

Article

Towards a Usability-Focused Security Culture Framework

Wesam Fallatah *, Steven Furnell and Christian Wagner

School of Computer Science, University of Nottingham, Nottingham NG8 1BB, UK;
steven.furnell@nottingham.ac.uk (S.F.); christian.wagner@nottingham.ac.uk (C.W.)

* Correspondence: wfallatah@gmail.com

Abstract

Organizations are facing a wide range of cyber threats. While technological advancements have resulted in sophisticated cybersecurity solutions, the effectiveness of these solutions is hindered when users do not properly engage with security measures. Usable security is critical to encourage people to incorporate proactive practices into their daily routine, which strengthens the wider security culture. Conversely, cumbersome and intrusive measures can lead to workarounds, errors, or neglect, compromising security efforts. This study addresses the limited research on how the usability of security measures influences security culture. A mixed-method approach was employed to characterize this relationship by investigating whether usable security can positively influence security culture. Data were gathered through a survey study with over 200 participants, followed by interviews with a smaller subset. The study then proposes a usability-focused framework that leverages the influence in addition to other essential elements to foster a robust security culture. The findings suggest that addressing common usability barriers can help organizations improve compliance, reduce security risks, and enhance the overall security culture.

Keywords: usable security; security culture; cybersecurity behavior

1. Introduction

There is an increasing recognition that human factors play an important role in cybersecurity. The importance of human-centric control is evident across industries, including technology, education, and healthcare, where it plays a significant role in managing cyber risks. There are a number of human factors that contribute to vulnerabilities, including apathy, ignorance, and unintentional mistakes. In order to reduce human errors, many organizations apply constraining approaches, which aim at limiting the influence of humans and the potential for error [1]. While these constraints can arguably minimize mistakes to a certain extent, organizations remain reliant on human judgment and decision-making, meaning employees need to be empowered with the skills and knowledge to identify and defend against cyber threats targeting humans, such as phishing and social engineering.

The human aspect of cybersecurity has been investigated over the past two decades. Foundational research by Adams and Sasse [2] challenged the dominant perception that users are the “weakest link” in the security chain, revealing that poorly designed security measures often drive insecure behavior. Subsequent studies showed that human–computer interaction approaches can produce usable and effective security [3] and that usability must be considered in security designs from the outset [4]. Herly [5] further suggested that users rationally dismiss security when the cost of compliance outweighs tangible benefits. Previous studies have established that security measures that fail to account for human



Academic Editor: Danda B. Rawat

Received: 16 December 2025

Revised: 7 February 2026

Accepted: 10 February 2026

Published: 12 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

factors and the drivers of users' security behaviors and actions are unlikely to be effective. Several theoretical frameworks have been developed to understand security behaviors. Protection Motivation Theory (PMT) indicates that security actions are influenced by threat appraisal and the ease of coping appraisal (response and self-efficacy) [6,7]. Also, the Technology Acceptance Model (TAM) suggests that perceived usefulness and ease of use are determinants of users' technology adoption [8], with these constructs further extended to security tools [9]. More recent work promotes approaches that maintain security behaviors through positive organizational practices rather than compliance enforcement [10].

Alongside this, organizations have increasingly recognized the significance of fostering a robust security culture, as such efforts play a critical role in safeguarding against breaches and other security threats. Establishing and maintaining a strong security culture requires identifying and promoting factors that encourage secure behavior and facilitate its transition into a broader organizational culture. Among these factors is the role of usability in security practices. Individual perception and interaction with security solutions and measures can significantly affect the effectiveness of security systems [11,12]. Although extensive research has investigated usable security and organizational security culture independently, fewer studies have explicitly integrated usable security as a foundational component of security culture. This gap underscores the need to investigate how usability factors can influence and strengthen organizational security cultures. Informed by existing evidence indicating that usability barriers undermine security compliance, the following hypotheses were developed:

H1: *There will be a positive correlation between users' perception of usable security measures and their behavior towards unusable security measures within the organization.*

H2: *A positive perception of usable security is negatively associated with the frequency of reported incidents of bypassing security measures.*

H3: *Ease of understanding and performing security actions predicts users' confidence with security policies within organizations.*

H4: *Ease of understanding and performing security actions is negatively associated with the frequency of reported security incidents.*

H5: *Organizational support and policies promoting reporting usable security issues positively influence employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches.*

This study examines the interplay between usable security and security culture and proposes a Usability-focused Security Culture Framework (USCF) that emphasizes usability as a foundational element to enhance security behaviors and foster a more positive security culture. By establishing a framework to foster a robust security culture, organizations can overcome usability barriers that might otherwise hinder their development. It also ensures that cybersecurity measures are designed with human factors in mind by aligning security and usability goals. This leads to more usable and effective cybersecurity systems, which ensure that all employees' actions in the workplace support a strong security culture.

The remainder of this paper is organized as follows. The background section reviews the relevant literature on security culture and usable security. The methodology section outlines research design, including survey and interview methods and analytical approaches. Findings are then discussed, followed by the introduction of the proposed Usability-focused Security Culture Framework (USCF). The paper concludes with a sum-

mary of contributions, an acknowledgement of the study's limitations, and suggestions for future research directions.

2. Background

Security culture has become a crucial concept that helps enhance an organization's resilience to cybersecurity threats. It creates an environment where cybersecurity becomes a shared responsibility between employees and beyond technological solutions. Investigating security culture can help identify gaps, increase awareness, and encourage behaviors that mitigate risks. This section explores security culture and its influential factors to then identify the extent to which usable security has been considered in prior studies, uncover existing research gaps, and characterize the linkage between usable security and security culture.

2.1. Security Culture Definitions

It is essential to underline the definitions of security culture in order to establish a clear understanding of its scope and aspects. This will also ensure that efforts to enhance security culture are well-aligned and effective, as interpretations can vary based on the context. The definitions in this section were identified through searches of Google Scholar, the University of Nottingham's library database, and publications from authoritative industry bodies. Search terms included "security culture" definition, "information security culture" definition, "organizational security culture" definition, "cybersecurity culture" definition, and "IT security culture" definition. The definitions were selected to highlight the range of perspectives in the field, including academic conceptualizations and practitioners' viewpoints. Definitions focusing on technical security configurations were excluded, as the current study concerns the organizational human factors. Table 1 highlights selected definitions suggested in studies.

Table 1. Security Culture Definitions.

Source	Definition
Al Sabbagh and Kowalski [13]	"The way our minds are programmed that will create different patterns of thinking, feelings and actions for providing the security process"
AlHogail and Mirza [14]	"The collection of perceptions, attitudes, values, assumptions and knowledge that guide how things are done in the organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behavior in a way that preserving the information security becomes a second nature."
Carpenter and Roer [15]	"the ideas, customs and social behaviors that impact the security of your organization."
CPNI [16]	"the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security."
Da Veiga and Eloff [17]	"the attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organization's systems and procedures at any point in time."
Dhillon [18]	"The collection of human attributes such as behaviors, attitudes, and values that facilitate the protection of all the information in the organization"

Table 1. *Cont.*

Source	Definition
ENISA [19]	“knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people’s behaviour with information technologies.”
Kraemer and Carayon [20]	“aspects of the organizational security philosophy that directly or indirectly affects the overall security of the network”
Mahfuth, et al. [21]	“an integration process of beliefs, perceptions, attitudes, values, assumptions and knowledge that guide, direct and manage employees’ perceptions and attitudes to influence employees’ security behavior or to find an acceptable behavior for employees when they are interacting with the information assets in their organizations”
Malcolmson [22]	“Security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organization, and behaviours they perform, which could potentially impact on the security of that organization, and that may, or may not, have an explicit, known, link to that impact.”
Martins and Elofe [23]	“the assumption about which type of information security behaviour is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organisation.”
Schlienger and Teufel [24]	“socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee”

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

2.2. Security Culture Influential Factors

Research addresses a variety of shared characteristics when investigating factors that have an impact on establishing and maintaining a strong security culture. As part of this study, a review of security culture influential factors was conducted in 2022. A literature search was conducted using Google Scholar and the University of Nottingham’s library database. Search terms included “security culture factors,” “information security culture factors,” “cyber security culture factors,” and “organizational security culture factors.” Studies published between 2010 and 2022 were included if they empirically investigated or proposed factors influencing security culture. A total of 22 studies met the inclusion criteria. Also, to ensure the relevance of these findings, a supplementary search was performed in 2025 using the same databases and search terms. No studies that substantially alter the conclusion drawn from the original review.

Factors were extracted through content analysis of each study’s findings. If a study used varying terminology for similar concepts, such as “management support” and “leadership commitment”, these were consolidated under a common label (i.e., management

and leadership support). Table 2 presents the influential factors and the total number of occurrences for each factor.

Table 2. Distribution of factors influencing security culture across studies.

Sources	ML	PP	AK	CM	RC	ET	Co	Be	TT	NC	Ac	EC	Tr	OS	Ct	SC	No. of Factors
Alfawaz, et al. [25]	✓	✓	✓			✓	✓					✓					6
AlHogail [26]	✓				✓		✓				✓	✓					3
AlHogail and Mirza [14]	✓			✓		✓											3
AlHogail and Mirza [27]	✓				✓		✓			✓	✓	✓					6
AlKalban et al. [28]					✓												1
Cruz [29]			✓														1
D’Arcy and Greene [30]							✓		✓						✓		3
Da Veiga [31]	✓	✓	✓	✓													4
Da Veiga and Eloff [17]	✓	✓		✓				✓									4
Da Veiga, et al. [32]	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓				10
Evrpidou, et al. [33]	✓	✓	✓			✓	✓		✓							✓	7
Georgiadou, et al. [34]			✓					✓	✓				✓	✓			5
Hassan and Ismail [35]			✓	✓	✓			✓						✓			5
Hassan, et al. [36]	✓	✓	✓												✓		4
Ioannou, et al. [37]	✓	✓					✓										3
Lopes and Oliveira [38]	✓		✓		✓	✓			✓						✓		6
Mahfuth, Yussof, Baker and Ali [21]								✓									1
Ruhwanya and Ophoff [39]	✓									✓							2
Sherif, et al. [40]	✓	✓	✓								✓						3
Tang, et al. [41]	✓	✓			✓		✓				✓						5
Tolah, et al. [42]	✓	✓		✓		✓						✓					5
Wiley, et al. [43]	✓		✓		✓				✓								4
Total No. of occurrences	16	10	11	6	8	6	6	5	6	3	3	3	2	2	3	1	

Note: ML = Management and leadership support; PP = Policies and Procedures; AK = Awareness and Knowledge; CM = Change Management; RC = Regulatory and Corporate Compliance; ET = Education & Training; Co = Communication; Be = Behavior; TT = Technical and Technological; NC = National Culture; Ac = Accountability; EC = Ethical Conduct; Tr = Trust; OS = Organization System (OS); Ct = Commitment; SC = Safety Culture.

The review identified sixteen influencing factors. These include management and leadership support, policies and procedures, awareness and knowledge, change management, regulatory and corporate compliance, education & training, communication, behavior, technical and technological, national culture, accountability, ethical conduct, trust, organization system, commitment, and safety culture. Figure 1 below presents the frequency with which each factor was discussed across the 22 studies reviewed. The count reflects the number of studies that identified an influencing factor, either as a primary finding or as a component of a framework.

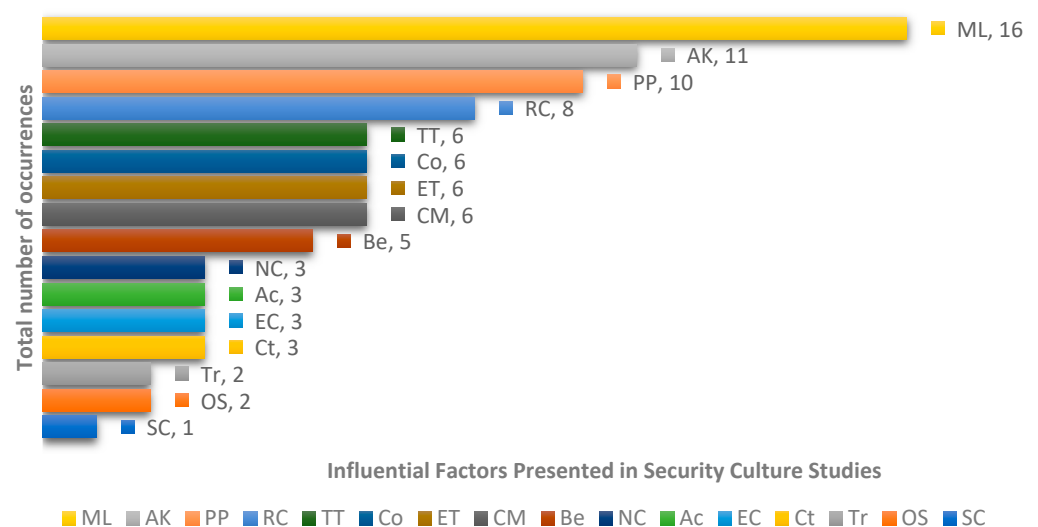


Figure 1. Frequency of factors influencing security culture across 22 studies (2010–2022).

Studies indicate that many factors influence security culture in organizations. A large number of studies emphasize the importance of top management and leadership support, as illustrated in Table 2. This support is arguably critical in enforcing and fostering other factors, such as increasing awareness and knowledge, applying policies and procedures, and complying with corporate governance [14,21,32]. Cybersecurity activities may not seem important without the support from top management; therefore, management must guide employees' security culture efforts and manage resources effectively [44]. Policies and procedures also appear in many papers as a vital factor. It is also worth noting that policies and procedures are frequently associated with users' awareness and knowledge, and the training programs organizations provide to their employees. For example, Chen, et al. [45] assert that security education, training, and awareness programs are key components that influence employees' understanding of organizational security policy and that the awareness will ultimately positively impact the overall security culture. By contrast, the lack of awareness and knowledge to implement the necessary policies and procedures might negatively impact the organization's security culture. However, despite top management's support for cybersecurity awareness and training programs, a recent study concludes that compliance is the primary driving factor while conducting awareness and training programs because regulations require businesses to provide regular cybersecurity awareness and training programs [46].

The remaining factors, like change management, communication, trust, and technological aspects, appear in multiple studies. Nevertheless, a further important implication is to consider all internal and external factors while establishing and maintaining a robust security culture, besides determining the degree to which the organization's security culture is dependent on each of them [32]. Notably, no study has directly stated the usability of security and addressed it as a factor influencing security culture, although a few studies identify usability as an integrated quality in other factors. For example, Furnell and Rajendran [47] emphasize that usability is an aspect that can enhance user behavior, Padayachee [48] asserts that usability increases the likelihood of compliance, and Hassan and Ismail [35] discuss how change management improves security through multiple elements, including usability. Although previous studies consider some aspects of usable security, no explicit connection has been identified between usable security and security culture.

2.3. Usable Security

There has been a significant development in technical security solutions that reduce security risks. However, these technologies do not provide sufficient protection against cybersecurity threats if users do not use them effectively. Usable security aims to design security systems and practices that take human capabilities and limitations into account. This enables users to perform security-related activities efficiently [4]. Usable security field developed from the understanding that security measures often fail not because of technical weaknesses but because of excessive cognitive and operational burdens on users [2]. When security measures are complex or difficult to understand and use, individuals may bypass them, leading to diminished overall security effort. Recognizing this, the "security by default" paradigm shifts responsibility from users to system designers in order to ensure products are delivered securely without requiring users' intervention [49].

Padayachee [48] suggests that usability enhances compliance likelihood, but Herley argues that users reject security practices when the perceived cost of compliance, including time, effort, and disruption of primary tasks, exceeds the perceived benefits for the user. This implies that non-compliance often arises from the users' rational cost-benefit assessments rather than negligence or malicious intentions. Furnell and Thomson [50] highlight the gap between security awareness and users' actual behavior, suggesting that

mere awareness of security is insufficient without corresponding usability improvements. In addition, Sasse [51] emphasizes that fear-based security communication is ineffective, as it causes anxiety without providing actionable guidance. More constructive approaches focus on designing security measures that align with users' tasks and mental models [3,52].

Recent research has extended these concepts to organizational contexts. Sasse [10] advocates a "reboot" of security awareness, focusing on how corporations can encourage and sustain good security behavior through positive reinforcement and usable security rather than compliance-driven instructions. Also, the emergence of remote and hybrid work has further highlighted the importance of usable security, since working remotely can introduce distinct challenges in maintaining secure practices [53–55].

Despite the substantial body of work, usable security has not been examined as a factor influencing organizational security culture. Some studies acknowledge usability as an attribute of other factors. For example, Furnell and Rajendran [47] note that usability can improve secure behavior, and Padayachee [48] suggests that usability enhances the likelihood of compliance. However, there is a lack of research that positions usability as a foundational element of security culture. This gap motivates the current study's investigation of the relationship between usable security and security culture.

Notably, usable security research has established that usability can improve security outcomes at the individual and system level, and security culture studies have identified various organizational factors that shape user behaviors. However, limited attention has been given to the intersection of these areas. In particular, no current framework explicitly positions usability as a foundational factor in fostering organizational security culture. This study addresses this gap by investigating the relationship between usable security and security culture and proposing a framework that integrates usable security considerations into organizational security culture development.

3. Methodology

3.1. Data Collection

This study received ethical approval from the University of Nottingham (application reference number CS-2022-R32). The study designed data collection methods to gather insights based on people's cybersecurity experiences and how usability influences their behavior in managing it within their organizations. This involved conducting a survey study with 203 participants, followed by semi-structured interviews. The goal of combining these methods is to strengthen the study's conclusions [56]. All participants provided informed consent prior to their engagement in the study. Survey participants consented electronically before proceeding, and interview participants provided verbal consent. Data was stored securely and anonymized during analysis to ensure the protection of participant confidentiality. Both the survey and semi-structured interviews were utilized to measure the extent to which the usability of security influences security culture.

3.1.1. Survey Design and Implementation

The survey was designed to collect participants' perceptions of usable security measures and their relationship to organizational security culture. Given that existing instruments do not specifically address the role of usable security in shaping security culture, the survey was developed from the ground up rather than adapting existing instruments. The survey was administered via Jisc Online Survey (JOS) and consisted of 25 items, organized into five sections. The complete survey instrument is provided in Appendix A.1.

The first section collected participants' demographic information (i.e., age, gender, educational background, job title, geographic location, and the organization's industry). The second section assessed participants' perceptions of security culture through Likert-

scale items and open-ended questions to evaluate how usable security and other factors influence security culture in their organizations. The third section focused on usable security, combining Likert-scale items with open-ended and closed-ended questions to explore participants' perceptions of usable security and its impact on their organizations. The fourth section also included a Likert-scale item and an open-ended question to determine how study participants assess the impact of usable security on their organization's security culture. The final section used multiple-choice and open-ended questions to identify the main drivers and barriers to people complying with cybersecurity practices in their organizations. To ensure uniform interpretation, participants were provided with definitions of the key terms:

- Cybersecurity usability issues are difficulties users encounter while using security-related tools or systems, such as lengthy security procedures that hinder productivity, confusing user interfaces, or difficulty remembering processes (e.g., complex passwords).
- Cybersecurity actions refer to user behaviors to safeguard systems and data, including regular software updates, strong passwords, data backup, and identifying suspicious emails or messages.
- Cybersecurity technologies encompass tools, software, and hardware solutions like firewalls, antivirus software, and encryption mechanisms protecting systems, networks, and data.
- Cybersecurity procedures include documented processes and guidelines addressing security risks and maintaining a proactive security posture, such as access control policies and security training and awareness sessions.

The survey aimed to obtain detailed insights into the perceptions of the usability of security measures within their workplace and a means of understanding the complex dynamics of security practices in the organization's settings. Also, several survey items were designed to operationalize the hypotheses presented in Section 1. For instance, Q16 items measured perceptions of usable security (independent variable for H1–H5), whereas Q14 items captured behavioral responses to difficult security actions (dependent variable for H1). Q15 assessed bypassing behavior (H2), and Q11 measured the participants' confidence in cybersecurity competence (H3, H5). The survey was estimated to take 8–10 min to complete.

3.1.2. Semi-Structured Interviews

Participants had the option to participate in the survey only by filling it out or in the survey and the interview by completing the survey and providing their contact details for a follow-up interview. The part involved follow-up interviews aimed at gaining deeper insight into users' behaviors and attitudes towards security usability in their workplace, identifying areas that could promote a positive security culture. Eighteen participants expressed interest in taking part in the interview part of the study, but only eight showed up and completed the interviews. The interview process started by revisiting noticeable parts from the open-ended responses to enable the participants to express their thoughts further. That was followed by an open-to-close question format, with questions encouraging participants to share their opinions and concerns openly. The semi-structured interview guide is provided in Appendix A.2. This planned yet customizable approach helps gather in-depth data [57], making semi-structured interviews an essential supplement to the survey discussed in the previous section.

3.1.3. Pilot Study

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

3.1.4. Participant Recruitment Techniques

The study utilized a combination of convenience sampling and snowball sampling techniques to recruit participants. It is worthwhile noting that convenience and snowball sampling are both valuable recruitment strategies in studies with limited resources and time. Convenience sampling, in which readily available and willing participants are selected, is practical and cost-effective, particularly in exploratory research phases or preliminary studies, since it requires minimal planning and expense [58]. As a further advantage, snowball sampling is particularly effective at engaging hard-to-reach populations using existing participants and networks. Hence, increasing engagement [59,60]. Furthermore, combining these sampling methods results in a more diverse and representative sample, allowing detailed data to be collected from individuals who might not be accessible with one of these methods alone [61,62].

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

Participants:

The study's 203 participants were drawn from a diverse population. The majority of respondents ($\approx 70\%$) were between the ages of 22 and 44, with a smaller representation from older groups. The participants' gender distribution was balanced (113 males, 89 females, and 1 other). Participants were generally educated; over 90% had a bachelor's degree or higher, 37% held a master's degree, and 19% a doctoral degree. Only a small proportion (6 participants) reported a disability affecting technology use. Professional responsibilities varied, though operational roles accounted for nearly half (49%), followed by managerial roles (29%) and senior leadership (9%). Organizations represented a wide range of industries, dominated by education (27%), IT (24%), and energy (12%), with additional representation from other industries, such as healthcare, finance, manufacturing, and others. Geographically, the majority of organizations were located in Europe (33%) and the Middle East (32%). North America (13%), Asia (9%), Africa (4%), Australia/Oceania (4%), and South America (3%) were also represented. Organization sizes ranged from small to large enterprises. However, 58% of participants came from organizations with 1000+ employees, with the remaining from mid-sized and smaller firms. A subset of the

respondents indicated willingness to participate in the second phase of the study. From this group, eight participants completed the follow-up interviews. Table 3 provides a summary of the interviews' participant demographics.

Table 3. Interviews participant demographics.

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

3.2. Data Analysis

As indicated in the data collection section, this study utilizes a mixed-method approach, integrating quantitative and qualitative methods to effectively evaluate the impact of cybersecurity usability on the overall security culture in organizations. Quantitative data acquired via a survey instrument were analyzed using statistical methods such as correlation and regression tests in the Statistical Package for the Social Sciences (SPSS) to test the study hypotheses and investigate the relationship between relevant variables derived from closed-ended survey questions. This mixed-method approach helps provide an in-depth perspective of the research topic by combining the breadth of the quantitative analysis and the depth of the qualitative interpretation.

3.2.1. Quantitative Data Analysis

The quantitative data obtained from the investigation process is analyzed using descriptive statistical analysis. This facilitates a comprehensive understanding of the data, the relationships identified through the research, and the significance of the results. The analysis included descriptive analysis of the survey responses and hypothesis testing. The five hypotheses were tested using appropriate statistical methods based on variable types and distributional properties, as shown in Table 4.

Table 4. Statistical tests for hypothesis testing.

Hypothesis	Independent Variable	Dependent Variable	Statistical Test
H1	Perception of usable security (Q16)	Security behaviors (Q14)	Spearman correlation; Multiple linear regression
H2	Perception of usable security (Q16)	Bypassing behavior (Q15; binary)	Mann–Whitney U test
H3	Ease of understanding/performing security (Q16a,b)	Confidence in compliance (Q11b)	Multiple linear regression
H4	Ease of understanding/performing security (Q16a,b)	Reporting difficulties (Q17; binary)	Logistic regression
H5	Organizational support for reporting (Q16f,g)	Confidence in identifying/reporting vulnerabilities (Q11c)	Multiple linear regression

For correlation analysis, Spearman's rank correlation was used where normality was violated. For regression, adjusted R^2 values indicate explained variance, and standardized coefficients (β) indicate relative predictor strength. Variance inflation factors ($VIFs < 5$, indicating no concern) were used to assess multicollinearity. Statistical significance was set at $\alpha = 0.05$.

3.2.2. Qualitative Data Analysis

Qualitative data from open-ended survey responses and interview transcripts were analyzed using reflexive thematic analysis following Braun and Clarke [63]'s six-phase approach:

Phase 1 (Familiarization): Interview recordings were transcribed, and all open-ended responses and transcripts were repeatedly read.

Phase 2 (Coding): Preliminary codes were generated throughout the dataset.

Phase 3 (Themes generation): Codes were aggregated into potential themes.

Phase 4 (Themes review): Themes were reviewed against coded extracts and the complete dataset.

Phase 5 (Themes definition): Themes were defined and named, and subthemes were also identified where applicable.

Phase 6 (Writing up): The conclusive analysis was generated with explanatory quotations from the study.

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

4. Results

4.1. Insights from the Quantitative Findings

4.1.1. Survey Findings

Cybersecurity Competence Confidence: While the study respondents reported high foundational knowledge and compliance confidence, there was a clear indication that additional focus is needed on identifying and reporting vulnerabilities. This aligns with prior research findings suggesting that knowledge alone does not ensure proactive security behavior [64].

Usability Challenges in Cybersecurity: Nearly half of the participants reported facing usability issues "very often" (10%) or "often" (35%), with an additional 35% reporting occasional issues, suggesting that usability challenges are prevalent across all organizational contexts.

Response to Unusable Cybersecurity Measures: The majority of respondents indicated that they would seek assistance from their colleagues when faced with challenging cybersecurity tasks. Nonetheless, 57% of participants expressed a high probability of finding a way around the action, 23% indicated that they would ignore security measures in order to complete broader tasks, and 28% of respondents indicated they would likely or very likely stop the task.

Bypassing Cybersecurity Measures: 30% of participants admitted to bypassing cybersecurity measures due to usability issues, while the other 70% reported never bypassing.

Agreement on the Usability of Cybersecurity Measures: A significant portion of participants feel that security actions are neither easy to understand (41% disagreed or strongly disagreed) nor easy to perform (43% disagreed or strongly disagreed). 46% of respondents feel that there is no balance between usability and security measures in their organizations. Also, the results showed that while mechanisms for reporting security incidents may already be in place, they could be improved in terms of accessibility or communication.

Reporting and Resolution of Cybersecurity Issues: There is a significant gap between how issues are reported and how they are resolved. Only 25% of participants reported cybersecurity concerns, and among them, 22% felt the issues were resolved satisfactorily. The large number of respondents who do not report issues is concerning, as it may indicate issues that are not being reported, which could result in unresolved security vulnerabilities. Even when issues are reported, a tiny fraction of respondents feel that they have been resolved satisfactorily.

Impact of Usable Cybersecurity on Organizational Culture: There is a strong consensus that usable cybersecurity has a positive impact on organizational security culture. The vast majority of respondents (89% combined strongly agree and agree) believe that usable cybersecurity would encourage them to make sensible decisions while adhering to security protocols. Also, 83% of respondents reported that they are more likely to report security issues if cybersecurity is made easier to use.

Cybersecurity Best Practice Motivators: The most frequently cited motivator for following cybersecurity best practices was finding them easy to perform, followed by management enforcement.

Cybersecurity Practice Adherence Barriers: The majority of participants believe that the complexity of cybersecurity measures and their lack of convenience are the main barriers, followed by insufficient management support and inadequate training.

4.1.2. Hypotheses Testing

Prior to conducting hypothesis testing, normality was assessed using Kolmogorov–Smirnov and Shapiro–Wilk tests. Both tests indicated significant deviations from normality for crucial variables ($p < 0.05$), which require nonparametric testing for correlation analyses (see Appendix B, Table A1).

H1: *There will be a positive correlation between users' perception of usable security measures and their behavior towards unusable security measures within the organization.*

H1 investigates the relationship between usability perceptions and security behaviors. Spearman's rank-order correlation revealed a statistically significant positive correlation between users' perceptions of usable security measures (Q16 mean) and their behavioral responses towards unusable security measures (Q14 mean), $r_s(199) = 0.179$, $p = 0.011$ (see Appendix B, Table A2). This suggests that higher perceptions of usability are associated with more positive security behaviors.

Furthermore, subgroup analysis by department reveals that the correlation between usability perceptions and security behaviors was significant for employees in non-IT/cybersecurity departments, but not for those in IT/cybersecurity roles (see Appendix B, Tables A3–A6).

To further examine the predictive relationship between usability perceptions and security behaviors, multiple linear regression was conducted. With security behaviors (Q14 items) as predictors and usability perceptions (Q16 mean) as the outcome, the model was statistically significant, $F(6, 184) = 4.745$, $p < 0.001$, explaining 10.6% of variance (Adjusted $R^2 = 0.106$). The significant predictors included "Stop the task as I can't complete the action"

($\beta = 0.197$, $p = 0.006$) and “Complain/report to the responsible person or team” ($\beta = 0.267$, $p < 0.001$). Variance inflation factors were below 5, indicating no multicollinearity concerns (see Appendix B, Table A7).

Also, the reverse model (usability perceptions (Q16 items) predicting security behaviors (Q14 mean)) was significant, $F(7, 155) = 2.524$, $p = 0.017$, Adjusted $R^2 = 0.062$. The significant predictor was “ease of reporting security issues”, ($\beta = 0.132$, $p = 0.005$) (see Appendix B, Tables A8 and A9).

H2: *A positive perception of usable security is negatively associated with the frequency of reported incidents of bypassing security measures.*

H2 looks into usability perceptions and bypassing behavior. Given violations of normality assumptions (Shapiro–Wilk $p = 0.009$) and the binary nature of the dependent variable, Mann–Whitney U tests were conducted. There was no statistically significant difference in the overall usability perception means between those who had bypassed (Yes) versus those who had not (No) ($p = 0.093$). However, examining the individual items of the independent variable revealed two items with significant differences: “I feel that the security actions in my organization strike a good balance between security and usability” and “My organization provides adequate support for employees to understand and perform effective security actions”. Participants who had bypassed security measures perceived less balance between security measures and usability (U test, $p = 0.045$) and felt less support for understanding and performing security actions in their organizational settings ($p = 0.041$) than those who had not bypassed (see Appendix B, Table A10). This suggests that perceived balance and organizational support may be protective factors against bypassing behavior.

H3: *Ease of understanding and performing security actions predicts users’ confidence with security policies within organizations.*

Multiple linear regression was conducted to investigate if the perceived ease of understanding and performing security actions predicted confidence in following cybersecurity requirements. The model was statistically significant, $F(2, 196) = 33.311$, $p < 0.001$, explaining 24.6% of variance (Adjusted $R^2 = 0.246$) (see Appendix B, Table A11).

“Ease of performing security actions” was a significant predictor, ($B = 0.301$, $\beta = 0.319$, $t = 2.623$, $p = 0.009$), indicating that employees are more likely to follow cybersecurity requirements when they can execute security measures easily. Ease of understanding approached but did not reach significance ($B = 0.187$, $\beta = 0.202$, $t = 1.665$, $p = 0.098$) (see Appendix B, Table A12). This suggests that promoting usable security practices can cultivate a positive security culture by making compliance more accessible and intuitive.

H4: *Ease of understanding and performing security actions is negatively associated with the frequency of reported security incidents.*

Logistic regression examined whether ease of understanding and performing security actions predicts reporting cybersecurity issues. Generally, the model was statistically significant, $\chi^2(2) = 7.722$, $p = 0.021$, correctly classifying 74.5% of cases. However, ease of understanding was not a significant predictor ($B = 0.398$, Wald = 2.049, $p = 0.152$), but ease of performing security actions was significant ($B = -0.706$, Wald = 5.962, $p = 0.015$, $\text{Exp}(B) = 0.494$) (see Appendix B, Tables A13–A15). This suggests that organizations should focus on enhancing the practical aspects of their security measures to reduce operational challenges.

H5: *Organizational support and policies promoting reporting usable security issues positively influence employees' confidence in identifying and reporting cybersecurity vulnerabilities or breaches.*

Multiple linear regression examined whether employees' confidence in identifying and reporting cybersecurity vulnerabilities was predicted by organizational support and policies promoting reporting issues. The model was statistically significant, $F(2, 170) = 11.738$, $p < 0.001$, explaining 11.1% of variance (Adjusted $R^2 = 0.111$) (see Appendix B, Table A16). Both predictors were significant:

Organizational policies promoting reporting ($B = 0.181$, $\beta = 0.168$, $t = 2.020$, $p = 0.045$), and organizational responsiveness to staff feedback ($B = 0.243$, $\beta = 0.232$, $t = 2.780$, $p = 0.006$) (see Appendix B, Tables A17 and A18). This indicates that organizational support for staff feedback and rules to promote reporting usable security issues increases employee confidence in identifying and reporting cybersecurity vulnerabilities. It means that proactive organizational actions motivate and encourage workers to respond to cybersecurity threats because actions such as communicating clear policies and providing useful training demonstrate a genuine commitment to security that employees perceive as achievable, thereby increasing their motivation to defend against threats. Organizations should promote policies that encourage communication about cybersecurity issues to increase employees' confidence and proactive behavior in managing cybersecurity risks. Table 5 summarizes the hypothesis testing results.

Table 5. Summary of hypotheses testing results.

Hypothesis	Test	Key Statistic	<i>p</i> -Value	Result
H1	Spearman correlation	$r_s = 0.179$	0.011	Supported
H2	Mann–Whitney U	—	0.093 (overall)	Partially supported *
H3	Multiple regression	Adjusted $R^2 = 0.246$	<0.001	Supported
H4	Logistic regression	$\chi^2 = 7.722$	0.021	Partially supported **
H5	Multiple regression	Adjusted $R^2 = 0.111$	<0.001	Supported

* Individual items (balance, support) showed significant differences ($p < 0.05$). ** Ease of performing (not understanding) was the significant predictor.

4.2. Insights from Qualitative Findings

4.2.1. Open-Ended Responses

Thematic analysis of responses in the open-ended section of the survey yielded three main themes, each comprising multiple subthemes as follows:

Theme 1: Usability Challenges in Cybersecurity

Subtheme 1.1: Bypassing due to usability issues. Participants reported many situations in which they had to bypass security measures. Most commonly, participants used colleagues' credentials when their own access was unavailable. For example, participants reported:

“Due to an access error, my credentials did not work as they should to generate a report I needed urgently. I asked a colleague for his credentials in order to complete the actions.”

“I had to send an attachment to my personal email so I can open it.”

Subtheme 1.2: Difficulties with cybersecurity technologies and procedures. Participants reported challenges across several categories:

- Authentication issues: Difficulties with multi-factor authentication, complex password requirements, and inconsistent login procedures across systems.
- Unclear reporting policies: Uncertainty about what to report and to whom.
- External device restrictions: Blocked USB ports and printer connectivity issues.

- General policy issues: Complex procedures, restricted email access, inflexible software approval, firewall restrictions, performance degradation from security tools, and disruptive updates. Comments from the participants include:

“I don’t like complicated processes or language. Also, it’s so annoying to read and follow long steps and then fail to solve the issue.”

“I had to disable 2FA in order to get an account to function properly.”

“I could not access my email as it was protected by two-step verification, and I did not have my phone at that particular time.”

Theme 2: Perceptions of Usable Security and Security Culture

Subtheme 2.1: Views on usable security. Participants emphasized that usability should be considered from early stages of security implementation:

“Security has to be considered early on in the development process, and it should be easy to use for everyone.”

“If you introduce very complex cybersecurity procedures, you need to provide support, knowledge, and training.”

Subtheme 2.2: Relationship between usable security and security culture. Participants recognized the link between usability and cultural outcomes:

“To have strong security culture, it’s important to consider usable security and make it clear and easy to understand.”

“Ensuring ‘usable cybersecurity’ . . . should encourage good cybersecurity habits and discourage workarounds—which could lead to a ‘healthier’ cybersecurity culture.”

Theme 3: Recommendations for Improvement

Participants offered practical recommendations across five subthemes:

Subtheme 3.1: Improving reporting and support. Participants called for dedicated reporting systems and simplified processes:

“Single sign-on for various web services/pages. . . For reporting, the IT department wants you to fill out a long form, which dissuades people from reporting.”

Subtheme 3.2: Simplicity over complexity. There was consensus that cybersecurity measures must be simplified:

“Make it simple, more will follow.”

Subtheme 3.3: Consideration of human factors. Participants emphasized designing for people, not just accounts:

“People often equate usability with user interfaces. . . But the fundamental issue here is that security to date deals with accounts and user IDs. Until we can make it work for a person, all the user interface and experience improvements will mean little.”

Subtheme 3.4: Collaborative effort. Participants highlighted the need for cross-departmental collaboration:

“There is often a disconnect between the perceived ease of usability of security actions and the technical know-how of the end user.”

Subtheme 3.5: Continuous education and awareness. Participants emphasized ongoing training rather than one-time sessions:

“Continuing cybersecurity training and raising awareness during the year and not only one time.”

Table 6 summarizes the identified themes and subthemes from the open-ended responses part of the survey.

Table 6. Identified Themes and Subthemes of the Open-Ended Responses.

Themes	Subthemes
Theme 1—Usability Challenges in Cybersecurity	Subtheme 1.1—Bypassing cybersecurity technology or procedures due to usability issues to complete tasks Subtheme 1.2—Difficulties encountered while using cybersecurity technologies or following cybersecurity procedures, including: • Authentication issues • No clear policies for reporting security issues • External devices issues • Cybersecurity policy issues
Theme 2—Perceptions and Feedback on Usable Security and Security Culture	Subtheme 2.1—Views and Feedback on Usable Security Subtheme 2.2—Feedback relevant to the relationship between usable security and security culture
Theme 3—Recommendations for Improvement	Subtheme 3.1—Improving Reporting and Support Subtheme 3.2—Simplicity beats complexity Subtheme 3.3—Consideration of the Human Aspect of the Stakeholders Subtheme 3.4—Collaborative effort is needed Subtheme 3.5—Continuous Education and Awareness

4.2.2. Semi-Structured Interviews

Thematic analysis of eight semi-structured interviews identified five themes:

Theme 1—Usability Impact on Security Behavior

This theme focuses on user behavior and security measures. A security measure's effectiveness depends on its usability. Employees perceive security measures differently depending on a number of factors, including urgency, background, and level of security awareness. Even people with a high level of awareness will disregard these measures if they are not usable. When users encounter complex security measures that frustrate them and prevent them from completing their tasks efficiently, they often adopt unsafe workarounds, undermining the intended security controls. Further, most participants said their organization's procedures for reporting security incidents are unclear. However, they acknowledged that there are good policies that have positively changed employee behavior. One participant, who is a cybersecurity educator, noted: "I'm fully aware that I shouldn't share my credentials... I teach these stuff and yet, in reality, I had to do it on occasion in order to get something working or something done" (P1). Several participants indicated uncertainty about reporting procedures, with one stating they would "keep quiet" rather than report incidents to avoid blame (P6). However, participants also acknowledged positive examples, such as external email warning banners that reduced phishing susceptibility.

Theme 2—Usability Impact on Productivity

Participants consistently linked unusable security to reduced productivity:

"The lack [of usability] can hinder employee's productivity." (P7)

"Once we are scared [of security measures]... you are not as productive as you should be because the feeling of fear has already overtaken some part of yourself." (P6)

Implementing security measures can often interfere with essential tasks, which can lead to employee frustration and non-compliance. This suggests that participants felt that workplace security must support employee productivity rather than hinder it.

Theme 3—Training and Awareness

Effective security cultures are built on the foundation of informed users. In order to ensure that all employees remain informed about the latest security threats and can prevent those, tailored training is required for employees considering different educational

backgrounds and cultural contexts in order to ensure they understand and can contribute to cybersecurity efforts. Although participants did not explicitly articulate it, the author's analysis indicates that there should be a reward system for employees who take the initiative to protect their organization's information systems.

Theme 4—Regulations and Compliance

Regulations play a significant role in driving security practices within organizations. European participants frequently referenced GDPR, while P8 (United States) noted multiple regulatory frameworks, including HIPAA. Nevertheless, participants observed that usability is often not integrated into compliance efforts: "Usability things are not very well integrated because nobody bothers." (P6). The current regulations should, however, ensure that the usability aspect is taken into account to make it easier for individuals and organizations to comply. It is also imperative to include a method of collecting feedback from all stakeholders regarding their experiences and what they find difficult to adhere to.

Theme 5—Geographical and Cultural Impact

An organization's geographical location affects employee perceptions of security and how they interact with it. Many cultural norms, legal frameworks, and other factors can affect security and how people respond to it. In addition, specific challenges might affect cybersecurity's usability in certain areas but may not apply elsewhere. Participants from different geographical locations described how regional and cultural contexts shape their security practices. P3 described Estonia's integrated digital infrastructure as a model: "Whatever aspect you want to do. . . it's all hassle-free. . . I basically go through the police portal, and it's like a heartbeat." On the other hand, P1 described challenges in South Africa, including infrastructure issues (power outages affecting authentication) and varied technological literacy among students entering university. P2 also noted cultural variation in security attitudes among colleagues from different countries.

5. Synthesis of Findings

As evidenced by the key findings, usability barriers continue to hinder employees' cybersecurity compliance. The majority of employees (79%) seek assistance from colleagues when faced with unusable cybersecurity tasks instead of directly contacting the organization or seeking help from the responsible department. Also, the study demonstrates that while most employees attempt to work around security requirements by consulting their peers, 23% admit they will ignore them in order to complete their tasks, and 28% are likely to abandon the task altogether if security measures become a barrier. Considering this, it is apparent that usability issues must be addressed. Usability is not simply about creating easy measures, but it is about making security understandable and achievable so users can make informed decisions. When users understand why security is important and how to implement it effectively, compliance becomes second nature rather than a burden to avoid.

This section organizes the study's main findings into categories, identifying the types of usable security issues encountered. Each of the categories is followed by a solution. The solutions form mediating strategies that can help address usability barriers.

1. Communication

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

- There is a lack of confidence and proactive behavior in managing cybersecurity risks among employees.

Suggested solution: Effective Communication

Establishing clear channels for effective communication is essential to ensure that employees' concerns are addressed promptly and resolved satisfactorily. It is equally important to keep all employees well-informed about security policies and best practices, ensuring that every action by the employees is aligned with the organization's security goals. Effective communication fosters understanding, collaboration, and trust within an organization [65]. An organization's management has a significant role to play in developing effective communication, which in turn results in improved productivity [66] and increases employee confidence and proactive behavior.

2. Support

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

Suggested solution: Management Support

Top management must play a central role in shaping and reinforcing the cybersecurity culture within an organization [31–33,37,40,67]. A strong leadership commitment to certain practices or policies may lead employees to recognize their significance [68]. Conversely, if employees perceive that top management is unconcerned about a particular issue, they may disregard or overlook it despite its importance. The leadership of an organization must actively enforce and promote security initiatives in order to develop a robust security culture. This will ensure that all factors contributing to a secure environment are given a high priority. Employees should feel supported and valued when they report concerns or incidents. Employees must be confident that their feedback will be addressed sufficiently without fear of reprisal or shame. For example, a company where management visibly supports cybersecurity programs and fosters open communication about risks is likely to experience higher employee engagement. In contrast, organizations with leadership that downplays security concerns may experience greater neglect, such as employees who fail to report suspicious activity or ignore security incidents.

3. Training and Education

- Employees need training that specifically addresses their challenges, which include authentication difficulties, unclear reporting policies, problems with external devices, and issues with other cybersecurity policies.
- Employees feel that continuous training and education are essential to address security challenges while doing their work. In addition, there is a potential for training to develop users' security expertise, thereby reducing their susceptibility to usability barriers.

Suggested solution: Tailored Training

Everyone can realize the value of training, regardless of their role or position within the organization. However, if training programs do not address the employees' specific needs, they may be a waste of time and resources for both the employee and the company as a whole. This can also lead to a decrease in employees' acceptance of cybersecurity training [69]. Also, according to research, factors such as trust, apathy, regulatory control, and worry affect users' behavioral intention to adopt cybersecurity training [70]. It is important that organizations take into account such factors when developing cybersecurity

training programs. In general, organizations should adhere to best practices, which include delivering training programs at the right time and in the proper scope to maximize the benefits of training.

4. Organizational and Regional Culture

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

Suggested solution: Cultural Aligned Strategies

A company's regional and organizational cultures impact its employees' behavior in adhering to cybersecurity measures by influencing their perception of the importance of cybersecurity and how it is integrated into their daily routines. Research has shown that norms have a significant impact on how individuals behave within an organization [71,72]. As an example, in regions where collective responsibility and compliance are cultural norms, people may be more likely to see cybersecurity requirements as essential and be willing to comply with them. Alternatively, in cultures where individual autonomy is prioritized or security is not taken seriously, strict measures may be viewed as obstacles that reduce motivation to adhere to them. Furthermore, an organizational culture emphasizing cybersecurity awareness and aligning cybersecurity practices with employees' workflows encourages compliance. Integrating security protocols into existing workflows will ensure that security protocols do not hinder productivity. Thus, organizations should facilitate an engaging, culturally appropriate environment that emphasizes the benefits of cybersecurity for individuals and organizations. Specifically, organizations can motivate their employees to adopt necessary cybersecurity measures by focusing on usability and aligning security practices with their cultural context and day-to-day activities.

There is a profound interconnectivity between these mediating strategies when shaping an organization's cybersecurity posture. Effective communication helps to ensure that security practices are clearly understood, while management support reinforces security's importance throughout the organization and facilitates factors that make security more usable. Providing employees with tailored training that meets their specific needs ensures that educational material is relevant, and integrating cultural factors into security strategies warrants that security strategies are applicable to the region and organization. As a result, the combination of these strategies creates an environment that fosters positive cybersecurity behaviors. A summary of the proposed solutions that will serve as mediating strategies is shown in Figure 2. Nonetheless, reinforcing these behaviors at the right time is still essential by implementing a real-time intervention method. One effective way to achieve that is through cybersecurity nudges. While the mediating strategies address the main issues identified in the study, cybersecurity nudges function as a supplementary method to provide users with a timely means to make the right security decisions, ultimately leading to a more robust security culture. Incorporating nudges into the study aligns with its focus on usability by addressing the human factor in cybersecurity.

Nudge as a Supporting Theory

Nudge theory is derived from behavioral economics and is primarily applied to influence behavior. In general, a nudge (some studies refer to it as Choice Architecture) is a method that changes people's behavior without limiting their options or radically altering their incentives [73]. The nudge concept has been applied to many disciplines, including healthcare, education, business, and AI, to influence behavior [74–77]. In the context of the

human aspect of cybersecurity, nudges can be used to guide people's choices and behaviors through positive reinforcement, ensuring that security measures are designed to steer employees toward secure behavior without restricting them. Cybersecurity nudges can significantly impact improving organizational security postures, and they are effective in various contexts, such as increasing security awareness, reducing operational risk, improving decision-making, and changing behavioral patterns [78,79]. For example, organizations can integrate password meters with hints (e.g., suggestions of using passphrases or password managers) to make passwords usable yet robust and provide immediate feedback that nudges employees toward selecting stronger passwords that are easy to remember. Password meters can provide real-time visual input on password strength, which helps users to create strong passwords without the need to be involved in complex security rules.

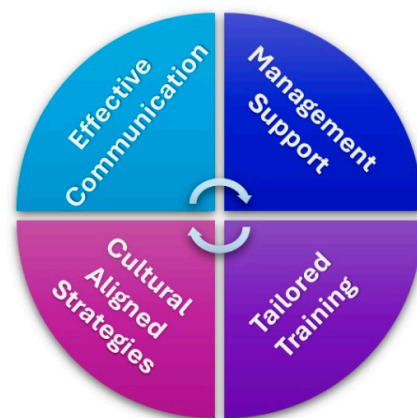


Figure 2. Mediating strategies.

6. Introducing a Usability-Focused Security Culture Framework

This study proposes a framework that provides a structured method for organizations to strengthen their security culture through a human-centric lens.

6.1. The USCF

The framework presented in Figure 3 focuses on prioritizing usability and strategically integrating mediating strategies and security nudges to effectively influence employee behavior, leading to a strong security culture.

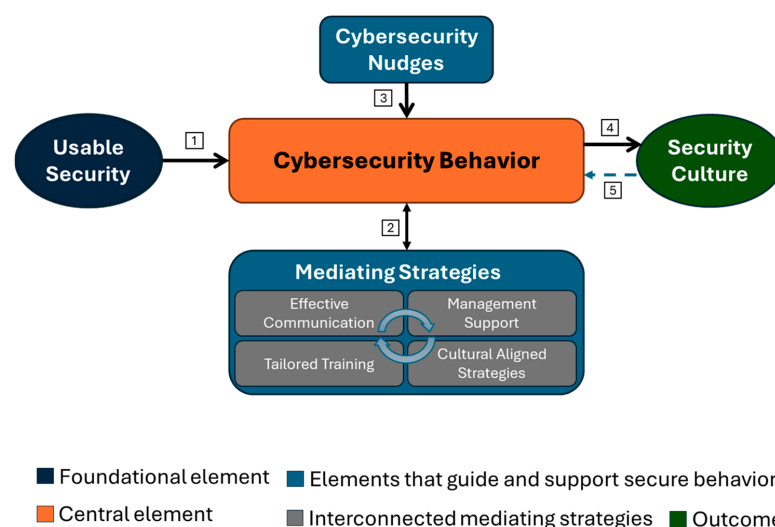


Figure 3. Usability-focused security culture framework. Stages 1-5 represent the numbers in the arrows. The arrow explanations are within the stages description.

- **Stage 1—Implementing Usable Security Mechanisms:** The first stage in operationalizing the framework focuses on implementing usable security. The objective of this stage is to ensure usable security measures (i.e., usability concepts are utilized to enable cybersecurity concepts). In this stage, usability must be prioritized to ensure that security mechanisms are intuitive for employees and easier to adopt in their day-to-day activities. Usable security has a direct and significant influence on cybersecurity behavior, meaning that regardless of their IT or security literacy, individuals in organizations are more likely to comply with security practices when they are easy to use and align with their regular workflows.
- **Stage 2—Devising and Adapting Mediating Strategies:** Mediating strategies are an essential component of the framework. In this stage, the strategies should not remain static; they should be continuously tailored and adapted to meet the organization's evolving needs and challenges. These strategies maintain a dynamic nature, ensuring employees are well-informed, supported, and trained to adhere to security best practices. There is a two-way relationship between mediating strategies and cybersecurity behavior; these strategies directly shape the actions of users, while feedback on employees' behavior can inform how these strategies are adjusted over time.
- **Stage 3—Introducing Security Nudges:** The introduction of security nudges is imperative to reinforcing secure behaviors. As the name implies, nudges are subtle prompts or reminders designed to assist in making secure decisions at critical moments without the feeling of being intrusive. This stage serves as a practical, real-time reinforcement that aligns employee behavior with cybersecurity requirements.
- **Stage 4—Cultivating Cybersecurity Behavior:** Upon implementing the components in the previous stages successfully, employees are able to improve their cybersecurity behaviors and comply with security practices. Over time, these behaviors contribute to the development of an organizational security culture. In this context, cybersecurity should not be viewed as a set of isolated activities but rather as an integral part of daily operations.
- **Stage 5—Reinforcing Security Culture:** Ultimately, security culture has a feedback effect on employees' cybersecurity behavior. When employees observe secure behavior embedded within the organizational culture, this collective adherence to security practices can reinforce their own cybersecurity actions and decisions.

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

6.2. Framework Implementation Guidelines

To implement the framework, there should be an initial assessment in order to understand how people within the organization behave around security practices. This concept is also supported by research [80–82] and also by some of the participants in the interview part of this study. For instance, P3, who has extensive experience in the cybersecurity industry, asserts that “the best course of action is to start with what people already know and are familiar with.” That would also help determine the pain points and what kind of

issues related to usability employees encounter. It is imperative to involve stakeholders early in the process to ensure alignment [83,84], and they acknowledge milestones to reinforce positive behavior among employees. A number of tools are available to evaluate the usability of organizational systems, including the System Usability Scale (SUS) [85], which is the most widely used measure of users' perception of usability and is likely to continue to be so for some time to come [86] and Google's HEART Framework [87], which measures user satisfaction, task success rates, and overall system efficiency. The Human-Computer Interaction (HCI) community has widely adopted such tools to identify usability issues and provide recommendations for improving users' experience. Next, it is recommended to refer to stages 1–4 to define clear objectives and develop a targeted action plan, considering the assessment results in the initial phase. The final stage is to implement the plan, and this is where the framework elements begin to engage actively.

After executing the plan, any wins, whether big or small, should be acknowledged to reinforce positive actions and sustain compliance. Various studies assert the value of acknowledging wins within organizations [88–90]. Moreover, the implementation plan involves ongoing feedback and reviews to maintain progress and identify any areas that require improvement. This study recommends the following approach for the feedback and improvement process:

1. Obtain employee feedback through appropriate channels (e.g., surveys, feedback forms, anonymous suggestion boxes) in order to gain insight into the usability of security measures.
2. Adjust and review measures as necessary:
 - Review security measures periodically based on feedback or changing emerging cybersecurity threats.
 - Maintain the usability of security tools and make iterative improvements as necessary.
3. Security Culture Review:
 - Conduct an annual security culture assessment to evaluate the progress against the initial objectives. This can be achieved by employing relevant existing tools and platforms, which (at the time of writing) would include but not be limited to those offered by providers such as KnowBe4, CybSafe, and the International Civil Aviation Organization.
 - Adjust objectives and the action plan based on the results of the review.

Figure 4 summarizes the framework implementation process.

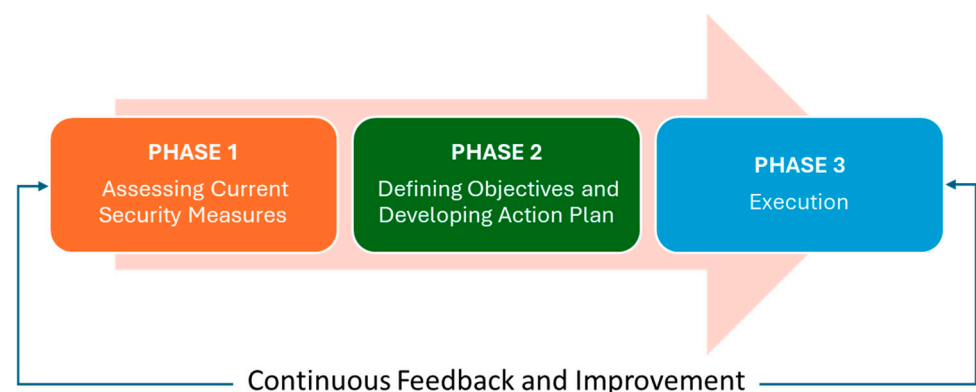


Figure 4. Framework Implementation Phases.

6.3. Framework Evaluation

This study combined participant feedback with expert review in order to offer a holistic view and robust evaluation process. While participants' feedback ensures the framework is relevant to end-users, expert reviews provide insights into real-world practice, ensuring that the framework aligns with the broader practices in cybersecurity and the impact of its usability. In addition, usable security and security culture intersect many aspects, including behavioral and organizational dimensions; therefore, combining feedback from experts and the study participants captures this diversity. The participants' educational background and experts' expertise add strength and enhance the credibility of the study output. With this in mind, the following sections illustrate the USCF evaluation process.

6.3.1. Evaluators Recruitment

The participants from the original study who completed both the survey and the interview ($n = 8$) and who serve as end-users of the framework were contacted to determine their willingness to take part in the evaluation process. This was ten to twelve months after their involvement, depending on when their original interviews occurred, though all were approached simultaneously for the evaluation stage. An email was sent, and six participants expressed interest in reviewing the framework and examining its relevance to their organizations' contexts. Additionally, a human-centered cybersecurity group, maintained by the NIST Human-Centered Technologies Group with expert members in the field, was invited to participate in the evaluation process. The purpose of inviting the experts was to obtain additional feedback from a second independent group that had not previously been exposed to the project but was considered collectively to have strong backgrounds in cybersecurity usability and culture. The experts were informed that, in the earlier phases of the study, surveys and interviews had been conducted to inform the framework's design and that this final evaluation process would ensure the framework's relevance and effectiveness. Additionally, since the experts were not part of the study from the outset, basic demographic information was collected to better understand their backgrounds and perspectives. This included gender, age range, highest level of education, organization size, and country. Three experts submitted complete feedback, bringing the total number of evaluators to nine: six from the earlier stages and three experts who joined at this final stage. Table 7 below illustrates the demographics of the evaluators.

Table 7. Evaluators Demographics.

Unique ID	Gender	Age Range	Highest Level of Education	Organization Size	Country
E1	Female	35–44	Doctoral	1000 or more	Saudi Arabia
E2	Male	25–34	Master's	1000 or more	Estonia
E3	Male	25–34	Master's	1000 or more	United Kingdom
E4	Female	35–44	Master's	50–249	Armenia
E5	Male	25–34	Doctoral	1000 or more	Finland
E6	Female	35–44	Doctoral	1000 or more	Sweden
E7	Female	35–44	Master's	1000 or more	United States
E8	Male	35–44	Master's	Less than 50	United Kingdom
E9	Male	52	Bachelor's	50–249	United States

6.3.2. The Evaluation Process

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

- **Framework Documentation:** This document introduced the framework, included a diagram of the framework and its components, and outlined its steps and phases. Each step was accompanied by a brief explanation of its purpose and activities. Also, a visual representation of the implementation phases was included to aid comprehension.
- **Explanatory Video:** A 10:32 min narrated slideshow with subtitles to explain the framework concept. The video covers an explanation of the framework's core concept and an overview of the phases involved in implementing the framework.

The evaluators were asked to provide general feedback, specifically regarding the practical value of the framework for organizations and any areas they believed required clarification or improvement.

6.4. Analysis and Reflection on the Evaluators' Feedback

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

- **Theme 1: Alignment with Key Issues and Practical Value**

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

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

- **Theme 2: Clarity and Presentation**

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

Response: Since some evaluators commented on the overall visualization of the framework, the visual design of the framework has consequently been enhanced to ensure that the shapes, boxes, and colors convey specific meanings. Figure 3 presents the resulting refined version of the framework. In addition, to help demonstrate how the USCF might be practically applied, three illustrative case studies are presented below. These are hypothetical scenarios designed to show how organizations across different sectors and sizes could implement the framework. The outcomes presented are based on the literature and practical application of usable security interventions (e.g., [91–94]) besides the findings from the current study, rather than empirical data from actual implementations.

WID Organization Industry: Finance Employee count: 50K	Case Study 1
Description/Challenge: The organization operates across Europe, North America, and the Middle East and adheres to NIST CSF, ISO, and CIS controls. The organization has a remote working policy and allows Bring Your Own Device (BYOD) practice, which adds to the challenges of ensuring compliance with security measures. Employees had difficulty adhering to password management policies despite following robust frameworks due to their complexity, which resulted in repeated credential-related breaches. As a result, the organization had to balance compliance with these controls with addressing usability issues that discouraged adoption.	
Objectives: The primary objective was to align the USCF with existing controls (NIST CSF, ISO, and CIS) in an effort to increase employee compliance with security measures and simplify security procedures without compromising compliance, especially in remote working and BYOD environments.	
Method(s) to Achieve the Objectives: Based on an initial assessment using the SUS and surveys, the organization discovered that employees reuse passwords due to complex policies, struggled with confusing BYOD guidelines, and encountered problems with remote access. As part of Stage 1 of the framework, the company introduced an integrated password manager with single sign-on (SSO) to address usability issues and simplified guidelines for BYOD. As part of Stage 2, the organization utilized mediating strategies, such as clear communication and tailored training for remote working policies, targeting employees who work remotely. In Stage 3, security nudges were deployed to offer employees timely guidance without overwhelming them, such as automatic password reminders and alerts when suspicious links are posted. By implementing these measures, cybersecurity behaviors were improved, password reuse was reduced, and secure procedures were adhered to more consistently. Employees were recognized for small achievements to reinforce positive engagement. In Stage 5, an embedded security culture is developed that is supported by regular reviews and feedback loops that facilitate the maintenance of momentum and relevance.	
Projected Results: The implementation of the USCF improved alignment with existing controls (e.g., complementing the existing NIST Protect and Identify functions) while also addressing the human aspect of security processes. Credential-related breaches decreased, and employee satisfaction with security tools improved. BYOD compliance also increased, ensuring consistent standards across personal and corporate devices. Employees become active participants in maintaining compliance, even in remote and flexible work environments, given that the security processes are intuitive and manageable. In turn, this created a more human-centric, robust security culture that balanced usability and security needs.	

NottsTele Industry: ICT Employee count: 150	Case Study 2
Description/Challenge: An Information & Communication SME based in Nottingham was frequently targeted by ransomware and phishing attacks. There was confusion around software patching responsibilities and the adoption of multi-factor authentication (MFA) among employees. The limited resources of the small organization made handling these threats more difficult.	
Objectives: A key objective was to simplify the implementation of the UK Cyber Essentials [95] strategies and to ensure that employees understood their role in mitigating security threats, in particular phishing attacks and ransomware attacks.	
Method(s) to Achieve the Objectives: Based on employee interviews and observations, a preliminary assessment revealed that employees felt MFA was overly complicated, resulting in long login delays and frustration. In addition, many users failed to update critical software patches due to unclear instructions on when and how to do so. The organization redesigned its MFA process by implementing a one-click tool that significantly reduced the time spent on authentication. The training sessions addressed common misconceptions about updates and provided concise guidelines regarding patching schedules and procedures. During team meetings, management and leadership stressed the importance of timely patching and helped desk support to address any onboarding hurdles. In order to further boost compliance, Security Nudge introduced creative and humorous interventions. For instance, employees were reminded of upcoming patch deadlines with playful graphics and humorous one-liners. The nudges reinforced the usability-centered measures and cultivated security habits by making critical security tasks more engaging. The employees' collective behavior shaped the company's culture, and every individual felt the responsibility of protecting the company.	
Projected Results: Employee behavior has been positively influenced by usability improvements and engaging nudges. The adoption rate of MFA increased, while the patching completion rate improved. In response to security threats, employees reported feeling more confident and proactive. As a result of this behavioral shift, the company was able to cultivate a proactive security culture, facilitating consistency and responsible behavior throughout the organization by making controls easier to use despite limited resources.	
University X Industry: Education Employee count: 20K	Case Study 3
Description/Challenge: A large university with international students, faculty, and staff required a robust security strategy to protect sensitive research data, personal information, and IT infrastructure. The university faced challenges resulting from the users' diverse cultural and professional backgrounds.	
Objectives: The main objective was to secure critical assets by improving secure access controls, which ensure encryption of sensitive data and foster a positive security culture across the university environment.	

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

Projected Results: As a result of improved communication and tailored interventions, encryption compliance rates increased. Also, management created a sense of accountability, reinforcing the importance of secure behavior. Consequently, faculty, staff, and students adhered to security practices consistently, which led to a positive security culture. This enabled individuals to protect critical assets proactively while maintaining academic and operational efficiency.

- **Theme 3: Scalability and Integration**

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

Response: The adaptability of the framework ensures that it can be applied in various organizational contexts. SMEs can utilize the framework by focusing on cost-effective tools and strategies, such as open-source security platforms and streamlined assessments. On the other hand, larger organizations can leverage advanced analytics or automation to tailor interventions to specific users or departments. As an example, multinational corporations may utilize behavioral analytics to detect anomalies in employee behavior and implement targeted training sessions or nudges to enhance the situation. In addition, since evaluators pointed out that the framework should align with the existing cybersecurity framework, it is important to note that the framework is intended to complement the existing cybersecurity frameworks by addressing the often-overlooked usability and human dimensions of security.

6.5. General Reflection

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

of the issues raised in the feedback have already been addressed in the full version, which provides detailed explanations of the framework and its implementation phases.

7. Conclusions

This study focused upon usable cybersecurity as an enabler for fostering a robust security culture. The influence of usable security on security culture has remained largely unexplored. Therefore, the primary aim of this research was to examine how cybersecurity usability influences security culture in organizations. This study integrated quantitative and qualitative data to understand how usable security measures influence security culture. Statistical analysis and hypothesis testing offer a basis for understanding trends and general attitudes, while a qualitative perspective offers valuable context into perceptions and experiences, facilitating a deeper understanding of concepts that cannot be expressed through numbers. The results of quantitative studies indicate that the usability of security measures is strongly associated with compliance behaviors. Employees adhere to security measures more often when they find them easy to understand and perform. These findings are further supported by qualitative insights that reveal specific cases of employees adhering to usable security measures or bypassing security measures due to usability issues, including complex authentication methods, difficulties using external devices, and unclear policies. The interpretation of the findings contributed to the development of a framework that promotes a positive security culture by integrating usable security principles with essential practices.

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

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

The mediating strategies, which are an integral part of the USCF, are intended to be dynamic and adaptable in order to address specific usability challenges. For instance, communication strategies should prioritize clarity and simplicity, presenting security policies and procedures in an accessible language and supplemented by visual aids such as infographics. Similarly, it is necessary to use tailored approaches; for example, the IT department may benefit from advanced security simulations, while the customer-facing teams may require practical training on how to secure client data. To ensure that these

strategies remain relevant and effective over time, organizations must incorporate regular feedback from employees. For example, an employee or a department may suggest that quarterly feedback sessions are more convenient than annual reviews since they allow for quicker adjustments to security measures.

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

As for the implementation phases, it is crucial to conduct an initial assessment of the security tools to understand how employees interact with them and identify usability issues. Usability testing can be used to validate the effectiveness of new tools before they are fully implemented or existing ones to identify usability issues. Also, during this phase, various methods are utilized to gather information about employee behaviors, pain points, and experiences. A number of tools can be used to conduct this assessment, including the SUS or the HEART Framework. In addition to usability testing sessions, observation methods can also be used to observe employees as they carry out security-related tasks, including logging into systems, for example, or identifying phishing emails. It is also possible to identify recurring challenges by reviewing security incident logs and employee feedback from prior training programs. For example, an employee who has difficulty remembering complex passwords may require solutions such as password managers or simple passphrase policies. Utilizing these tools and methods, one can generate actionable insights regarding usability barriers during the assessment phase.

8. Limitations of the Research

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

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

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

9. Directions for Future Work

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

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

Moreover, the increasing interest in human-AI interaction for enhanced security presents an opportunity for future research. AI could be a valuable addition by automating key elements of functionality based on a prior understanding of user preferences and behaviors, and augmenting the existing cybersecurity efforts. Integrating AI could enhance organizations' ability to create usable cybersecurity solutions that align with human workflows and promote a strong security culture. This could also simplify the user experience by reducing the need for explicit security-related interactions and decisions, therefore minimizing user fatigue and errors.

Author Contributions: Conceptualization, W.F. and S.F.; methodology, W.F.; validation, W.F.; formal analysis, W.F.; investigation, W.F.; resources, W.F. and S.F.; data curation, W.F.; writing—original draft preparation, W.F.; writing—review and editing, W.F. and S.F.; visualization, W.F. and S.F.; supervision, S.F. and C.W.; project administration, W.F.; funding acquisition, S.F. All authors have read and agreed to the published version of the manuscript.

Funding: No funding was received for this research.

Institutional Review Board Statement: The study was approved by the Ethics Committee of the University of Nottingham (Application Reference Number CS-2022-R32).

Informed Consent Statement: Informed consent was obtained from all participants involved in the study.

Data Availability Statement: The original contributions presented in this study are included in the article. Additional information and inquiries can be requested from the corresponding authors.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Appendix A.1. Survey Questionnaire



The Influence of Usable Security on Security Culture Survey

Welcome to our study

Information Sheet

This study aims to determine the potential influence of the usability of cybersecurity technologies and processes on organisational security culture. We are interested in gathering your insights based upon your own experiences of dealing with cybersecurity and how usability affects your behaviour while doing so.

This research will be conducted in two phases:

- In Phase 1, you are asked to complete this survey to help us understand your perceptions of the usability of cybersecurity and its impact on your organisation.
- Phase 2 of the research will involve a follow-up interview. This phase aims to help us understand users' behaviours and attitudes towards the usability of security in your workplace.

You can choose to participate in either Phase 1 only, by just filling in this questionnaire, or both Phases, by filling in this questionnaire and providing your contact details at the end so that we can contact you to arrange an interview.

Participating in the survey involves the use of an online data storage platform, but the collection process does not seek to gather any sensitive information about you or your organisation and so the risk is minimal. We will store the data collected, which is anonymised, on the OneDrive server of the University of Nottingham. If you choose to provide your contact information during Phase 1, it will solely be used to invite you to join Phase 2. The overall insights from both Phases will be used to help identify areas that

may promote positive security culture.

Also, to help understand the key terms used in this survey, we would like to provide some brief definitions for your reference:

- **Cybersecurity usability issues** are difficulties that users encounter while using security-related tools or systems. These can include issues such as lengthy security procedures that hinder productivity, confusing user interfaces, or difficulty remembering how to do things (e.g. complex passwords).
- **Cybersecurity actions** refer to user actions to safeguard systems and data, such as performing regular software updates, strong passwords, data backup, and identifying suspicious emails or messages.
- **Cybersecurity technologies** include tools, software, and hardware solutions such as firewalls, antivirus software, and encryption mechanisms that protect systems, networks, and data.
- **Cybersecurity procedures** include documented processes and guidelines that help address security risks and maintain a proactive security posture. This includes elements such as access control policies and security training and awareness sessions.

This study has been approved by the University of Nottingham's School of Computer Science Ethics Committee. The reference number for this approval is **CS-2022-R32**.

Wesam Fallatah

Wesam.Fallatah@nottingham.ac.uk

Consent to participate

As a participant in this study, you should...

- understand that your participation is voluntary
- understand the aims and objectives of the research
- understand what the research requires you to do
- accept the risks of participation
- understand what data will be collected and the purposes for which the data will be used
- understand safeguards will be put in place to protect your data and your legal rights
- understand that you will not be identified unless the use of identifiable data has been requested

- understand that you can withdraw at any time without explanation
- understand that once you have completed the study and submitted your answers, it will not be technically possible to withdraw the data

1. By clicking below, I confirm that I have read the above and consent to participate *
Required

☐ Yes

3 / 20

General information

About you

2. What is your age?

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65 or above

3. What gender do you identify as?

- ☐ Male
- ☐ Female
- ☐ Prefer not to say
- ☐ Other

3.a. If you selected Other, please specify:

4. Highest level of education completed:

- ☐ High school or less

4 / 20

- ☐ College/Diploma
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctoral degree
- ☐ Professional degree
- ☐ Other

4.a. If you selected Other, please specify:

5. Do you have any disabilities that impact your ability to use technology?

- ☐ Yes
- ☐ No
- ☐ Prefer not to say

5.a. Please specify:

6. What is your role/position in your organisation?

- ☐ Director / Executive / C-level role
- ☐ Managerial role (including supervisory and middle management)
- ☐ Operational role (including admin assistants, analysts, specialists, and technicians)
- ☐ Other

6.a. If you selected Other, please specify:

6.b. Please select what applies to you from the following:

- ☐ I work in the cybersecurity department
- ☐ I work in the IT department, including the cybersecurity team if applicable
- ☐ I work in a department other than the cybersecurity or IT department
- ☐ Other

6.b.i. If you selected Other, please specify:

About your organisation

7. What is the primary industry of your organisation?

- ☐ Healthcare and social assistance
- ☐ Information technology and communication
- ☐ Energy supply
- ☐ Water supply, waste management, and remediation services
- ☐ Education
- ☐ Finance and insurance
- ☐ Construction
- ☐ Manufacturing
- ☐ Agriculture
- ☐ Transportation
- ☐ Real estate/rental and leasing

- ☐ Arts, entertainment, and recreation
- ☐ Accommodation or food services
- ☐ Public administration
- ☐ Other

7.a. If you selected Other, please specify:

8. What is the geographic region of your organisation?

- ☐ North America
- ☐ South America
- ☐ Europe (including UK)
- ☐ Asia
- ☐ Middle East
- ☐ Africa
- ☐ Australia/Oceania
- ☐ Other

8.a. If you selected Other, please specify:

9. What is the size of your organisation (number of employees)?

- ☐ Less than 50
- ☐ 50-249

- ☐ 250-499
- ☐ 500-999
- ☐ 1000 or more

Security culture in the organisation

10. To what extent do you agree that shared attitudes, behaviours, and beliefs about cybersecurity within your organisation promote shared responsibility for maintaining cybersecurity?

- ☐ Strongly agree
- ☐ Agree
- ☐ Neutral
- ☐ Disagree
- ☐ Strongly disagree
- ☐ Don't know / unable to answer

11. How confident are you in

	Very confident	Confident	Neutral	Unconfident	Very unconfident	Don't know / unable to comment
Your understanding of cybersecurity principles and best practices	☐	☐	☐	☐	☐	☐
Following cybersecurity requirements in your organisation	☐	☐	☐	☐	☐	☐

Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace	☐	☐	☐	☐	☐	☐
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

12. Please feel free to offer any additional thoughts or feedback that you feel would be relevant to your organisation's security culture. *Optional*

Usability of cybersecurity

13. How often do you encounter usability issues while using cybersecurity technologies or following cybersecurity procedures in your organisation?

- ☐ Very often
- ☐ Often
- ☐ Occasionally
- ☐ Rarely
- ☐ Never

14. How likely would you do the following if you found a cybersecurity action difficult to perform

	Very likely	Likely	Neutral	Unlikely	Very unlikely	Don't know / unable to comment
Ignore it to complete my wider task	☐	☐	☐	☐	☐	☐
Stop the task as I can't complete the action	☐	☐	☐	☐	☐	☐
Try my best to perform the action and complete the task	☐	☐	☐	☐	☐	☐
Find my own ways around the action	☐	☐	☐	☐	☐	☐
Complain/report to the responsible person or team (e.g., my supervisor, the IT department, or the cybersecurity team)	☐	☐	☐	☐	☐	☐

Seek help from my colleagues



15. Have you ever had to bypass a cybersecurity technology or procedures due to usability issues?

☐ Yes

☐ No

15.a. Please describe the situation briefly:

Your answer should be no more than 1000 characters long.

16. To what extent do you agree or disagree with the following statements:

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Don't know / unable to comment
I feel that the security actions in my organisation are easy to understand	☐	☐	☐	☐	☐	☐
I feel that the security actions in my organisation are easy to perform	☐	☐	☐	☐	☐	☐

I feel that the security actions in my organisation strike a good balance between security and usability	☐	☐	☐	☐	☐	☐
I can easily report any potential security issues or breaches that I may come across	☐	☐	☐	☐	☐	☐
My organisation provides adequate support for employees to understand and perform effective security actions	☐	☐	☐	☐	☐	☐
My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures	☐	☐	☐	☐	☐	☐
My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously	☐	☐	☐	☐	☐	☐

17. Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?

- ☐ Yes
- ☐ No

17.a. Please explain the nature of the difficulty you encountered:

Your answer should be no more than 1000 characters long.

17.b. Have the difficulties been resolved to your satisfaction?

☐ Yes

☐ No

18. Please feel free to offer any additional thoughts or feedback that you feel would be relevant to the usability of cybersecurity in your organisation. *Optional*

Usable security and security culture

19. To what extent do you agree or disagree with the following statements:

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Don't know / unable to comment
Usable cybersecurity would encourage me to take sensible decisions while following cybersecurity requirements put in place	☐	☐	☐	☐	☐	☐
Usable cybersecurity would contribute to increased compliance with cybersecurity policies among my colleagues	☐	☐	☐	☐	☐	☐
The emphasis on following easy-to-use cybersecurity will make me more likely to report potential cybersecurity issues	☐	☐	☐	☐	☐	☐
The usability of cybersecurity will improve users' security behaviours in the organisation	☐	☐	☐	☐	☐	☐

The emphasis on the usability of cybersecurity will contribute to a stronger sense of responsibility for maintaining the security in my organisation	☐	☐	☐	☐	☐	☐
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

20. Please feel free to offer any additional thoughts or feedback relevant to the relationship between usable security and security culture. *Optional*

Measuring factors influencing security culture

21. What would be the main drivers for you to follow cybersecurity best practices in your organisation (please select all that apply)?

- ☐ Finding cybersecurity actions easy to perform
- ☐ Management and leadership enforcement
- ☐ Complying with the national regulatory or corporate requirement
- ☐ Understanding the risks associated with not following the best practices
- ☐ Attending more cybersecurity training courses
- ☐ Attending more security awareness sessions
- ☐ Other

21.a. If you selected Other, please specify:

22. What would prevent you from following cybersecurity best practices in your organisation (please select all that apply).

- ☐ Lack of convenience and the complexity of performing cybersecurity actions
- ☐ Lack of management and leadership support to comply with cybersecurity requirements
- ☐ Lack of cybersecurity training
- ☐ Lack of raising awareness for cybersecurity
- ☐ I think cybersecurity issues are the cybersecurity department's job. They should deal with them
- ☐ I cannot adopt the same security requirements in my own device as I do on the organisation's devices
- ☐ Nothing would

17 / 20

☐ Other

22.a. If you selected Other, please specify:

23. Do you have suggestions for how the usability of cybersecurity could be further improved in your organisation?

☐ Yes

☐ No

23.a. Please provide your suggestion(s) here:

24. Please feel free to offer any additional thoughts or feedback relevant to factors influencing security culture. *Optional*

Invitation to the 2nd part of the study

25. We are interested in following up to get further insights. If you would be willing to be contacted for an interview that would last ~20 minutes to discuss areas that may promote positive security culture in organisations, please type your email in the box below. If you are not interested, please feel free to click finish to end this survey. *Optional*

Thank you for taking part in the study!

Your contribution is valuable and appreciated.

If you have concerns or if you would like to view a summary of the results of this study, please email Wesam Fallatah at Wesam.Fallatah@nottingham.ac.uk

20 / 20

Appendix A.2. Semi-Structured Interview Guide

The planned duration for each interview is approximately 20 min.

The interview questions are built upon the participants' responses from the initial questionnaire to allow for more elaboration. In addition, the following questions were brought to the conversation:

- (a) Do you feel that cybersecurity usability issues affect your overall productivity and effectiveness in carrying out your day-to-day tasks?
- (b) Can you tell me if there are any specific cybersecurity actions or processes that you find more challenging than others due to issues related to usability? How would you suggest improving them?

- (c) Does management and leadership support affect the implementation of usable security measures? What actions have been taken or could be taken in this regard?
- (d) What strategies can be employed to effectively balance usability and cybersecurity measures in your organisation?
- (e) Do you believe the usability of cybersecurity measures impacts your ability (or your colleagues') to comply with security expectations or good practices?
- (f) Can you share an example from your organization where the usability of cybersecurity has positively or negatively impacted security culture?
- (g) Considering your organisation's geographical location, are there cultural or regional factors influencing security culture and the usability of cybersecurity? How can these factors be considered in improving security practices?

Appendix B. Statistical Output for Hypothesis Testing

Table A1. Normality test.

Tests of Normality						
	Kolmogorov–Smirnov ^a			Shapiro–Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Q14 MEAN	0.161	199	0.000	0.970	199	0.000
Q16 MEAN	0.074	199	0.009	0.981	199	0.009

a. Lilliefors Significance Correction.

Table A2. H1 (Q14 and Q16) correlation result.

Correlations				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	0.179 *
		Sig. (2-tailed)		0.011
		N	200	199
	Q16 MEAN	Correlation Coefficient	0.179 *	1.000
		Sig. (2-tailed)	0.011	
		N	199	202

*. Correlation is significant at the 0.05 level (2-tailed).

Table A3. Correlation of employees in cybersecurity dept.

Correlations ^a				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	−0.090
		Sig. (1-tailed)		0.293
		N	39	39
	Q16 MEAN	Correlation Coefficient	−0.090	1.000
		Sig. (1-tailed)		0.293
		N	39	39

a. Please select what applies to you from the following: = I work in the cybersecurity department.

Table A4. Correlation of employees in IT dept including cybersecurity (if applicable).

Correlations ^a				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	0.146
		Sig. (1-tailed)		0.153
		N	51	51
	Q16 MEAN	Correlation Coefficient	0.146	1.000
		Sig. (1-tailed)		0.153
		N	51	51

a. Please select what applies to you from the following: = I work in the IT department, including the cybersecurity team if applicable.

Table A5. Correlation of employees in departments other than the cybersecurity or IT Dep.

Correlations ^a				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	0.255 **
		Sig. (1-tailed)		0.007
		N	95	94
	Q16 MEAN	Correlation Coefficient	0.255 **	1.000
		Sig. (1-tailed)		0.007
		N	94	96

a. Please select what applies to you from the following: = I work in a department other than the cybersecurity or IT department. **. Correlation is significant at the 0.01 level (1-tailed).

Table A6. Correlation of employees who selected other.

Correlations ^a				
			Q14 MEAN	Q16 MEAN
Spearman's rho	Q14 MEAN	Correlation Coefficient	1.000	−0.523 *
		Sig. (1-tailed)		0.023
		N	15	15
	Q16 MEAN	Correlation Coefficient	−0.523 *	1.000
		Sig. (1-tailed)		0.023
		N	15	16

*, Correlation is significant at the 0.05 level (1-tailed). a. Please select what applies to you from the following: = Other.

Table A7. Correlation coefficients (dependent variable: Q16 Mean).

Coefficients ^a							
Model	Unstandardized Coefficients		Standardized Coefficients		t	Sig.	Collinearity Statistics
	B	Std. Error	Beta				Tolerance VIF
(Constant)	1.643	0.390			4.218	0.000	
Ignore it to complete my wider task (Scale reversed)	0.002	0.061	0.002		0.028	0.977	0.728 1.374

Table A7. *Cont.*

Coefficients ^a							
Stop the task as I can't complete the action	0.144	0.052	0.197	2.755	0.006	0.921	1.085
Try my best to perform the action and complete the task	0.008	0.071	0.009	0.114	0.909	0.843	1.186
Find my own ways around the action (Scale reversed)	0.077	0.062	0.099	1.231	0.220	0.722	1.384
Complain/report to the responsible person or team	0.209	0.058	0.267	3.629	0.000	0.872	1.147
Seek help from my colleagues	0.030	0.070	0.032	0.432	0.666	0.885	1.130

a. Dependent Variable: Q16 MEAN.

Table A8. Model summary of H1 with Q14's mean being the dependent variable.

Model Summary ^b									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	0.320 ^a	0.102	0.062	0.532	0.102	2.524	7	155	0.017

a. Predictors: (Constant): —I feel that the security actions in my organisation are easy to perform; —I feel that the security actions in my organisation are easy to understand; —My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously; —My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures; —I can easily report any potential security issues or breaches that I may come across; —I feel that the security actions in my organisation strike a good balance between security and usability; —My organisation provides adequate support for employees to understand and perform effective security actions. b. Dependent Variable: Q14 MEAN.

Table A9. Correlation coefficients (dependent variable: Q14 Mean).

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

a. Dependent Variable: Q14 MEAN.

Table A10. H2 test summary.

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

a. The significance level is 0.050. b. Asymptotic significance is displayed.

Table A11. Model summary of Q16's mean being the independent variable and Q11 the dependent variable.

Model Summary ^b									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change
1	0.504 ^a	0.254	0.246	0.907	0.254	33.311	2	196	0.000

a. Predictors: (Constant), I feel that the security actions in my organisation are easy to perform, I feel that the security actions in my organisation are easy to understand. b. Dependent Variable: Following cybersecurity requirements in your organisation.

Table A12. H3's correlation coefficients (dependent variable: cybersecurity compliance).

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

Dependent Variable: Following cybersecurity requirements in your organisation

Table A13. H4's prediction classification table.

Classification Table ^a				
Observed	Predicted			Percentage Correct
	Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?			
		Yes	No	
Have you reported any difficulties in using cybersecurity technologies or following cybersecurity procedures to the responsible person or team in your organisation?	Yes	0	51	0
	No	0	149	100
Overall Percentage = 74.5				

a. The cut value is 0.500.

Table A14. H4's model coefficients.

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

Table A15. H4's Variable in the Equation.

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

Table A16. H5's model summary.

Model Summary ^b									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	Change Statistics			
						F Change	df1	df2	Sig. F Change
1	0.348 ^a	0.121	0.111	1.147	0.121	11.738	2	170	0.000

a. Predictors: (Constant); —My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously; —My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures. b. Dependent Variable: Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace.

Table A17. Summary of H5's ANOVA test.

ANOVA ^a					
Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	30.909	2	15.455	11.738	0.000 ^b
Residual	223.819	170	1.317		
Total	254.728	172			

a. Dependent Variable: Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace. b. Predictors: (Constant); —My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously; —My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures.

Table A18. H5 A's correlation coefficients (dependent variable: identifying and reporting cybersecurity incidents).

Coefficients ^a					
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.397	0.254		5.489	0.000
1 My organisation has policies/initiatives to promote reporting any difficulties while using cybersecurity technologies or following cybersecurity procedures	0.181	0.090	0.168	2.020	0.045
My organisation takes staff feedback and concerns about cybersecurity technologies and procedures seriously	0.243	0.087	0.232	2.780	0.006

a. Dependent Variable: Your ability to identify and report cybersecurity vulnerabilities or breaches in the workplace.

References

1. Zimmermann; Verena; Schöni, L.; Schaltegger, T.; Ambuehl, B.; Knieps, M.; Ebert, N. Human-Centered Cybersecurity Revisited: From Enemies to Partners. *Commun. ACM* **2024**, *67*, 72–81. [\[CrossRef\]](#)
2. Adams, A.; Sasse, M.A. Users Are Not the Enemy. *Commun. ACM* **1999**, *42*, 40–46. [\[CrossRef\]](#)
3. Sasse, M.A.; Brostoff, S.; Weirich, D. Transforming the ‘Weakest Link’—A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technol. J.* **2001**, *19*, 122–131. [\[CrossRef\]](#)
4. Sasse, M.A.; Flechais, I. *Usable Security: Why Do We Need It? How Do We Get It?* O'Reilly: Springfield, MO, USA, 2005.
5. Herley, C. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In Proceedings of the 2009 Workshop on New Security Paradigms Workshop, Oxford, UK, 8–11 September 2009.
6. Rogers, R.W. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *J. Psychol.* **1975**, *91*, 93–114. [\[CrossRef\]](#)
7. Floyd, D.L.; Prentice-Dunn, S.; Rogers, R.W. A Meta-Analysis of Research on Protection Motivation Theory. *J. Appl. Soc. Psychol.* **2000**, *30*, 407–429. [\[CrossRef\]](#)
8. Davis, F.D. A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results. Doctoral Dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 1985.
9. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Q.* **2010**, *34*, 523–548. [\[CrossRef\]](#)
10. Sasse, M.A.; Hielscher, J.; Friedauer, J.; Buckmann, A. Rebooting It Security Awareness—How Organisations Can Encourage and Sustain Secure Behaviours. In Proceedings of the European Symposium on Research in Computer Security, Copenhagen, Denmark, 26–30 September 2022.
11. Parsons, K.; McCormac, A.; Butavicius, M.; Ferguson, L. *Human Factors and Information Security: Individual, Culture and Security Environment*; Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation: Edinburgh, Australia, 2010.
12. Ng, B.-Y.; Kankanalli, A.; Xu, Y.C. Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [\[CrossRef\]](#)
13. Al Sabbagh, B.; Kowalski, S. Developing Social Metrics for Security Modeling the Security Culture of It Workers Individuals (Case Study). In Proceedings of the 5th International Conference on Communications, Computers and Applications (MIC-CCA2012), Istanbul, Turkey, 12–14 October 2012.
14. AlHogail, A.; Mirza, A. Information Security Culture: A Definition and a Literature Review. In Proceedings of the 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia, 17–19 January 2014.
15. Carpenter, P.; Roer, K. *The Security Culture Playbook, An Executive Guide to Reducing Risk and Developing Your Human Defense Layer*; Wiley: Hoboken, NJ, USA, 2022.
16. CPNI. *Security Culture*; Centre for the Protection of National Infrastructure: London, UK, 2022. Available online: <https://www.cpni.gov.uk/security-culture> (accessed on 1 September 2022).
17. Da Veiga, A.; Eloff, J.H.P. A Framework and Assessment Instrument for Information Security Culture. *Comput. Secur.* **2010**, *29*, 196–207. [\[CrossRef\]](#)
18. Dhillon, G. *Principles of Information Systems Security: Texts and Cases*; John Wiley & Sons Incorporated: Hoboken, NJ, USA, 2007.
19. ENISA. *Cyber Security Culture in Organisations*; European Union Agency for Network and Information Security: Athens, Greece, 2017.
20. Kraemer, S.; Carayon, P. Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists. *Appl. Ergon.* **2007**, *38*, 143–154. [\[CrossRef\]](#)
21. Mahfuth, A.; Yussof, S.; Baker, A.A.; Ali, N. A Systematic Literature Review: Information Security Culture. In Proceedings of the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, Malaysia, 16–17 July 2017.
22. Malcolmson, J. What Is Security Culture? Does It Differ in Content from General Organisational Culture? In Proceedings of the 43rd Annual 2009 International Carnahan Conference on Security Technology, Zurich, Switzerland, 5–8 October 2009.
23. Martins, A.; Elofe, J. Information Security Culture. In *Security in the Information Society*; Springer: New York, NY, USA, 2002; pp. 203–214.
24. Schlienger, T.; Teufel, S. Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. In Proceedings of the 14th International Workshop on Database and Expert Systems Applications, Prague, Czech Republic, 1–5 September 2003.
25. Alfawaz, S.; Nelson, K.; Mohannak, K. Information Security Culture: A Behaviour Compliance Conceptual Framework. In Proceedings of the Information Security 2010: AISC'10 Proceedings of the Eighth Australasian Conference on Information Security [Conferences in Research and Practice in Information Technology], Brisbane, Australia, 19–20 January 2010; Volume 105.
26. AlHogail, A. Design and Validation of Information Security Culture Framework. *Comput. Hum. Behav.* **2015**, *49*, 567–575. [\[CrossRef\]](#)
27. AlHogail, A.; Mirza, A. A Proposal of an Organizational Information Security Culture Framework. In Proceedings of the International Conference on Information, Communication Technology and System (ICTS), Surabaya, Indonesia, 24 September 2014.

28. AlKalbani, A.; Deng, H.; Kam, B. *Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure*; RMIT University: Melbourne, Australia, 2015.
29. Cruz, R.M. Teleworking and Cyber Security in the Higher Education Institutions, Dominican Republic Case. *Int. J. Bus. Manag. Stud.* **2022**, *3*, 15–19.
30. D’Arcy, J.; Greene, G. Security Culture and the Employment Relationship as Drivers of Employees’ Security Compliance. *Inf. Manag. Comput. Secur.* **2014**, *22*, 474–489. [\[CrossRef\]](#)
31. Da Veiga, A. An Approach to Information Security Culture Change Combining Adkar and the Isca Questionnaire to Aid Transition to the Desired Culture. *Inf. Comput. Secur.* **2018**, *26*, 584–612. [\[CrossRef\]](#)
32. Da Veiga, A.; Astakhova, L.V.; Botha, A.; Herselman, M. Defining Organisational Information Security Culture—Perspectives from Academia and Industry. *Comput. Secur.* **2020**, *92*, 101713. [\[CrossRef\]](#)
33. Evripidou, S.; Ani, U.; Watson, J.D.M.; Hailes, S. Security Culture in Industrial Control Systems Organisations: A Literature Review. In Proceedings of the Human Aspects of Information Security & Assurance (HAISA), Mytilene, Greece, 6–8 July 2022.
34. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Working from Home During COVID-19 Crisis: ACyber Security Culture Assessment Survey. *Secur. J.* **2022**, *35*, 486–505. [\[CrossRef\]](#)
35. Hassan, N.H.; Ismail, Z. A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia-Soc. Behav. Sci.* **2012**, *65*, 1007–1012. [\[CrossRef\]](#)
36. Hassan, N.H.; Maarop, N.; Ismail, Z.; Abidin, W.Z. Information Security Culture in Health Informatics Environment: A Qualitative Approach. In Proceedings of the 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, Malaysia, 16–17 July 2017.
37. Ioannou, M.; Stavrou, E.; Bada, M. Cybersecurity Culture in Computer Security Incident Response Teams: Investigating Difficulties in Communication and Coordination. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019.
38. Lopes, I.; Oliveira, P. Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In *New Perspectives in Information Systems and Technologies*; Springer: Cham, Switzerland, 2014; Volume 1, pp. 277–286.
39. Ruhwanya, Z.; Ophoff, J. Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzania. In Proceedings of the International Conference on Social Implications of Computers in Developing Countries, Dar es Salaam, Tanzania, 1–3 May 2019.
40. Sherif, E.; Furnell, S.; Clarke, N. An Identification of Variables Influencing the Establishment of Information Security Culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*; Springer: Cham, Switzerland, 2015; pp. 436–448.
41. Tang, M.; Li, M.; Zhang, T. The Impacts of Organizational Culture on Information Security Culture: A Case Study. *Inf. Technol. Manag.* **2015**, *17*, 179–186. [\[CrossRef\]](#)
42. Tolah, A.; Furnell, S.; Papadaki, M. An Empirical Analysis of the Information Security Culture Key Factors Framework. *Comput. Secur.* **2021**, *108*, 102354. [\[CrossRef\]](#)
43. Wiley, A.; McCormac, A.; Calic, D. More than the Individual: Examining the Relationship between Culture and Information Security Awareness. *Comput. Secur.* **2020**, *88*, 101640. [\[CrossRef\]](#)
44. Uchendu, B.; Nurse, J.R.C.; Bada, M.; Furnell, S. Developing a Cyber Security Culture: Current Practices and Future Needs. *Comput. Secur.* **2021**, *109*, 102387. [\[CrossRef\]](#)
45. Chen, Y.; Ramamurthy, K.; Wen, K.-W. Impacts of Comprehensive Information Security Programs on Information Security Culture. *J. Comput. Inf. Syst.* **2015**, *55*, 11–19. [\[CrossRef\]](#)
46. Bada, M. *Stakeholder Analysis: Motives, Needs, and Drivers for Cybersecurity Awareness Training in Modern Work Environments*; AwareGO: Reykjavík, Iceland, 2022.
47. Furnell, S.; Rajendran, A. Understanding the Influences on Information Security Behaviour. *Comput. Fraud. Secur.* **2012**, *2012*, 12–15. [\[CrossRef\]](#)
48. Padayachee, K. Taxonomy of Compliant Information Security Behavior. *Comput. Secur.* **2012**, *31*, 673–680. [\[CrossRef\]](#)
49. CISA; NSA; FBI; ACSC; CCCS; CERT; NCSC-NZ; NCSC-UK; BSI; NCSC-NL; et al. Secure by Design. Available online: https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf (accessed on 4 February 2026).
50. Furnell, S.; Thomson, K.-L. From Culture to Disobedience: Recognising the Varying User Acceptance of It Security. *Comput. Fraud. Secur.* **2009**, *2009*, 5–10. [\[CrossRef\]](#)
51. Sasse, A. Scaring and Bullying People into Security Won’t Work. *IEEE Secur. Priv.* **2015**, *13*, 80–83.
52. Cranor, L.F. *Security and Usability: Designing Secure Systems That People Can Use*; O’Reilly Media, Inc.: Springfield, MO, USA, 2005.
53. Alotaibi, F.; Furnell, S.; He, Y. Cyber Security Awareness and Education Support for Home and Hybrid Workers. In Proceedings of the International Symposium on Human Aspects of Information Security and Assurance, Kent, UK, 4–6 July 2023.
54. Furnell, S.; Shah, J.N. Home Working and Cyber Security—an Outbreak of Unpreparedness? *Comput. Fraud. Secur.* **2020**, *2020*, 6–12. [\[CrossRef\]](#)

55. Whitty, M.T.; Moustafa, N.; Grobler, M. Cybersecurity When Working from Home During Covid-19: Considering the Human Factors. *J. Cybersecur.* **2024**, *10*, tyae001. [\[CrossRef\]](#)
56. Schoonenboom, J.; Johnson, R.B. How to Construct a Mixed Methods Research Design. *Koln. Z. Soziol. Sozialpsychol.* **2017**, *69*, 107.
57. Kvale, S.; Brinkmann, S. *Interviews: Learning the Craft of Qualitative Research Interviewing*; Sage: Thousand Oaks, CA, USA, 2009.
58. Emerson, R.W. Convenience Sampling Revisited: Embracing Its Limitations through Thoughtful Study Design. *J. Vis. Impair. Blind.* **2021**, *115*, 76–77. [\[CrossRef\]](#)
59. Naderifar, M.; Goli, H.; Ghaljaie, F. Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research. *Strides Dev. Med. Educ.* **2017**, *14*, 1–6. [\[CrossRef\]](#)
60. Valerio, M.A.; Rodriguez, N.; Winkler, P.; Lopez, J.; Dennison, M.; Liang, Y.; Turner, B.J. Comparing Two Sampling Methods to Engage Hard-to-Reach Communities in Research Priority Setting. *BMC Med. Res. Methodol.* **2016**, *16*, 146. [\[CrossRef\]](#)
61. Kirchherr, J.; Charles, K. Enhancing the Sample Diversity of Snowball Samples: Recommendations from a Research Project on Anti-Dam Movements in Southeast Asia. *PLoS ONE* **2018**, *13*, e0201710. [\[CrossRef\]](#)
62. Petersen, R.D.; Valdez, A. Using Snowball-Based Methods in Hidden Populations to Generate a Randomized Community Sample of Gang-Affiliated Adolescents. *Youth Violence Juv. Justice* **2005**, *3*, 151–167. [\[CrossRef\]](#)
63. Braun, V.; Clarke, V. Using Thematic Analysis in Psychology. *Qual. Res. Psychol.* **2006**, *3*, 77–101. [\[CrossRef\]](#)
64. Zwilling, M.; Klien, G.; Lesjak, D.; Wiecheteck, Ł.; Cetin, F.; Basim, H.N. Cyber Security Awareness Knowledge Behavior: A Comparative Study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97.
65. Aksoy, C. Building a Cyber Security Culture for Resilient Organizations against Cyber Attacks. *İşletme Ekon. Ve Yönetim Araştırmaları Derg.* **2024**, *7*, 96–110. [\[CrossRef\]](#)
66. Sadia, A.; Salleh, B.M.; Kadir, Z.A.; Sanif, S. The Relationship between Organizational Communication Employees Productivity with New Dimensions of Effective Communication Flow. *J. Bus. Soc. Rev. Emerg. Econ.* **2016**, *2*, 93–100. [\[CrossRef\]](#)
67. Hu, Q.; Dinev, T.; Hart, P.; Cooke, D. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decis. Sci.* **2012**, *43*, 615–660. [\[CrossRef\]](#)
68. Krajcsák, Z. Leadership Strategies for Enhancing Employee Commitment in Tqm. *J. Manag. Dev.* **2019**, *38*, 455–463. [\[CrossRef\]](#)
69. Kävrestad, J.; Fallatah, W.; Furnell, S. Cybersecurity Training Acceptance: A Literature Review. In Proceedings of the International Symposium on Human Aspects of Information Security and Assurance, Kent, UK, 4–6 July 2023.
70. Fallatah, W.; Kävrestad, J.; Furnell, S. Establishing a Model for the User Acceptance of Cybersecurity Training. *Future Internet* **2024**, *16*, 294. [\[CrossRef\]](#)
71. Posey, C.; Folger, R. An Exploratory Examination of Organizational Insiders' Descriptive and Normative Perceptions of Cyber-Relevant Rights and Responsibilities. *Comput. Secur.* **2020**, *99*, 102038. [\[CrossRef\]](#)
72. Ameen, N.; Tarhini, A.; Shah, M.H.; Madichie, N.; Paul, J.; Choudrie, J. Keeping Customers' Data Secure: A Cross-Cultural Study of Cybersecurity Compliance among the Gen-Mobile Workforce. *Comput. Hum. Behav.* **2021**, *114*, 106531. [\[CrossRef\]](#)
73. Thaler, R.; Sunstein, C. Nudge: Improving Decisions About Health, Wealth and Happiness. In Proceedings of the Amsterdam Law Forum, Online, 24 September 2008.
74. Ebert, P.; Freibichler, W. Nudge Management: Applying Behavioural Science to Increase Knowledge Worker Productivity. *J. Organ. Des.* **2017**, *6*, 4. [\[CrossRef\]](#)
75. Caris, M.G.; Labuschagne, H.A.; Dekker, M.; Kramer, M.H.H.; van Agtmael, M.A.; Vandenbroucke-Grauls, C.M.J. Nudging to Improve Hand Hygiene. *J. Hosp. Infect.* **2018**, *98*, 352–358. [\[CrossRef\]](#)
76. Möhlmann, M. Algorithmic Nudges Don't Have to Be Unethical. *Harv. Bus. Rev.* **2021**, *22*, 1–7.
77. Weijers, R.J.; de Koning, B.B.; Paas, F. Nudging in Education: From Theory Towards Guidelines for Successful Implementation. *Eur. J. Psychol. Educ.* **2021**, *36*, 883–902. [\[CrossRef\]](#)
78. ISACA. Nudging Our Way to Successful Information Security Awareness. Available online: <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-1/nudging-our-way-to-successful-information-security-awareness> (accessed on 10 August 2024).
79. Zimmermann, V.; Renaud, K. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Trans. Comput.-Hum. Interact. (TOCHI)* **2021**, *28*, 1–45. [\[CrossRef\]](#)
80. ICAO. Self Assessment Questionnaire. Available online: <https://www.2023.icao.int/Security/Security-Culture/ICAO%20SC%20Resources/Forms/AllItems.aspx> (accessed on 1 September 2022).
81. Pfadenhauer, L.M.; Gerhardus, A.; Mozygemba, K.; Lysdahl, K.B.; Booth, A.; Hofmann, B.; Wahlster, P.; Polus, S.; Burns, J.; Brereton, L. Making Sense of Complexity in Context and Implementation: The Context and Implementation of Complex Interventions (Cici) Framework. *Implement. Sci.* **2017**, *12*, 21. [\[CrossRef\]](#)
82. Nilsen, P.; Bernhardsson, S. Context Matters in Implementation Science: A Scoping Review of Determinant Frameworks That Describe Contextual Determinants for Implementation Outcomes. *BMC Health Serv. Res.* **2019**, *19*, 189. [\[CrossRef\]](#)
83. Voinov, A.; Bousquet, F. Modelling with Stakeholders. *Environ. Model. Softw.* **2010**, *25*, 1268–1281. [\[CrossRef\]](#)
84. Silva, L.M.d.; Bitencourt, C.C.; Faccin, K.; Iakovleva, T. The Role of Stakeholders in the Context of Responsible Innovation: A Meta-Synthesis. *Sustainability* **2019**, *11*, 1766. [\[CrossRef\]](#)

85. Brooke, J. Sus-a Quick and Dirty Usability Scale. *Usability Eval. Ind.* **1996**, 189, 4–7.
86. Lewis, J.R. The System Usability Scale: Past, Present, and Future. *Int. J. Hum.–Comput. Interact.* **2018**, 34, 577–590. [[CrossRef](#)]
87. Rodden, K.; Hutchinson, H.; Fu, X. Measuring the User Experience on a Large Scale: User-Centered Metrics for Web Applications. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA, USA, 10–15 April 2010.
88. Stajkovic, A.D.; Luthans, F. Behavioral Management and Task Performance in Organizations: Conceptual Background, Meta-Analysis, and Test of Alternative Models. *Pers. Psychol.* **2003**, 56, 155–194. [[CrossRef](#)]
89. Pinder, C.C. *Work Motivation in Organizational Behavior*; Psychology Press: London, UK, 2014.
90. Kotter, J.P.; Akhtar, V.; Gupta, G. *Change: How Organizations Achieve Hard-to-Imagine Results in Uncertain and Volatile Times*; John Wiley & Sons: Hoboken, NJ, USA, 2021.
91. Haney, J.; Lutters, W. Security Awareness Training for the Workforce: Moving Beyond “Check-the-Box” Compliance. *Computer* **2020**, 53, 91–95. [[CrossRef](#)] [[PubMed](#)]
92. Verizon. *2025 Data Breach Investigations Report*; Verizon: New York, NY, USA, 2025.
93. Kirlappos, I.; Beauteament, A.; Sasse, M.A. “Comply or Die” Is Dead: Long Live Security-Aware Principal Agents. In Proceedings of the International Conference on Financial Cryptography and Data Security, Okinawa, Japan, 1–5 April 2013.
94. Egelman, S.; Cranor, L.F.; Hong, J. You’ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy, 5–10 April 2008.
95. GOV.UK. Cyber Essentials Scheme. Available online: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (accessed on 30 September 2025).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.