Table 4.3. Continued

Challenges Faced with Frequently Used Cybersecurity Tools and Platforms	Most Used Tool / Platform	2nd Most Used Tool / Platform
communicate effectively. These limitations create inefficiencies, requiring practitioners to supplement existing tools with manual workarounds or multiple overlapping solutions. Without more flexible, comprehensive, and integrated toolsets, we risk gaps in visibility, inefficiencies in response, and ultimately, diminished effectiveness in tackling complex problems.		
Device attribution	My main project is an asset tracking and data correlation software.	Endpoint protection service
Most challenges are related to integration between multiple tools -- for example, Splunk integration with ServiceNow for record creation or Qualys and Recorded Future with ServiceNow for vulnerability scoring.	ServiceNow (for the reporting, escalation, notifications, and traceability aspects)	Splunk
ServiceNow and Azure AD integration presents several challenges, particularly in identity management, automation, and access control. One key issue is ensuring seamless synchronization between Azure AD user attributes and ServiceNow, as discrepancies can lead to misalignment in user roles, permissions, and group memberships. Automating user provisioning and deprovisioning requires careful configuration of SCIM or API-based integrations, which can sometimes result in delays or failures due to API throttling or misconfigured workflows. Additionally, managing conditional access policies in Azure AD while ensuring ServiceNow adheres to those policies can introduce complexities, especially when enforcing least privilege access. Another challenge involves troubleshooting authentication and SSO (Single Sign-On) issues, as misconfigured SAML or OAuth settings can lead to	ServiceNow	Azure AD

Table 4.3. Continued

Challenges Faced with Frequently Used Cybersecurity Tools and Platforms	Most Used Tool / Platform	2nd Most Used Tool / Platform
login failures, requiring in-depth debugging across both platforms. Furthermore, ServiceNow's limited native support for Azure AD dynamic groups complicates role-based access control (RBAC), often necessitating custom scripting or manual workarounds. Lastly, keeping up with evolving compliance and security requirements means regularly reviewing integration configurations to prevent unauthorized access, data exposure, or disruptions to automated processes.		
There is a disconnect between what training/documentation the vendor provides and our experience with using the tools. Documentations alone are often insufficient, contain outdated steps, and have no suggestions for further troubleshooting beyond "contact your technical support team." Vendor training environments are helpful with understanding how the tool is meant to work, but solving errors is a matter of experience with the tool or working with the vendor technical support. The biggest challenges of using the tools includes: 1) Lots of initial configuration and troubleshooting. 2) Learning how to make the tool successfully accomplish its purpose. 3) Lack of quality support on some issues (cross-platform integrations involve two or more vendors who defer technical error responsibility to one another).	Microsoft Sentinel	Tenable
Customization of the tools to support specific needs	SailPoint	Ping Identity
Organizational alignment to industry best practices	NIST framework	Cybersecurity Education
documentation is not readily made for quick starting, no one has time to read 10s of pages.	Microsoft Defender for Endpoint	XWays
Small things like page not keeping filters when refreshed	Sentinel	Team dynamics
Incomplete documentation.	MS Intune	Defender in relationship to Intune

Table 4.3. Continued

Challenges Faced with Frequently Used Cybersecurity Tools and Platforms	Most Used Tool / Platform	2nd Most Used Tool / Platform
The tools are inconsistent, and ever changing. Settings that are remembered in some places are not remembered in others would be my biggest complaint.	Sentinel	Defender
Platform documentation for most tools contain large gaps and occasional inaccuracies.	GitHub Dependabot	Splunk SOAR
The CrowdStrike interface is difficult to use, as it is hard to remember where each feature is.	Splunk	CrowdStrike
Custom configurations	Axonius	Zscaler
The biggest challenge is always the balance of tool cost against budget constraints and maintaining a quality signal to noise ratio.	Datadog SIEM	Terraform
Changing UIs and the impact on my workflow to get stuff done	MS Defender	MFA apps
Alert fatigue & tuning for alerts, especially in SIEM. I have a lot of data sources, and the detection rule set is very robust. That's led to a high volume of alerts that I've had to manually create exclusions for over time.	Blumira	Cybernut
Finding information quickly. Navigating between sections of the platform. Viewing and editing data in small display windows.	Onspring	I observe screens and reports from the secondary tools, but I rarely use them directly except in training situations.
Half-baked apps that don't provide value and are in place due to contractual requirements. Marketing for add-ons getting in the way.	Snyk	Defender for Cloud
False positives which is normal for any security tool, as well as some UX issues like things taking too many clicks to perform a common operation.	Bug Crowd	Snyk
Developing more capabilities - skills and investment are low; overlapping requirements - governance is not best practice	Archer (GRC)	Purview
Often there is a lack of documentation regarding how the service performs its tests	BurpSuite for web	CrowdStrike

Table 4.3. Continued

Challenges Faced with Frequently Used Cybersecurity Tools and Platforms	Most Used Tool / Platform	2nd Most Used Tool / Platform
or what kinds of results you'll receive. In general, they tend to solve a specific problem and do little else.	penetration testing	
Learning curves for new professionals is often steep beyond tutorial or basic usage	Splunk and custom python	LLMs
Yes, i've faced a few challenges as a threat intel researcher using cybersecurity tools. first, alot of the tools like shodan or ghidra have a steep learning curve and theres not always good docs or training so it takes time to figure things out. also, platforms like virustotal and shodan can show outdated or noisy data, which means sometimes you get false alerts or waste time chasing stuff that's not actually a threat. some of the good features like virustotal intel or advanced shodan filters are behind paywalls, so unless you have enterprise access your limited in what you can do. when it comes to automating things with APIs, its hit or miss – the docs arent always clear and i've had to trial and error alot. finally some tools just have bad ux or no error messages at all so your stuck guessing what went wrong. it slows down the work especially when your trying to triage or pivot fast during an investigation.	VirusTotal	Shodan

my life... having direct links... open up in a new tab... limiting the number of clicks and the number of times I have to open a new window and copy-paste something... makes a big difference.” (Participant 23)

Another participant described the inefficiency of poor data integration between tools, which led to frequent platform switching and disrupted workflow as follows:

“...when you have like a Defender incident and then sends it over to Sentinel, a lot of the data that comes over isn't necessarily enough to work the incident, and you end up switching platforms and you move off a Sentinel and to the Defender for Endpoint when working an incident. I just find that really annoying because I feel like to a certain extent that kind of ruins the whole point of the SIEM.”
(Participant 17)

These findings align with broader observations in usable privacy and security research, where inadequate tool integration has been identified as a major theme (Garfinkel & Lipford, 2014). These insights point to a broader need for workflow-aware designs that support task continuity, minimize redundant actions, and enable users to stay focused on investigative goals rather than navigation mechanics. Additionally, there was strong interest in automation features such as pre-populated queries and automatic data enrichment, which could further reduce manual effort and accelerate response times. Workflow Efficiency is categorized as a core UX sub-theme because the challenges

revealed here directly affect practitioners' ability to complete tasks efficiently, minimize cognitive switching, and sustain usable security practices.

Performance & Reliability (Tools & Platforms Sub-theme 4)

Based on the interview data analysis, cybersecurity tools & platforms' performance, defined by search speed, query responsiveness, system stability, and so forth, was consistently identified by participants as a critical factor influencing their overall UX. Regardless of feature richness or interface design, slow or unstable systems were seen as direct impediments to efficiency and usability, particularly in time-sensitive contexts such as incident response. Participants emphasized that fast, reliable tools not only improve operational throughput but also reduce frustration and cognitive load. As one participant noted:

“So, you know, making sure the tools are fast, as fast as possible ... anything I can run a search on that does it quickly minimal number of clicks, minimal number of times that I have to go from one window to another. That all makes a big difference...” (Participant 23)

Beyond speed, reliability was also tied to the robustness of Application Programming Interfaces (APIs) and the availability of clear documentation for troubleshooting. Several participants expressed frustration with vague error messages and

inconsistent API behavior, which complicated scripting and automation efforts. One participant described reliability challenges with APIs as follows:

“I do have this problem all the time, specifically with CyberArk, like when you're calling API's they're... they have very generic errors and they... like it will say unauthorized. Sometimes it'll even say unauthorized, and that's not even what the error really is. And there's like a lot of with, like CyberArk especially, there's a lot of different reasons you can be unauthorized... like there's a lot of different authentication components there.” (Participant 21)

Participants valued reliability and robustness more highly than interface polish, especially in high-stakes environments where delays or errors could compromise response times or security effectiveness. Ultimately, the insights suggest that performance and reliability are foundational to cybersecurity tools & platforms' UX. This sub-theme reflects core UX challenges, as performance delays, timeouts, or unreliable APIs directly disrupt users' real-time interactions.

UI Quality & Impact of Changes (Tools & Platforms Sub-theme 5)

Multiple follow-up interview participants emphasized that the quality of User Interfaces (UI) in cybersecurity tools & platforms directly affects both usability and operational efficiency. A recurring theme was the trade-off between technical capability and interface design: tools with powerful back-ends were often hindered by outdated or

unintuitive UIs, while less feature-rich platforms gained favor due to their ease of use. Although experienced practitioners were generally willing to tolerate clunky interfaces, especially when the tool's functionality was strong, they still noted significant onboarding challenges for newcomers. For example, Magnet Axiom, a digital forensics tool was praised for its intuitive layout and colorful design, making it easier for new users to navigate and learn, whereas alternatives like XWays were described as “old-school,” requiring memorization and extra effort to use effectively.

Participants also highlighted issues with information architecture, describing some tools as unnecessarily complex, with poorly structured menu hierarchies and excessive layers of navigation. Another common concern was the overwhelming presentation of data without clear prioritization. As one participant explained:

“...the issue was that on this UI, when you have 50 SaaS application, let's say you have... not every customer will buy 50 applications. But like think about it, if you have 50 applications, you can't put all the information in on the UI to show all the apps, right? It has to be... It has to be visible, but at the same time, it has to be like a drop-down or something on those lines which... which makes sense, because your page will be lengthy.” (Participant 01)

Participants also expressed a strong preference for dashboards that support fast decision-making through clear visual cues and role-based filtering, findings resonate with

usable security research emphasizing transparency with respect to dashboards as a measure to help improve users' secure behavior (Reuter et al., 2022). While such point-in-time usability and interface concerns have been noted in the literature (Grobler et al., 2021; Di Nocera et al., 2023), participants also emphasized an often-overlooked problem: the disruptive effect of frequent design changes, such as renaming features, rearranging menus, shifting dashboards, etc., increased cognitive load and retraining time, particularly for cybersecurity professionals who had already adapted to previous versions. As one participant noted:

"I'd say the one thing with Microsoft Defender is that it seems like they do a lot of updates, and they're constantly, you know, working on that platform... once updates are shared and maybe the... the web page changes a little bit or some of the... the UX pieces changed, it seems like our teams were having to spend, you know, a... two to three days to really get caught up to speed, whereas with CrowdStrike it seems like things stayed the same, but the underlying technologies were being refreshed." (Participant 11)

Despite these frustrations, some participants acknowledged efforts toward consistency across product suites. Microsoft, for instance, was recognized for maintaining a relatively uniform UI across tools like Defender, Sentinel, Intune, etc., which eased transitions between them. However, even within such ecosystems, frequent

portal shifts and interface updates still led to what several participants described as “change fatigue.”

These findings reinforce the notion that UI design and changes are not merely aesthetic, they shape learnability, efficiency, and user confidence. Tools that offer customizable dashboards, consistent layouts, and intuitive navigation lower entry barriers for newcomers and reduce friction for seasoned professionals. Ultimately, participants called for interfaces that balance clarity, consistency, and adaptability without compromising usability through excessive or poorly communicated changes. UI Quality and Impact of Changes constitute a core UX sub-theme, highlighting challenges that immediately influence usability, learnability, and user confidence as interfaces evolve over time.

Documentation, Learnability, and Onboarding (Tools & Platforms Sub-theme 6)

During follow-up interviews, participants consistently highlighted challenges related to documentation, learnability, and onboarding when working with cybersecurity tools & platforms. A common frustration was the reliance on lengthy vendor-provided manuals, in some cases spanning 100 to 200 pages, which were seen as impractical for real-world use. Most users lacked the time to read extensive PDFs and instead sought concise, actionable resources to help them get started quickly. As one participant described:

“...these PDFs are like 200 pages long and you like no one has time to, like, read so many pages...” (Participant 25)

In response to these limitations, participants described a range of solutions and workarounds, including internal wikis or knowledge bases, informal playbooks, peer learning, YouTube tutorials, and so forth.

“So, what we would do is like we'd have to develop a Build Book or Run Book to say, hey, when we are going to develop a virtual machine, if it's a server, a Windows Server or Linux Server, here are some of the options that will be presented to you and we'll document what they mean within like a formal procedural / build book.” (Participant 11)

Participants expressed a strong preference for quick-start guides, one-pagers, and embedded contextual help resources (e.g., help icon, pop-up bubbles with useful information, etc.) that distill essential tasks and best practices into digestible formats. Diagrams, live environments, and bite-sized videos were also cited as helpful onboarding tools. A few follow-up interview participants envisioned the potential of AI-powered assistants embedded within cybersecurity tools & platforms, capable of answering “how-to” questions on demand by parsing vendor documentation and surfacing relevant steps on demand. This represents a core UX sub-theme, capturing challenges related to how

practitioners acquire the knowledge and confidence to use cybersecurity tools effectively in their daily workflows.

Feedback Loops & Issue Tracking (Tools & Platforms Sub-theme 7)

During follow-up interviews, participants described a multi-layered process for surfacing and resolving usability & UX issues within cybersecurity tools & platforms, beginning with informal peer-to-peer exchanges and escalating to formal tracking systems. Practitioners' frustrations were often initially voiced in casual conversations, through internal communication channels such as Slack or Microsoft Teams, where users would ask colleagues if they were experiencing similar problems or share quick comparisons between tools. As one participant explained:

“...what actually happens is it becomes a Teams chat to a manager... It's kind of like if there's a Slack channel or something, a little less formal, and there's not a formal paper trail.” (Participant 11)

Recurring issues that persisted were often then formally documented in Jira or an internal ticketing portal, ensuring that these issues could be tracked, prioritized, and assigned to relevant stakeholders (e.g., engineering teams or vendors), though participants noted not all feedback made it that far. Some issues remained unresolved or undocumented unless they reached a critical threshold.

In addition to internal feedback loops and issue tracking methods, participants described regular vendor touchpoints, often conducted under Non-Disclosure Agreements (NDAs), where cybersecurity professionals could share screens, highlight pain points, and request features.

Some teams maintained internal wikis or playbooks documenting workarounds, lessons learned, and simplified instructions, as outlined in the *Documentation, Learnability, and Onboarding* sub-section above. These resources served as institutional memory, especially valuable for onboarding new staff or revisiting recurring issues. One participant described it as follows:

“...the challenge, the way we work around with that is very... it's thorough documentation. We call it a playbook. So, every time we have to do something, we go back to the playbook and look where it is because we can't really change the tool, right? So unfortunately, if we could then, reorganize the tool.” (Participant 08)

Overall, the insights suggest that effective issue tracking in cybersecurity environments relies on both informal and formal feedback loops. While chat-based peer exchanges are important for rapid surfacing of problems, structured issue-tracking systems and vendor engagement are critical for resolution and long-term positive UX. Feedback Loops and Issue Tracking function as a supplementary UX sub-theme, where

challenges pertain to how organizations surface, document, and resolve usability & UX issues rather than the direct interaction itself.

Balancing Strong Security with Operational Realities (Tools & Platforms Sub-theme 8)

Lastly, the follow-up interview data analysis revealed how sector-specific risk tolerance shapes decisions around cybersecurity tools & platforms, particularly in balancing strong security controls against usability and operational realities. While healthcare organizations often prioritize usability to ensure uninterrupted care, finance and other regulated industries tend to favor stricter enforcement, even at the cost of UX. For instance, this trade-off was especially evident in healthcare settings, where strict Identity Provider (IdP) session timeouts, such as the recommended eight-hour sign-out policy, could have potentially life-threatening consequences during emergency scenarios, as one participant explained:

“...when I'm implementing Okta mostly for my customers... we always tell customers to at least sign out all the users from the identity provider session once a day, which is, once in eight hours... But, depending on the customer that I'm working with, mostly I have seen for healthcare customers, they are absolutely not okay with this... say practitioners or their nurses are using their websites... if there is an emergency scenario and a person can die within seconds, but then if you just... if you just tell them that, hey, well you, you just have to do an username

validation, authentication, etcetera, that would take somebody's life.”

(Participant 24)

Participants acknowledged that increasing usability can expand the attack surface, but emphasized the need for proportional responses rather than blanket restrictions. In breach scenarios, some organizations defaulted to immediate lockdowns, revoking access broadly before investigating root causes. While this approach maximized containment, it often disrupted workflows and created friction for practitioners.

Another example of balancing strong security with operational realities involved the cybersecurity tools & platforms sprawl, and the need for rationalization, as one participant described:

“They purchase like every solution under the sun just to say they have it, and don't do any... or shouldn't say don't, but do limited work to kind of figure out what they truly need in their organization. So, a lot of things end up being shelfware, used for like a specific... specific use case, and they end up kind of inflating their cyber budget to pay for all these solutions, when they can get away with probably half of the... half of the solutions in their environment. That happens all over the place.” (Participant 05)

Overall, the insights from this analysis show that balancing security with operational realities is not a one-size-fits-all challenge. Effective strategies require sector-aware considerations, proportional enforcement, and thoughtful communication to ensure that security measures do not inadvertently compromise operational realities. This represents a supplementary UX sub-theme, as the challenges reflect contextual trade-offs between stringent security controls and real-world usability, shaping the broader environment in which users operate.

(Sub-RQ2d) Theme 2: Policies & Standards

Sub-RQ2d: What are the UX challenges that Cybersecurity/IT teams in an organization face when implementing and/or managing their internal policies & standards?

This section addresses sub-RQ2d outlined above based on the data analysis of surveys and follow-up interviews. The sub-themes and illustrative excerpts from the interviews for the *Policies & Standards* theme are presented in **Table 4.4**. The codebook, including qualitative codes and their definitions, is provided in **Appendix G** for reference. The first four (4) of the five (5) interrelated sub-themes, namely *Accessibility & Centralization*, *Clarity & Understandability*, *Compliance & Framework Alignment*, and *Feedback, Enforceability, and Escalation* provide the analytic structure for the following subsections, where the survey results are integrated with qualitative insights from follow-up interviews, prior literature, the researcher's analysis and interpretive discussion. The *Potential Improvements (Future-Facing Ideas)* sub-theme is synthesized

within these discussions rather than treated separately, ensuring that recommendations are considered in relation to the specific challenges they address.

Accessibility & Centralization (Policies & Standards Sub-theme 1)

Survey responses indicated a high level of awareness regarding the existence of cybersecurity policies and standards within organizations, as shown in **Figure 4.8 (left)**. Among those who responded to the relevant question, 98.77% affirmed that their organization had such policies, and 1.23% (one participant) indicated otherwise.

Notably, the sole survey respondent who indicated that their organization didn't have cybersecurity policies & standards was an executive holding multiple concurrent leadership and technical roles in a public school system, who attributed the gap to the lean staffing and the constraints regarding the dispersal of responsibilities. While this instance was atypical, it illustrates how resource limitations can negatively impact engagement with governance documents and structures, even at senior levels.

In terms of accessibility, 80% of respondents to the relevant survey question reported that policies were accessible, while 12.5% expressed uncertainty ("maybe") and 7.5% reported lack of accessibility, as shown in **Figure 4.8 (right)**.

Follow-up interview data revealed that centralization and findability were key factors influencing the UX and usability of cybersecurity policies & standards.

Table 4.4. Sub-themes and excerpts from the overarching Policies & Standards theme that were derived from the thematic analysis of the follow-up interview data.

Theme: Policies & Standards	
Sub-theme	Example Quotes / Excerpts
Accessibility & Centralization	<i>“Yes, we have a team wiki where these policies and training guidances are published. And also, we get reminders like if any training has to be completed or you know, if there is a new guidance or any new policies that has been published, we get reminders over e-mail.” (Participant 24)</i> <i>“it's in a... centralized location in the sense of they're all kind of up in SharePoint, but they are... spread out across... different locations ... if you know what you're looking for, you can... find them.” (Participant 05)</i> <i>“Yes, there is an internal Wiki. And we also have an internal... internal bot on... on the... the messaging app that we use and basically you can just ask it anything and it's able to pull up the docs pretty quickly. So that is really helpful.” (Participant 02)</i> <i>“So, one of the things that we did is we work with our networking team. Actually, specifically, the team that was responsible for the web proxy filters... web proxy servers, such that when someone typed the word policy in their web browser, it would go to a central intranet site... the home of every policy...” (Participant 26)</i> <i>“...like a Wikipedia-like repository, which is easily searchable and can usually find something pretty quick. So, even just to... just basic searches in that repository, I can generally find things pretty fast, including our all of our policies, and so forth.” (Participant 23)</i>
Clarity & Understandability	<i>“...I think I would probably say this about any... any organization's to be honest, but they're... they're understandable, but they can also be very legalistic and general, and I think maybe sometimes providing an example of what they... what this means in practice would be useful.” (Participant 23)</i> <i>“I think examples are the best thing! As many given documented scenarios and examples you can provide just makes easy for non-legal people to interpret things like policies.” (Participant 02)</i> <i>“I think a lot of companies, right, there's cybersecurity policies and standards like legal documents, right? They're like 20 to 30 pages long. Like, no employee is ever reading all of it. Right? Like most people, just like glance over it, scroll through, accept, accept, accept. ...I think again, like you can have like those legally binding, you know, like long policies and standards. But like, I feel like you should have one pagers of, like, just summarizing the cybersecurity policies and standards...” (Participant 25)</i> <i>“...provide more clarity around which policies and procedures, or policies and standards staff need to</i>

Table 4.4. Continued

Theme: Policies & Standards	
Sub-theme	Example Quotes / Excerpts
	<i>adhere to... differences between US versus global... those policies can have contradicting information..."</i> (Participant 05) <i>"I would say the reduction or just kind of reducing overall the amount of acronyms. I think the acronyms are typically something that, once you're at, you know, three to five years in a role, you typically understand what the acronyms mean. But a lot of times when we're onboarding new college grads, they're obviously not understanding kind of the industry jargon and what not."</i> (Participant 11)
Compliance & Framework Alignment	<i>"We have a risk library, and a controls library, and not all the time they are in sync with our policies and standards."</i> (Participant 03) <i>"We see that a lot, and so companies will have this policy that's in alignment with ISO 27001 or NIST, but they don't have a technical control in place. They may just have a JIRA ticket, but then they don't have any like tracking all of those JIRA tickets... So, I think that visibility is typically the hard part because they don't have those tools in place to apply those restrictions along with the standards."</i> (Participant 11) <i>"Just make them all look like 800-53, they'll figure it out."</i> (Participant 15) <i>"So again, being aware of the... in the laws and regulations of company is subject to and agreed to do and making sure that the security team, whoever writes the policy team, is aware of and can track and put into, integrate those into their next policy update cycle is a current barrier."</i> (Participant 26) <i>"I'd say Global compliance issues. We understand GDPR for Europe, I believe PIPEDA for Canada, but some countries are now starting to develop their own compliance frameworks or data privacy regulations, and I think kind of staying up to speed on those. It's just a little hard at times... If our client decides, OK, we're going to set up the Chinese employee database in Europe, well, they may just have, you know, breached some type of regulation that they didn't even know that they did."</i> (Participant 11)
Feedback, Enforceability, and Escalation	<i>"...most of the standards will say something like - if a user wants to access a database administrator account, then they need to reach out to their manager or create a ServiceNow ticket or a JIRA ticket, right? But what actually happens is it becomes a Teams chat to a manager, and there's not formal documentation of hey this person has is requesting access to a privileged account, and this person now has the access to a privileged account."</i> (Participant 11) <i>"So, let's say you're trying to block a website. ...I'm going to block this website for XYZ, but then how about</i>

Table 4.4. Continued

Theme: Policies & Standards	
Sub-theme	Example Quotes / Excerpts
	<i>those exceptions? For those certain things, the exceptions are where the rubber meets the road, where policy has to have room to be both, a movable and I mean, relatable to what a reason would be for an exception to be made.</i>” (Participant 22) <i>“...they have a proper team... keeps updating all those policies and makes sure that new people who are joining, they also undergo through the same thing training and they're not left behind...”</i> (Participant 07) <i>“Infosec are seen as very very bad to a lot of people because we're basically the police. You know, It would be an ideal state where we can lock down the entire system, no one can use it, no actors can get inside, right? That would be great. But at the same time, you couldn't use the system. So, the balance would exist between letting people use the system and creating tools that would help them do it better.”</i> (Participant 22) <i>“So, it depends. We wrote the policy with the understanding that the campuses would write the standards. So, we give the policies, here's the policy, here's what we're supposed to do.”</i> (Participant 16)
Potential Improvements (Future-Facing Ideas)	<i>“...policies and procedures AI chatbot... what if I can just go and ask... and it just gives me an answer and like the page... it's just more smarter control F... with, like, you know, Copilot and Gemini...”</i> (Participant 25) <i>“a Confluence or Wiki style page... users are contributors as well, almost like a GitHub-style...”</i> (Participant 08) <i>“...sometimes vendor technologies where you might have limitations with the vendor, you... you're going to have easier knowledge transfer when someone leaves the company or gets promoted. They should really be putting those into kind of a vendor tool, where search capabilities are enhanced. User experience, downloading capabilities are enhanced.”</i> (Participant 03) <i>“So typically through like a Visio diagram or a very easy to follow PowerPoint slide, just a one-slider like a user experience journey for how it should look when you are requesting a privileged account, and the implications of not following this process. And those implications will try to highlight a few critical scenarios where things could go wrong.”</i> (Participant 11) <i>“It would be nice if we had like a high-level overview of that. It is kind of wordy, like especially like if you like intentionally want to go look at the policy. It's definitely like I gotta sit down and take a minute to actually thoroughly read through this.”</i> (Participant 17)

Table 4.4. Continued

Note: The example quotes/excerpts shown above are not exhaustive and are limited to a maximum of five (5) per sub-theme for convenience and clarity. A complete list of excerpts obtained from the thematic analysis is available upon request.

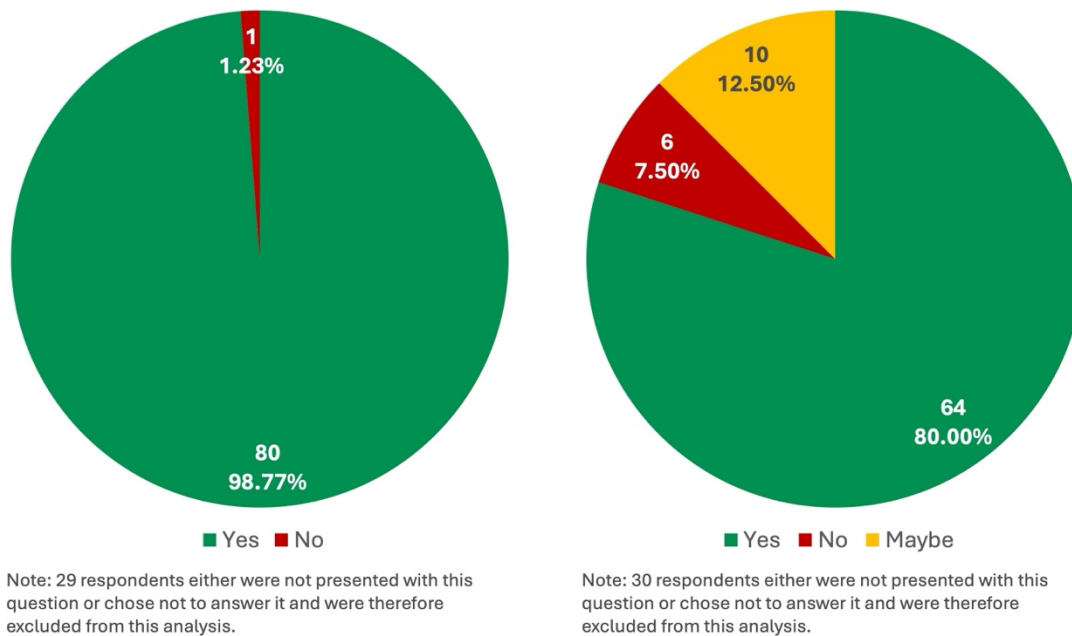


Figure 4.8. Charts showing survey responses to questions asking participants whether their organizations have specific cybersecurity policies & standards (left), and whether those cybersecurity policies & standards are easily accessible (right).

Participants described a range of solutions and potential future-facing improvements, such as internal search engines, team wikis, intranet redirects, and even AI-assisted search features, that helped users locate relevant documents quickly and conveniently. One participant described a particularly effective approach:

“So, one of the things that we did is we work with our networking team. Actually, specifically, the team that was responsible for the web proxy filters... web proxy servers, such that when someone typed the word policy in their web browser, it would go to a central intranet site... the home of every policy...” (Participant 26)

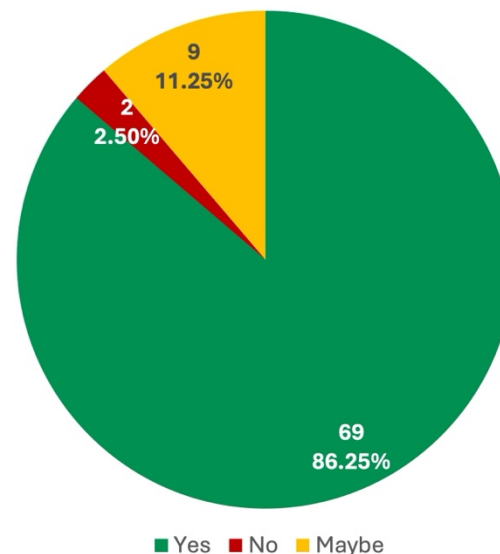
However, not all experiences were positive. A few participants noted that while policies & standards were technically centralized (e.g., stored in a single platform such as SharePoint), they were often spread across multiple folders or sites, making them difficult to locate without prior knowledge of naming conventions or structure. As one participant explained:

“it's in a... centralized location in the sense of they're all kind of up in SharePoint, but they are... spread out across... different locations ... if you know what you're looking for, you can... find them.” (Participant 05)

These findings underscore the importance of not just centralization, but intuitive access and searchability. Even when cybersecurity policies & standards are technically centralized, poor organization or lack of search optimization can introduce barriers that discourage engagement with the policies & standards and hinder the overall UX. Such dynamics are consistent with prior literature that highlights transparency as a critical dimension of policy specification and interaction in organizational contexts (Reuter et al., 2022). Accessibility and Centralization represent a core UX sub-theme, since the challenges identified here directly affect practitioners' ability to locate, access, and apply cybersecurity policies & standards efficiently in practice.

Clarity & Understandability (Policies & Standards Sub-theme 2)

When asked about understandability of cybersecurity policies & standards, 86.25% of respondents to the relevant survey question indicated that their organizations' policies were understandable, while 11.25% expressed uncertainty and 2.5% disagreed, as shown in **Figure 4.9**.



Note: 30 respondents either were not presented with this question or chose not to answer it and were therefore excluded from this analysis.

Figure 4.9. Charts showing survey responses to the question asking participants whether their organizations' cybersecurity policies & standards are understandable.

While the survey results suggest that most cybersecurity policies & standards are perceived as understandable, follow-up interviews revealed persistent challenges related to length, legalistic tone, and lack of practical guidance. Multiple participants described cybersecurity policies as overly verbose, often 20 to 30 pages long, and written in a style

more suited to legal or audit professionals than to cybersecurity professionals and everyday users. As one participant noted:

“...I think I would probably say this about any... any organization’s to be honest, but they’re... they’re understandable, but they can also be very legalistic and general, and I think maybe sometimes providing an example of what they... what this means in practice would be useful.” (Participant 23)

This format often led to disengagement, with cybersecurity professionals “scrolling through and accepting” rather than reading thoroughly. Participants expressed a strong preference for concise summaries, role-specific examples, and plain-language explanations that translate policy requirements into actionable guidance. One participant emphasized the value of illustrative content:

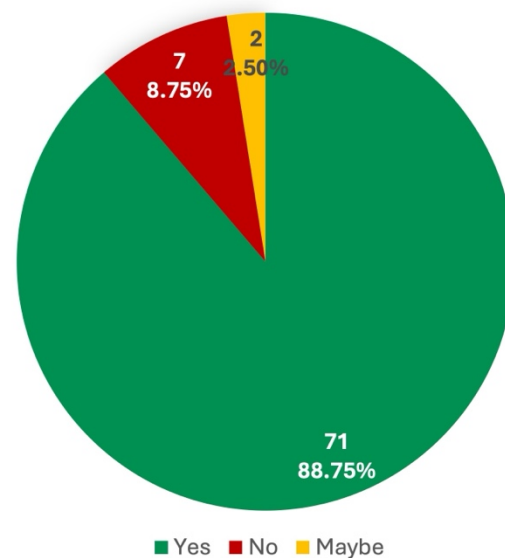
“I think examples are the best thing! As many given documented scenarios and examples you can provide just makes easy for non-legal people to interpret things like policies.” (Participant 02)

These findings suggest that while policies may meet formal compliance standards, their clarity and usability could be significantly improved through supplemental materials such as role-specific policy summaries, scenario-based examples, and visual formats (e.g., flowcharts). This is a core UX sub-theme, with challenges

centered on how clearly cybersecurity policies & standards convey expectations and reduce cognitive barriers for non-experts who must interpret and implement them.

Guidance & Support

Survey responses indicated that 88.75% of the participants who answered the relevant question regarding cybersecurity policies & standards' guidance felt that their organizations provided training or guidance, though a minority of 2.5% expressed uncertainty and 8.75% disagreed, as shown in **Figure 4.10**. This suggests that while guidance is generally present, there are areas for improvement.



Note: 30 respondents either were not presented with this question or chose not to answer it and were therefore excluded from this analysis.

Figure 4.10. Charts showing survey responses to the question whether they received any training or guidance on these cybersecurity policies & standards from their organizations.

While survey responses provided a high-level view, the follow-up interviews revealed that guidance & support from the organization, as well as challenges regarding cybersecurity policies & standards cannot be understood in the abstract, rather they manifest in specific organizational practices. Thematic analysis of the follow-up interview data showed that insights regarding guidance & support, and challenges led to the emergence of the following two (2) interconnected sub-themes: *Compliance & Framework Alignment* and *Feedback, Enforceability, and Escalation*. These sub-themes are discussed in detail as individual sub-sections below.

Challenges

Survey results indicated that challenges with respect to cybersecurity policies & standards were not universal but significant enough to merit attention: 23.75% of those who answered the survey question reported experiencing challenges with following or implementing cybersecurity policies & standards, 8.75% were uncertain, and 67.5% reported no challenges, as shown in **Figure 4.11**.

Taken together, nearly one-third of respondents experienced difficulties. **Table 4.5** outlines the challenges related to organizations' cybersecurity policies & standards, based on participants' responses to the open-ended (text-input) follow-up survey question. The key takeaways are as follows:

- Survey participants most often pointed to difficulties operationalizing policies, including unclear or aspirational language, inconsistent enforcement, and

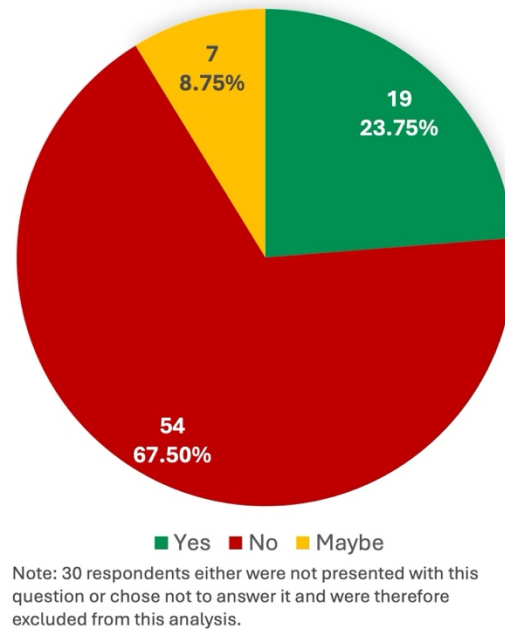


Figure 4.11. Chart showing survey responses to the question asking participants whether they face any challenges in following or implementing their organizations' cybersecurity policies & standards.

- challenges translating requirements into actionable controls.
- Many noted misalignment with organizational realities, such as outdated policies, conflicts with role-specific needs, fragmented tools, and resource or staffing constraints.
- Other concerns included poor communication and adoption, where cybersecurity policies & standards were skimmed or misunderstood, training was too generic, and updates or new requirements were not effectively communicated.

Follow-up interviews provided deeper insight into these challenges. Thematic analysis revealed that many of the issues were closely tied to the sub-themes discussed in the *Guidance & Support* sub-section above; *Compliance & Framework Alignment* and

Feedback, Enforceability, and Escalation, which are explored in the following sub-sections.

Compliance & Framework Alignment (Policies & Standards Sub-theme 3)

Follow-up interviews revealed that cybersecurity policies & standards are frequently shaped by external frameworks, laws, and regulations, including NIST CSF v2.0, ISO 27001:2022, HIPAA (for healthcare), PCI DSS (for financial services), state-specific regulations (e.g., NYDFS), among others. Participants emphasized the importance of aligning internal governance with these standards but noted persistent challenges in doing so. One recurring issue was the lag between updates to external frameworks and revisions to internal policies & standards, often due to unclear ownership or lack of structured review cycles. As one participant explained:

“So again, being aware of the... in the laws and regulations of company is subject to and agreed to do and making sure that the security team, whoever writes the policy team, is aware of and can track and put into, integrate those into their next policy update cycle is a current barrier.” (Participant 26)

In addition to update delays, participants described misalignment between organizations’ cybersecurity policies & standards and operational tools, such as risk and controls libraries. These gaps made it difficult to ensure that technical implementations reflected governance documents’ intent:

Table 4.5. Reported challenges related to organizations’ cybersecurity policies & standards, based on participants’ responses to the open-ended (text-input) survey question.

Challenges Faced with Organizations’ Cybersecurity Policies and Standards
Not easy to align business practices with the practices outlines in policy and standard
Enabling the cyber controls using current tools consistently has been a challenge
There is a homegrown solution for policy management that is not easy to decipher and maintain. Then tools are segmented so it’s not easy to consolidate cyber, regulatory, and compliance information.
The organization requires strict policies that do not align with the kind of work I do (i.e. cybersecurity consultant). Since my job is to understand vulnerabilities, exploits and security gaps, I need to configure system to be insecure so I may test them. However, the organizational policies frequently flag those insecurities unaware that they were placed on purpose.
Most policies tend to be aspirational rather than operational and require knowledge of a technical control in order to be operationalized and leveraged (e.g., USB restriction, privileged access request)
Policy and standard enforcement can sometimes be a challenge.
Interpretation of policy into applicable controls is a challenge and then Implementing controls across different cloud providers using different tools is challenge. Often people get stuck in how, rather than focusing on Why
It’s one thing to publish the docs, it’s another to get people to follow them.
Policy language can often be prescriptive but rely on standards and procedures that are not as mature, causing a slight discrepancy in what is overtly stated vs. actually done day to day
Make sure whether standard requirements are being met and in compliance
People, process and technology challenges
Policies are not always current.
Despite the policies and procedures being part of our employee onboarding process, with a culture of security engrained into our organizations, often the security policies and procedures are only skimmed or reviewed once. We are working on using tools to manage and implement more of our policies but when it comes to human centric then many times its at the discretion or interpretations of each individual creating discrepancies.
Consulting with IT pros with implementations
Implementing cybersecurity policies and procedures presents several challenges, often stemming from organizational resistance, resource constraints, and evolving threats. One of the primary hurdles is securing executive buy-in, as leadership may prioritize business operations over security investments, requiring strong justification of risks and compliance obligations.

Table 4.5. Continued

Challenges Faced with Organizations' Cybersecurity Policies and Standards
Additionally, user adoption can be difficult, as employees may perceive security controls as burdensome, leading to non-compliance or workarounds that introduce new vulnerabilities. Another challenge is aligning policies with regulatory requirements and industry standards while maintaining operational efficiency, especially in dynamic environments where new threats constantly emerge. Limited resources, both in terms of budget and skilled personnel, can further hinder the effective rollout and enforcement of security measures. Finally, maintaining and updating policies to address emerging risks, integrating security into existing workflows, and ensuring continuous monitoring and enforcement require ongoing effort and adaptability, making cybersecurity governance a continuous and complex process.
I would say collectively the biggest challenge with security policies is communicating across a broad audience how to interpret the policies down to “what am I expected to do in order to be compliant?” For example, there are some systems which cannot implement what a given policy demands for legitimate business reasons. Our technical teams must file for an exemption and implement other security controls in order to be seen as compliant with the policy. The challenge here is knowing not just what needs to be implemented, but how, and that may involve multiple teams working together across different tool platforms.
Onboarding, compliance
Organizational alignment. I.e. InfoSec policing versus ease of use for organizational tools. Basically – InfoSec as a policing body versus employee ease of use for login, tools and “solutioning.”
I think our IT documentation is adequate
Guidance can be weak on which available tools and procedures will satisfy each IT standard.
The policies are not consistently applied.
My primary challenge is exceptionally lean staffing. My job is actually made up of roughly 4 distinct full time roles (CTO, CISO, Security Analyst, Manager), and dividing workloads is difficult, as is achieving deep focus while trying to work on one project or area
Yeah, there's been a few challenges with cyber security awareness training. Sometimes the trainings are too basic and not really relevant to the kind of stuff i do in threat intel. Like they talk about phishing emails and password hygiene, which is good for general users but not super helpful for someone doing malware analysis or tracking threat actors. Also, some trainings are just long and boring, like slides with no real examples or hands-on stuff, so its hard to stay focused. Another issue is they don't update the content often, so we're seeing the same stuff every year and it gets repetitive. It would help more if they made trainings role-based or more interactive with real case examples we actually deal with in the field.
New policies on procurement of software that has a secure software development attestation is difficult to find and hasn't been

Table 4.5. Continued

Challenges Faced with Organizations' Cybersecurity Policies and Standards
adequately communicated across the organization

“We have a risk library, and a controls library, and not all the time they are in sync with our policies and standards.” (Participant 03)

These findings suggest that compliance activities, while necessary, may inadvertently reduce usability and engagement if they result in outdated documentation and fragmented operational workflows. This interpretation is consistent with prior research, which stresses that usable security requires not only compliance with standards but also regular review, timely updates, and transparency in policy administration (Reuter et al., 2022; Grobler et al., 2021). Participants suggested improvements such as automating update tracking when external standards and regulations change, to support timely review and updates of internal governance documentation and establishing clear ownership of update cycles to ensure accountability and continuity. This sub-theme reflects supplementary UX challenges, focusing on systemic alignment and traceability between organizational cybersecurity policies & standards, and regulatory frameworks that indirectly shape users’ experience with compliance processes.

Feedback, Enforceability, and Escalation (Policies & Standards Sub-theme 4)

The follow-up interviews with practitioners showed that enforcement of cybersecurity policies & standards varied widely across organizations, and was often shaped by reactive decision-making, informal escalation paths, and limited feedback mechanisms. While some organizations embedded enforcement into workflows, such as requiring acknowledgment at login or during personnel onboarding, others relied on

audits or ad hoc reviews, resulting in weak enforcement. Balancing enforcement of cybersecurity policies & standards with practical usability emerged as a challenge. One participant described the tension between locking down systems for security and maintaining usability for everyday operations as follows:

“Infosec are seen as very very bad to a lot of people because we're basically the police. You know, It would be an ideal state where we can lock down the entire system, no one can use it, no actors can get inside, right? That would be great. But at the same time, you couldn't use the system. So, the balance would exist between letting people use the system and creating tools that would help them do it better.” (Participant 22)

In terms of feedback and escalation, some participants described the gap between intended enforcement and actual practice, highlighting workarounds that professionals often used to bypass formal procedures. For example, instead of submitting formal access requests through approved systems, users might message their manager directly, resulting in gaps in auditability and accountability. As one participant described:

“...most of the standards will say something like - if a user wants to access a database administrator account, then they need to reach out to their manager or create a ServiceNow ticket or a JIRA ticket, right? But what actually happens is it becomes a Teams chat to a manager, and there's not formal documentation of hey

this person has is requesting access to a privileged account, and this person now has the access to a privileged account.” (Participant 11)

These findings suggest that effective enforcement requires more than policy language; it demands structured escalation paths, consistent documentation, and responsive feedback loops. Importantly, these mechanisms must also be usable, in the sense that procedures for requesting access or escalating issues should be seamless, intuitive, and integrated into existing workflows. Without these elements, enforcement risks becoming either overly rigid or inconsistently applied, negatively impacting the cybersecurity policies and standards’ overall UX. Feedback, Enforceability, and Escalation are treated as a supplementary UX sub-theme, emphasizing challenges in governance and communication mechanisms that support, but do not necessarily directly constitute, user interaction with policies & standards.

(Sub-RQ2e) Theme 3: Training & Awareness

Sub-RQ2e: What are the UX challenges that Cybersecurity/IT employees face when they are assigned tool or role-specific training?

This section addresses sub-RQ2e outlined above based on the data analysis of surveys and follow-up interviews. The sub-themes and illustrative excerpts from the interviews for the *Training & Awareness* theme are presented in **Table 4.6**. The codebook, including qualitative codes and their definitions, is provided in **Appendix G**

for reference. The first four (4) of the five (5) interrelated sub-themes, namely *Cadence & Frequency*, *Role-Specific Training*, *Effective Training Sources*, and *Challenges & Frustrations* provide the analytic structure for the following subsections, where the survey results are integrated with qualitative insights from follow-up interviews, prior literature, the researcher's analysis and interpretive discussion. The *Future Improvements & Innovations* sub-theme is synthesized within these discussions rather than treated separately, ensuring that recommendations are considered in relation to the specific challenges they address.

Availability

Survey results suggest that organizations generally recognize the importance of cybersecurity training & awareness, though perceptions of emphasis varied. Among those who responded, 54.32% indicated “definitely yes” and 28.4% “probably yes” when asked whether their organization prioritizes cybersecurity education, awareness, and training, as shown in **Figure 4.12 (left)**. A smaller portion expressed uncertainty (7.41%) or disagreement (6.17% “probably not” and 3.7% “definitely not”). Beyond overall prioritization, the question of whether employees received role-specific education and training from their organization revealed additional nuances. While 74.07% of respondents reported receiving role-specific training, 23.46% of respondents indicated that no such training was provided, as shown in **Figure 4.12 (right)**.

Taken together, the survey findings suggest that while cybersecurity training

Table 4.6. Sub-themes and excerpts from the overarching Training & Awareness theme that were derived from the thematic analysis of the follow-up interview data.

Theme: Training & Awareness	
Sub-theme	Example Quotes / Excerpts
Cadence & Frequency	<i>"...the frequency of the trainings can be an issue because, I think it gets sent to us once in every quarter, and that's like a lot, lot, lot of trainings has to be completed... they might think that I'm just spending time endlessly on completing trainings that you know, it is just a burden at some point"</i> (Participant 24) <i>"I think we do like an annual training. I mean that's at a very high-level, it's for all employees, it's not just for engineers."</i> (Participant 21) <i>"...it's nice that they cover it and you can, you know, we're allowed to study while we're at work. So, it's not like you have to go home and work on it every night."</i> (Participant 17) <i>"So, like for example, my team gets trained in Microsoft and Azure security components, right? Others get trained in identity or security operations centers, things like that, right? And there's usually a requirement each year for you to meet something, at least. Hey, you got to get one certification or two, or something like that..."</i> (Participant 08) <i>"I think a lot of us in cyber departments just subscribe to that yearly training. Your kind of yearly, every six-months phishing training... it's all those kind of corporate pushes."</i> (Participant 03)
Role-Specific Training Approach	<i>"So yes, I do have sensitive information that I work with, but I don't have, I've not received like... I've received training which is like common across the entire company. Yeah. So, maybe a... a specific training would have helped."</i> (Participant 01) <i>"I get to work with some financial institutions which, you know, right, have a lot of regulatory scrutiny and therefore because of that, I get to take some specialized trainings, right? ... That are mandated by SEC or other like governmental agencies, because of the fact that I get to handle some sensitive information, some banking information, so on and so forth. So, I would consider those as my role specific training because of the fact that I am getting introduced to these new type of data that is heavily regulated and governed."</i> (Participant 06) <i>"So, like for example, my team gets trained in Microsoft and Azure security components, right? Others get trained in identity or security operations centers, things like that, right? And there's usually a requirement each year for you to meet something, at least. Hey, you got to get one certification or two, or something like</i>

Table 4.6. Continued

Theme: Training & Awareness	
Sub-theme	Example Quotes / Excerpts
	<i>that” (Participant 08)</i> <i>“...one of the areas that we're trying to address... I would consider it to be to be a point of opportunity would be establishing a baseline of security knowledge. And as I mentioned, the governance team comes from, you know, sometimes non-technical backgrounds. I have two lawyers on the team. They're starting to understand, you know, technical things, right? They're starting to get their hands dirty. But it's not like I'm going to have them... I'm not going to give them a Hack The Box license and say, okay, you're making the most out of it, right.” (Participant 10)</i> <i>“...my son and daughter... when they turned 16, they wanted to get a driver's license and the state of Georgia made them to do certain things to and your pay fee, and Georgia says they're good to drive. What if we took that idea and said what about someone who has elevated access, someone who's in System Administrator, or maybe a database administrator? ... Here is extra role-specific training or awareness, and just like your driver's license eventually needs to be updated, we're going to every year, have you go through this training because you have special rights and you have special privileges on our network.” (Participant 26)</i>
Effective Training Sources	<i>“I've done some SANS trainings and those they're pretty intense, but they I think are very informative and... and like I... I think I have actually learned a lot from those, and I have been able to implement some of the things I learned there into my work every day.” (Participant 21)</i> <i>“...the ones offered through LinkedIn... LinkedIn, and a series of... I mean different professionals and individuals putting trainings out there.... simple videos... So, I mean I found those pretty useful, pretty easy to kind of go through.” (Participant 04)</i> <i>“I've been trying to take certifications although not very successful in the last year or two, but hmm, those are, yeah, there are, like, you know, AWS, Azure, GCP, they've been introducing new certificates every year... I can name a few that I have already, which I find incredibly helpful, which are AZ500, SC900, AZ 900 and then AWS Solution Architect, right? So, all these are like incredibly helpful from looking you know into the cloud services with like a security lens.” (Participant 06)</i> <i>“It has to be hands-on. So, most recently for the Ops team, we... we engage with Hack The Box and it's just, right, like it's labs, hands-on things you can compete against each other. It's... it's active, engaged learning,</i>

Table 4.6. Continued

Theme: Training & Awareness	
Sub-theme	Example Quotes / Excerpts
	<i>right? It's trial and error.” (Participant 10)</i> <i>“I mean, yeah, in the cybersecurity world, you're probably familiar with, like, the SANS Institute. Right? Like, they do cybersecurity trainings, for like, cybersecurity practitioners. So yeah, like at my company, like, you know, usually an employee does one course a year, and I think those trainings are, you know, particularly helpful in doing our job.” (Participant 25)</i>
Challenges & Frustrations	<i>“The biggest thing is like finding the time to be able to do it... like getting dedicated time to actually attend these, rather than trying to balance it on top of, you know, all the other responsibilities... it can be difficult to find the time to get in and... and attend some of these trainings.” (Participant 05)</i> <i>“I can go over some very boring documentation... after about 30 to 45 minutes, I'm like, I'm just going to give up and ask... it was one incredibly simple thing that they did and I just didn't realize there was this tiny little button on the screen that they could click on.” (Participant 23)</i> <i>“I think that the broadness is pretty good. I think the depth is pretty bad... for example, for security you should understand networking pretty well... I think most people don't. They just... networking is like a haze in their mind, right? ...you can see that when we have a... a... a security problem and the network is involved, people are usually very lost on how to handle it and it's... it's not something that you learn through a one-month training. It actually requires a few years of training, and like retraining again and again, and learning, it's tough.” (Participant 08)</i> <i>“I actually had to develop a training for a client and the training was just on, like clean desk policy - not writing down your passwords and what not. So, in developing a 30-slide presentation, we were kind of told like if we could just cut the training down, they felt that their employees would not be, you know, very receptive to an hour-long training and that they wanted something that could be in the realm of 15 to 20 minutes” (Participant 11)</i> <i>“There is some required training for end-users, but I would say it's minimally, it's not very good.” (Participant 18)</i>
Future Improvements & Innovations	<i>“I think real life scenarios, I mean, I think the phishing simulations can be very useful if we were to implement training alongside of that. I mean I think we have a lot of current threats that seem to really be persisting in our environment. Sometimes it would be really nice to educate users about it if it was possible.”</i>

Table 4.6. Continued

Theme: Training & Awareness	
Sub-theme	Example Quotes / Excerpts
	(Participant 17) <i>“...if it's just your quarterly or yearly compliance training, people just click, click, click, click, click, click... So, I think it's more consequence-based in terms of like this guy's actually doing something incorrectly. Let me educate, let me do some real-time education that he violated his policy, educate, educate, do training right now or else you'll be fined... Then it registers, right? Like okay, I know that real-time I did something wrong, and I had to do something else to fix it.”</i> (Participant 09) <i>“Other times we've had a 'live' environment. I put that in quotations because it's kind of, you know, fake user data and whatnot, but just being able to kind of go and see what a console looks like when you're going to create a group or if you're going to kind of de-provision access to a certain resource. Those examples are typically much more helpful.”</i> (Participant 11) <i>“And we need a training button in Sentinel, that way when they... if something happens with our account, then you hit the training...”</i> (Participant 15)
Note: The example quotes/excerpts shown above are not exhaustive and are limited to a maximum of five (5) per sub-theme for convenience and clarity. A complete list of excerpts obtained from the thematic analysis is available upon request.	

initiatives are broadly present, their distribution is uneven, with some groups or roles underserved. These survey findings provided the basis for deeper exploration through follow-up interviews, where participants elaborated on role-specific training that they found meaningful and useful, as well as areas where they believed additional support was necessary. These sub-themes are discussed in the following subsections.

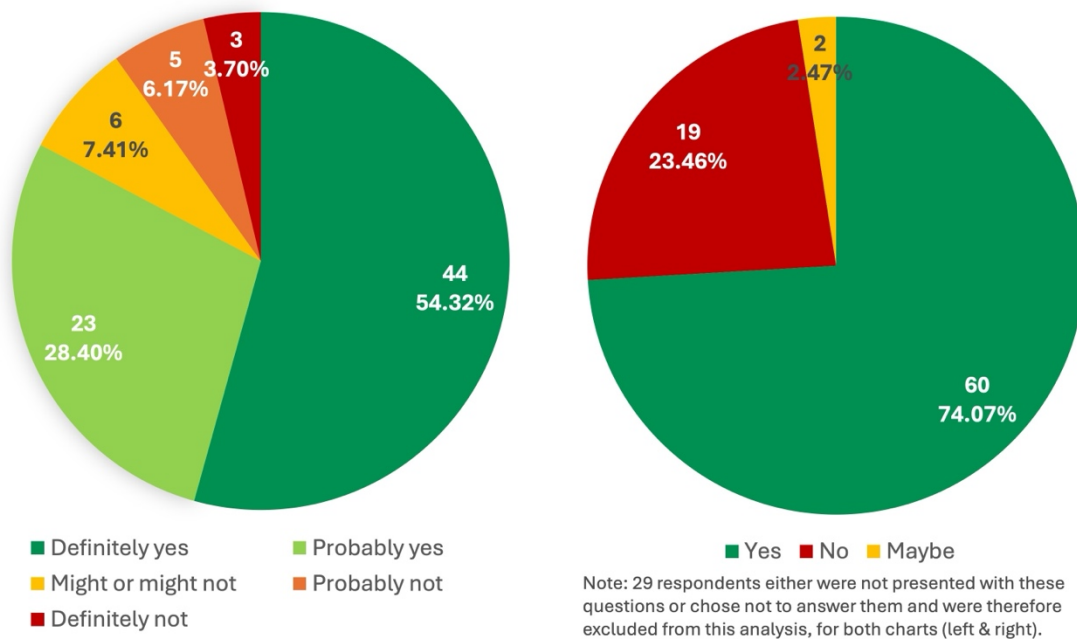


Figure 4.12. Charts showing survey responses to questions asking participants whether they believe that their organizations prioritize cybersecurity education, awareness, and training for their employees (left), and whether they receive role-specific cybersecurity

Cadence & Frequency (Training & Awareness Sub-theme 1)

Survey results showed variation in how often role-specific cybersecurity education & training was provided. Among respondents, the largest share (46.77%) reported receiving role-specific cybersecurity training from their organization annually,

followed by 20.97% bi-annually, 16.13% quarterly, 11.29% more than quarterly, and a small minority (4.84%) less than annually, as shown in **Figure 4.13**. This distribution suggests that most organizations adopt a yearly or biannual cadence, with fewer providing higher-frequency trainings.

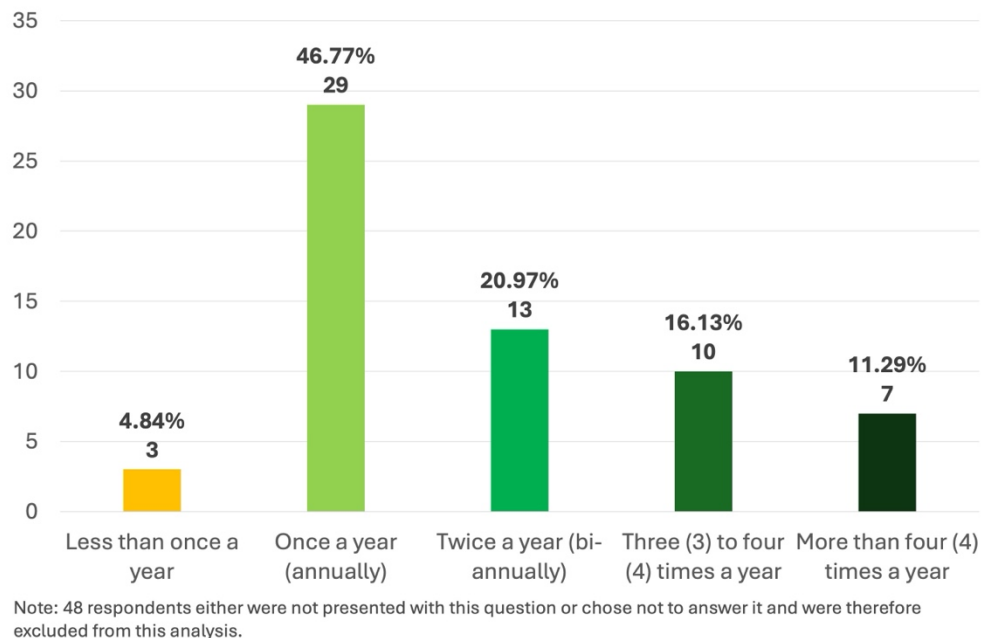


Figure 4.13. Chart displaying survey responses to the question about how frequently participants receive role-specific cybersecurity education & training from their organization.

Follow-up interview data reinforced this variability and highlighted the burden of volume and frequency for some cybersecurity professionals. While some practitioners appreciated regular training opportunities, others described quarterly cycles as excessive, particularly when multiple modules were assigned at once. As one participant noted:

“...the frequency of the trainings can be an issue because, I think it gets sent to us once in every quarter, and that's like a lot, lot, lot of trainings has to be completed... they might think that I'm just spending time endlessly on completing trainings that you know, it is just a burden at some point” (Participant 24)

Practitioners also emphasized that while training was typically completed during work hours, the sheer volume of required modules could make it feel like a compliance exercise rather than a meaningful learning opportunity. Some participants appreciated that their organizations’ allowed time during the workday to complete training, which helped reduce friction and improve participation:

“...it's nice that they cover it and you can, you know, we're allowed to study while we're at work. So, it's not like you have to go home and work on it every night.” (Participant 17)

These findings suggest that while training cadence is often driven by compliance requirements, organizations must balance frequency with content relevance and cognitive load. Overloading users with training can reduce engagement and retention, turning awareness efforts into a checkbox exercise rather than a meaningful learning experience. Cadence & Frequency form a core UX sub-theme, with challenges focused on the usability of training delivery that determine how effectively practitioners engage with and apply cybersecurity learning.

Role-Specific Training Approach (Training & Awareness Sub-theme 2)

The follow-up interviews highlighted a strong preference among participants for cybersecurity training tied to job functions and corresponding risk levels. Participants contrasted generic, one-size-fits-all cybersecurity training modules with targeted instruction for privileged users such as system administrators, database administrators, developers, financial officers, etc., describing the latter as indispensable. Contractors and third-party vendors were also identified as requiring tailored approaches. As one participant explained:

“I get to work with some financial institutions which, you know, right, have a lot of regulatory scrutiny and therefore because of that, I get to take some specialized trainings, right? ... That are mandated by SEC or other like governmental agencies, because of the fact that I get to handle some sensitive information, some banking information, so on and so forth. So, I would consider those as my role specific training because of the fact that I am getting introduced to these new type of data that is heavily regulated and governed.” (Participant 06)

A recurring metaphor mentioned by participants was the “driver’s license” model: just as additional certification is required before operating more complex vehicles, elevated system privileges should require targeted, higher-level training. This framing illustrates how cybersecurity professionals conceptualized the link between accountability and preparedness, positioning role-specific and risk-based training as a

prerequisite for responsibility rather than merely a periodic compliance requirement. As one participant described:

“...my son and daughter... when they turned 16, they wanted to get a driver's license and the state of Georgia made them to do certain things to and your pay fee, and Georgia says they're good to drive. What if we took that idea and said what about someone who has elevated access, someone who's in System Administrator, or maybe a database administrator? ... Here is extra role-specific training or awareness, and just like your driver's license eventually needs to be updated, we're going to every year, have you go through this training because you have special rights and you have special privileges on our network.”

(Participant 26)

These preferences for role-specificity and risk-based approach to cybersecurity training and education align with Reuter et al.'s (2022) observation that tailorability is a key principle of usable security with regards to cybersecurity training, and with Grobler et al.'s (2021) argument that cybersecurity training & awareness initiatives are limited in their efficacy if they are not targeted. This is a core UX sub-theme, reflecting challenges in ensuring that training content aligns with practitioners' roles, responsibilities, and operational contexts, thereby enhancing perceived usefulness and retention.

Effective Training Sources (Training & Awareness Sub-theme 3)

Follow-up interview data highlighted a range of sources that participants found effective for cybersecurity training, spanning both external providers and internal resources. Participants consistently praised hands-on, tool-specific, and practitioner-led formats over generic cybersecurity training content that felt like “check-the-box” exercises, often disconnected from daily realities. Among external sources, SANS Institute courses were frequently cited as particularly valuable for a wide variety of cybersecurity topics, including incident response, forensics, among others. These courses were described as rigorous but highly applicable to real-world scenarios:

“I mean, yeah, in the cybersecurity world, you're probably familiar with, like, the SANS Institute. Right? Like, they do cybersecurity trainings, for like, cybersecurity practitioners. So yeah, like at my company, like, you know, usually an employee does one course a year, and I think those trainings are, you know, particularly helpful in doing our job.” (Participant 25)

Practitioners also pointed to vendor-provided training, such as Microsoft Azure, AWS, GCP, CrowdStrike, and so forth, as useful for building platform or tool-specific expertise, especially in cloud and endpoint security. Certifications like AZ-500 and AWS Solutions Architect were mentioned as helpful for applying a security lens to technical domains. In addition to formal certification courses, participants valued bite-sized and flexible formats, such as LinkedIn Learning videos and internal cybersecurity training

that drew upon real-world security incidents. Peer-led sessions, annual cybersecurity awareness events, and interactive platforms like “Hack The Box” were also mentioned as engaging and effective. As one participant noted:

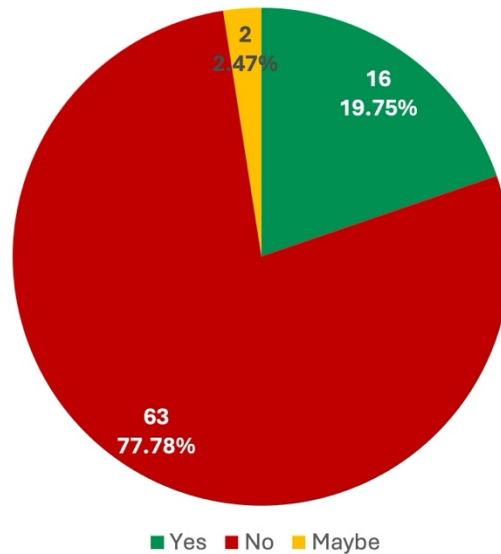
“...the ones offered through LinkedIn... LinkedIn, and a series of... I mean different professionals and individuals putting trainings out there.... simple videos... So, I mean I found those pretty useful, pretty easy to kind of go through.” (Participant 04)

A suggestion aligned with emphasis on real-world relevance, and supported by published usable security research, is the use of “embedded training” (Garfinkel & Lipford, 2014). For instance, this approach involves sending phishing-like emails to employees, where the embedded links redirect users to educational pages that inform them that they’ve fallen for a simulated phishing attempt and provide real-time training. This is a core UX sub-theme because the identified challenges and recommendations to address them focus on which sources (e.g., hands-on labs, vendor courses, peer-led sessions) actually support effective learning in practice, versus sources that feel “check-the-box”.

Challenges (Training & Awareness Sub-theme 4)

Survey findings suggest that while most respondents did not perceive significant challenges with respect to cybersecurity education, awareness, and training,

approximately one-fifth of respondents reported otherwise. Among those who answered, 19.75% indicated “yes” when asked whether they encountered any challenges specific to cybersecurity education, awareness, and training, 2.47% said “maybe,” and 77.78% reported “no,” as shown in **Figure 4.14**.



Note: 29 respondents either were not presented with this question or chose not to answer it and were therefore excluded from this analysis.

Figure 4.14. Chart showing survey responses to the question asking participants whether they encountered any challenges specific to cybersecurity education, awareness, and training.

Taken together, nearly one-fourth of respondents experienced difficulties. **Table 4.7** outlines the challenges related to organizations’ role-specific cybersecurity training & awareness initiatives based on participants’ responses to the open-ended (text-input) follow-up survey question. The key takeaways are as follows:

- Multiple participants noted lack of relevance and tailoring, with cybersecurity training often being too generic, outdated, or repetitive, failing to address role-specific needs (e.g., developers, threat intel analysts) or real-world scenarios.
- Engagement and adoption were major hurdles, including low prioritization by leadership, lack of time, unengaging formats, incorrect assignments, and persistent difficulties in securing user buy-in.
- Additional concerns centered on resource and implementation gaps, such as insufficient budgets, failure to translate training into practice, and training programs lagging behind the pace of evolving threats.

The follow-up interview analysis provided additional insights regarding these challenges. For instance, a common challenge was time constraints, with participants struggling to balance training requirements alongside other responsibilities. Even when training was considered valuable, the lack of dedicated time to complete it meaningfully was a barrier:

“The biggest thing is like finding the time to be able to do it... like getting dedicated time to actually attend these, rather than trying to balance it on top of, you know, all the other responsibilities... it can be difficult to find the time to get in and... and attend some of these trainings.” (Participant 05)

Others pointed to structural and cultural barriers, including poorly mapped role-to-training requirements, outdated training platforms, one-size-fits-all approaches to training that undermined relevance, and a lack of visible commitment from leadership. Despite these challenges and frustrations, participants also described emerging practices aimed at addressing such challenges. For example, some organizations experimented with gamified training, interactive scenarios, and peer-led sessions, which were perceived to be more engaging and relatable than static compliance modules. One participant described a future improvement aimed at addressing challenges with training as follows:

“...if it's just your quarterly or yearly compliance training, people just click, click, click, click, click, click... So, I think it's more consequence-based in terms of like this guy's actually doing something incorrectly. Let me educate, let me do some real-time education that he violated his policy, educate, educate, do training right now or else you'll be fined... Then it registers, right? Like okay, I know that real-time I did something wrong, and I had to do something else to fix it.” (Participant 09)

These insights align with broader scholarship emphasizing the importance of human-centric and adaptable approaches to cybersecurity training (Grobler et al., 2021; Reuter et al., 2022). This is treated as a supplementary UX sub-theme synthesizing systemic obstacles (time, budgets, leadership buy-in, platform constraints) that indirectly shape the usability of training experiences and their adoption.

Table 4.7. Reported challenges related to role-specific cybersecurity training & awareness initiatives, based on participants' responses to the open-ended (text-input) survey question.

Challenges Faced with Role-specific Cybersecurity Training
Sometimes the policies in place by the company don't really match with how the tools are implemented within the system, making it more difficult to use the provided tools to meet policies (like password storage policies but having restricted access to the preferred password manager.).
No budget for training
Tailoring training to specific types of end users
Maintaining engagement long enough for the lessons to stick.
Occasionally, automatic training assignments are incorrectly assigned - meaning we are assigned training that is not required and time could be wasted.
Prioritization of role-specific security training is not taking place
Learning new techniques require substantial investment
Getting staff to focus on importance of the training
From my perspective it's less about a training issue on how to stay secure but it's communicate the likelihood of the employee being targeted and the impact, with limited repercussions.
I personally find our cyber security awareness program to not be keeping up with our rapid pace of changing technology. There is a reason why threat actors continue using textbook old methods, and it's because they are still effective today. My personal belief is that our training needs to be more engaging with the relevancy of our audience in the form of short videos, interactive training sessions, and basic computer skills courses that include security awareness best practices. Cyber security training should no longer be just a buzzword, but a life skill. Security threats exist everywhere from personal homes, to schools, your workplace, and your favorite restaurants.
Not challenging enough
Not enough time to do more of it!
Achieving buy-in. I've attempted to implement sec awareness training with fidelity, but I still have a percentage of users who consistently do not complete. With phishing simulations, I struggle with false positives. I'm overwhelmed by the number of users who submit spam messages or entirely legitimate messages as phishing. Like with the SIEM, i suffer from alert fatigue frequently
Determining the best content to use for videos. Had to purchase software to generate scorm content

Table 4.7. Continued

Challenges Faced with Role-specific Cybersecurity Training
Software developers not implementing knowledge that they learn in secure programming training despite the fact that they have gone through training many times
Yea, i've faced a few challenges with cybersecurity education and awareness training. most of the time the trainings are super basic and not really useful for someone in threat intel. they usually cover stuff like not clicking on phishing links or using strong passwords, which is fine for general staff but not helpful for ppl doing malware analysis or looking at threat actor behavior. also, a lot of the content is outdated or gets repeated every year with no updates, so it feels like your just doing it to check a box. theres usually no hands-on stuff or real case examples, so its hard to stay engaged or actually learn anything new. i think training would be way better if it was role-based and more focused on real threats we deal with.

Summary of Key Findings

The following eight (8) sub-themes highlight key findings related to the UX of cybersecurity tools & platforms. Additional patterns and insights are discussed in detail in *Chapter 4 (Results & Discussion)*.

1. **Procurement & Integration** - Procurement of cybersecurity tools & platforms is driven primarily by compliance, risk reduction, cost, and vendor obligations, with usability/UX rarely considered and largely treated as an informal afterthought, highlighting a gap in literature that the recommendations in the proposed Usable Security Community Profile (see *Chapter 5*), as an outcome of this dissertation study helps address.
2. **Consolidation vs. Best-of-Breed** - Organizations often favored integrated platform suites (e.g., Microsoft suite, which includes Microsoft Defender) over best-of-breed tools (e.g., CrowdStrike, for EDR) that are often technically superior, with decisions shaped by cost savings, license bundling, and ecosystem lock-in, highlighting that UX extends beyond interface design to how tools are selected, bundled, and embedded within broader enterprise ecosystems.
3. **Workflow Efficiency** - Practitioners highlighted inefficiencies such as excessive clicks, manual “glue work” (copying and pasting information between systems), lack of state persistence, and poor integration between tools. For example, when switching from Microsoft Defender to Sentinel to work on an incident, not all necessary information transfers over, requiring repeated platform switching and manual data entry. These insights underscore the need for workflow-aware

designs and automation that minimize redundancy and keep focus on investigative tasks.

4. **Performance & Reliability** - Performance and reliability directly impacted the overall UX of cybersecurity tools & platforms, with recurring frustrations around slow response times, vague error messages (e.g., CyberArk), and weak API support. Participants emphasized that speed, stability, and dependable integrations were critical, especially in time-sensitive contexts like Incident Response scenarios.
5. **UI Quality & Impact of Changes** - Frequent UI updates (e.g., within Microsoft tools) caused “change fatigue” and retraining overhead, while stable UIs (e.g., CrowdStrike) were preferred. Participants also cited challenges such as cluttered navigation, inconsistent layouts, and outdated interfaces (e.g., XWays), reinforcing that interface consistency and clarity are vital to usability and efficiency.
6. **Documentation, Learnability, and Onboarding** - Long PDFs and dense vendor manuals hindered onboarding, leading practitioners to favor concise, actionable formats such as internal playbooks, quick-start guides, short videos, and contextual help resources to accelerate learning.
7. **Feedback Loops & Issue Tracking** - Practitioners relied on a mix of informal peer exchanges (through Teams, Slack, etc.) and formal ticketing systems (e.g., Jira, ServiceNow), with some effective UX improvements arising when feedback was systematically captured, tracked, and shared with vendors.

8. **Balancing Security vs. Operations** - Participants emphasized that overly rigid security controls (e.g., eight-hour IdP timeouts in Okta) can disrupt critical workflows, like in healthcare settings, highlighting the need for sector-aware, proportionate security measures that balance operational continuity.

The following five (5) sub-themes highlight key findings related to the UX of cybersecurity tools & platforms. Additional patterns and insights are discussed in detail in *Chapter 4 (Results & Discussion)*.

1. **Accessibility & Centralization** - While most practitioners reported that cybersecurity policies and standards were accessible, their usability depended heavily on effective centralization and searchability; intuitive access solutions such as intranet redirects and internal search tools enhanced engagement, whereas fragmented storage, poor organization, and lack of search optimization often hindered it. Such insights were consistent with prior literature emphasizing transparency as crucial to policies & standards UX.
2. **Clarity & Understandability** - Although policies were generally viewed as understandable, participants criticized their excessive length and legalistic tone, emphasizing the need for concise, role-specific summaries, scenario-based examples, and visual formats (e.g., flowcharts) to make policy requirements more actionable.
3. **Compliance & Framework Alignment** - Cybersecurity policies & standards are largely shaped by external frameworks & regulations (e.g., NIST CSF, ISO

- 27001, HIPAA, PCI DSS, etc.), yet practitioners noted update delays & outdated documentation, unclear ownership, and misalignment between governance documents and operational tools.
4. **Feedback, Enforceability, and Escalation** - Enforcement varied widely across organizations, with informal workarounds (e.g., Teams chats replacing ticket requests) undermining consistency and accountability, emphasizing the need for structured escalation paths and responsive feedback loops.
 5. **Potential Improvements** - Practitioners proposed forward-looking enhancements such as an AI-powered chatbot to answer policy-related queries, the inclusion of concise, Visio diagrams or one-slide overviews of policies to improve accessibility and engagement, among others.

The following five (5) sub-themes highlight key findings related to the UX of cybersecurity tools & platforms. Additional patterns and insights are discussed in detail in *Chapter 4 (Results & Discussion)*.

- **Cadence & Frequency** - Training frequency varied widely, from annual to quarterly cycles, with some practitioners valuing regular refreshers while others reported training fatigue and reduced engagement when training volume became excessive or compliance-driven.
- **Role-Specific Training Approach** - Participants strongly preferred role-specific, risk-based training tailored to privilege levels (e.g., system or database administrators), emphasizing that elevated access should entail higher

accountability and periodic re-certification. This aligns with prior literature that emphasize that training & awareness initiatives are limited in their efficacy if they are not targeted.

- **Effective Training Sources** - Practitioners favored practical, scenario-based, and bite-sized training formats (e.g., embedded simulations, short videos, etc.) over generic modules, praising external sources such as SANS Institute and vendor-led programs (e.g., Microsoft Azure, AWS, etc.) for their real-world relevance and hands-on applicability.
- **Challenges & Frustrations** - Practitioners cited time constraints, one-size-fits-all content, outdated materials, and low leadership prioritization as barriers to effective cybersecurity training, emphasizing the need for adaptive, engaging, and role-relevant learning approaches.
- **Future Improvements & Innovations** - Participants envisioned innovative improvements and training approaches such as just-in-time-training, embedding training buttons within cybersecurity tools, and so forth.

CHAPTER FIVE

NIST CSF-BASED USABLE SECURITY COMMUNITY PROFILE

Overview

This chapter presents the NIST Cybersecurity Framework (CSF)-based Usable Security Community Profile, which represents the primary outcome of this dissertation. The development of this Community Profile directly addresses **RQ3**: What are the UX elements that are critical for organizations from a Usable Security standpoint, and how can they be integrated into a NIST CSF Community Profile? Building upon the findings discussed in *Chapter 4 (Results and Discussion)*, this Community Profile was developed using the generalizable NIST CSF Community Profile templates published as part of **Phase I (Template Development)**, detailed in **Appendix E** (Rajarathnam & Singh, 2023), as well as the official template and guidance released by NIST (NIST, 2024; Pascoe et al., 2024). The resulting Profile synthesizes recurring issues, data-driven recommendations, and informative references drawn from both scholarly and industry sources. Its overarching goal is to help practitioners improve the usability and user experience (UX) of cybersecurity tools and platforms, policies and standards, and training initiatives within organizational settings.

Community Profile Structure & Components

Sub-RQ3a: What UX principles are most critical for inclusion in a cybersecurity framework?

Sub-RQ3b: Which NIST CSF Core components (such as Functions and Categories) are relevant to or impacted by Usable Security considerations?

Sub-RQ3c: What are the UX challenges that organizations face when developing or maintaining their tool or role-specific training?

This section addresses Sub-RQ3a, Sub-RQ3b, and Sub-RQ3c above based on the analysis of survey and interview data, the researcher’s interpretation, and feedback from four (4) cybersecurity experts (please refer to *Chapter 3*). **Table 5.1** introduces the NIST CSF-based Usable Security Community Profile, with the following sub-sections elaborating on each column. The data-driven, user-centered recommendations outlined in *Recommendations & Considerations* subsection, together with the *Informative References* and *Priority & Rationale*, address Sub-RQ3a by identifying the UX considerations most relevant for inclusion in the Community Profile. The *NIST CSF 2.0 Core Categories and Outcomes* subsection addresses Sub-RQ3b by explaining the rationale for mapping findings at the Category level of the CSF Core. Finally, *Issues - from Data Analysis* (summarized from *Chapter 4*) addresses Sub-RQ3c by capturing the UX challenges organizations face in developing and maintaining cybersecurity tools and role-specific training, along with their policies and standards.

NIST CSF 2.0 Core Categories and Outcomes

Each merged row spanning all five (5) columns in **Table 5.1** represents a NIST CSF v2.0 Core Category (e.g., GV.PO) and its corresponding Core Outcome (e.g.,

Organizational cybersecurity policy is established, communicated, and enforced for GV.PO). These labels and color palette for the row background/highlights are drawn directly from the NIST CSF v2.0 (National Institute of Standards and Technology, 2024a, 2024b; Pascoe et al., 2024).

The Community Profile developed in this study is scoped at the Category level (e.g., ID.AM: Asset Management) rather than the more granular Sub-Category level (e.g., ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded). This reflects both the nature of the dataset and the study's objectives. As described in *Chapters 3 & 4*, survey and interview findings were analyzed thematically, yielding practitioner-reported challenges and recommendations related to cybersecurity tools & platforms, policies & standards, and role-specific training & awareness initiatives. These insights mapped most directly to broad Categories such as Risk Assessment (ID.RA), Asset Management (ID.AM), and Data Security (PR.DS). Category-level scoping is especially appropriate for this study's focus on usable security and organizational cybersecurity UX, where issues such as policy readability, tool interoperability, and training fatigue are cross-cutting and span multiple Sub-Categories. Presenting the Profile at this level avoids unnecessary fragmentation, enhances clarity for practitioners, and frames findings at the level of abstraction most relevant to usability and human-centered outcomes. Consistent with NIST guidance (Pascoe et al., 2024), which emphasizes tailoring Profiles to community needs and highlighting the most relevant outcomes, this scoping is a deliberate methodological choice.

Relevant Artifacts

This corresponds to the first column on the left in **Table 5.1** and identifies one or more of the three (3) themes from the data analysis: Tools & Platforms, Policies & Standards, and Training & Awareness, that are most relevant to each NIST CSF Core Category. For cybersecurity tools & platforms, specific examples (e.g., Splunk, CrowdStrike, Microsoft Defender) are listed based on those cited by multiple survey participants as among their top two (2) most used in daily work (see **Table 4.2**). These examples are provided for reference only and are not intended as a comprehensive inventory of all applicable tools or platforms. The issues and recommendations noted in the table may likewise extend to other cybersecurity tools & platforms beyond those explicitly listed. Although this column is not designated as “Recommended” or “Optional” in the NIST CSF v2.0 Community Profile template and guidance (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024), it is highly relevant to this Community Profile and outlines the applicability for the key issues identified, as well as the recommendations and considerations presented in this Profile.

Issues - from Data Analysis

This corresponds to the second column from the left in **Table 5.1** and presents the key issues identified through the analysis and interpretation of the survey and follow-up interview data for each NIST CSF Core Category and Outcome (as shown in the merged row above with background highlighting). Although this column is not designated as “Recommended” or “Optional” in the NIST CSF v2.0 Community Profile template and

guidance (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024), it is highly relevant to this Community Profile and provides the foundation for the recommendations and considerations presented here. These issues have been summarized from the findings reported in *Chapter 4 (Results and Discussion)*. In some cases, issues are marked as not applicable (N/A) because no consistent, participant-reported UX concerns could be attributed directly to those Categories (e.g., GV.OC or RC.RP) at the Category level. While related concerns, such as policy accessibility, tool interface changes, or alert fatigue, etc. were well supported by participant evidence, they aligned more clearly with other CSF Categories. To maintain methodological rigor and avoid over-interpretation, this iteration therefore designates such rows as N/A.

Priority & Rationale

This corresponds to the third column from the left in **Table 5.1** and presents the priority assigned to each NIST CSF Core Category and Outcome (as indicated in the merged row above with background highlighting). This column consolidates the Priority and Rationale elements, both designated as “Recommended” in the NIST CSF v2.0 Community Profile template and guidance (National Institute of Standards and Technology, 2024; Pascoe et al., 2024), into a single entry for easy readability. Priorities are expressed on a Low/Medium/High scale, as determined by the researcher and validated through Expert Reviews (please refer to *Chapter 3*). Categories with multiple, strong, and recurring cybersecurity UX issues (please refer to *Issues - from Data Analysis*, second column of **Table 5.1**), such as GV.PO, were rated High. Categories with

fewer issues or effective workarounds, such as ID.IM, were rated Low. Categories with notable but less severe issues, for instance, those affecting newcomers more than experienced practitioners, such as PR.IR, were rated Medium. Finally, Categories with no directly attributable cybersecurity UX issues (marked N/A) were also designated N/A for priority.

Recommendations & Considerations

This corresponds to the fourth column from the left in **Table 5.1** and presents the data-driven, user-centered recommendations and considerations associated with each NIST CSF Core Category and Outcome (as indicated in the merged row above with background highlighting). These recommendations are directly tied to the key issues identified for each Category (please refer to *Issues - from Data Analysis*, second column of **Table 5.1**), based on analysis of the survey and interview data, the researcher's interpretation, and validation through Expert Reviews (please refer to *Chapter 3*). While this column is designated as "Optional" in the NIST CSF v2.0 Community Profile template and guidance (National Institute of Standards and Technology, 2024; Pascoe et al., 2024), it is especially relevant in this study and represents one of its primary contributions. The recommendations are intended to support cybersecurity professionals in improving the usability and overall user experience of cybersecurity tools & platforms, policies & standards, and role-specific training and awareness initiatives within their specific organizational contexts.

Informative References

This corresponds to the fifth and final column in **Table 5.1** and lists the informative references associated with the key issues and recommendations for each NIST CSF Core Category and Outcome (as indicated in the merged row above with background highlighting). Unlike many published NIST CSF Community Profiles (National Institute of Standards and Technology (NIST), 2021; Rajarathnam & Singh, 2023), which typically cite only standards and frameworks such as COBIT or ISO/IEC 27001, this Profile uniquely integrates a combination of peer-reviewed journal articles, conference papers, industry frameworks, and practitioner guidance directly relevant to the identified issues (please refer to *Issues – from Data Analysis*, second column of **Table 5.1**) and recommendations (see *Recommendations & Considerations*, fourth column of **Table 5.1**). The inclusion of academic and practitioner sources was based on the researcher’s determination and validated through Expert Reviews (please refer to *Chapter 3*). Although designated as “Optional” in the NIST CSF v2.0 Community Profile template and guidance (National Institute of Standards and Technology, 2024; Pascoe et al., 2024), this column provides valuable context and actionable suggestions from relevant resources for practitioners and represents one of the key contributions of this study.

Table 5.1. NIST CSF-based Community Profile for Usable Security, based on available templates and guidance (National Institute of Standards and Technology (NIST), 2024; Pascoe et al., 2024; Rajarathnam & Singh, 2023).

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
GV.OC - The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood				
Cybersecurity Policies & Standards	• N/A - no specific UX-related issues identified for this Category. Please refer to other Categories for Cybersecurity Policies & Standards' UX issues	N/A - no consistent reported UX issues; adjacent issues mapped under other CSF categories.	• N/A	• N/A
GV.RM - The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions				
Cybersecurity Policies & Standards	• Misalignment between policies & standards and operational tools (e.g., risk & control libraries)	Low - Policies & Standards are widely accessible, understandable, and well-communicated, despite misalignment issues.	• Tracking legal/regulatory updates and aligning policies & standards update cycles to match	• Guidance - Governance and Risk Model (GRM) (Cybersecurity Risk Foundation, 2025) • Blog - Tracking Regulatory Changes (Barona, 2025; Couto, 2025; Kappel, 2025)
GV.RR - Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated				
Cybersecurity	• Inconsistent policies &	Medium -	• Structured escalation paths,	• Conference Paper -

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale²	Recommendations & Considerations	Informative References
Policies & Standards	standards' enforcement and practitioners' workarounds to bypass formal procedures	Recurring UX issues identified (see <i>Chapter 4</i>); however, Policies & Standards are accessible, understandable, well-communicated, and informal workarounds exist.	consistent documentation, and responsive feedback loops for Policies & Standards	Workarounds-based Learning (Kirlappos et al., 2014)
GV.PO - Organizational cybersecurity policy is established, communicated, and enforced				
Cybersecurity Policies & Standards	• Long, legalistic, and difficult to digest policies • Outdated policies & standards, out of compliance with recent legal/regulatory updates • Inconsistent policies & standards' enforcement and practitioners' workarounds to bypass formal procedures • Difficulties translating policies & standards into actionable controls • Misalignment between policies	High - Multiple strong recurring UX-related identified by participants (see <i>Chapter 4</i>)	• Accessibility improvements through internal search engines, intranet redirects, AI-assisted search features • Plain-language explanations, real-world or role-specific examples, simplified summaries (e.g., one-pagers) to improve understandability • Tracking legal/regulatory updates and aligning policies & standards update cycles to match	• Guidance - Policies & Standards templates (SANS Institute, n.d.) • Conference Paper - Workarounds-based Learning (Kirlappos et al., 2014) • Guidance - Plain Language Guide and Resources - (U.S. General Services Administration

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale²	Recommendations & Considerations	Informative References
	& standards and operational tools (e.g., risk & control libraries)		• Structured escalation paths, consistent documentation, and responsive feedback loops for Policies & Standards	(GSA), 2025)
GV.OV - Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy				
Cybersecurity Policies & Standards	• N/A - no specific UX-related issues identified for this Category. Please refer to other Categories for Cybersecurity Policies & Standards' UX issues	N/A - no consistent, participant-reported UX issues identified. While adjacent UX issues exist, they are mapped to other CSF Categories.	• N/A	• N/A
GV.SC - Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders				
Cybersecurity Tools & Platforms Procurement Criteria Cybersecurity Policies & Standards	• UX / usability considerations not included or assigned low weight in cybersecurity tools & platforms procurement criteria	Medium - UX considerations are often informally included in procurement criteria, though assigned low weight	• Formalize UX / usability considerations in cybersecurity tools & platforms procurement criteria	• Research Article - Usability Considerations in IT Systems' Procurement (Saari et al., 2024) • Guidance - Cybersecurity Tools

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale²	Recommendations & Considerations	Informative References
				& Platforms' Procurement Priorities (US Cybersecurity & Infrastructure Security Agency (CISA), 2025)
ID.AM - Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy				
Wiz, Splunk, Microsoft Purview, ServiceNow, Archer, Prisma Cloud Role-specific Cybersecurity Training	• Cybersecurity tools & platforms sprawl; multiple tools with overlapping capabilities • Integration and interoperability challenges between multiple tools & platforms (e.g., Splunk and ServiceNow) • Training programs lagging behind the pace of evolving threats	High - Multiple strong recurring UX issues identified by participants (see <i>Chapter 4</i>)	• Cybersecurity tools & platforms portfolio rationalization, where feasible • Increased integration and interoperability support from vendors, and internal documentation of workarounds where applicable (e.g., through playbooks) • Timely updates to training based on evolving threats, referring to effective external sources for training (e.g., SANS Institute), as needed	• Guidance - Portfolio Rationalization (US Chief Information Officers (CIO) Council, n.d.) • Guidance - SANS Cybersecurity Courses and Certifications (SANS Institute, n.d.) • Guidance - Cybersecurity Workforce Training Guide (US CISA,

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
				2021)
ID.RA - The cybersecurity risk to the organization, assets, and individuals is understood by the organization				
Splunk, Qualys, Tenable, Wiz, Archer Cybersecurity Policies & Standards	- Tools & Platforms are hard or unintuitive for non-experts (e.g., Splunk), steep learning curves - Misalignment between policies & standards and operational tools (e.g., risk & control libraries, enterprise risk management processes)	Medium - Recurring UX issues identified, (see <i>Chapter 4</i>) However, some issues identified impact beginners or non-experts more than experienced professionals.	- Support from organizations for role-specific training for risk/scanning tools and processes in the form of allowing dedicated time and resources for training - Structured escalation paths, consistent documentation, and responsive feedback loops for Policies & Standards	Conference Paper - Workarounds-based Learning (Kirlappos et al., 2014)
ID.IM - Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions				
ServiceNow, Microsoft Teams / alt. collaboration tools Cybersecurity Policies & Standards	Informal documentation of insights and workarounds to bypass formal procedures (e.g., messages via MS Teams instead of ServiceNow/Jira, leading to logging and accountability gaps)	Low - informal documentation of insights and workarounds exist, even if not formally documented.	Improving the UX of formal documentation and escalation processes (e.g., integrating AI-enabled tools to pull insights from informal messages into tools like ServiceNow/Jira)	Conference Paper - Workarounds-based Learning (Kirlappos et al., 2014)
PR.AA - Access to physical and logical assets is limited to authorized users, services, and hardware, and is managed commensurate with the assessed risk of unauthorized access				
Okta,	Generic or non-descriptive	High - Multiple	Development of internal	Guidance - NIST

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale²	Recommendations & Considerations	Informative References
CyberArk, SailPoint, Microsoft Entra ID, Azure PIM Cybersecurity Policies & Standards Role-specific Cybersecurity Training	errors and insufficient or outdated documentation (e.g., CyberArk), resulting in practitioners troubleshooting largely on their own • Balancing strict security measures with operational realities (e.g., enforcing 8-hour IdP session time-outs in Okta, which may not be feasible in healthcare/emergency response)	strong recurring UX identified by participants (see <i>Chapter 4</i>).	documentation of solutions and workarounds to common errors and issues, as applicable (e.g., through playbooks) • Support from organizations for role-specific IAM training (e.g., vendor-provided training) in the form of allowing dedicated time and resources for training • AI-enabled search to allow easy navigation of documentation and troubleshooting • Measures to balance strong security with operational realities (e.g., IdP session time-outs once every 2-3 days instead of 8 hours in healthcare/emergency response)	SP 800-63 Digital Identity Guidelines (National Institute of Standards and Technology (NIST), n.d.) • Guidance - Role-specific Cybersecurity Training (Haney et al., 2023) • Guidance - Cybersecurity Workforce Training Guide (US CISA, 2021)
PR.AT - The organization's personnel are provided cybersecurity awareness and training so they can perform their cybersecurity-related tasks				
Role-specific Cybersecurity Training	• Training often being too generic, outdated, long, or repetitive, failing to address role-	Medium - Training widely prioritized and	• Targeted role-specific and risk-based training, with real world examples	• Guidance - Role-specific Cybersecurity

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale²	Recommendations & Considerations	Informative References
	specific needs • Lack of dedicated time to complete training • Training programs lagging behind the pace of evolving threats • Training fatigue	offered, though recurring issues persist, as outlined in <i>Chapter 4</i> .	• Just-in-time and consequence-based training • Organizational leadership allowing dedicated time to complete training • Referring to effective external sources for training (e.g., SANS Institute), as needed • Switching to shorter-format training (e.g., bite-size videos), where applicable	Training (Haney et al., 2023) • Research Article - Training Guidance (Haney & Lutters, 2020) • Guidance - SANS Cybersecurity Courses and Certifications (SANS Cybersecurity Courses, n.d.)
PR.DS - Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information				
Microsoft Defender , Microsoft Purview , Proofpoint , Prisma Cloud , Qualys , Tenable , Palo Alto Cybersecurity	• Workflow inefficiencies (e.g., lack of ability to customize out-of-the-box policies in Microsoft Purview) • Cybersecurity tools & platforms sprawl; multiple tools with overlapping capabilities • Frequent UI changes - change fatigue (e.g., Microsoft Defender)	High - Multiple strong recurring UX identified by participants (see <i>Chapter 4</i>).	• Workflow-aware designs with customizable out-of-the-box policies, etc. that reduce cognitive load and repetitive manual tasks • Cybersecurity tools & platforms portfolio rationalization, where feasible • Maintain internal documentation (e.g., onboarding notes, playbooks,	• Guidance - Portfolio Rationalization (US Chief Information Officers (CIO) Council, n.d.) • Guidance - Microsoft Secure by Design UX Toolkit (Roehl, 2025)

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
Policies & Standards			etc.) for major UI changes, and push vendors for stable UI rollouts, where possible	
PR.PS - The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability				
Splunk, Microsoft Sentinel, Microsoft Defender, CrowdStrike, Wiz, Palo Alto, ServiceNow	• Integration and interoperability challenges between multiple tools & platforms (e.g., Splunk and ServiceNow) • Frequent UI changes - change fatigue (e.g., Microsoft Defender) • Tools & Platforms are hard or unintuitive for non-experts (e.g., CrowdStrike), steep learning curves • Cybersecurity tools & platforms sprawl; multiple tools with overlapping capabilities • Workflow inefficiencies (e.g., switching back-and-forth between Microsoft Defender and Sentinel, lack of state persistence - saved filters, search queries, user preferences, etc.)	High - Multiple strong recurring UX identified by participants (see <i>Chapter 4</i>).	• Stronger cross-tool pipelines from vendors through increased data-sharing, consistent formats/standards, etc. • Maintain internal documentation (e.g., onboarding notes, playbooks, etc.) for major UI changes, and push vendors for stable UI rollouts, where possible • Support from organizations for role-specific training for risk/scanning tools in the form of allowing dedicated time and resources for training • Cybersecurity tools & platforms portfolio rationalization, where feasible • Stronger cross-tool pipelines from vendors through	• Guidance - Portfolio Rationalization (US Chief Information Officers (CIO) Council, n.d.) • Research Article - Training Guidance (Haney & Lutters, 2020) • Guidance - Microsoft Secure by Design UX Toolkit (Roehl, 2025)

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
			increased data-sharing, consistent formats/standards, etc. • Workflow-aware designs with saved filters, search queries, user preferences, auto-hyperlinking indicators, etc. that support easy navigation and reduce cognitive load and repetitive manual tasks	
PR.IR - Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience				
ServiceNow, Microsoft Sentinel, Palo Alto Cybersecurity Policies & Standards	- Tools & Platforms are hard or unintuitive for non-experts (e.g., Palo Alto), steep learning curves - Misalignment between policies & standards and operational tools (e.g., risk & control libraries, enterprise risk management processes)	Medium - Recurring UX issues identified (see <i>Chapter 4</i>). However, some UX issues impact beginners or non-experts more than experienced professionals.	- Support from organizations for role-specific training for risk/scanning tools and processes in the form of allowing dedicated time and resources for training - Tracking legal/regulatory updates and aligning policies & standards update cycles to match	- Research Article - Training Guidance (Haney & Lutters, 2020) - Blog - Tracking Regulatory Changes (Barona, 2025; Couto, 2025; Kappel, 2025)
DE.CM - Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events				
Splunk, CrowdStrike, Microsoft	Workflow inefficiencies (e.g., switching back-and-forth between Microsoft Defender and	High - Multiple strong recurring UX issues	Increased integration and interoperability support from vendors, and internal	Guidance - Security by Default and Design

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
Sentinel, Wiz, Palo Alto Prisma Cloud, Defender for Endpoint Role-specific Cybersecurity Training	Sentinel, lack of state persistence - saved filters, search queries, user preferences, etc.) • Integration and interoperability challenges between multiple tools & platforms (e.g., Splunk and ServiceNow) • Overwhelming dashboards	identified by participants (see <i>Chapter 4</i>).	documentation of workarounds where applicable (say through playbooks) • Stronger cross-tool pipelines from vendors through increased data-sharing, consistent formats/standards, etc. • Workflow-aware designs with saved filters, search queries, user preferences, auto-hyperlinking indicators, etc. that support easy navigation and reduce cognitive load and repetitive manual tasks • Improve dashboards' visibility - make it clear, simple, and customizable based on practitioner's role	Approach (US CISA, 2023) • Guidance - Microsoft Secure by Design UX Toolkit (Roehl, 2025) • Guidance - Dashboard Design Guidelines (Laubheimer, 2017)
DE.AE - Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents				
Splunk, Microsoft Sentinel, Wiz, CrowdStrike	• Workflow inefficiencies (e.g., switching back-and-forth between Microsoft Defender and Sentinel, lack of state persistence	Medium - Recurring UX issues identified by participants (see <i>Chapter 4</i>).	• Stronger cross-tool pipelines from vendors through increased data-sharing, consistent formats/standards, etc.	• Guidance - Security by Default and Design Approach (US CISA, 2023)

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
Role-specific Cybersecurity Training	- saved filters, search queries, user preferences, etc.)		Workflow-aware designs with saved filters, search queries, user preferences, auto-hyperlinking indicators, etc. that support easy navigation and reduce cognitive load and repetitive manual tasks	Guidance - Microsoft Secure by Design UX Toolkit (Roehl, 2025)
RS.MA - Responses to detected cybersecurity incidents are managed				
ServiceNow, Microsoft Teams / alt. collaboration tools Cybersecurity Policies & Standards	N/A - no specific UX-related issues identified for this Category. Please refer to other Categories for Cybersecurity Policies & Standards' and Training-related UX issues	N/A - no consistent reported UX issues; adjacent issues mapped under other CSF categories.	N/A	N/A
RS.AN - Investigations are conducted to ensure effective response and support forensics and recovery activities				
Kali Linux, BurpSuite Pro, Splunk, Sentinel, CrowdStrike, VirusTotal Role-specific Cybersecurity Training	- Alert fatigue, false positives, and noisy data (e.g., VirusTotal) - Overwhelming dashboards	Medium - Recurring UX issues identified by participants (see <i>Chapter 4</i>).	- Development of internal documentation of solutions and workarounds to common errors and issues, as applicable (e.g., through playbooks) - Improve dashboards' visibility - make it clear, simple, and customizable based on practitioner's role	- Research Article - Alert Fatigue (Tariq et al., 2025) - Guidance - Dashboard Design Guidelines (Laubheimer, 2017)

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale²	Recommendations & Considerations	Informative References
RS.CO - Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies				
ServiceNow, Microsoft Teams / alt. collaboration tools) Cybersecurity Policies & Standards	• N/A - no specific UX-related issues identified for this Category. Please refer to other Categories for Cybersecurity Policies & Standards' and Training-related UX issues	N/A - no consistent reported UX issues; adjacent issues mapped under other CSF categories.	• N/A	• N/A
RS.MI - Activities are performed to prevent expansion of an event and mitigate its effects				
ServiceNow, Splunk, Microsoft Defender, Palo Alto, CrowdStrike Role-specific Cybersecurity Training	• Frequent UI changes - change fatigue (e.g., Microsoft Defender) • Tools & Platforms are hard or unintuitive for non-experts (e.g., CrowdStrike), steep learning curves • Cybersecurity tools & platforms sprawl; multiple tools with overlapping capabilities	High - Multiple strong recurring UX issues identified by participants (see <i>Chapter 4</i>).	• Maintain internal documentation (e.g., onboarding notes, playbooks, etc.) for major UI changes, and push vendors for stable UI rollouts, where possible • Support from organizations for role-specific training for risk/scanning tools in the form of allowing dedicated time and resources for training • Cybersecurity tools & platforms portfolio rationalization, where feasible	• Guidance - Portfolio Rationalization (US Chief Information Officers (CIO) Council, n.d.) • Guidance - Cybersecurity Workforce Training Guide (US CISA, 2021)
RC.RP - Restoration activities are performed to ensure operational availability of systems and services affected by				

Table 5.1. Continued

NIST CSF Core Category - NIST CSF Core Outcome				
Relevant Artifacts ¹	Issues - from Data Analysis (Summarized from <i>Chapter 4</i>)	Priority & Rationale ²	Recommendations & Considerations	Informative References
cybersecurity incidents				
Cybersecurity Policies & Standards Role-specific Cybersecurity Training	• N/A - no specific UX-related issues identified for this Category. Please refer to other Categories for Cybersecurity Policies & Standards' and Training-related UX issues	N/A - no consistent reported UX issues; adjacent issues mapped under other CSF categories.	• N/A	• N/A
RC.CO - Restoration activities are coordinated with internal and external parties				
Cybersecurity Policies & Standards	• N/A - no specific UX-related issues identified for this Category. Please refer to other Categories for Cybersecurity Policies & Standards UX issues	N/A - no consistent reported UX issues; adjacent issues mapped under other CSF categories.	• N/A	• N/A
¹ Cybersecurity tools & platforms listed here are cited by multiple survey participants among their top two (2) most used in their work (see Table 4.2); provided for reference, not a comprehensive list. Font colors - blue, purple, and green are used to indicate relevant artifacts corresponding to the three (3) themes from the thematic analysis: Tools & Platforms, Policies & Standards, and (Role-specific) Training & Awareness respectively (see Figure 4.1). ² Specific font colors - yellow, orange, and red denote priority levels: low, medium, and high, respectively Gray font color is used across all columns to indicate Not Applicable (N/A).				

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

Overview

This dissertation set out to develop a NIST Cybersecurity Framework (CSF)-based Usable Security Community Profile; that is, domain-specific implementation guidance tailored to the practical realities of cybersecurity professionals in the United States. Drawing on a mixed-methods study involving 110 survey respondents and follow-up interviews with 26 practitioners, the research explored how User Experience (UX) challenges manifest across three (3) thematic areas within organizations: cybersecurity tools and platforms, policies and standards, and role-based training initiatives (please refer to *Chapter 4*). Using thematic analysis (Braun & Clarke, 2006; Goyanes et al., 2025) of the survey and interview data, combined with the researcher's interpretation, triangulation, and feedback from four (4) cybersecurity experts (please refer to *Chapter 3*), a NIST CSF-based Usable Security Community Profile was developed following available templates and guidance (National Institute of Standards and Technology, 2024; Pascoe et al., 2024; Rajarathnam & Singh, 2023), as presented in *Chapter 5*. The resulting Profile consolidates recurring issues, data-driven recommendations, and informative references from both scholarly and industry sources, with the overarching goal of improving the usability and user experience of cybersecurity tools and platforms, policies and standards, and training initiatives. This chapter discusses how organizations can apply the Community Profile, and concludes by outlining the study's theoretical,

methodological, and practical contributions, as well as its limitations and directions for future research.

Applying the Usable Security Community Profile

Organizations can apply the NIST CSF-based Usable Security Community Profile developed in *Chapter 5* as a foundational reference point, or baseline Profile, for enhancing the usability and UX of their cybersecurity programs. The Community Profile provides a structured, data-driven framework that organizations can adapt and refine to reflect their unique missions, regulatory requirements, technology stacks, and cybersecurity professionals' needs.

In practice, an organization may begin by mapping its current cybersecurity practices against the outcomes, issues, and recommendations outlined in the Community Profile. This exercise can reveal where existing policies, tools, or training programs align with usable security principles, and where barriers persist. The organization can then use this analysis to develop an Organizational Profile, a customized implementation roadmap that tailors the Community Profile's guidance to its specific context, priorities, and risk environment.

Over time, organizations can also establish baseline usability measures, such as workflow efficiency, task success rates, or user-reported satisfaction, to monitor progress as they implement recommendations and guidance provided from the Usable Security

Community Profile. Through iterative updates, feedback loops, and benchmarking across peer organizations, the Community Profile can serve not only as a starting point for adoption, but also as a living framework for promoting more human-centered cybersecurity practices across the sector.

Contributions of the Study

This PhD dissertation makes contributions at the theoretical, methodological, and practical levels, advancing the understanding of usable security within real-world organizational settings, aligned with the NIST CSF and demonstrating how user-centered considerations can be systematically incorporated into cybersecurity governance and practice.

Theoretical Contributions

This study advances scholarship at the intersection of cybersecurity and user experience (UX) by addressing a clear gap in the published literature: the lack of discussions on widely adopted standards or frameworks for usable security, especially in organizational settings (Di Nocera et al., 2023; Rajarathnam & Singh, 2024). By situating usable security within the structure of a NIST CSF-based Community Profile, this dissertation directly responds to that gap.

It also represents one of the earliest efforts to apply the Community Profile templates and guidance introduced in the latest iteration of the NIST CSF v2.0 (National

Institute of Standards and Technology, 2024a, 2024b; Pascoe et al., 2024). Whereas most existing profiles have been developed by practitioners for sector-specific contexts and uses cases such as manufacturing, election infrastructure, ransomware mitigation, and so forth (NIST, 2021; Rajarathnam & Singh, 2023) based on the 2018 version (v1.1), this dissertation provides an early scholarly application of the 2024 version (v2.0), extending its use to the domain of usable security.

Methodological Contributions

This research combines surveys, follow-up interviews, and expert reviews with cybersecurity professionals to inform the design of a NIST CSF-based Community Profile. By incorporating UX-oriented issues into the Profile structure, the study demonstrates how user-centered considerations can be systematically integrated into a standards-based framework.

A further methodological contribution lies in the comprehensive documentation of the process. This dissertation provides detailed descriptions of the steps taken, the rationale for methodological decisions (see *Chapter 3*), the study instruments (**Appendices A - D**), generalizable template (**Appendix E**) (Rajarathnam & Singh, 2023), pilot phase (**Appendix F**) (Rajarathnam & Singh, 2024), and codebook (**Appendix G**). This level of transparency enables other researchers to replicate or adapt the approach in future studies. Such documentation is uncommon, as most existing Community Profiles have been developed by practitioners with comparatively little

methodological detail (National Institute of Standards and Technology (NIST), 2021; Rajarathnam & Singh, 2023). By presenting the design process in a scholarly format, this dissertation establishes a reference point for future researchers seeking to apply and develop NIST CSF-based Community Profiles in other fields.

Practical Contributions

Finally, this study contributes a practitioner-facing Community Profile that organizations can adapt to improve the usability and UX of their cybersecurity tools & platforms, policies & standards, and role-specific training initiatives. The Profile provides data-driven recommendations supported by scholarly and professional informative references, offering cybersecurity professionals in organizational settings actionable guidance in several areas, including but not restricted to the following:

- Incorporating UX considerations into procurement criteria for cybersecurity tools & platforms
- Addressing common usability & UX issues with widely used cybersecurity tools & platforms.
- Improving the accessibility and understandability of organizational cybersecurity policies & standards
- Ensuring that cybersecurity training & awareness programs are role-specific, targeted, and easy to engage with.

These practical contributions deliver a resource that organizations can use to improve the everyday experience of cybersecurity practitioners while aligning with the structure of the NIST CSF.

Limitations and Future Directions

This section outlines the key limitations of the study and identifies potential directions for future research that build on its findings.

Limitations

This study has a few limitations that define the scope and boundaries of its findings. First, the research was conducted within a US-based organizational context, drawing on the perspectives of cybersecurity professionals working in US organizations. As such, the findings may not fully generalize to international contexts, where regulatory, cultural, and operational considerations (e.g., ISO/IEC 27001 adoption, GDPR applicability, and so forth) may differ. Cross-country comparisons were outside the scope of this dissertation, but future research may extend this work by examining how usable security considerations manifest in international settings.

Second, the study faced sampling constraints. Participation was voluntary, and the resulting dataset was more qualitative than quantitative. While this design was advantageous for producing detailed insights through thematic analysis and descriptive statistics, it limited the ability to conduct inferential statistical analyses. Informal

discussions with some participants suggested that reluctance to disclose organizational practices, particularly regarding specific cybersecurity tools and platforms, may have contributed to this limitation, despite clear assurances of anonymization in the informed consent process.

Third, qualitative coding was conducted by a single coder using a thematic analysis approach (Braun & Clarke, 2006), based on a published AI-assisted protocol (Goyanes et al., 2025). While this approach enhanced transparency, efficiency, and traceability of coding decisions, the reliance on a single coder may still introduce interpretive bias. This limitation was mitigated through iterative discussions of the codebook and emergent themes with the dissertation committee, composed of multiple researchers with extensive expertise in qualitative research methodologies, ensuring analytical rigor and consistency.

Finally, the study relied on self-reported practitioner data. Such perspectives are essential for capturing lived experiences and UX challenges, but they may also reflect subjective interpretations, recall bias, or organizational culture. Observational studies or system-level measures of usability were beyond the scope of this dissertation but represent valuable avenues for future work.

Future Research Directions

Next steps include sharing the NIST CSF-based Usable Security Community Profile with NIST to contribute to their growing library of Community Profiles and demonstrate how usability and UX considerations can be operationalized within the context of the NIST CSF. This would also help validate the Profile's applicability and relevance for broader dissemination across US organizations.

Future research could involve conducting case studies with organizations that seek to apply the NIST CSF-based Usable Security Community Profile, adapting it to their unique operational needs and security environments. Such studies would offer valuable insights into how the Profile can be tailored, implemented, and evaluated in real-world organizational contexts, revealing both its practical strengths and areas for improvement. Building on this line of inquiry, future work could also explore longitudinal studies that evaluate how the adoption of Profile-driven recommendations influences usability and UX outcomes over time. These studies can measure changes in practitioner satisfaction, workflow efficiency, and error rates before and after implementation, providing insights and evidence of long-term impact.

Additionally, incorporating quantitative usability metrics, such as task success rates, error frequencies, and time-on-task, alongside practitioner-reported qualitative data would provide a richer, multidimensional understanding of usable security challenges and improvements.

Together, these extensions would strengthen the evidence base for usable security and further enhance the practical value of NIST CSF-based Community Profiles in guiding organizations toward more human-centered cybersecurity practices.

REFERENCES

- Aljedaani, B., Ahmad, A., Zahedi, M., & Ali Babar, M. (2021). Security Awareness of End-Users of Mobile Health Applications: An Empirical Study. *MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 125–136. <https://doi.org/10.1145/3448891.3448952>
- Alshamsi, A., & Andras, Prof. P. (2019). User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies*, 126, 94–110. <https://doi.org/10.1016/j.ijhcs.2019.02.004>
- Assistant Secretary for Public Affairs. (2013, June 9). *Glossary | Usability.gov*. Department of Health and Human Services. <https://www.usability.gov/what-and-why/glossary/u/index.html>
- Babbie, E. R. (2020). *The Practice of Social Research* (15th ed.). Cengage. <https://www.cengage.com/c/the-practice-of-social-research-15e-babbie/9780357360767/>
- Barona, K. (2025, May 1). *5 Steps for Monitoring Regulatory Changes | Cycore*. <https://cycoresecure.com/blogs/5-steps-for-monitoring-regulatory-changes>
- Bevan, N. (2009). *What is the difference between the purpose of usability and user experience evaluation methods*. <https://www.semanticscholar.org/paper/What-is-the-difference-between-the-purpose-of-and-Bevan/cba74036995821ca560d31bf397c695a460a63a5>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>

- Clarivate. (n.d.). Web of Science Core Collection. *Clarivate*. Retrieved January 31, 2024, from <https://clarivate.com/products/scientific-and-academic-research/research-discovery-and-workflow-solutions/webofscience-platform/web-of-science-core-collection/>
- Couto, E. D. (2025, January 7). Regulatory Compliance: How to Monitor Changes Effectively in 2025. *Visualping*. <https://visualping.io/blog/regulatory-compliance-monitoring>
- Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th edition). SAGE Publications, Inc. <https://study.sagepub.com/creswellrd4e>
- Cybersecurity and Infrastructure Security Agency (CISA). (2021, February 1). *What is Cybersecurity?* | CISA. <https://www.cisa.gov/news-events/news/what-cybersecurity>
- Cybersecurity Risk Foundation. (2025). *CRF Governance and Risk Model v2025*. <https://crfsecure.org/research/crf-governance-and-risk-model/>
- Dhakal, K. (2022). NVivo. *Journal of the Medical Library Association : JMLA*, 110(2), 270–272. <https://doi.org/10.5195/jmla.2022.1271>
- Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. *Information*, 14(12), Article 12. <https://doi.org/10.3390/info14120641>
- Distler, V., Fassel, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L. F., & Koenig, V. (2021). A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Transactions on Computer-Human Interaction*, 28(6), 43:1-43:50. <https://doi.org/10.1145/3469845>

- Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs-principles and practices. *Health Services Research*, 48(6 Pt 2), 2134–2156. <https://doi.org/10.1111/1475-6773.12117>
- Fowler, F. J. (2013). *Survey Research Methods* (5th ed.). SAGE Publications, Inc.
- Garfinkel, S., & Lipford, H. R. (2014). *Usable Security: History, Themes, and Challenges*. Morgan & Claypool Publishers.
- Goyanes, M., Lopezosa, C., & Jordá, B. (2025). Thematic analysis of interview data with ChatGPT: Designing and testing a reliable research protocol for qualitative research. *Quality & Quantity*. <https://doi.org/10.1007/s11135-025-02199-3>
- Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, 4, 583723. <https://doi.org/10.3389/fdata.2021.583723>
- Haney, J., Jacobs, J., & Furman, S. (2023). *Federal cybersecurity role-based training approaches, successes, and challenges* (No. NIST SP 1288; p. NIST SP 1288). National Institute of Standards and Technology (U.S.). <https://doi.org/10.6028/NIST.SP.1288>
- Haney, J., & Lutters, W. (2020). Security Awareness Training for the Workforce: Moving Beyond “Check-the-Box” Compliance. *Computer*, 53(10), 10.1109/mc.2020.3001959. <https://doi.org/10.1109/mc.2020.3001959>
- Haney, J. M., Theofanos, M., Acar, Y., & Prettyman, S. S. (2018). “We make it a big deal in the company”: Security Mindsets in Organizations that Develop Cryptographic Products. 357–373. <https://www.usenix.org/conference/soups2018/presentation/haney-mindsets>

- Kappel, R. (2025, June 22). Best 12 Regulatory Change Management Software of 2025. *Centraleyes*. <https://www.centraleyes.com/best-regulatory-change-management-software/>
- Kelly, B., Margolis, M., McCormack, L., LeBaron, P. A., & Chowdhury, D. (2017). What Affects People's Willingness to Participate in Qualitative Research? An Experimental Comparison of Five Incentives. *Field Methods*, 29(4), 333–350. <https://doi.org/10.1177/1525822X17698958>
- Khodadadi, T., Javadianasl, Y., Rabiei, F., Alizadeh, M., Zamani, M., & Chaeikar, S. S. (2021). A Novel Graphical Password Authentication Scheme with Improved Usability. *2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 01–04. <https://doi.org/10.1109/ISAECT53699.2021.9668599>
- Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from “Shadow Security:” Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. *Proceedings 2014 Workshop on Usable Security*. Workshop on Usable Security, San Diego, CA. <https://doi.org/10.14722/usec.2014.23007>
- Kuusisto, A., Saranto, K., Korhonen, P., & Haavisto, E. (2023). Quality of information transferred to palliative care. *Journal of Clinical Nursing*, 32(13–14), 3421–3433. <https://doi.org/10.1111/jocn.16453>
- Laubheimer, P. (2017, June). *Dashboards: Making Charts and Graphs Easier to Understand*. Nielsen Norman Group. <https://www.nngroup.com/articles/dashboards-preattentive/>
- Lennartsson, M., Kävrestad, J., & Nohlberg, M. (2021). Exploring the meaning of usable security – a literature review. *Information & Computer Security*, 29(4), 647–663. <https://doi.org/10.1108/ICS-10-2020-0167>

- Lim, H. W., Poh, G. S., Xu, J., & Chittawar, V. (2020). \mathsf{PrivateLink}: Privacy-Preserving Integration and Sharing of Datasets. *IEEE Transactions on Information Forensics and Security*, 15, 564–577. IEEE Transactions on Information Forensics and Security. <https://doi.org/10.1109/TIFS.2019.2924201>
- Lumivero. (n.d.). *NVivo*. Lumivero. Retrieved June 18, 2024, from <https://lumivero.com/products/nvivo/>
- Mathis, F. (2021). [DC] VirSec: Virtual Reality as Cost-Effective Test Bed for Usability and Security Evaluations. *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 705–706. <https://doi.org/10.1109/VRW52623.2021.00235>
- National Center for Science and Engineering Statistics. (2024). *Cybersecurity Workforce Supply and Demand Report*.
- National Institute of Standards and Technology (NIST). (n.d.). *NIST SP 800-63 Digital Identity Guidelines*. Retrieved September 26, 2025, from <https://pages.nist.gov/800-63-4/>
- National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.04162018>
- National Institute of Standards and Technology (NIST). (2021, May 14). *Examples of Framework Profiles*. NIST. <https://www.nist.gov/cyberframework/csf-11-archive/community-profiles>

- National Institute of Standards and Technology (NIST). (2024a). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.
<https://doi.org/10.6028/nist.cswp.29>
- National Institute of Standards and Technology (NIST). (2024b, February 20). *CSF 2.0 Profiles*. NIST. <https://www.nist.gov/cyberframework/profiles>
- Nielsen, J. (2012, January 3). *Usability 101: Introduction to Usability*. Nielsen Norman Group (NN/g). <https://www.nngroup.com/articles/usability-101-introduction-to-usability/>
- Nightingale, A. (2009). A guide to systematic literature reviews. *Surgery (Oxford)*, 27(9), 381–384. <https://doi.org/10.1016/j.mpsur.2009.07.005>
- NIST National Cybersecurity Center for Excellence (NCCoE). (n.d.). *Examples of Community Profiles | NCCoE*. Retrieved July 15, 2025, from <https://www.nccoe.nist.gov/examples-community-profiles>
- Nwokedi, U. O., Onyimbo, B. A., & Rad, B. B. (n.d.). Usability and Security in User Interface Design: A Systematic Literature Review. *International Journal of Information Technology and Computer Science*, 8(5), 72.
- OIT UTK. (n.d.). *Web Surveys | Office of Innovative Technologies*. Retrieved September 27, 2024, from <https://oit.utk.edu/research/websurveys/>
- 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., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>

- Pascoe, C., Nethery Snyder, J., & Scarfone, K. (2024). *A Guide to Creating CSF 2.0 Community Profiles*. National Institute of Standards and Technology.
<https://doi.org/10.6028/nist.cswp.32.ipd>
- PRISMA. (n.d.). *PRISMA 2020 flow diagram*. PRISMA Statement. Retrieved September 26, 2024, from <https://www.prisma-statement.org/prisma-2020-flow-diagram>
- Qualtrics Support. (n.d.). *Survey Methodology & Compliance Best Practices*. Retrieved June 12, 2024, from <https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/survey-methodology-compliance-best-practices/>
- Rajarathnam, S., & Singh, V. (2023, May). *Poster: A Template for developing NIST CSF Profiles* [Poster]. IEEE Symposium on Security and Privacy (S&P). https://sp2023.ieee-security.org/downloads/SP23-posters/sp23-posters-paper31-final_version_2_page_abstract.pdf
- Rajarathnam, S., & Singh, V. (2024). Systematic Literature Review of Cybersecurity and User Experience. *IEEE Cyber Awareness and Research Symposium (CARS)*, 1–9.
<https://doi.org/10.1109/CARS61786.2024.10778869>
- Rajarathnam, S., & Singh, V. (2025, Oct 27 - 30). Assessing the Cybersecurity User Experience (UX) in an Organizational Context [Paper presentation]. *IEEE Cyber Awareness and Research Symposium (CARS)*, Grand Forks, ND, USA
- Regmi, P. R., Waithaka, E., Paudyal, A., Simkhada, P., & van Teijlingen, E. (2016). Guide to the design and application of online questionnaire surveys. *Nepal Journal of Epidemiology*, 6(4), 640–644. <https://doi.org/10.3126/nje.v6i4.17258>

- Reuter, C., Iacono, L. L., & Benlian, A. (2022). A quarter century of usable security and privacy research: Transparency, tailorability, and the road ahead. *Behaviour & Information Technology*, 41(10), 2035–2048.
<https://doi.org/10.1080/0144929X.2022.2080908>
- Roehl, S. (2025, March 18). Secure by design: A UX toolkit. *Microsoft Design*.
<https://microsoft.design/articles/secure-by-design-a-ux-toolkit/>
- Rubin, H. J., & Rubin, I. S. (2011). *Qualitative Interviewing: The Art of Hearing Data* (3rd ed.). SAGE Publications, Inc. <https://us.sagepub.com/en-us/nam/qualitative-interviewing/book234196>
- Saari, T., Savolainen, K., Tyllinen, M., Viitanen, J., & Nieminen, M. (2024). Addressing Usability and Complexity in Procurement of IT Systems. *Journal of User Experience*, 20(1), 27–45.
- Sandelowski, M. (2000). Combining Qualitative and Quantitative Sampling, Data Collection, and Analysis Techniques in Mixed-Method Studies. *Research in Nursing & Health*, 23(3), 246–255. [https://doi.org/10.1002/1098-240X\(200006\)23:3%253C246::AID-NUR9%253E3.0.CO;2-H](https://doi.org/10.1002/1098-240X(200006)23:3%253C246::AID-NUR9%253E3.0.CO;2-H)
- Sanders, M., Walsh, K. P., & Wheeler, L. B. (2021). *Effective survey design for research: Asking the right questions to get the data you need*.
- SANS Institute. (n.d.-a). *Cybersecurity Policies and Standards*. SANS Institute. Retrieved October 21, 2025, from <https://www.sans.org/information-security-policy>
- SANS Institute. (n.d.-b). *SANS Cybersecurity Courses*. SANS Institute. Retrieved October 6, 2025, from <https://www.sans.org/cyber-security-courses>

- Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D., & Becker, C. (2019). “I don’t see why I would ever want to use it”: Analyzing the Usability of Popular Smartphone Password Managers. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 1937–1953.
<https://doi.org/10.1145/3319535.3354192>
- ServiceNow. (2021, January 15). *Cybersecurity: Same Threats, New Challenges*. Forbes.
<https://www.forbes.com/sites/servicenow/2021/01/15/cybersecurity-same-threats-new-challenges/>
- Sharma, R., Wazid, M., & Gope, P. (2021). A blockchain based secure communication framework for community interaction. *Journal of Information Security and Applications*, 58, 102790. <https://doi.org/10.1016/j.jisa.2021.102790>
- Silva, R., & Neiva, F. (2016). *Systematic Literature Review in Computer Science—A Practical Guide*. <https://doi.org/10.13140/RG.2.2.35453.87524>
- Sun, H.-M., Chen, S.-T., Yeh, J.-H., & Cheng, C.-Y. (2018). A Shoulder Surfing Resistant Graphical Authentication System. *IEEE Transactions on Dependable and Secure Computing*, 15(2), 180–193. *IEEE Transactions on Dependable and Secure Computing*.
<https://doi.org/10.1109/TDSC.2016.2539942>
- Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., Alamoodi, A. H., Kiah, M. L. M., Jumaah, F. M., & Alaa, M. (2019). Comprehensive review and analysis of anti-malware apps for smartphones. *Telecommunication Systems*, 72(2), 285–337. <https://doi.org/10.1007/s11235-019-00575-7>

- Tariq, S., Baruwat Chhetri, M., Nepal, S., & Paris, C. (2025). Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. *ACM Comput. Surv.*, 57(9), 224:1-224:38. <https://doi.org/10.1145/3723158>
- Tenable. (2016, March 29). *NIST Cybersecurity Framework Adoption Linked to Higher Security Confidence According to New Research from Tenable Network Security*. Tenable®. <https://www.tenable.com/press-releases/nist-cybersecurity-framework-adoption-linked-to-higher-security-confidence-according>
- Theofanos, M. (2020). Is Usable Security an Oxymoron? *Computer*, 53(2), 71–74. <https://doi.org/10.1109/mc.2019.2954075>
- Tracy, S. J. (2019). *Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact* (2nd ed.). John Wiley & Sons.
- US Chief Information Officers (CIO) Council. (n.d.). *The Application Rationalization Playbook*. <https://www.cio.gov/assets/files/Application-Rationalization-Playbook.pdf>
- US Cybersecurity & Infrastructure Security Agency (CISA). (2021). *Cybersecurity Workforce Training Guide*. <https://www.cisa.gov/resources-tools/resources/cybersecurity-workforce-training-guide>
- US Cybersecurity & Infrastructure Security Agency (CISA). (2023). *Shifting The Balance Of Cybersecurity Risk: Principles And Approaches For Secure By Design Software*. https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf
- US Cybersecurity & Infrastructure Security Agency (CISA). (2025, January 13). *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products* | CISA. <https://www.cisa.gov/resources->

tools/resources/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting

U.S. Department of Homeland Security (DHS). (2009). *A Roadmap for Cybersecurity Research*. https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf

U.S. General Services Administration (GSA). (2024, March 13). *Usability – Digital.gov*. Digital.Gov. <https://digital.gov/topics/usability/>

U.S. General Services Administration (GSA). (2025, September 23). *Plain Language Guide Series – Digital.gov*. <https://digital.gov/guides/plain-language>

UTK Graduate School. (n.d.). *Graduate School Deadlines*. The Graduate School. Retrieved September 25, 2025, from <https://gradschool.utk.edu/academics/graduation/graduation-deadlines/>

UTK IRB. (n.d.). *HRPP Forms and Templates*. Research Integrity & Assurance. Retrieved September 27, 2024, from <https://research.utk.edu/research-integrity/human-research-protection-program/for-researchers/hrpp-forms-and-templates/>

UTK Library. (n.d.). *A-Z Databases*. Retrieved May 14, 2024, from <https://libguides.utk.edu/az.php>

Wolf, F., Kuber, R., & Aviv, A. J. (2019). “Pretty Close to a Must-Have”: Balancing Usability Desire and Security Concern in Biometric Adoption. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–12. <https://doi.org/10.1145/3290605.3300381>

APPENDICES

APPENDIX A: INVITATION LETTER

IRB Application Details

IRB Application Number: UTK IRB-24-08536-XM

IRB Approval Date: January 15, 2025

Disclaimer

The following study invitation and follow-up email draft verbiage is based on templates provided by the UTK IRB (UTK IRB, n.d.). Please note that the actual emails sent to participants were adapted from the draft below to reflect the specific context, communication mode, the researcher's familiarity with the participants, etc.

Draft Initial Invitation Email

Dear [Prospective Participant's Name],

My name is Shreenandan Rajarathnam, a doctoral student in the School of Information Sciences, College of Communication & Information at the University of Tennessee, Knoxville. You may recall our previous interactions during [insert details of prior encounters, if applicable].

I am conducting a research study approved by the Institutional Review Board at the University of Tennessee, Knoxville (UTK). Your participation could greatly contribute to

our understanding of Cybersecurity User Experience (UX). Additionally, if you think any of your team members or colleagues would be interested in participating, please feel free to forward this email or share the survey link with them. Their input would be valuable as well.

Study Purpose: The purpose of this study is to develop a NIST CSF-based Community Profile for the Usable Security field based on understanding and assessing organizations' Cybersecurity User Experience (UX) in a real-world organizational setting and identify potential challenges to implementation.

Eligibility Criteria: You have experience with cybersecurity tools, infrastructure, and practices at your organization.

Time Commitment: If you agree to be in the study, your participation will last for less than three (3) hours over the course of seven (7) months (Nov 2024 – May 2025) and will involve one (1) online questionnaire of approximately 12 min, an optional online or in-person discussion lasting up to one (1) hour if you choose, and less than one (1) hour of follow-up communication as needed, preferably via email.

Location: Questionnaire will be conducted online via Qualtrics, Interview (as needed) will be conducted online or in-person, as you prefer. If online, it will be conducted via Zoom (or suitable alternate). If in-person, it will be conducted at a mutually convenient location.

As a participant, you will be asked to complete one (1) online survey questionnaire, with the option to participate in one (1) follow-up interview (online or in-person) if you choose, and any additional follow-up communication as needed. Your personal information will be kept anonymous. You will not be paid for participating in the survey. However, you will receive a \$50 gift card for participating in the follow-up interview, if selected and/or you opted to participate in it.

If you have questions or want to determine your eligibility, please contact me at srajarat@vols.utk.edu or <researcher's mobile number>. You may also reach out to my advisor, Professor Vandana Singh, at vandana@utk.edu or <researcher's mobile number>.

Being in this study is up to you. You can say no now or leave the study later. Either way, your decision won't affect your relationship with the researchers or the University of Tennessee.

Thank you for considering being a part of our study. Please feel free to reach out to me if you have any questions or concerns.

Best regards,

Shreenandan (Nanda)

--

Shreenandan Rajarathnam

Graduate Student (PhD) & Graduate Teaching Associate

Communication and Information | University of Tennessee, Knoxville (UTK)

Email: srajarat@vols.utk.edu

Mobile: <researcher's mobile number>

Draft Follow-up Email

Dear [Prospective Participant's Name],

Once again, thank you so much for your participation in our study regarding Cybersecurity User Experience (UX). As part of the study procedures, I am reaching out to request clarification and/or additional context regarding your [survey/interview] responses to ensure the accuracy and completeness of the data collected.

Specifically, I would like to ask about the following: [Insert specific question(s) or topic(s) requiring clarification or additional context] Your input is greatly appreciated and will help refine the study findings. Please feel free to reply to this email at your earliest convenience. If you have any questions or need further clarification regarding this request, do not hesitate to reach out.

Thank you for your time and valuable contributions to this study.

Best regards,

Shreenandan (Nanda)

--

Shreenandan Rajarathnam

Graduate Student (PhD) & Graduate Teaching Associate

Communication and Information | University of Tennessee, Knoxville (UTK)

Email: srajarat@vols.utk.edu

Mobile: <researcher's mobile number>

APPENDIX B: DRAFT SURVEY INSTRUMENT

IRB Application Details

IRB Application Number: UTK IRB-24-08536-XM

IRB Approval Date: January 15, 2025

Disclaimer

The survey was distributed via Qualtrics and included conditional logic, that is, not all questions were shown to every participant. Some follow-up questions were automatically skipped depending on how participants responded to previous items.

Default Question Block (in Qualtrics)

Q1.

Organizational Cybersecurity UX

This survey request is to research Cybersecurity User Experience (UX) in a real-world organizational setting. As part of this research, you will be asked to respond to up to 32 survey questions. Please be assured that your responses will be kept confidential.

The study should take you approximately less than 12 min to complete, and you will not be paid for completing this survey. Your participation in this research is voluntary. You have the right to withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Principal Investigator in the study to discuss this research, please email Dr. Vandana Singh at vandana@utk.edu, or Shreenandan Rajarathnam at srajarat@vols.utk.edu.

By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

Please note that this survey will be best displayed on a laptop or desktop computer. Some features may be less compatible for use on a mobile device.

- ☐ I consent, begin the study
- ☐ I do not consent, I do not wish to participate

Demographics Info Block (in Qualtrics)

Q2. What is your gender identity?

- ☐ Male
- ☐ Female
- ☐ Non-binary / third gender
- ☐ Prefer not to say

Q3. Choose one or more race(s) that you consider yourself to be:

- ☐ White
- ☐ Black or African American
- ☐ American Indian or Alaska Native

- ☐ Asian
- ☐ Native Hawaiian or Pacific Islander
- ☐ Other (please specify)

Q4. What is the highest level of education you have completed?

- ☐ Some high school or less
- ☐ High school diploma or GED
- ☐ Some college, but no degree
- ☐ Associates or technical degree
- ☐ Bachelor's degree
- ☐ Graduate or professional degree (MA, MS, MBA, PhD, JD, MD, DDS etc.)
- ☐ Prefer not to say

Q5. What best describes your employment status?

- ☐ Working full-time
- ☐ Working part-time

Roles & Responsibilities Block (in Qualtrics)

Q6. What is your current job title or role in the organization?

- ☐ Cybersecurity Professional
- ☐ IT Professional (Non-cybersecurity)
- ☐ Manager

- Executive
- Tech Support
- Other (please specify)

Q7. Are you involved in the cybersecurity tools & platforms procurement?

- Yes
- No
- Maybe

(The following question will be asked based on the answer to the question above)

Q8. What is your level of involvement in the cybersecurity tools & platforms procurement process?

- No involvement
- Minimal involvement (e.g. occasional feedback)
- Moderate involvement (e.g. participating in vendor evaluations)
- High involvement (e.g. leading the procurement process)
- Not sure / not applicable

Cybersecurity UX Part I (Tools & Platforms) Block (in Qualtrics)

Q9. Do you use any cybersecurity tools & platforms as part of your work? (e.g. Titus email classification, Microsoft Defender for Endpoint, etc.)

- Yes

- No
- Maybe

(The following questions 10 - 18 will be asked based on the answer to the question above)

Q10. What cybersecurity tools & platforms do you use as part of your work?

Q11. What is the most used cybersecurity tool/platform related to your work?

Q12. What is the frequency of usage for the most used cybersecurity tool/platform related to your work?

- Less than once a week
- Once a week
- 2 - 3 times a week
- 4 - 6 times a week
- Daily

Q13. What is the second most used cybersecurity tool/platform related to your work?

Q14. What is the frequency of usage for the second most used cybersecurity tool/platform related to your work?

- Less than once a week
- Once a week
- 2 - 3 times a week
- 4 - 6 times a week
- Daily

Q15. Are these cybersecurity tools & platforms usable? Select all aspects of Usability that apply

- ☐ Learnability: Easy to learn
- ☐ Efficiency: Efficient in performing the desired task
- ☐ Memorability: Able to remember enough to use it effectively after initial use
- ☐ Errors: Low frequency and severity of errors, as well as ease of recovery from them
- ☐ Satisfaction: Overall pleasantness of the design and user experience
- ☐ Not Usable (none of the above)

Q16. In terms of usability, how do the perceived benefits of the Cybersecurity tools or platforms you use most frequently compare to their actual benefits in practice?

- Aligned with actual benefits
- Somewhat aligned with actual benefits
- Not aligned at all
- N/A or unsure

Q17. Has your organization provided or mandated formal training on how to use the cybersecurity tools & platforms effectively?

- ☐ Yes
- ☐ No
- ☐ Maybe

Q18. Have you experienced any challenges in using these cybersecurity tools & platforms?

- ☐ Yes
- ☐ No
- ☐ Maybe

(The following question will be asked based on the answer to the question above)

Q19. Please describe the challenges you face(d)

Cybersecurity UX Part II (Policies & Standards) Block (in Qualtrics)

Q20. Does your organization have specific cybersecurity policies & standards?

- ☐ Yes
- ☐ No
- ☐ Maybe

(The following questions 21 - 24 will be asked based on the answer to the question above)

Q21. Are these cybersecurity policies & standards easily accessible?

- ☐ Yes
- ☐ No
- ☐ Maybe

Q22. Are these cybersecurity policies & standards understandable?

- ☐ Yes
- ☐ No
- ☐ Maybe

Q23. Have you received any training or guidance on these cybersecurity policies & standards from the organization?

- ☐ Yes
- ☐ No
- ☐ Maybe

Q24. Do you face any challenges in following or implementing these cybersecurity policies & standards?

- ☐ Yes

- No
- Maybe

(The following question will be asked based on the answer to the question above)

Q25. Please describe the challenges you face(d)

Cybersecurity UX Part III (People & Training) Block (in Qualtrics)

Q26. Do you believe that your organization prioritizes cybersecurity education, awareness, and training for its employees?

- Definitely not
- Probably not
- Might or might not
- Probably yes
- Definitely yes

Q27. Do you have role-specific cybersecurity education and training programs from the organization?

- Yes
- No
- Maybe

Q28. How often do you receive role-specific cybersecurity education and training from the organization?

- ☐ Never
- ☐ Less than once a year
- ☐ Once a year (annually)
- ☐ Twice a year (bi-annually)
- ☐ Three (3) to four (4) times a year
- ☐ More than four (4) times a year

Q29. Have you encountered any challenges specific to cybersecurity education, awareness, and training?

- ☐ Yes
- ☐ No
- ☐ Maybe

Q30. Please describe the challenges you face(d)

Interview Interest Block (in Qualtrics)

Q31. Do you wish to participate in a follow-up interview?

- ☐ Yes
- ☐ No
- ☐ Maybe

(The following question will be asked based on the answer to the question above)

Q32. Please provide your name & email ID so we can contact you

APPENDIX C: INFORMED CONSENT FORM

IRB Application Details

IRB Application Number: UTK IRB-24-08536-XM

IRB Approval Date: January 15, 2025

Disclaimer

The content below is based on the UTK IRB Informed Consent Form template (UTK IRB, n.d.). The final version provided to participants closely follows the format and structure of the referenced template, with minimal adjustments to suit the specific context, such as dates adjusted based on the IRB application approval.

Informed Consent Verbiage

Consent for Research Participation

Research Study Title: PhD Dissertation Project: Developing a NIST CSF-Based Usable Security Community Profile

Researcher(s): Dr. Vandana Singh, College of Emerging and Collaborative Studies, and School of Information Sciences, University of Tennessee, Knoxville
Shreenandan Rajarathnam, School of Information Sciences, University of Tennessee, Knoxville

Why am I being asked to be in this research study?

We are asking you to be in this research study because you have experience with cybersecurity tools, infrastructure, and practices, that we would like to study, specifically in the context of understanding the Cybersecurity User Experience (UX) in a real-world organizational setting. This interview is a follow-up to the previously completed survey questionnaire. The knowledge gained from these will help us provide recommendations to enhance the UX of cybersecurity tools, infrastructure, and practices, that will be a contribution to the field of Usable Security.

What is this research study about?

The purpose of the research study is assess the Cybersecurity UX of tools & platforms, policies & standards, and training initiatives in a real-world organizational setting and identify potential challenges to implementation. The findings from the study will be synthesized to develop generalizable recommendations for the field of Usable Security, and by extension the field of Cybersecurity, in the form of a National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)-based Community Profile for Usable Security.

How long will I be in the research study?

If you agree to be in the study, your participation will last for less than three (3) hours over the course of seven (7) months (Nov 2024 - May 2025) and will involve one (1) online / in-person discussion of approximately up to one (1) hour if you choose, and less than one (1) hour of follow-up communication as needed, preferably via email. This is in

addition to the one (1) online survey questionnaire of approximately 12 min that you have already completed.

What will happen if I say “Yes, I want to be in this research study”?

If you agree to be in this study, we will ask you to meet with us either online via Zoom (or suitable alternative) or in-person at a mutually convenient location for a discussion (individual or group), during fall 2024 (Oct - Dec 2024) and spring 2025 (Jan - May 2025). The discussion will be recorded (audio) for the purpose of logging the transcript of the discussion to help with the research, participant anonymity will be maintained through appropriate measures such as safe storage and obfuscation or redaction of personally identifiable information, as applicable. Video recording (if virtual meeting) is optional, and the video will be deleted after data analysis.

What happens if I say “No, I do not want to be in this research study”?

Being in this study is up to you. You can say no now or leave the study later. Either way, your decision won’t affect your relationship with the researchers or the University of Tennessee.

What happens if I say “Yes” but change my mind later?

Even if you decide to be in the study now, you can change your mind and stop at any time. If you decide to stop before the study is completed, you can let us know via email

or verbally on Zoom (or alternative) / phone call. We will exclude the transcript and video (as applicable) of our discussion from our study and will delete any copies.

Are there any possible risks to me?

We don't know of any more risks to you than experienced in everyday life, from being in this study.

Are there any benefits to being in this research study?

We do not expect you to benefit from being in this study. Your participation may help us to learn more about learn more about learn more about ways to improve the User Experience (UX) of Cybersecurity tools, infrastructure, and practices. We hope the knowledge gained from this study will benefit others in the future.

Who can see or use the information collected for this research study?

We will protect the confidentiality of your information by deleting the audio / video recording of our discussion from our laptops or external drive (if applicable) after August 2025. Documents such as the discussion transcript, consent form, and so forth will be stored in accordance with the University's secure data storage guidelines.

If information from this study is published or presented at scientific meetings, your name and other personal information will not be used.

We will make every effort to prevent anyone who is not on the research team from knowing that you gave us information or what information came from you. Although it is

unlikely, there are times when others may need to see the information we collect about you. These include:

- People at the University of Tennessee, Knoxville who oversee research to make sure it is conducted properly.
- Government agencies (such as the Office for Human Research Protections in the U.S. Department of Health and Human Services), and others responsible for watching over the safety, effectiveness, and conduct of the research.
- If a law or court requires us to share the information, we would have to follow that law or final court ruling.

What will happen to my information after this study is over?

We will/will not keep your information to use for future research on the topic of Cybersecurity UX. Your name and other information that can directly identify you will be deleted from your research data collected as part of the study.

We may share your research data with other researchers without asking for your consent again, but it will not contain information that could directly identify you.

Will I be paid for being in this research study?

If you participate in the interview portion of the study, you will be compensated with a \$50 gift card for a pre-selected vendor such as Amazon, Target, or equivalent, determined by the research team.

- Survey participation: Please note that participants who only completed the survey portion of the study will not receive any compensation.
- When and how payment will be issued: If you participate in the interview, the gift card will be provided to you electronically via email within two (2) months of completing the interview. If you do not have access to email, alternative arrangements for delivery can be made.
- To facilitate the distribution of the gift card, we will need your name and email address. We do not anticipate collecting any additional personal information for the purposes of compensation.

If you have any questions regarding compensation, feel free to ask the research team.

Will it cost me anything to be in this research study?

It will not cost you anything to be in this study.

What else do I need to know?

N/A

Who can answer my questions about this research study?

If you have questions or concerns about this study, or have experienced a research related problem or injury, contact the researchers, Dr. Vandana Singh (vandana@utk.edu or <researcher's mobile number>) or Shreenandan Rajarathnam (srajarat@vols.utk.edu, <researcher's mobile number>).

For questions or concerns about your rights or to speak with someone other than the research team about the study, please contact:

Institutional Review Board

The University of Tennessee, Knoxville

Phone: 865-974-7697

Email: utkirb@utk.edu

Statement of Consent

I have read this form, been given the chance to ask questions and have my questions answered. If I have more questions, I have been told who to contact. I understand that I am agreeing to be in this study. I can keep a copy of this consent information for future reference. If I do not want to be in this study, I do not need to do anything else.

Consent for use of images

I agree that photographs/video recordings of me from this research may be analyzed for research purposes.

APPENDIX D: DRAFT INTERVIEW QUESTIONS

IRB Application Details

IRB Application Number: UTK IRB-24-08536-XM

IRB Approval Date: January 15, 2025

Disclaimer

Please note that not all the questions mentioned below may apply to every participant, and their relevance may vary based on their survey responses. Additionally, follow-up interviews may include specific supplementary questions to further explore themes emerging from survey responses.

Opening statement example (after introductions)

Hello [participant's name], I'm Shreenandan Rajarathnam, the researcher from the survey on Cybersecurity UX in organizational setting that you participated earlier in [month & year of participation]. Thank you for your willingness to join a follow-up interview to explore your insights further. Please note that by continuing with this interview, you are verbally consenting to participate and have your responses recorded and used for research as outlined in the consent form.

Potential interview questions for the pilot study are as follows:

Roles & Responsibilities

1. Can you please explain your role in your (or your client) organization from a cybersecurity standpoint?
2. Could you describe the selection criteria used when procuring cybersecurity tools & platforms?
3. (Follow-up) Was UX one of the factors or criteria considered during the procurement process?

Cybersecurity UX Part I (Tools & Platforms)

4. Have you ever benchmarked the Usability / UX of your organization's cybersecurity tools & platforms against industry standards or best practices?
5. Have you ever received any complaints or feedback from your employees about the UX of your cybersecurity tools & platforms?
6. (Follow-up) Are you documenting these UX-related complaints and feedback?
7. (Follow-up) How are you addressing (or plan on addressing) these UX-related complaints and feedback?
8. At present, how do you balance the need for security with the need for Usability / UX?
9. Can you describe the challenges you or your team have experienced using these (from survey) cybersecurity tools & platforms?
10. (Follow-up) How do you work around these challenges?

Cybersecurity UX Part II (Policies & Standards)

11. Do you know where to find your organization's cybersecurity policies & standards?
12. What steps, if any, do you suggest to improve the understandability of the cybersecurity policies & standards?
13. Could you describe the challenges you've faced while trying to adhere to these cybersecurity policies & standards?
14. (Follow-up) Did you receive any guidance or suggestions to overcome these challenges you encountered while trying to adhere to these cybersecurity policies & standards?
15. (Follow-up) What kind of support do you think would help you better adhere to these cybersecurity policies & standards?

Cybersecurity UX Part III (People & Training)

16. Could you describe any role-specific cybersecurity training or education that you found particularly helpful or informative?
17. Are there any areas in which you believe you need additional cybersecurity education or training?
18. What kinds of role-specific cybersecurity education and training do you think would be most effective for employees?
19. Could you describe the challenges specific to cybersecurity education, awareness, and training?

20. (Follow-up) How are you (or plan on) addressing these challenges specific to cybersecurity education, awareness, and training?

Interest in Providing Feedback for the Usable Security Community Profile)

21. Based on the data collected from the surveys and interviews, we will develop a NIST CSF-based Community Profile tailored to the Usable Security field. Would you be interested in reviewing and providing feedback on our recommendations once the Profile is drafted?

APPENDIX E: NIST CSF (V1.1) PROFILE TEMPLATE

Overview

To understand the foundational structure of NIST CSF Community Profiles, originally referred to simply as Profiles under NIST CSF v1.1 (NIST, 2018), a research study was conducted to review and identify the common elements and key differences among the 14 published Profiles (NIST, 2021). The outcome of this study was a generalizable template that captures the recurring elements across the published examples, establishing a foundation for developing new NIST CSF Profiles in unaddressed domains or emerging sectors. This work constituted **Phase I (Template Development)** of the dissertation study and addressed **RQ1**: What are the standard elements of a NIST CSF Community Profile? The findings from this work were presented as a research poster at the 2023 IEEE Security & Privacy (S&P) Symposium (Rajarithnam & Singh, 2023).

Approach & Outcome

A document analysis was conducted on the 14 publicly available NIST CSF v1.1 Profiles (NIST, 2021). Each Profile was examined for the presence (denoted by “√”) or absence (denoted by “X”) of common elements, as summarized in **Table 6.1**. This analysis enabled the identification of required elements (included across multiple Profiles) and optional elements (present in at least one Profile). These recurring elements form the basis of a generalizable Profile template, depicted in **Figure 6.1**. These elements are summarized as follows:

- **Introduction and Context:** Provides background on the NIST CSF and introduces the specific domain, industry sector, or use case (e.g., manufacturing, election infrastructure, ransomware mitigation, etc.). It explains why a Profile is relevant to that sector and the context for applying the Framework.
- **General Tips:** Offers broad, actionable guidance on cybersecurity hygiene and risk mitigation practices, such as blocking access to untrusted resources or maintaining backups (for the Ransomware Mitigation Profile), tailored to the Profile’s scope.
- **Methodology/Development Approach:** Describes how the Profile was developed (e.g., stakeholder workshops, interviews, collaborative sessions). For example, the Election Infrastructure Profile used stakeholder workshops to identify and rank the top three (3) NIST CSF categories most critical to mission objectives.
- **Business / Mission Objectives:** Defines the strategic and operational goals relevant to the domain, such as “Maintain Human Safety” or “Maintain Production Goals”, and so forth. These objectives serve as the bridge between business priorities and cybersecurity activities.
- **NIST CSF Mapping:** Aligns the identified objectives to the NIST CSF Core functions, categories, and subcategories. This mapping helps organizations in the respective domain or industry sector visualize how their mission objectives relate to specific security activities and desired outcomes.

- **Implementation Measures and Prioritization:** Suggests specific actions, controls, or initiatives that organizations can undertake to enhance their cybersecurity posture. These measures can be prioritized based on risk level, resource availability, or strategic importance based on the business objectives.
- **Impact Tiers:** Some Profiles categorize activities or controls according to their expected impact or risk severity. Including Impact Tiers enables organizations to assign priority levels, such as High, Moderate, or Low Impact, facilitating tiered implementation strategies that reflect mission criticality and risk appetite.
- **References to Other Standards:** Incorporates mapping to other frameworks and best practices (e.g., COBIT 5, ISO/IEC 27001, NIST SP 800 series) to encourage interoperability and cross-framework alignment and serve as guidance and reference materials.

Study Significance

With the release of the next iteration of the NIST Cybersecurity Framework (CSF), namely the version 2.0 (NIST, 2024), NIST published its own generalizable Community Profile template (NIST, 2024) and accompanying guidance (Pascoe et al., 2024). Although the development of that template occurred independently of this study, its publication further reiterated the relevance and necessity of creating a standardized, generalizable approach for developing NIST CSF Profiles.

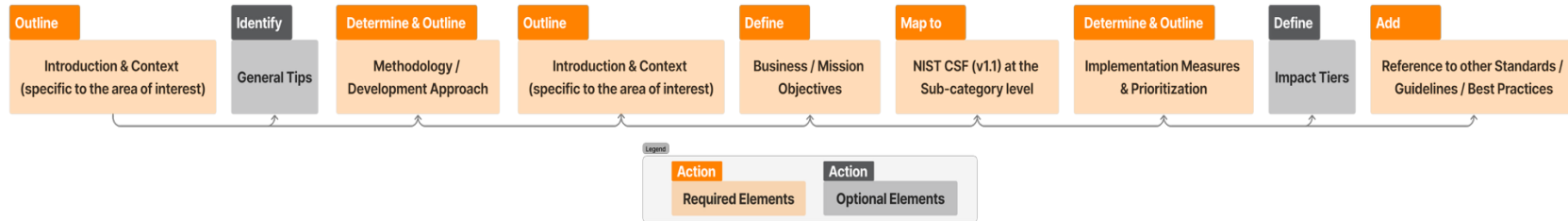
Table 6.1. Common elements included (“√”) or not included (“X”) in the published examples of NIST CSF v1.1 Profiles. Reproduced from Rajarathnam & Singh (2023), IEEE Security & Privacy Symposium Poster: “A Template for Developing NIST CSF Profiles”.

Document Name	Intro & Context	General Tips	Methodology ^a	Business Obj.	NIST Mapping	Impl. Measures	Impact Tiers	References ^b
NISTIR 8183 – Cybersecurity Framework Manufacturing Profile	N/A - redundant, updated version below (NISTIR 8183r1 – Cybersecurity Framework Version 1.1 Manufacturing Profile Rev. 1)							
NISTIR 8374 – Ransomware Risk Management: A Cybersecurity Framework Profile	√	X	X	X	√	X	X	√
NISTIR 8183r1 – Cybersecurity Framework Version 1.1 Manufacturing Profile Rev. 1	√	X	√	√	√	√	X	√
NISTIR 8310 (Draft) – Cybersecurity Framework Election Infrastructure Profile	√	X	√	√	√	√	X	√
NIST IR 8323 Revision 1 – Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of PNT Services	√	X	X	√	√	X	X	√
NIST TN 2051 – Cybersecurity Framework Smart Grid Profile	√	X	X	√	√	X	X	√
White Paper NIST CSWP 27 (Draft) Cybersecurity Profile for Hybrid Satellite Networks (HSN) Final Annotated Outline	N/A - obsolete (Draft), updated version (Final) is just an annotated outline / whitepaper providing an overview of the Profile that will be created							
How to Use the Cybersecurity Framework Profile for Connected	√	X	√	√	√	√	X	X

Table 6.1. Continued

Document Name	Intro & Context	General Tips	Methodology ^a	Business Obj.	NIST Mapping	Impl. Measures	Impact Tiers	References ^b
Vehicle Environments – U.S. Transportation								
Cybersecurity Framework Profile Excel for Connected Vehicle Environments – U.S. Transportation	N/A - Excel file containing the mapping for row above (How to Use the Cybersecurity Framework Profile for Connected Vehicle Environments – U.S. Transportation)							
Cybersecurity Framework Botnet Threat Mitigation Profile – Cybersecurity Coalition	✓	X	X	X	✓	✓	X	✓
Cybersecurity Framework DDoS Threat Mitigation Profile – Cybersecurity Coalition	✓	X	X	X	✓	✓	X	✓
The Profile – Cyber Risk Institute	✓	X	✓	✓	✓	✓	✓	✓
Framework Payroll Profile – IRS Security Summit	✓	X	X	X	X	X	X	✓
Cybersecurity Framework Profile: White House Fact Sheet – Seamless Transition	X	✓	X	X	✓	X	X	X

Figure 6.1. Proposed template for a Framework Profile based on NIST CSF v1.1, developed using common elements identified across published Framework Profile examples. Reproduced from Rajarathnam & Singh (2023), IEEE Security & Privacy Symposium Poster: “A Template for Developing NIST CSF Profiles”.



APPENDIX F: PILOT PHASE SUMMARY

Overview

This Appendix summarizes key takeaways from **Phase II (Pilot Study)** of this dissertation, which addressed Sub-RQs 2a and 2b (shown below) under **RQ2**: What are the UX challenges faced by Cybersecurity/IT teams in an organization? Findings from this phase have been accepted for presentation at the 2025 IEEE Cyber Awareness Research Symposium (Rajarathnam & Singh, 2025). The pilot study laid the foundation for the full dissertation by refining study instruments and documents based on practitioner feedback (**Appendices A - D**). These refined instruments were subsequently used for data collection in the broader study. The pilot study received Institutional Review Board (IRB) approval (ID: UTK IRB-23-07689-XM) and adhered to ethical standards including informed consent, confidentiality, and data de-identification.

Sub-RQ2a: What are the UX challenges faced by organizations when using their cybersecurity tools & platforms, policies & standards, and practices?

Sub-RQ2b: What are the potential challenges of implementing a framework for assessing Cybersecurity UX in an organizational setting?

Introduction and Context

Following the completion of the Systematic Literature Review (SLR) (please refer to *Chapter 2*) and formulation of the research questions (please refer to *Chapter 3*), a pilot study was conducted with 10 cybersecurity professionals from a local

organization. The purpose was to better understand the User Experience (UX) challenges practitioners encounter in relation to their organization's cybersecurity tools & platforms, policies & standards, and training initiatives. The pilot also explored potential challenges of implementing a framework for assessing cybersecurity UX in an organizational setting. Insights from this phase were instrumental in refining the study design, instruments, and analysis procedures for the broader dissertation research.

Pilot Study Methodology

This pilot study employed a mixed-methods explanatory sequential design (Creswell, 2014; Fetter et al., 2013; Sandelowski, 2000) to assess the feasibility of evaluating cybersecurity UX across tools & platforms, policies & standards, and training within organizational contexts. The pilot study began with an online survey capturing insights from professionals in diverse cybersecurity roles, followed by semi-structured interviews to further explore key issues identified from survey results. This sequential approach ensured that insights from the surveys informed the design of the follow-up interviews, an approach later applied in the main dissertation study (please refer to *Chapter 3*).

The Qualtrics-based survey included a mix of closed- and open-ended questions on participants' experiences with cybersecurity tools, policies, training, and associated UX challenges, along with demographic and role-specific information. The survey instrument consisted of up to 30 questions, later expanded to 32 for the broader study

(please refer to **Appendix B**). Participants were recruited through purposive and snowball sampling from a manufacturing-sector organization with more than 10000 employees, located within 250 miles of the authors' institution. Given the pilot nature of the study, a small but intentionally selected sample of 10 participants was used to ensure diverse representation across executive, managerial, and professional cybersecurity roles. This approach supported the testing of research design elements and refinement of instruments in preparation for a larger-scale implementation involving 100+ participants across multiple US organizations as part of this dissertation study.

Quantitative data were analyzed using descriptive statistics (frequencies, percentages, and means) and visualized with Microsoft Excel tools such as PivotTables, formulas, and charts. Qualitative responses from open-ended survey questions informed refinements to the interview protocol, which adopted a semi-structured, responsive format (Rubin & Rubin, 2011; Tracy, 2019) allowing flexibility in exploring practitioners' experiences.

The follow-up interview for the pilot phase was conducted in person at participants' workplace offices. Qualitative data collected was analyzed using thematic analysis (Braun & Clarke, 2006), facilitated by NVivo (Dhakal, 2022; Lumivvero, n.d.), to identify recurring UX-related patterns and themes. These findings were then compared with survey insights to strengthen interpretive depth and triangulation. The interview

protocol was updated based on practitioners' feedback for the broader dissertation study (please refer to **Appendix D**).

Results Summary

The key takeaways from the pilot study are summarized below. These findings provide an overview of how cybersecurity professionals experience usability and UX challenges across tools & platforms, policies & standards, and training & awareness initiatives within their organization. Detailed results and analyses, with charts, tables, and relevant quotes from participants are set to be published in the corresponding conference paper accepted for presentation at the 2025 IEEE Cyber Awareness Research Symposium (Rajarithnam & Singh, 2025).

Tools & Platforms

Participants reported active involvement in cybersecurity tools & platforms' procurement, though the degree of involvement varied by role. Executives were more likely to lead procurement efforts or play an important role in vendor evaluations, whereas lower-level cybersecurity professionals primarily contributed feedback as needed. A key finding was that UX considerations were not formally incorporated into procurement processes; instead, they were assessed informally through observation.

Daily operations relied on multiple tools & platforms spanning diverse cybersecurity domains, such as Identity and Access Management (IAM), Security

Operations, and so forth. Participants noted overlapping functionalities and the cognitive burden of switching between tools, underscoring the need for tool rationalization and integration. Sophisticated, highly configurable platforms such as Splunk Security Information and Event Management (SIEM) were cited for their steep learning curves and lack of structured support systems. Similarly, Carbon Black Endpoint Detection and Response (EDR) was described as challenging to deploy without prior experience, despite extensive documentation.

Table 6.2, reproduced from the accepted conference paper (Rajaratnam & Singh, 2025), outlines the specific usability & UX challenges reported by participants. Overall, these findings highlight the need for stronger training and onboarding related to cybersecurity tools & platforms, and for formal inclusion of UX consideration in procurement decisions.

Table 6.2. Cybersecurity Tools & Platforms’ Usability & UX Challenges. Adapted from Rajaratnam & Singh (2025), IEEE Cyber Awareness and Research Symposium paper: “Assessing the Cybersecurity User Experience (UX) in an Organizational Context”.

Role	Cybersecurity Tools & Platforms’ Usability & UX Challenges
Executive	• Complex learning curves for most tools & platforms • Tool sprawl, or the sheer number of tools available • Varying levels of complexity and use
Cybersecurity Professional	• Limited bandwidth to fulfill all required tasks • Difficulty initiating significant changes requiring business buy-in, sufficient capital, and cross-team support • Securing business buy-in to prioritize cybersecurity • Learning to deploy and manage tools & platforms effectively with minimal prior knowledge • Steep learning curve for highly customizable tools like Splunk

Table 6.2. Continued

Other: Information Security Project Manager	• Bit9 blocks applications despite that being the intended purpose
Please note: the challenges outlined above are summarized and not presented in their original wording.	

Policies & Standards

Most practitioners confirmed that their organization maintains accessible and comprehensible cybersecurity policies & standards, and that employees receive formal guidance on them. However, implementation and compliance emerged as persistent challenges. Participants noted resistance when enforcing changes, particularly when compliance required workflow adjustments and/or business buy-in.

Table 6.3, reproduced from the accepted conference paper (Rajaratnam & Singh, 2025), outlines the specific cybersecurity policies & standards' usability and UX challenges reported by participants. These findings reveal a disconnect between policy intent and practical adoption, emphasizing the need to balance security rigor with operational feasibility and to engage relevant stakeholders early in the policy implementation process.

Training & Awareness

Nearly all participants indicated that cybersecurity training is prioritized within their organization, but training depth and frequency varied. Most employees receive

annual foundational sessions, while specialized, role-specific training for cybersecurity professionals remains inconsistent. Participants often learned to manage complex tools through trial, documentation, or peer assistance, rather than formal training, education, and awareness programs. While general awareness training (e.g., phishing identification) was considered effective, more scenario-based, role-tailored, and hands-on training was recommended to enhance applied learning and engagement.

Table 6.3. Cybersecurity Policies & Standards’ Usability & UX Challenges. Adapted from Rajarathnam & Singh (2025), IEEE Cyber Awareness and Research Symposium paper: “Assessing the Cybersecurity User Experience (UX) in an Organizational Context”.

Role	Cybersecurity Policies & Standards’ Usability & UX Challenges
Executive	• N/A - participants did not mention any challenges
Cybersecurity Professional	• Obtaining business buy-in to execute at the desired level • Pushback from administrators on implementing changes to become compliant with standards • Policy adherence may not always be 100%, requiring adjustments based on the organization’s business needs
Other: Information Security Project Manager	• N/A - participants did not mention any challenges
Please note: the challenges outlined above are summarized and not presented in their original wording.	

Practitioner Feedback & Study Instruments’ Refinement

The follow-up interview part of the pilot study also served as an informal expert review for refining the study instruments, namely the survey questionnaire and interview protocol. Participants highlighted an ambiguity in survey items; specifically, the need to distinguish between general and role-specific training. Accordingly, subsequent iterations

of the survey were modified to explicitly address this distinction. Other changes were also made, such as capturing specific tool names for richer context.

The pilot phase also helped identify logistical improvements for scaling the study, such as offering monetary incentives to encourage participation (Kelly et al., 2017), given the time constraints among cybersecurity professionals. These insights informed the design for the larger, multi-organization study and establishing a plan for post-analysis Expert Review phase involving experienced practitioners to validate the findings and recommendations in the broader dissertation study.

Pilot Study Conclusion

Overall, the pilot study confirmed that while cybersecurity teams value policy accessibility and general training, usability gaps in tools, fragmented integration, and limited role-specific training continue to hinder operational efficiency and adoption. The findings also demonstrated the feasibility of the mixed-methods design and provided practical feedback for refining instruments and procedures. The pilot thus established methodological groundwork for the broader dissertation study (**phases III & IV**) aimed at developing a NIST CSF-based Usable Security Community Profile that integrates UX considerations into organizational cybersecurity practice.

APPENDIX G: CODEBOOK

Overview

This appendix presents the codebook developed for the thematic analysis (Braun & Clarke, 2006; Goyanes et al., 2025) of follow-up interview data in **Table 6.4**. It includes the thematic framework comprising overarching themes, sub-themes, and associated qualitative codes. Each code is accompanied by a brief definition and a verbatim coded excerpt/quote from the data to illustrate its application. The coded excerpts/quotes are intended as representative examples and do not encompass the full range of coded responses.

Table 6.4. Codebook: Themes, sub-Themes, and qualitative codes with definitions and illustrative coded excerpts (example quotes, verbatim) from follow-up interviews

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Tools & Platforms	UX & Usability challenges faced by practitioners when implementing or operating cybersecurity tools & platforms within their organization, along with recommendations to address them	N/A - theme
Procurement & Integration	Examines decision criteria and integration considerations when selecting and acquiring cybersecurity tools & platforms	N/A - sub-theme
Conditional weighting of UX	UX considerations for tools & platforms' procurement vary based on anticipated user groups and use-cases	<i>"I'll say increasingly user experience matters. Um and we... we divide it into two buckets. If it's a tool that's going to really be... that we run it, but other people are going to use it... or other folks outside of cyber are going to are going to interface with it a lot, then we're paying more attention to user experience obviously"</i> (Participant 10)
Cost-driven procurement	Tools & Platforms' procurement dominated by cost efficiency over other factors	<i>"...there is a big obviously cost component. So, uh, a lot of time a customer will say, OK, my existing vendor, I have three existing vendors that can do X, Y and Z, you can do. I need this new capability, but can you... can this new vendor do this new capability, and also, replace my other three capabilities so that I'm not spending a lot of money and I don't have a lot of complexity in my environment? Blah blah blah. So, there's</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>a... there's a cost in business per component too, like can I save money while meeting my requirements, or do I have to pay an arm and a leg to meet this new requirement? And is it worth, right?" (Participant 09)</i>
Ease of integration & interoperability	Simplicity and intuitiveness with which cybersecurity tools & platforms integrate with other systems, tools, and platforms within the organization	<i>"So, I think from a like core requirements perspective people will ask - do you have customizable dashboards? How flexible is the solution? Can you integrate with other solutions? And that's like more of a product capability perspective, but then how easy is it to integrate becomes like a UX thing. Like, can I go integrate with ServiceNow, or can I integrate with a third-party SIEM solution?" (Participant 09)</i>
Familiarity-driven procurement	Tools & Platforms' procurement decisions dominated by staff familiarity or prior experience with a vendor	<i>"...we have to learn the platform? So, we didn't go with like, for example, we didn't go with a tool like Microsoft Entra ID for identity governance because the team was familiar with the SailPoint platform. So, familiarity with our resources was the number one priority. The second action item was support from the vendor." (Participant 11)</i>
Legal & compliance considerations in procurement	Ensuring that cybersecurity tools & platforms procurement decision-making include regulatory, contractual, and legal obligations and requirements (e.g., HIPAA, PCI, state mandates)	<i>"Yeah, the criteria I've used in my security career, all spanning all the places I worked at, has been that threefold: 1. Making sure that complying with whatever regulations or laws are in place... HIPAA and... PCI and state of Tennessee requirements... The second criteria was... any obligations the company had... either in providing services for someone or requesting a third party provided service on our behalf to make sure that those obligations were met... And then finally... the safeguards that are appropriate to defend whatever the organization that was to make sure that it met</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>those needs as well.</i> ” (Participant 26)
Low UX priority	Minimal weighting of User Experience (UX), compared with technical capability, cost-effectiveness, and other procurement criteria	<i>“So yes, UX would be one of the options. One of the criteria, but it's not an important one. Always detections, all those things comes first.”</i> (Participant 01)
Security capability-driven procurement	Emphasis on security effectiveness and advanced features as the primary selection criterion for tools & platforms	<i>“Uh, first and foremost, I think it's, you know, from a feature capability requirement perspective like can this solution achieve what I'm like needing to achieve? Like what is the outcome I'm trying to achieve - security outcome I'm trying to achieve, right? Let's say it's blocking sensitive data from leaving my environment via e-mail. Can this solution actually do that? That's like the bare minimum requirement, right?”</i> (Participant 09)
Consolidation vs. Best-of-breed	Explores strategic trade-offs between adopting integrated vendor ecosystems and specialized tools & platforms that excel in a particular function or domain	N/A - sub-theme
Cross-platform consistency	Consistent terminologies, design logic, navigation patterns, and workflows across tools & platforms from the same vendor ecosystem, reducing learning time and cognitive load while switching between products	<i>“I primarily am responsible for Intune and then use Sentinel and Defender also. One thing is... not completely, but at least Microsoft tries to stay consistent across the different products. So, at least you're not totally learning a new UI moving from one to the other. Now, they could be more consistent for sure, but that is one thing that's helpful.”</i> (Participant 18)
Ecosystem lock-	Dependence on a single vendor's	<i>“Maybe when it comes time to renew my license, if it costs</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
in	integrated suite of tools (e.g., Microsoft suite) that promotes efficiency and interoperability at the cost of flexibility, diversity of solutions, and negotiating power	<i>more money to have a get duplicate product, those decisions as business issue by Microsoft clearly point to, they want to keep me all in Microsoft things, Intune for Mobile Device Management, EntraID for Active Directory in the clouds, and all the things that they have in label to keep people kind of in that ecosystem” (Participant 26)</i>
Opportunity for portfolio rationalization	Opportunities for organizations to reduce the number of cybersecurity tools & platforms with overlapping capabilities in their portfolio to reduce cost and operational overhead	<i>“Microsoft Defender - I'd say it's just as relevant because Defender provides the Endpoint Detection and Response, but it also provides e-mail security capabilities, so that you don't have to bring in CrowdStrike and ProofPoint. You can kind of just have Defender be slapped across multiple security functions, and it all has the same management console.” (Participant 11)</i>
Workflow Efficiency	Considers how design and configurability affect task completion and productivity	N/A - sub-theme
Desire for streamlined workflow	Preference for simplified, frictionless task flows that minimize steps and interruptions, enabling faster, more efficient security operations	<i>“...what can I then do to make sure that people who are paid to look in a SOC monitor, SOC wall, look at the alerts, look at the things that happening, and make sure that they have the training and support they need so that they can reduce the time, from the time and alarm goes off. Or maybe an alarm doesn't go off, or maybe it's safeguards not working like it should, or an agent's not effective, or if not installed, how quickly can I shorten the gap that they can recognize and respond to something?” (Participant 26)</i>
Fragmented workflows &	Frequent transitions between multiple tools or windows due to	<i>“...when you have like a Defender incident and then sends it over to Sentinel, a lot of the data that comes over isn't</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
context switching	poor integration that disrupt task flow and increase cognitive effort	<i>necessarily enough to work the incident, and you end up switching platforms and you move off a Sentinel and to the Defender for Endpoint when working an incident. I just find that really annoying because I feel like to a certain extent that kind of ruins the whole point of the SIEM.” (Participant 17)</i>
Lack of state persistence	Absence of features that retain users' previous settings, filters, or search history within tools & platforms, forcing repetitive manual work or reconfiguration	<i>“Even something simple as just accessing your Sentinel environments, we have to click through the same filters and buttons and do the same 5 steps every single time just to look at, for instance, that are assigned to us for today and there's no way to bookmark the page, no way to save that search query. No way, no way to do that stuff.” (Participant 14)</i>
Limited tools customization	Constraints in cybersecurity tools & platforms that prevent users from modifying default configurations, therefore causing repetitive manual work	<i>“So, I guess I'll give an example from like the DLP space with, you know... you know Purview... if the customer is having, experiencing you know, a large amount of false positives for however... how their data is structured on some of these data elements, Microsoft doesn't give you the ability to customize those out-of-the-box policies. So, it requires them then to go through and manually recreate and then tweak from there, without necessarily the visibility into some of the initial configuration that Microsoft had on the those sensitivity or sensitive data elements. So, they... they have to go from the ground up rather than, you know, the ability to kind of customize, and you know, an existing data element or policy that that the vendor has... has configured.” (Participant 05)</i>
Minimizing clicks & repetitive	Streamlining interfaces to reduce unnecessary clicks or repeated	<i>“...one way that some people look at is how many clicks. How many times do I have to click before I get to what I'm looking</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
actions	steps, improving speed and efficiency in high-frequency investigative tasks	<i>for, and ideally the fewer clicks, the better, because it may for one investigation. Yeah, I might have to click two or three more times. But if I'm doing this hundreds of times a day, literally being able to take two clicks out of my process will save me a lot of time”</i> (Participant 23)
Performance & Reliability	Focuses on technical stability and contextual relevance of tools & platforms' functioning and outputs	N/A - sub-theme
Expectation of API parity	Desire for console capabilities to be equally available and supported through well-documented APIs, including error references and troubleshooting guidance that enable seamless automation and integration	<i>“...basically everything that you can do in a console in a tool, you should be able to do it in API also. And if they had sufficient documentation on that, on their APIs, on the types of error codes you can receive, and I guess common like a documentation on common troubleshooting things”</i> (Participant 21)
Lack of contextual information	Tools & Platforms' failure to provide sufficient context or risk-based prioritization to help cybersecurity professionals understand severity and relevance of alerts and results	<i>“Yeah, but with that, again, we've seen teams, you know, getting frustrated with certain tools because of the fact that there is no enough context there, you know... You know, some of them doesn't take like a risk-based approach to give them some priority on what needs to be worked on.”</i> (Participant 06)
Lack of troubleshooting guidance	Absence or inadequacy of vendor-provided information and documentation to interpret and resolve errors and malfunctions, forcing users to self-diagnose or seek workarounds	<i>“I do have this problem all the time, specifically with CyberArk, like when you're calling API's they're... they have very generic errors and they... like it will say unauthorized. Sometimes it'll even say unauthorized, and that's not even what the error really is. And there's like a lot of with, like CyberArk especially, there's a lot of different reasons you can</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>be unauthorized and like it cause like there's a lot of different authentication components there.” (Participant 21)</i>
Task times out	Tool fails to complete its task or exceeds time limit, leading to incomplete analysis or user workarounds	<i>“As a developer I've only pushed up a small change. But I'm having to wait 30 odd minutes and then after that I get like a timeout on the job or something. And again, there's no... none of my changes have been scanned and at that point if I force merge, I'm introducing a new vulnerability, potentially, which was missed.” (Participant 02)</i>
UI Quality & Impact of Changes	Refers to how User Interface (UI) design and frequent updates affect the overall cybersecurity tools & platforms' UX	N/A - sub-theme
Desire for dashboard clarity	Preference for dashboards that visualize or summarize key metrics and status within tools & platforms	<i>“...in a dashboard, or in a queue that says typically you know, red is bad typically, green is good? Is it clear for the analyst? For the engineer? For incident responder? For the CISO, to be able to very quickly make eye contact with what... how's our status right now? How are we doing and what are some things that perhaps we should do before we go home today to make sure some of that red, or maybe all that red that goes away to the extent possible? So, making it easier to kind of have that dashboard or that visual to see what's where's my to-dos, and make sure that I to do them, whatever my role would be from junior SOC analyst to Senior cybersecurity executive, that what does it look like? How could we get accustomed to then where necessary you know, click into or see the details, see the packet capture, see all the bad things that are happening, but kind of start at that high level. And</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>then from there drill into what I need.” (Participant 26)</i>
Desire for UI consistency	Preference for stable, uniform visual design and layout across tools & platforms, reducing learning effort, confusion and frustration when navigating different products or after interface updates	<i>“I primarily am responsible for Intune and then use Sentinel and Defender also. One thing is... not completely, but at least Microsoft tries to stay consistent across the different products. So, at least you're not totally learning a new UI moving from one to the other. Now, they could be more consistent for sure, but that is one thing that's helpful.” (Participant 18)</i>
Expectation of customizable dashboards	Desire for personalization and tailored reporting capabilities in tools & platforms	<i>“...something that cybersecurity, like, stakeholders always ask for is like from a dashboarding perspective and an ability to customize your dashboards and generate executive reporting.” (Participant 09)</i>
Frequent UI changes	Recurrent interface redesigns that disrupt established workflows and require practitioners to put in additional effort to adjust to the system	<i>“I'd say the one thing with Microsoft Defender is that it seems like they do a lot of updates, and they're constantly, you know, working on that platform. So, the only issues that I've come across is that once updates are shared and maybe the... the web page changes a little bit or some of the... the UX pieces changed, it seems like our teams were having to spend, you know, a... two to three days to really get caught up to speed, whereas with CrowdStrike it seems like things stayed the same, but the underlying technologies were being refreshed.” (Participant 11)</i>
Outdated or legacy UI design	Persistent use of dated interfaces requiring memorization and manual workarounds	<i>“Citrix, it's still the old-school style, where it's like you gotta... you gotta really know the tool. And you gotta remember it and maybe take notes and keep track of it because you will forget if you don't use it in a month.” (Participant 08)</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Documentation, Learnability, and Onboarding	Focuses on how users acquire proficiency and navigate documentation for cybersecurity tools & platforms	N/A - sub-theme
AI-assisted contextual navigation & learning	Integration of AI or LLM-based assistants within tools & platforms that help users find functions or interpret documentation, and provide real-time task-specific guidance	<i>“Like if you think about Azure Portal for example where you configure Azure, it's... there's so... so many places to go, it's really tough to... to find what you need. I think the one thing that might be helping you more recently, but not 100%, but might be... is a little bit of the AI enhanced capabilities where you can actually search for things and they'll try to find what you want or bring you something towards what you need.”</i> (Participant 08)
Challenging onboarding	Steep learning curves due to complex processes, insufficient guidance, task inefficiencies, and lack of clear documentation	<i>“...the onboarding part is super challenging for a lot of companies like when they buy the tool they... they face a lot of challenges just installing the tool right because oftentimes just to get a SIEM installed, it takes 13 months, right? 13 months. Like just 13 months of a different team spending time to like set up one tool. That's like average for industry wide. Of course, it would be less for small companies, but like large companies, it takes more than 13 months, because you have different disparate sources of these logs, and you have to like get these logs into a SIEM, right? So that's like a challenge.”</i> (Participant 01)
Discoverability and navigation friction	Difficulty locating features and documentation due to poor Information Architecture (IA) and UX design	<i>“Like if you think about Azure Portal for example where you configure Azure, it's... there's so... so many places to go, it's really tough to... to find what you need. I think the one thing that might be helping you more recently, but not 100%, but</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>might be... is a little bit of the AI enhanced capabilities where you can actually search for things and they'll try to find what you want or bring you something towards what you need."</i> (Participant 08)
Easy bite-size-videos	Short, focused video tutorials to help users with tools & platforms-related learning and onboarding	<i>"So, what we have done is like we have made like bite-size... bite-size videos. Once you onboard like a platform, you'll get these bite-size videos to just go through the user journey and it makes it easier for... for customers to... versus like just clicking through some links."</i> (Participant 01)
Embedded & contextual help	In-product guidance that delivers task-specific support within the interface, enabling users to access relevant instructions without leaving their workflows	<i>"One of the things that we added recently and has been received pretty well is: within every page in the in the product, there's a small help icon, and if you will learn something more about that specific page, you can click on that help icon and it will just pull up the documentation for it."</i> (Participant 02)
Hidden knowledge gaps	Difficulty recognizing or assessing tools & platforms knowledge that isn't explicitly documented, making it hard for practitioners to identify what they still need to learn	<i>"...so a lot of it with tools that I find is... is going from beginner, you know to advanced beginner, to journeyman to expert. And not really knowing when have I reached any of those stages because I may not have realized that this tool has a lot more functionality or capabilities and I'm not even aware of, and that's very challenging to kind of know what you don't know."</i> (Participant 23)
Incomplete or insufficient vendor documentation	Vendor-provided guidance that omits implementation details or advanced steps, forcing practitioners to seek additional help to complete tasks	<i>"...to me the user documentation is not always great, and it seems that when it is there, it's usually incomplete. We joke about Microsoft usually having pretty good documentation, but it's like they leave out the last 20% you need, which is the parts you really need."</i> (Participant 18)

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Overly long documentation	Lengthy or dense manuals that discourage practitioners from reading or referencing due to the time and effort required	<i>"...these PDFs are like 200 pages long and you like no one has time to, like, read so many pages"</i> (Participant 25)
Reliance on playbooks (procedural workarounds)	Dependence on internally maintained step-by-step documentation to help practitioners complete tasks when tools lack intuitive design or learnability	<i>"...it's thorough documentation. We call it a playbook. So, every time we have to do something, we go back to the playbook and look where it is because we can't really change the tool, right? So unfortunately, if we could then, reorganize the tool."</i> (Participant 08)
Visual & experiential learning aids	Use of diagrams, demos, and sandbox environments to reinforce comprehension and retention related to tools & platforms	<i>"Good diagrams that kind of show all the connectors and all the flows. I think that typically helps going through and just having someone lecture for the time being and going through a PowerPoint that's very text heavy, typically that doesn't do it for me. Other times we've had a live environment. I put that in quotations because it's kind of, you know, fake user data and whatnot, but just being able to kind of go and see what a console looks like when you're going to create a group or if you're going to kind of de-provision access to a certain resource. Those examples are typically much more helpful."</i> (Participant 11)
Feedback Loops & Issue Tracking	Examines how practitioners raise, track, and resolve UX and other issues related to cybersecurity tools & platforms	N/A - sub-theme
Formal issue-tracking &	Use of structured ticketing systems (e.g., Jira, ServiceNow) to log,	<i>"But like a lot of organizations formally we'll create a ticket using Jira in our case, so that it's documented and the</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
escalation	assign, and manage issues, ensuring accountability and documented resolution workflows	<i>engineers have something that they can then assign themselves to and work on to try to fix the problem.”</i> (Participant 23)
Informal peer support and escalation channels	Reliance on colleagues and ad-hoc communication (e.g., Slack, Teams) for discussing issues or feedback, over formal documentation and tracking, improving speed and responsiveness but at the cost of traceability	<i>“But what actually happens is it becomes a Teams chat to a manager, and there's not formal documentation of hey this person has is requesting access to a privileged account, and this person now has the access to a privileged account. It's kind of like if there's a Slack channel or something, a little less formal, and there's not a formal paper trail.”</i> (Participant 11)
Reliance on vendor support	Dependence on vendor representatives or external support channels to resolve tools & platforms issues, when internal documentation and peer resources are insufficient or inaccurate	<i>“I would say first I would go to my more senior teammates and see if they understand it. And... and then if they still don't get it, then we would reach out to the vendor.”</i> (Participant 21)
Balancing Strong Security with Operational Realities	Examines tensions between maintaining strict security controls and preserving operational efficiency, such as avoiding critical systems' disruption	N/A - sub-theme
Containment-first (deny-all) response	Immediate lockdown of systems to stop potential compromise before gradually restoring access based on risk assessment or verified need	<i>“They just do a deny all for everything and then they're like, OK, we'll see about what we want to allow later, but we have to contain the situation right now.”</i> (Participant 24)
Context-based	Adjusting or relaxing security	<i>“...when I'm implementing Okta mostly for my customers... we</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
security exceptions	controls in high-risk or time-sensitive operational contexts (e.g., healthcare emergencies) to prevent safety or usability consequences	<i>always tell customers to at least sign out all the users from the identity provider session once a day, which is, once in eight hours... But, depending on the customer that I'm working with, mostly I have seen for healthcare customers, they are absolutely not okay with this... say practitioners or their nurses are using their websites... if there is an emergency scenario and a person can die within seconds, but then if you just... if you just tell them that, hey, well you, you just have to do an username validation, authentication, etcetera, that would take somebody's life.” (Participant 24)</i>
Legacy environment constraints	Challenges arising from maintaining and securing older, mission-critical systems that can't be easily modified or updated without disrupting operations	<i>“...one of the biggest, I think difficulties is... is just that, navigating that legacy environment and what, you know, and... and I... I want to say up front so that we're on the same page right. What I mean by that is there's, you know, there's tech here from... from ages long ago that are still because it's the type of, you know, we work for a healthcare organization and a lot of times if it works, you don't touch it.” (Participant 10)</i>
Tool sprawl	Accumulation of numerous tools & platforms resulting in overlapping functionality, underutilized shelfware, and inflated budgets	<i>“They purchase like every solution under the sun just to say they have it, and don't do any... or shouldn't say don't, but do limited work to kind of figure out what they truly need in their organization. So, a lot of things end up being shelfware, used for like a specific... specific use case, and they end up kind of inflating their cyber budget to pay for all these solutions, when they can get away with probably half of the... half of the solutions in their environment. That happens all over the place.” (Participant 05)</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Policies & Standards	UX & Usability challenges faced by practitioners when implementing or managing cybersecurity policies & standards within their organization, along with recommendations to address them	N/A - theme
Accessibility & Centralization	Examines how storage structures and search mechanisms influence practitioners' engagement with their organizations' cybersecurity policies & standards	N/A - sub-theme
Centralized repository	Existence or need for a single organized location (e.g., internal wiki) for storing cybersecurity policies & standards in an organization	<i>"And recently, we... we created a way forward where they're more accessible than before. There's a separate web page internally through our intranet, we'll call it, that has all the policy and standards and is also part of the onboarding process as well."</i> (Participant 22)
Dispersed policy storage	Policies & Standards are scattered across multiple locations, or multiple sub-locations within one platform, making access dependent on prior knowledge	<i>"...it's in a... I guess a centralized location in the sense of they're all kind of up in SharePoint, but they are... in the... in they're like... they're spread out across... across kind of different locations of like, the information security teams' SharePoint sites and pages. So, yeah. If you know what you're looking for, that you can... you can find them relatively easily. But if you wanted to go out and just say, like, you know, someone who's just like, what is the policy for, for X, they might have a little bit more difficulty to find it"</i> (Participant 05)

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Poor searchability	Difficulty locating policies & standards due to poor search functionality or inconsistent metadata	<i>“They have a homegrown tool where they have added all their policies and standards. So, it's a system that can take in a Word document and display it on a web browser, and so that is something where they have built their own search capability. So, it's hard to search. You might put in like cybersecurity, and there's a reference to that in HR policies for any reasons. Maybe it's like the legal requirements. So, it's a very simple search that you know, that doesn't really prioritize each of those in relative. So, those kind of get bogged down. So, whether it's your full-blown information security standard, your cryptography standard, and so on and so forth. It's not really easy to find because you'll get a lot of noise when you search the tool.”</i> (Participant 03)
Clarity & Understandability	Focuses on how language, structure, and supporting materials affect cybersecurity policies & standards' comprehension and practical implementation	N/A - sub-theme
Ambiguous policy applicability	Unclear or overlapping policies that leave staff uncertain about which rules to apply in specific contexts	<i>“...provide more clarity around which policies and procedures, or policies and standards staff need to adhere to. Specifically, kind of some of those differences between US versus global. Sometimes those policies can have contradicting information”</i> (Participant 05)
Excessive jargon	Use of specialized terminology and abbreviations that create comprehension barriers for new or non-expert users	<i>“I would say the reduction or just kind of reducing overall the amount of acronyms. I think the acronyms are typically something that, once you're at, you know, three to five years in a role, you typically understand what the acronyms mean.</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>But a lot of times when we're onboarding new college grads, they're obviously not understanding kind of the industry jargon and what not.</i> ” (Participant 11)
Legalistic policy language	Use of legal and compliance verbiage in policies & standards that obscures practical meaning and makes guidance hard for cybersecurity professionals to apply	<i>“I think I would probably say this about any... any organization’s to be honest, but they’re... they’re understandable, but they can also be very legalistic and general, and I think maybe sometimes providing an example of what they... what this means in practice would be useful.”</i> (Participant 23)
Need examples	Need for real-world illustrations or documented scenarios to help practitioners interpret and apply policies & standards	<i>“I think examples are the best thing! As many given documented scenarios and examples you can provide just makes easy for non-legal people to interpret things like policies.”</i> (Participant 02)
Overly long & verbose policies	Policies & Standards written in dense, wordy, or excessively detailed language that hinder quick comprehension and reduce practitioner engagement	<i>“...when it's policies and standards, most companies are like, yeah, read this 30-page document and like, acknowledge the terms and conditions”</i> (Participant 25)
Provide supplemental implementation guidance	Providing additional documentation (e.g., processes and procedures) to help practitioners operationalize high-level policy statements	<i>“You oftentimes you don't have like the liberty to write stuff in like somewhat plain English that everyone can understand in like a governance policy document. But you can do that you know, even with standards, right? If that's one level lower, that can talk about how to do certain things. But certainly, the processes, procedures and like guidance documents that you develop for these can be our implementation guidance”</i> (Participant 06)
Compliance &	Addresses how organizations	N/A - sub-theme

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Framework Alignment	adopt, interpret, and integrate external standards, frameworks, and best practices to meet regulatory and risk-management obligations	
Global compliance complexity	Difficulty maintaining compliance with various international regulations (e.g., GDPR, PIPEDA, etc.), leading to potential violations	<i>“I'd say Global compliance issues. We understand GDPR for Europe, I believe PIPEDA for Canada, but some countries are now starting to develop their own compliance frameworks or data privacy regulations, and I think kind of staying up to speed on those. It's just a little hard at times because we don't understand, you know, in the context of a transaction, if we're working with a company that's going to buy a company that's based out of China, if we don't understand China's policies and regulations around data migration, data sharing for employees and... and customers. If our client decides, OK, we're going to set up the Chinese employee database in Europe, well, they may just have, you know, breach some type of regulation that they didn't even know that they did.”</i> (Participant 11)
Risk-control-policy misalignment	Disjunction between organizations' risk and control libraries with their cybersecurity policies & standards	<i>“We have a risk library, and a controls library, and not all the time they are in sync with our policies and standards.”</i> (Participant 03)
Standards adoption and framework alignment	The process of formally adopting or aligning organizational cybersecurity policies & standards with recognized external standards and frameworks (e.g., NIS, ISO,	<i>“The NIS Network Information Security Standards, right? The NIS standards, we can find them. We... we follow, adopt a lot of these guidelines”</i> (Participant 08)

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
	NIST, etc.)	
Feedback, Enforceability, and Escalation	Captures how cybersecurity policies & standards are communicated, updated, and enforced through formal and informal channels	N/A - sub-theme
Automated update notifications	System-generated alerts that inform users of newly-issued or revised policies & standards, ensuring timely awareness and compliance	<i>“And also, we get reminders like if any training has to be completed or you know, if there is a new guidance or any new policies that has been published, we get reminders over e-mail.”</i> (Participant 24)
Bypassing formal workflows	Bypassing formal procedures (e.g., JIRA/ServiceNow tickets) through informal communication & workarounds (e.g., Teams chat), that can undermine enforcement and auditability	<i>“...most of the standards will say something like - if a user wants to access a database administrator account, then they need to reach out to their manager or create a ServiceNow ticket or a JIRA ticket, right? But what actually happens is it becomes a Teams chat to a manager, and there's not formal documentation of hey this person has is requesting access to a privileged account, and this person now has the access to a privileged account.”</i> (Participant 11)
Low policy engagement	Tendency to skim, scroll through, or superficially acknowledge cybersecurity policies & standards without genuine engagement	<i>“If you read it, I think it is understandable. However, do I think a lot of people read it? No.”</i> (Participant 09)
Ownership & accountability	The clarity (or lack thereof) in defining who holds the responsibility for developing, enforcing, and maintaining	<i>“So, it depends. We wrote the policy with the understanding that the campuses would write the standards. So, we give the policies, here's the policy, here's what we're supposed to do. It's up to the campuses and the colleges on the campuses to</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
	policies & standards	<i>take those policies and run their own standards.</i> ” (Participant 16)
Policy flexibility and handling exceptions	Allowing reasonable deviations from security rules to address valid operational needs while keeping policies & standards' enforcement practical and context-aware	<i>“So, let's say you're trying to block a website. Sounds simple, doesn't it? Right? I'm going to block this website for XYZ, but then how about those exceptions? For those certain things, the exceptions are where the rubber meets the road, where policy has to have room to be both, a movable and I mean, relatable to what a reason would be for an exception to be made.”</i> (Participant 22)
Policy lifecycle management	Continuous review, update, and enforcement of policies through structured governance and onboarding processes	<i>“So again, being aware of the... in the laws and regulations of company is subject to and agreed to do and making sure that the security team, whoever writes the policy team, is aware of and can track and put into, integrate those into their next policy update cycle is a current barrier.”</i> (Participant 26)
Potential Improvements (Future-facing Ideas)	Envisions enhancements that can make cybersecurity policies & standards more usable	N/A - sub-theme
Collaborative policy documentation	Use of wiki- or Confluence-style platforms that allow staff to contribute updates or comments	<i>“...one of the things I've seen other organizations doing that may work better, which I don't think it's done at <participant's org name>, is having like a... a Confluence or Wiki style page, where people can actually contribute, and make changes, and it's more like an interactive environment, versus a policy that's fixed in a PDF, and nobody can change it, right? So, like if you can go in there and comment, say, hey this doesn't apply to Azure anymore, this thing has changed and then somebody can review that. So, the actual users are contributors as well, almost like a GitHub-style”</i> (Participant

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		08)
Intelligent document discovery	Convenient and intuitive documentation accessibility of policies & standards through integrated tools such as AI chatbots and smart search features	<i>“So, one of the things that we did is we work with our networking team. Actually, specifically, the team that was responsible for the web proxy filters... web proxy servers, such that when someone typed the word policy in their web browser, it would go to a central intranet site and on that internet site, the home of every policy...”</i> (Participant 26)
Need for concise summaries	Demand for simplified one-pagers or short versions of lengthy policies & standards designed to improve readability, comprehension, and user engagement	<i>“I think a lot of companies, right, there's cybersecurity policies and standards like legal documents, right? They're like 20 to 30 pages long. Like, no employee is ever reading all of it. Right? Like most people, just like glance over it, scroll through, accept, accept, accept. No. Unless, like, you know, like at my company at least, you have to do training based on like the Policies and standards, you sort of do need to read them. But I think again, like you can have like those legally binding, you know, like long policies and standards. But like, I feel like you should have one pagers of, like, just summarizing the cybersecurity policies and standards”</i> (Participant 25)
Need for vendor policy platforms	Demand for vendor policy platforms to support easy knowledge transfer and accessibility of policies & standards	<i>“...sometimes vendor technologies where you might have limitations with the vendor, you... you're going to have easier knowledge transfer when someone leaves the company or gets promoted. They should really be putting those into kind of a vendor tool, where search capabilities are enhanced. User experience, downloading capabilities are enhanced. It's a single source to this website, its independent, it's not really part of like a... IT service management catalog, helpdesk. I've</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>recommended this, it just hasn't came forth by putting it in a vendor tool. So yeah, things like ServiceNow, Archer, MetricStream” (Participant 03)</i>
Training & Awareness	UX & Usability challenges faced by practitioners regarding role-specific cybersecurity training, education, and awareness initiatives within their organization, along with recommendations to address them	N/A - theme
Cadence & Frequency	Examines training scheduling and repetition and their impact on engagement and retention	N/A - sub-theme
Checkbox exercise	Routine, compliance-mandated security awareness training that are perceived as obligatory corporate requirements	<i>“...a lot of us in cyber departments just subscribe to that yearly training. You're kind of yearly, every six-months phishing training. I forget which month it is, you know, your cybersecurity awareness month. I got an e-mail. It's like fraud, Security Awareness month in the banking industry. So yeah, it's all those kind of corporate pushes.” (Participant 03)</i>
Training frequency & volume burden	Excessive or frequent training requirements that create fatigue and reduce motivation to meaningfully engage with security content	<i>“...the frequency of the trainings can be an issue because, I think it gets sent to us once in every quarter, and that's like a lot, lot, lot of trainings has to be completed.” (Participant 24)</i>
Role-specific Training	Focuses on tailoring training & education to specific job functions and responsibilities	N/A - sub-theme

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
Need for tailored training	Demand for specific cybersecurity training based on practitioners' roles & responsibilities	<i>"I think we do like an annual training. I mean that's at a very high-level, it's for all employees, it's not just for engineers. But maybe it would be beneficial to do a more detailed training for engineers"</i> (Participant 21)
Regulatory-mandated training	Legally required or compliance-driven cybersecurity training for personnel handling sensitive or regulated data	<i>"I get to work with some financial institutions which, you know, right, have a lot of regulatory scrutiny and therefore because of that, I get to take some specialized trainings, right?... That are mandated by SEC or other like governmental agencies, because of the fact that I get to handle some sensitive information, some banking information, so on and so forth. So, I would consider those as my role specific training because of the fact that I am getting introduced to these new type of data that is heavily regulated and governed."</i> (Participant 06)
Targeted guidance based on privileged access	Cybersecurity training and education tailored to users with elevated system or network privileges, focusing on heightened risk awareness and responsible use of elevated access	<i>"So, if an executive has XYZ access, they're kind of guided as to what more... more information related to that access"</i> (Participant 22)
Effective Training Sources	Highlights preferred formats and platforms that promote active learning	N/A - sub-theme
Hands-on & experiential learning	Active, practice-based training through simulations, labs, and gamified platforms that help in real-world skills development	<i>"...let's say for phishing and stuff, we do get tests periodically where you have to report to the cybersecurity phishing center within the firm, that this e-mail you found was a phishing email, and that gets you credit for doing that. So, they keep</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
		<i>conducting those tests whenever they feel that, you know, they need to do it. And the idea is, you shouldn't fail. You should be able to identify that that's actually a phishing e-mail."</i> (Participant 07)
LinkedIn training videos	Simple training videos hosted on LinkedIn that can be accessed by other members, and are perceived as accessible and easy to follow	<i>"...the ones offered through LinkedIn... LinkedIn, and a series of... I mean different professionals and individuals putting trainings out there. Like simple videos... like to go through. So, I mean I found those pretty useful, pretty easy to kind of go through."</i> (Participant 04)
Vendor-issued professional training	Formal role-based training or certification offered by technology vendors (e.g., AWS, Azure, SANS Institute) that enhance specific expertise and professional credibility	<i>"I mean, yeah, in the cybersecurity world, you're probably familiar with, like, the SANS Institute. Right? Like, they do cybersecurity trainings, for like, cybersecurity practitioners. So yeah, like at my company, like, you know, usually an employee does one course a year, and I think those trainings are, you know, particularly helpful in doing our job"</i> (Participant 25)
Challenges & Frustrations	Identifies barriers to meaningful learning and motivation in cybersecurity training, education, and awareness initiatives	N/A - sub-theme
Certification stress	Anxiety or pressure stemming from the need to obtain or maintain professional certifications, often due to job expectations or career advancement demands	<i>"So, right now, there is a push from my organizations, at least my team, my vertical, to get certified in CISSP... In this year, so I don't know if you know like CISSP is a lot, lot, lot to deal with, you know, people with 20 years of experience even sometimes don't pass that exam. So, I guess we are all struggling with that this year"</i> (Participant 24)
Click-through	Superficial completion of required	<i>"...if it's just your quarterly or yearly compliance training,</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
compliance	security training, driven by obligation rather than genuine engagement or learning	<i>people just click, click, click, click, click, click and then they're like? right. So, I think it's more consequence-based in terms of like this guy's actually doing something incorrectly. Let me educate, let me do some real-time education that he violated his policy, educate, educate, do training right now or else you'll be fined”</i> (Participant 09)
Insufficient training depth	Frustration related to cybersecurity training emphasizing surface-level or time-bound modules that fail to develop foundational understanding required for complex tasks	<i>“I think that the broadness is pretty good. I think the depth is pretty bad. ...for example, for security you should understand networking pretty well. That's my... that's my thought. And I... I think most people don't. They just... networking is like a haze in their mind, right? They don't really understand what's going on, and you can see that when we have a... a... a security problem and the network is involved, people are usually very lost on how to handle it and it's... it's not something that you learn through a one-month training. It actually requires a few years of training, and like retraining again and again, and learning, it's tough.”</i> (Participant 08)
Time constraints	Lack of dedicated time preventing employees from attending or completing cybersecurity training alongside job duties	<i>“The biggest thing is like finding the time to be able to do it. So, I think... yeah, I guess that... that last question around education, training, do you think would be most effective for employees? Maybe it's not necessarily a role-specific training, but more so like getting dedicated time to actually attend these, rather than trying to balance it on top of, you know, all the other responsibilities, and it can... it can be difficult to find the time to get in and... and attend some of these trainings.”</i> (Participant 05)
Training &	Declining engagement toward	<i>“I actually had to develop a training for a client and the</i>

Table 6.4. Continued

Categorization (Theme, sub-theme, code)	Definition	Coded Excerpts/Quotes (Examples, Verbatim)
documentation fatigue	repetitive or lengthy cybersecurity training & education, leading organizations to shorten or simplify content to improve participation	<i>training was just on, like clean desk policy - not writing down your passwords and what not. So, in developing a 30-slide presentation, we were kind of told like if we could just cut the training down, they felt that their employees would not be, you know, very receptive to an hour-long training and that they wanted something that could be in the realm of 15 to 20 minutes” (Participant 11)</i>
Future Improvements & Innovations	Envisions emerging, technology-enabled approaches for adaptive and just-in-time training	N/A - sub-theme
Real-time & consequence-based training	Immediate or consequence-driven training & education triggered by users' actions or risky behavior	<i>“...if it's just your quarterly or yearly compliance training, people just click, click, click, click, click, click and then they're like? right. So, I think it's more consequence-based in terms of like this guy's actually doing something incorrectly. Let me educate, let me do some real-time education that he violated his policy, educate, educate, do training right now or else you'll be fined” (Participant 09)</i>
Scenario-based & real-world training	Cybersecurity training & education that uses realistic scenarios and actual or contextually relevant examples to build practical awareness and reinforce applied learning	<i>“Or you know, just don't fall for SMS or e-mail scams like things like that are basic, yeah? But some really get into like even if they want to do a training on phishing, for example, some give like real time examples, right? Hey, you're getting an email with the following so and so statement. What would you do, right? So, having more like real examples in those trainings would help.” (Participant 06)</i>
Note: Each qualitative code is accompanied by a single coded excerpt or quote (verbatim) from the follow-up interview data, provided solely as an illustrative example. These excerpts do not reflect the full range of statements associated with each code. Dark gray font color, combined with indented text, is used to indicate (qualitative) codes.		

VITA

Shreenandan Rajarathnam is a former Senior Associate in PricewaterhouseCoopers' (PwC) Cybersecurity & Privacy practice who joined the PhD program at the University of Tennessee, Knoxville (UTK), to pursue research in making cybersecurity more user-friendly. He has client experiences specializing in data protection, data governance, and cloud security in the financial services industry for a Fortune 500 client.

Shreenandan received his Bachelor of Engineering (BE or BEng) degree in Computer Science & Engineering from PES University, Bengaluru, India (PES Institute of Technology at the time) in 2016. He earned his Master of Science degree in Information Management (Specialized Pathway: Privacy, Trust, Security & Ethics) from the University of Illinois at Urbana-Champaign (UIUC), in 2018. He has submitted this dissertation towards the completion of his doctoral (PhD) degree in Information Science from the School of Information Sciences (SIS), College of Communication and Information (CCI), UTK in 2025. His research interests include cybersecurity and User Experience (UX). He has earned the following academic and professional certifications: EC-Council Certified Ethical Hacker (CEH), Microsoft Certified: Azure Fundamentals, Google UX Design Professional, and UTK Center for the Integration of Research, Teaching, and Learning (CIRTL) Associate.

During his doctoral studies, Shreenandan served as a Graduate Teaching Associate (GTA) in SIS, CCI, UTK, where he collaborated with multiple scholars on Information Science research projects and taught the following undergraduate courses (in-person and online/asynchronous formats) as the primary/sole instructor: INSC 430 - Foundations of User Experience (Fall 2023, Spring 2024, Spring 2025, and Fall 2025) and INSC 305 - Internet and Society (Fall 2024). He has presented a research poster and multiple research papers at IEEE conferences and is currently working on multiple manuscripts to be submitted to peer-reviewed journals in the near future.

In 2024, he received the Graduate Student Research Award from UTK Graduate School. He has also served as the Vice President of the CCI Graduate Student Association (GSA), UTK representing his school (SIS) for multiple years. He has also served in the SIS Full-time Faculty Search Committee and the Diversity, Equity, and Inclusion (DEI) Committee, CCI, UTK. Upon completion of his PhD, he plans to pursue a career in the cybersecurity industry.