

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
Δ.Π.Μ.Σ. ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ (ΜΒΑ)
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ



Cybersecurity Culture Maturity Index (CCMI): Evaluating Cultural Maturity Through the Lens of the Individual



Μπαλταγιάννης Νικόλαος (mba25038)

ΕΠΙΒΛΕΠΩΝ: Δρ. Βούζας Φώτης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΣΣΑΛΟΝΙΚΗ

2026

Table of Contents

Περίληψη	5
Abstract	6
1 Introduction	7
1.1 Background and Rationale	7
1.2 Research Objectives and Questions	8
1.3 Scope and Delimitations	9
1.4 Significance of the Study	10
1.5 Structure of the Dissertation	11
2 Literature Review	12
2.1 Foundations of Cybersecurity and Information Security	12
2.2 The Evolution of GRC: From Compliance to Strategic Enabler	13
2.3 Hybrid Work and the New Cybersecurity Landscape	15
2.4 Digital Wellbeing and Security Behavior	18
2.5 Leadership Competencies for Cyber GRC Professionals	19
2.6 HRM as a Driver of Security Culture	21
2.7 Human Factors in Cybersecurity Risk Management	23
2.8 Gaps in Current Literature and Future Research Directions	24
3 Research Methodology	26
3.1 Research Philosophy and Approach	26
3.2 Research Design: Individual-Level Strategy	26
3.3 Data Collection	27
3.4 Sample Selection and Recruitment	28
3.5 Data Analysis Techniques	29
3.6 Ethical Considerations	29
3.7 Limitations of the Methodology	30
4 Development of the Cybersecurity Culture Maturity Index (CCMI)	31
4.1 Conceptual Framework of the CCMI	31
4.2 Questionnaire Design	32
4.3 Scoring Model and Index Calculation	33

4.4	CCMI Application Examples	34
4.5	Validation Strategy.....	36
5	Data Analysis and Findings	37
5.1	Overview of Respondents	37
5.2	Descriptive Statistics and Reliability.....	39
5.3	Group Comparisons	41
5.4	Correlation Analysis	43
5.5	Analysis of Variance Across Groups	46
5.6	Principal Component Analysis	48
5.7	Cluster Analysis	50
5.8	Integrated Interpretation of Findings.....	51
5.9	Summary.....	52
6	Discussion	53
6.1	Revisiting the Research Questions.....	53
6.2	Interpretation of Key Findings	54
6.3	Theoretical Implications	55
6.4	Practical Implications	56
6.5	Limitations of the Study.....	58
6.6	Directions for Future Research	59
7	Proposed Framework	60
7.1	Purpose and Scope of the Framework	60
7.2	Design Principles	61
7.3	The Cybersecurity Culture Maturity Framework (CCMF)	62
7.4	Maturity Levels and Progression Pathways	63
7.5	Application Scenarios	64
7.6	Implementation Guidelines.....	66
7.7	Benefits and Strategic Value.....	67
8	Conclusions and Recommendations	68
8.1	Summary of the Study.....	68
8.2	Contributions to Knowledge.....	69
8.3	Recommendations for Organizations	70

8.4	Recommendations for Policymakers and Regulators	71
8.5	Final Reflections	72
9	Appendices	73
9.1	Appendix A: CCMI Questionnaire	73
	Bibliography	77

Περίληψη

Καθώς οι απειλές στον κυβερνοχώρο γίνονται ολοένα και πιο σύνθετες και διαδεδομένες, οι οργανισμοί καλούνται να υπερβούν τα τεχνικά μέτρα και τα πλαίσια συμμόρφωσης, ώστε να οικοδομήσουν ανθεκτικές στρατηγικές ασφάλειας. Κεντρικό στοιχείο αυτής της εξέλιξης αποτελεί η καλλιέργεια ώριμης κουλτούρας κυβερνοασφάλειας — μιας κουλτούρας που ενδυναμώνει τα άτομα, ευθυγραμμίζει τις οργανωσιακές αξίες με ασφαλείς συμπεριφορές και προσαρμόζεται στις απαιτήσεις της υβριδικής εργασίας και της ψηφιακής ευημερίας.

Η παρούσα μελέτη παρουσιάζει τον Δείκτη Ωριμότητας Κουλτούρας Κυβερνοασφάλειας (CCMI), ένα δομημένο εργαλείο αξιολόγησης που επικεντρώνεται στο άτομο και αποτυπώνει την ωριμότητα της κουλτούρας κυβερνοασφάλειας μέσα από πέντε βασικούς πυλώνες: Ηγεσία & Εμπιστοσύνη, Εμπλοκή Ανθρώπινου Δυναμικού, Ψηφιακή Ευημερία, Επίγνωση & Συμπεριφορά Ασφάλειας, και Ενσωμάτωση Υβριδικής Εργασίας. Με βάση ένα δείγμα 100 επαγγελματιών από διαφορετικούς τομείς και ρόλους, η έρευνα εφαρμόζει στατιστικές τεχνικές — όπως περιγραφική ανάλυση, πίνακες συσχέτισης, ανάλυση διακύμανσης (ANOVA), ανάλυση κύριων συνιστωσών (PCA) και ομαδοποίηση (clustering) — για να αναδείξει πρότυπα, αλληλεξαρτήσεις και προφίλ ωριμότητας.

Τα ευρήματα δείχνουν ότι η κουλτούρα κυβερνοασφάλειας αποτελεί ένα συνεκτικό και πολυδιάστατο φαινόμενο, με ισχυρές σχέσεις μεταξύ των πυλώνων και σημαντικές διαφοροποιήσεις ανάλογα με τα δημογραφικά και οργανωσιακά χαρακτηριστικά. Η μελέτη προτείνει επίσης το Πλαίσιο Ωριμότητας Κουλτούρας Κυβερνοασφάλειας (CCMF), ένα πρακτικό μοντέλο που μεταφράζει τα αποτελέσματα του CCMI σε τέσσερα επίπεδα ωριμότητας, προσφέροντας στους οργανισμούς έναν στρατηγικό χάρτη πορείας για αξιολόγηση, στοχευμένες παρεμβάσεις και συνεχή βελτίωση.

Τοποθετώντας την ατομική αντίληψη ως στρατηγικό πλεονέκτημα, η παρούσα έρευνα συμβάλλει στον εξελισσόμενο διάλογο για την ανθρωποκεντρική κυβερνοασφάλεια. Παρέχει θεωρητικές γνώσεις και πρακτικά εργαλεία για οργανισμούς που επιδιώκουν να καλλιεργήσουν κουλτούρες ασφάλειας που είναι συμπεριληπτικές, προσαρμοστικές και ανθεκτικές στον σύγχρονο ψηφιακό κόσμο.

Abstract

As cybersecurity threats become increasingly complex and pervasive, organizations must look beyond technical controls and compliance frameworks to build resilient security postures. Central to this evolution is the cultivation of a mature cybersecurity culture—one that empowers individuals, aligns organizational values with secure behaviors, and adapts to the realities of hybrid work and digital wellbeing.

This study introduces the Cybersecurity Culture Maturity Index (CCMI), a structured, individual-centric instrument designed to assess cybersecurity culture maturity across five key pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. Drawing on a sample of 100 professionals from diverse sectors and roles, the research applies statistical techniques—including descriptive analysis, correlation matrices, ANOVA, principal component analysis, and cluster segmentation—to uncover patterns, interdependencies, and maturity profiles.

Findings reveal that cybersecurity culture is a coherent, multidimensional construct, with strong interrelationships among its components and significant variation across demographic and organizational contexts. The study further proposes the Cybersecurity Culture Maturity Framework (CCMF), a practical model that translates CCMI results into four maturity levels, offering organizations a strategic roadmap for benchmarking, targeted interventions, and continuous improvement.

By positioning individual perception as a strategic asset, this research contributes to the evolving discourse on human-centered cybersecurity. It provides both theoretical insights and actionable tools for organizations seeking to foster inclusive, adaptive, and resilient security cultures in an increasingly hybrid and digitally intensive world.

1 Introduction

1.1 Background and Rationale

In recent years, the cybersecurity landscape has evolved far beyond the delivery of technical controls and the ticking-off of compliance checklists. As threats grow more complex and organizations become increasingly distributed—especially through hybrid and remote work—resilience now depends as much on people as on technology. Human-centered strategies, psychological safety, and cultural resilience have come to the fore alongside firewalls, incident-response plans, and governance frameworks. It is no longer sufficient to treat “culture” as an abstract, monolithic organizational attribute; each employee experiences, interprets, and enacts cybersecurity culture in their own way, shaped by their role, their work setting, and their organizational context.

This shift reflects a broader movement in cybersecurity research toward personalized risk awareness, behavioral analytics, and adaptive governance. By focusing on individual perceptions, the study aims to capture the nuanced ways in which leadership behaviors, HR practices, digital wellbeing, and hybrid-work dynamics combine to shape an employee’s sense of security and cultural maturity. To operationalize those insights, the research develops the Cybersecurity Culture Maturity Index (CCMI)—a structured instrument that records perceptions across five socio-technical pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration.

Unlike traditional culture models that require multiple voices from within the same organization and thereby impose an implicit consensus, the CCMI is designed to operate at the individual level. This makes comparative analysis possible across sectors, sizes, roles, and contexts without demanding intra-organizational unanimity. A single response per participant yields both personal insight and, when aggregated, an indirect view of organizational maturity—all while preserving the integrity of the individual voice. The CCMI thus delivers a scalable, inclusive, and empirically grounded tool that reflects the realities of modern work and the diversity of employee perspectives. It positions individual perception not as a limitation, but as a strategic asset in building resilient, human-centered security cultures.

As the thesis unfolds, it becomes clear that the study does more than invent and apply an index. Using data from 100 participants, later chapters explore descriptive patterns, interdependencies, and contrasts in the raw scores; test for differences across organizational and demographic groups; use principal component analysis to uncover underlying dimensions; employ clustering to reveal natural groupings of low, moderate, and high maturity; and interpret those results in light of existing theory. Chapter 7 goes further still, synthesizing the empirical insights into the Cybersecurity

Culture Maturity Framework (CCMF), offering a practical roadmap for interpreting CCMI results and planning concrete interventions. Chapter 6 teases out the theoretical and practical implications of what emerged, and Chapter 8 ties everything together with conclusions and recommendations.

1.2 Research Objectives and Questions

The primary objective of this research is to understand how individual employees perceive the maturity of cybersecurity culture within their organizational environments and to translate those perceptions into actionable insights. This study aims to move beyond abstract, top-down models of culture and instead capture the lived experience of employees—recognizing that culture is shaped and sustained through everyday interactions, perceptions, and behaviors.

To achieve this, the study sets out to:

- Design and validate a structured instrument—the Cybersecurity Culture Maturity Index (CCMI)—that reliably captures individual assessments across five key domains: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration.
- Identify patterns, strengths, and gaps in how cybersecurity culture is perceived across different roles, sectors, and organizational types.
- Examine whether and how these perceptions vary based on demographic and organizational factors such as company size, sector, tenure, gender, and the presence of formal HR or cybersecurity functions.
- Uncover latent dimensions within the data using principal component analysis, to better understand the underlying structure of cybersecurity culture maturity.
- Detect natural groupings of respondents through cluster analysis, revealing distinct maturity profiles that may benefit from tailored interventions.
- Develop a practical framework—the Cybersecurity Culture Maturity Framework (CCMF)—that translates CCMI results into strategic guidance for organizations seeking to benchmark, interpret, and improve their cybersecurity culture.

These objectives are addressed through the following research questions:

- How do individual employees perceive the maturity of cybersecurity culture in their organizations, and what does an aggregated view reveal about organizational readiness?

- Which cultural dimensions are most strongly associated with higher overall maturity, and how do they interrelate?
- Are there significant differences in cybersecurity culture perception across organizational types (e.g., small vs. large, public vs. private, with or without HR/CISO functions) or demographic groups (e.g., role, sector, tenure, gender)?
- What underlying dimensions or latent components emerge from the data, and what do they reveal about the structure of cybersecurity culture?
- Do natural clusters of respondents appear, suggesting distinct maturity profiles that call for differentiated strategies?
- Can the CCMI be applied as a diagnostic tool that informs organizational strategy and supports the development of a practical maturity framework?

1.3 Scope and Delimitations

This study focuses on the individual perception of cybersecurity culture maturity across diverse organizational contexts. Rather than evaluating the collective culture of a single organization, the research captures how employees personally assess the presence and effectiveness of cultural drivers such as Leadership, HRM Involvement, Digital Wellbeing, Security Behavior, and Hybrid Work Integration.

Each participant provides a self-assessment based on their experience within their current work environment. This approach enables comparisons across sectors, organizational sizes, and roles, without requiring multiple responses from within the same organization. It also allows for the aggregation of individual perceptions to form an indirect view of organizational maturity, while preserving the integrity of personal experience.

The scope includes professionals from both public and private sectors, spanning various functions such as Management, HR, IT/Security, or others. All participants are currently employed in one of three work arrangements: Hybrid, Remote, or Flexible On-Site (roles primarily on-site with occasional fieldwork or remote work when required), reflecting the evolving nature of digital work and its implications for cybersecurity culture. Organizational characteristics such as company size, sector, role, tenure, and the existence of key functions (e.g., CISO, HR department) are recorded and used as variables in the analysis to identify patterns and differences in perceived maturity.

The study does not aim to evaluate technical infrastructure, compliance documentation, or incident response capabilities. It also does not include longitudinal tracking or post-intervention evaluation. The data are cross-sectional and based entirely on self-reported perceptions, which, while valuable for capturing subjective

experience, are inherently limited by potential biases such as social desirability, recall error, or role-based visibility. These limitations are acknowledged and further discussed in Chapter 6.5.

1.4 Significance of the Study

As cybersecurity threats grow in number, sophistication, and unpredictability, it becomes increasingly clear that technical controls alone are not sufficient to ensure organizational resilience. A strong cybersecurity posture depends on a well-developed culture—one that empowers individuals, aligns shared values with security priorities, and adapts to the realities of hybrid work, digital fatigue, and organizational complexity.

This study contributes to that evolving paradigm in several important ways. First, it introduces the Cybersecurity Culture Maturity Index (CCMI), a validated instrument that operationalizes cybersecurity culture across five socio-technical domains: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. The CCMI captures individual-level perceptions, offering a scalable and inclusive method for assessing culture maturity in diverse organizational contexts.

Second, the study demonstrates that these five dimensions are strongly interdependent, and that maturity varies meaningfully across demographic and organizational factors. Through statistical analysis the research reveals that cybersecurity culture is not monolithic but multidimensional, context-sensitive, and shaped by individual experience.

Third, the study extends the boundaries of cybersecurity culture research by incorporating Digital Wellbeing and Hybrid Work Integration as core cultural dimensions. These areas are often overlooked in traditional models, yet the findings show they are integral to how employees perceive and engage with security practices in modern work environments.

Fourth, the research delivers both conceptual and practical value. Chapter 6 interprets the empirical findings in light of existing literature on socio-technical systems, leadership, HR practices, and human factors, offering new insights into how culture operates and evolves. Chapter 7 introduces the Cybersecurity Culture Maturity Framework (CCMF), a strategic model that translates CCMI results into maturity levels, progression pathways, and implementation guidelines. This framework equips organizations with a roadmap for cultural development, enabling them to move from reactive compliance to proactive resilience.

Finally, the study positions individual perception not as a limitation, but as a strategic asset. By listening to employees and understanding how they experience cybersecurity

culture, organizations can design more effective interventions, foster engagement, and build cultures that are not only secure but also inclusive, adaptive, and aligned with their mission.

1.5 Structure of the Dissertation

The dissertation is organized into eight chapters, each contributing to the development, application, and interpretation of the Cybersecurity Culture Maturity Index (CCMI) and the Cybersecurity Culture Maturity Framework (CCMF). The structure reflects a logical progression from theoretical foundations to empirical analysis and practical implementation.

- **Chapter 1** introduces the research context, rationale, objectives, and scope. It outlines the significance of measuring cybersecurity culture maturity through individual perception and sets the stage for the development of the CCMI and CCMF.
- **Chapter 2** presents a comprehensive literature review, covering the foundations of Cybersecurity, the evolution of Governance, Risk, and Compliance (GRC), the impact of Hybrid Work, Digital Wellbeing, Leadership competencies, HRM practices, and Human Factors in cybersecurity behavior.
- **Chapter 3** details the research methodology, emphasizing the individual-level application of the CCMI. It outlines the philosophical approach, data collection strategy, sample design, scoring models, and ethical considerations, along with a discussion of limitations.
- **Chapter 4** describes the development of the CCMI, including its conceptual pillars, questionnaire design, scoring logic, and validation strategy. It explains how the index captures individual perceptions and supports comparative analysis across roles and organizational types.
- **Chapter 5** presents the data analysis and findings, including descriptive statistics, cross-group comparisons, correlation analysis, principal component analysis, cluster segmentation, and an integrated interpretation of results.
- **Chapter 6** offers a critical discussion of the findings, interpreting them in light of the research questions and existing literature. It explores theoretical and practical implications, acknowledges limitations, and proposes directions for future research.
- **Chapter 7** introduces the Cybersecurity Culture Maturity Framework (CCMF), translating CCMI results into a strategic model. It defines maturity levels, progression pathways, application scenarios, implementation guidelines, and the strategic value of the framework.

- **Chapter 8** concludes the study by summarizing key findings, outlining contributions to theory and practice, offering recommendations for organizations and policymakers, and reflecting on the broader significance of the research.

This structure supports a coherent and methodologically transparent exploration of cybersecurity culture maturity, grounded in individual experience and designed to inform both academic inquiry and professional practice.

2 Literature Review

2.1 Foundations of Cybersecurity and Information Security

The conceptual distinction between cybersecurity and information security has long been a subject of academic debate, yet it remains foundational for understanding the broader landscape of digital protection. Information security refers to the safeguarding of data in all its forms—digital, physical, or verbal—ensuring its confidentiality, integrity, and availability (Humphreys, 2008; Taherdoost, 2022). Cybersecurity, on the other hand, focuses specifically on the protection of digital systems, networks, and infrastructures from unauthorized access, disruption, or destruction (Craig et al., 2014; van Niekerk, 2013; Bay, 2016). While the two domains share common principles, their operational scope and strategic implications differ significantly.

The CIA Triad—confidentiality, integrity, and availability—has traditionally served as the cornerstone of both fields. However, van der Ham (2021) critiques its binary interpretation, arguing that it oversimplifies the complexity of modern risk environments. For instance, restoring confidentiality through a technical patch may not address the underlying systemic vulnerability, leading to reactive rather than strategic security postures. This critique aligns with the broader shift toward resilience-focused frameworks, such as the NIST Cybersecurity Framework (CSF), which emphasizes continuous functions—Identify, Protect, Detect, Respond, and Recover—over static controls (van der Ham, 2021; Humphreys, 2008).

ISO/IEC standards provide structured guidance for implementing security controls and aligning organizational practices with global expectations. ISO/IEC 27001 remains the most widely adopted standard for information security management systems (ISMS), while ISO/IEC 27032:2012 offers a definition of cybersecurity as the “preservation of the confidentiality, integrity, and availability of information in cyberspace” (Taherdoost, 2022). This distinction is illustrated through practical examples: a physical data breach constitutes an information security incident, whereas a social media leak of the same data falls under cybersecurity.

Scholars have attempted to define cybersecurity in ways that reflect its multifaceted nature. Craigen et al. (2014) describe it as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.” This definition highlights the strategic and institutional dimensions of cybersecurity, extending beyond technical defense to include governance, legal frameworks, and adversarial engagement between humans and machines. Similarly, van Niekerk (2013) emphasizes the protection of digital identities, behaviors, and interactions, noting that cybersecurity encompasses personal privacy, digital rights, and national infrastructure.

The socio-technical framing of cybersecurity is further reinforced by ISO’s definition of cyberspace as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form” (Bay, 2016). This perspective underscores that cybersecurity is not merely a technical function but a dynamic construct shaped by human behavior, infrastructure, and systemic interdependencies.

Historical perspectives also enrich our understanding of information security. Alexei & Alexei (2023) trace cryptographic practices back to 400 BC, when Spartans used the scytale for secure military communication. This long-standing tradition illustrates that the protection of information has always been a strategic concern, evolving alongside technological and societal developments.

As digital ecosystems grow in complexity, the convergence of cybersecurity and information security calls for integrated approaches that address both technological and organizational dimensions. Knapp et al. (2006), Veiga & Eloff (2002), and Schlienger & Teufel (2003) argue that security strategies must evolve to encompass not only system-level protections but also cultural, behavioral, and governance factors. This includes fostering a security-conscious organizational culture, aligning leadership with risk management priorities, and embedding compliance into everyday operations.

Ultimately, the transition from reactive defense to proactive resilience requires a shift in mindset—one that views security not as a technical constraint but as a strategic enabler of trust, continuity, and innovation. This foundational understanding sets the stage for exploring how governance, leadership, HRM, and digital wellbeing contribute to the development of a resilient cybersecurity culture in hybrid work environments.

2.2 The Evolution of GRC: From Compliance to Strategic Enabler

Governance, Risk Management, and Compliance (GRC) have evolved significantly over the past two decades, transitioning from a reactive compliance mechanism to a strategic enabler of organizational resilience and cybersecurity maturity. Initially perceived as a set of regulatory obligations, GRC frameworks now serve as

foundational structures for aligning security practices with business objectives, fostering accountability, and embedding a culture of continuous improvement (Mira da Silva, 2011; Handoko et al., 2020; Papazafeiropoulou & Spanaki, 2015).

Governance provides the strategic compass of an organization, guiding decisions through leadership structures, ethical standards, and transparent policies. Risk management, in turn, enables organizations to anticipate and mitigate threats—ranging from financial uncertainty to cyber incidents—through proactive assessment and cross-functional collaboration. Compliance ensures adherence to legal and regulatory standards, protecting organizations from penalties and reputational damage while reinforcing integrity and trust (Humphreys, 2008; Nicho et al., 2017).

Mira da Silva (2011) defines integrated GRC as a holistic approach that aligns strategy, processes, technology, and people to ensure principled performance. Fragmented GRC practices—often siloed across departments—can undermine transparency and decision-making. To address this, organizations must embed GRC responsibilities into core business units, shifting from isolated compliance efforts to enterprise-wide governance models.

Among the most influential frameworks shaping modern GRC are the ISO/IEC 27000 series and the OCEG GRC Capability Model. ISO/IEC 27001, in particular, offers a structured methodology for implementing and continuously improving information security management systems (ISMS), integrating people, policies, and technologies to manage risk and support operational excellence. Its alignment with GDPR further reinforces its relevance in data protection and legal accountability (Humphreys, 2008; Taherdoost, 2022).

The OCEG model promotes a dynamic view of GRC, defining it as “the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty, and act with integrity.” This perspective encourages organizations to treat GRC not as a compliance checklist but as a strategic capability that interacts with every team and process across the enterprise (Papazafeiropoulou & Spanaki, 2015).

Despite the growing adoption of GRC frameworks, many organizations face challenges in implementation. Common barriers include fragmented responsibilities, lack of executive engagement, and limited cross-functional coordination. Piggin (2014) highlights that in industrial environments, operational technology risks are often managed in isolation, creating gaps in security and oversight. Similarly, Papazafeiropoulou & Spanaki (2015) point to technical complexity, organizational unreadiness, and weak control frameworks as obstacles to effective GRC deployment.

Successful implementation requires mature internal structures, trained IT teams, and strong leadership to navigate conflicting priorities and vendor selection. Without these

elements, GRC solutions may fail to integrate effectively, increasing operational risk rather than reducing it. Humphreys (2008) emphasizes the importance of continuous risk assessment and monitoring, noting that insider threats—whether intentional or accidental—pose significant challenges that must be addressed through access controls, training, and incident response protocols.

The financial sector, as one of the most regulated and IT-dependent industries, has been a leading adopter of GRC frameworks. Humphreys (2008) reports that 90% of financial organizations have implemented or are considering IT GRC solutions. However, even in such environments, GRC is often presented in fragmented ways, making it difficult for non-specialists to grasp its strategic value. This underscores the need for simplified communication and cross-functional integration.

To overcome these challenges, organizations are encouraged to adopt integrated platforms, foster collaboration across departments, and invest in leadership development. A key success factor is the alignment of GRC initiatives with organizational culture and strategic priorities, ensuring that security and compliance are perceived not as external constraints but as enablers of performance and innovation (Nicho et al., 2017; Piggini, 2014).

In this context, digital governance becomes increasingly relevant. Papazafeiropoulou & Spanaki (2015) argue that GRC information systems must support not only compliance but also strategic alignment and organizational learning. This requires a shift from static rule enforcement to dynamic capability building, where GRC becomes embedded in decision-making and innovation processes.

Ultimately, the evolution of GRC reflects a broader transformation in how organizations approach cybersecurity and resilience. By integrating governance, risk, and compliance into strategic planning and cultural development, organizations can cultivate a proactive security posture that supports long-term sustainability and competitive advantage.

2.3 Hybrid Work and the New Cybersecurity Landscape

The rise of hybrid work has fundamentally reshaped the cybersecurity landscape, introducing new vulnerabilities and organizational complexities that extend beyond traditional perimeter-based models. Employees now operate across diverse environments—corporate offices, remote locations, and public spaces—often relying on personal devices and unsecured networks. This decentralization increases exposure to phishing, endpoint attacks, and unauthorized access, especially when security protocols are inconsistently applied (Thangavel, 2025; Przybyszewski et al., 2024).

Hybrid work not only challenges technical infrastructure but also disrupts established security behaviors and oversight mechanisms. IT departments face difficulties in

maintaining consistent policies across varied endpoints, while employees may lack clarity regarding secure practices outside the corporate environment. Przybyszewski et al. (2024) emphasize the need for tailored risk assessments and adaptive controls that reflect the fluidity of work locations and device usage. Without strategic coordination between technology and human resources, security gaps may persist and escalate.

The pandemic accelerated the digitalization of services and interactions, expanding the digital footprint of organizations and increasing their exposure to cyber threats. As more employees and customers operate within digital channels, the attack surface grows, leading to a rise in hacking attempts and data breaches globally. Mikołajczyk (2024) and Reyes-Quezada (2025) highlight the lack of refined metrics for measuring risky behaviors among remote and hybrid employees, underscoring the need for behavioral analytics and continuous monitoring.

Thangavel (2025) argues that hybrid work renders traditional security models insufficient, prompting a shift toward identity-based and behavior-based approaches. Security awareness in hybrid environments is no longer limited to training modules—it encompasses cognitive understanding, emotional engagement, and behavioral commitment. Achieving consistent security outcomes across diverse contexts requires a resilient mindset and adaptive infrastructure.

Organizational support plays a decisive role in shaping cybersecurity behavior. Employees who perceive strong institutional backing—such as clear policies, responsive IT support, and regular training—are more likely to adopt secure practices and resist social engineering attempts. In hybrid settings, where autonomy is higher and supervision is limited, the presence of supportive structures fosters a sense of shared responsibility and reduces the likelihood of negligent actions (Thangavel, 2025).

At the same time, hybrid work environments introduce challenges related to digital wellbeing. Reyes-Quezada (2025) identifies hyperconnectivity—the constant and often uncontrollable reliance on digital platforms—as a major risk factor. The blurring of boundaries between work and personal life can lead to burnout, reduced vigilance, and increased susceptibility to cyber threats. Inclusive communication strategies, equitable resource allocation, and targeted technical support are essential for transforming digital wellbeing from a reactive concern into a proactive driver of resilience and performance.

Mikołajczyk (2024) notes that most organizations employing white-collar workers intend to adopt hybrid models that offer autonomy over location, schedule, and work methods. While this flexibility enhances job satisfaction and work–life balance, it also demands a reconfiguration of managerial oversight and cybersecurity governance.

Krajčák et al. (2023) elaborate that hybrid work blends traditional office routines with remote arrangements, often involving personal devices and varied ICT infrastructures. This model introduces risks such as inconsistent availability, reduced supervision, and blurred accountability.

Popovici & Popovici (2020) reinforce that remote work brings both opportunities and challenges. While it has been linked to increased productivity and reduced attrition, it also presents risks such as social isolation, reduced access to training, and difficulty in building a cohesive organizational culture. Prolonged remote work may negatively affect health, performance, and security awareness, with consequences that extend beyond the individual to the organization.

Henke et al. (2022) found that only 12% of organizations were prepared for the shift to remote work, yet many employees adapted successfully. Their findings suggest that hybrid and remote work models are not temporary solutions but enduring transformations. Alasoini et al. (2025) introduce the concept of self-directed hybrid work, where employees choose when and where to work. While this model enhances autonomy and efficiency, it also requires strong self-management skills and organizational support to maintain security and productivity.

Flores (2019) and Galanti et al. (2021) highlight the dual nature of remote work. While it reduces commuting costs and boosts performance, it also introduces challenges such as isolation, blurred boundaries, and difficulty collaborating. Key skills for thriving remotely include independent task management, troubleshooting, and minimizing distractions. Managerial mistrust and lack of clear policies can undermine trust and security awareness.

Alexander et al. (2021) reveal that while many organizations intend to embrace hybrid work, few provide clear expectations, leaving employees uncertain. More than a quarter of surveyed workers would consider changing jobs if forced back to full on-site work. These findings highlight the strategic importance of transparent communication, inclusive policy design, and responsiveness to employee needs in shaping the future of hybrid work.

To address the fluidity and unpredictability of hybrid environments, organizations must adopt adaptive cybersecurity models that emphasize resilience over rigidity. Static policies and one-size-fits-all controls often fail to capture the nuances of distributed workforces. Reyes-Quezada (2025) argues that sustainable performance in hybrid settings depends on dynamic strategies that integrate technical safeguards with behavioral insights and continuous feedback. By fostering a culture of vigilance and embedding security into everyday workflows, organizations can enhance their capacity to anticipate, absorb, and recover from cyber disruptions.

2.4 Digital Wellbeing and Security Behavior

Digital wellbeing has emerged as a critical factor influencing security behavior, particularly in hybrid work environments where employees face continuous connectivity, multitasking, and blurred boundaries between personal and professional life. These conditions often lead to cognitive overload, emotional fatigue, and reduced vigilance—factors that increase susceptibility to cyber threats (Abeele, 2020; Büchi, 2024; Reyes-Quezada, 2025).

Abeele (2020) conceptualizes digital wellbeing as a dynamic experiential state shaped by affective and cognitive appraisals of mobile connectivity. It reflects the ambivalence of our relationship with technology, where benefits and drawbacks coexist. Büchi (2024) expands this view by framing digital wellbeing as a multidimensional construct encompassing emotional states, domain satisfaction, and overall life quality within media-saturated environments. These perspectives highlight that digital wellbeing is not merely a personal trait but a systemic outcome shaped by technological design, organizational culture, and individual resilience.

In hybrid work settings, digital wellbeing is often compromised by hyperconnectivity, technostress, and the erosion of work–life boundaries. Reyes-Quezada (2025) describes digital wellbeing as an ecosystemic outcome, influenced by institutional support, equity, and psychological safety. Without proactive strategies—such as “right to disconnect” policies, digital hygiene practices, and workload balancing—employees may experience burnout, disengagement, and diminished security awareness.

Mikołajczyk (2024) emphasizes that managerial roles are particularly vulnerable to digital fatigue, which affects decision-making and risk perception. She argues that the issue is not hybrid work itself, but its poor organization and lack of digital hygiene. Technostress arises from the interaction between users and technology, manifesting as irritability, low motivation, and disengagement. Information overload and digital availability—even during breaks—can prevent recovery and sustain stress hormone levels, reducing resilience and increasing vulnerability to cyber threats.

Galanti et al. (2021), applying the Job Demands–Resources (JD-R) model, show that family–work conflict and social isolation are key job demands that reduce productivity and engagement while increasing stress—factors that directly undermine cybersecurity awareness. Triplett (2022) adds that burnout and security fatigue can lead to human errors, such as poor authentication practices and reduced adherence to security policies. Distraction and cognitive overload are common precursors to cybersecurity incidents, especially when employees are emotionally depleted.

The design of ICT systems and digital habits significantly influence how individuals engage with security protocols. Roffarello & Russis (2022) argue that Digital Self-Control Tools (DSCTs)—such as screen time trackers, notification controls, and focus

modes—function as behavioral interventions that help users regain control over their technology use. Their meta-analysis shows that DSCTs can reduce digital overuse and distractions, though gaps remain in theoretical grounding and long-term evaluation.

Poorly designed systems that overwhelm users with alerts or complex authentication procedures may lead to avoidance or circumvention. Abeele (2020) warns against simplistic solutions like screen time restrictions, which may sacrifice the positive aspects of connectivity. Instead, she proposes optimizing the ambivalence of digital life—maximizing controlled pleasure and functional support while minimizing loss of control and impairment. Büchi (2024) echoes this view, arguing that digital media should be treated as a complex environment that shapes human communication and wellbeing.

Reyes-Quezada (2025) argues that employee resilience is a strategic asset in hybrid work environments. Resilience enables individuals to manage stress, adapt to digital demands, and maintain security awareness under pressure. Organizations that invest in wellbeing initiatives—such as mental health support, digital detox policies, and leadership modeling—foster a workforce that is both engaged and security-conscious.

Individual differences also play a role in shaping security behavior. Przybyszewski et al. (2024) found that personality traits such as extroversion, neuroticism, and conscientiousness influence compliance with cybersecurity protocols. Demographic factors like age and gender also correlate with varying levels of cyber awareness and vulnerability. These findings suggest that digital wellbeing and security interventions must be tailored to diverse user profiles.

Thangavel (2025) reinforces that environmental factors—such as organizational support, technology infrastructure, and work environment security—are stronger predictors of cybersecurity consciousness than work arrangement type. His study shows that hybrid workers exhibit high levels of cybersecurity awareness when supported by robust systems. These findings challenge the assumption that remote or hybrid work inherently increases risk, and instead highlight the importance of cultivating supportive environments that empower secure behavior.

In sum, digital wellbeing is not a peripheral concern but a central determinant of cybersecurity behavior. By promoting digital self-regulation, designing humane systems, and supporting employee resilience, organizations can cultivate a culture where security is sustained not by enforcement, but by wellbeing.

2.5 Leadership Competencies for Cyber GRC Professionals

In today's complex cybersecurity landscape, leadership competencies have become a decisive factor in shaping organizational resilience and security culture. Cybersecurity leaders are no longer confined to technical oversight; they are expected to engage

strategically across departments, influence executive decision-making, and foster a culture of awareness and accountability (Anderson et al., 2022; Auffret et al., 2017).

The role of the Chief Information Security Officer (CISO) exemplifies this shift. Modern CISOs must balance technical expertise with strategic agility, emotional intelligence, and the ability to communicate effectively with both technical teams and senior stakeholders. Their influence spans boardrooms, risk committees, and operational units, requiring a multidimensional skill set that includes trust-building, adaptability, and cultural fluency (Triplett, 2022; Critical Success Factors for Cyber Security Leaders, 2025).

Anderson, Ahmad & Chang (2022) describe cybersecurity leadership as a metacognitive balancing act—leaders must reflect on past decisions, adapt to emerging threats, and select appropriate paradigms for each situation. This strategic agility distinguishes cybersecurity leaders from traditional IT managers and positions them as cultural architects within the organization.

The value of advanced education, such as an MBA, is increasingly recognized in cybersecurity leadership. While certifications like CISSP and CISM validate technical proficiency, they often lack depth in organizational behavior, strategic management, and leadership development. An MBA equips cybersecurity professionals with the business acumen needed to align security initiatives with enterprise goals, navigate regulatory environments, and influence cross-functional decision-making (Triplett, 2022; Critical Success Factors, 2025).

Credibility is a cornerstone of effective cybersecurity leadership. Robert Coles (GSK CISO) emphasizes that the primary role of the CISO is to convince stakeholders that cyber threats are unacceptable risks. This requires courage, character, and a track record of strategic contributions. Steve Katz, one of the first CISOs in the field, underscores the importance of understanding the business and integrating security into its core processes.

Jokinen (2005) identifies global leadership competencies—such as self-awareness, inquisitiveness, and commitment to personal transformation—as foundational traits for effective leaders. These traits support emotional stability, empathy, and cognitive flexibility, which are essential for navigating ambiguity and complexity in digitally driven environments. Behavioral competencies like relationship management, network building, and experiential learning further enhance a leader's ability to influence and adapt.

Leadership also plays a critical role in policy enforcement and cultural alignment. Knapp et al. (2006) found that top management support directly impacts the effectiveness of security policies. Without consistent enforcement and visible commitment from leadership, even the most robust policies remain ineffective. As one

CISSP stated, “Enforcement is without a doubt the most critical information security policy issue.”

In hybrid and remote work environments, leadership presence becomes even more vital. Popovici & Popovici (2020) highlight that managers must lead by example, set clear expectations, and foster inclusive communication to support employee wellbeing and engagement. Mikołajczyk (2024) adds that digital wellbeing is now a core leadership responsibility, requiring emotional resilience, conscious technology use, and the ability to model healthy digital habits.

Ultimately, cybersecurity leadership is not defined solely by technical mastery. It is shaped by the ability to lead people, manage complexity, and align security with organizational purpose. As organizations face increasing digital threats and operational uncertainty, the demand for cyber GRC professionals who combine strategic insight, emotional intelligence, and business credibility will continue to grow.

2.6 HRM as a Driver of Security Culture

Human Resource Management (HRM) plays a pivotal role in shaping and sustaining a resilient cybersecurity culture. Beyond administrative functions, HRM influences recruitment, onboarding, performance management, and employee development—all of which directly affect attitudes and behaviors toward cybersecurity (Humphreys, 2008; Alhogail & Mirza, 2014).

Structured HR procedures—such as background checks, access control, and termination protocols—are essential for mitigating insider threats and aligning with standards like ISO/IEC 27001. These controls embed security into daily operations and establish a baseline of trust and accountability across the organization (Humphreys, 2008; Alnatheer, 2015).

Training and recognition programs coordinated by HR are instrumental in reinforcing secure behavior. Role-specific education and behavioral reinforcement increase the likelihood that employees internalize best practices (Alhogail & Mirza, 2014). Reward systems that acknowledge secure conduct—such as incident reporting or policy compliance—can shift perceptions of cybersecurity from obligation to shared value. Jokinen (2005) adds that leadership development initiatives integrating security awareness into managerial competencies amplify cultural alignment across all levels.

Strategic collaboration between HR and IT departments is essential, especially in hybrid work environments. Lim et al. (2009) and Krajčík et al. (2023) highlight that joint efforts are needed to address end-user education, connectivity, and inclusion. When HR professionals understand technical security and IT teams appreciate behavioral dynamics, co-designed onboarding, access controls, and incident response protocols become both technically sound and behaviorally informed.

HRM also contributes directly to cybersecurity risk management by shaping workforce resilience. Reyes-Quezada (2025) and Mikołajczyk (2024) emphasize that digital wellbeing must be structurally supported through workload management, screen-free policies, and leadership modeling. HR must define expected digital behaviors and ensure they become part of everyday practice. Popovici & Popovici (2020) argue that organizations have a moral duty to combat indifference toward virtual workspace risks, and HR is central to that mission.

Triplett (2022) reminds us that security policies are not merely administrative tools but cultural instruments. When HRM helps embed these policies into everyday behavior, they become part of the organization's identity. Przybyszewski et al. (2024) caution against treating users as adversaries, noting that such approaches erode trust and hinder cultural engagement. Instead, HRM should foster psychological safety and empower employees as the first line of defense.

Veiga & Eloff (2002), Alhogail & Mirza (2014), and Schlienger & Teufel (2003) define information security culture (ISC) as “the way things are done” regarding security. They emphasize that acceptable behavior must be institutionalized across individual, group, and organizational levels. HRM plays a key role in shaping these norms—through policies, awareness programs, and leadership modeling—so that security becomes part of everyday life. A strong ISC turns employees into “human firewalls” who actively protect information assets.

Lim et al. (2009) further clarify that ISC must be embedded into organizational culture (OC) to be effective. They describe three relationship types: ISC as separate, as a subculture, or fully embedded. Only in the third case does security become a shared responsibility, with employees feeling ownership and motivation to protect information. HRM is instrumental in guiding organizations toward this integrated model.

Alnatheer (2015) identifies eight critical success factors for cultivating ISC: top management support, effective security policies, awareness, training, risk assessment, compliance, ethical conduct, and organizational culture. Each factor is directly influenced by HRM practices. For example, HR can ensure that ethical standards are communicated and upheld, that training programs are ongoing and role-specific, and that compliance is monitored and reinforced. Without these foundations, security culture remains fragmented and ineffective.

Van Niekerk (2010) adds a managerial lens, arguing that security culture must be in equilibrium across four levels: visible behavior (artifacts), espoused values, tacit assumptions, and knowledge. If management increases the “demand” for security through stricter policies, HR must ensure a matching increase in employee awareness, motivation, and competence. Otherwise, the culture becomes unstable, and behavior

unpredictable. HRM is thus essential in maintaining elasticity and balance across these cultural layers.

Finally, HR can accelerate the credibility of cybersecurity professionals by supporting leadership development. As noted in *Critical Success Factors (2025)*, HR departments can subsidize education, facilitate cross-functional assignments, and promote network connectedness. These practices help build trust, bridge silos, and prepare future CISOs to operate strategically across the enterprise.

2.7 Human Factors in Cybersecurity Risk Management

Human factors have long been acknowledged as a critical dimension in cybersecurity risk management, yet their complexity and variability continue to challenge organizations. Unlike technical vulnerabilities, human-related risks are shaped by psychological states, behavioral tendencies, and organizational dynamics. These include stress, fatigue, disengagement, and cultural misalignment—all of which can significantly influence how individuals perceive and respond to cyber threats (Triplett, 2022; Edegbeme-Beláz et al., 2020).

In hybrid work environments, emotional exhaustion and cognitive overload are particularly prevalent. Reyes-Quezada (2025) highlights that low engagement and technostress correlate with increased susceptibility to phishing and policy violations. Mikołajczyk (2024) adds that managerial roles are especially vulnerable to digital fatigue, which impairs decision-making and risk perception. Alexander et al. (2021) found that poor communication and uncertainty exacerbate burnout, while inclusive dialogue and frequent updates improve wellbeing and performance.

The concept of digital resilience has emerged as a key competency in this context. Defined as the ability to regulate technology use, maintain psychological flexibility, and adopt healthy digital habits, digital resilience enables individuals to adapt to demanding environments without compromising security behavior (Reyes-Quezada, 2025). Organizational culture plays a decisive role in fostering this resilience—cultures that value autonomy, boundary respect, and psychological safety tend to support more consistent and secure behavior.

Trust and psychological safety are foundational to effective cybersecurity practices. Auffret et al. (2017) emphasize that when employees feel safe to report incidents and admit mistakes, they act more transparently and responsibly. Anderson et al. (2022) argue that emotionally intelligent leadership—marked by empathy and inclusive decision-making—enhances organizational resilience. In contrast, cultures that treat users as adversaries or rely heavily on surveillance tend to erode trust and hinder engagement (Przybyszewski et al., 2024).

Hybrid work also introduces challenges related to decentralization and visibility. Krajčák et al. (2023) note that remote employees may feel isolated or disconnected, which can lead to inconsistent adherence to security protocols. Henke et al. (2022) stress the importance of soft skills—such as self-discipline, digital literacy, and adaptability—in maintaining secure practices across distributed teams. Popovici & Popovici (2020) call for regulatory frameworks that protect teleworkers' wellbeing and reinforce human-centric cybersecurity strategies.

The literature consistently identifies insider behavior as a greater threat than external attacks. Veiga & Eloff (2002) and Alhogail & Mirza (2014) argue that the success of security controls depends on the dependability of those who implement and use them. Lim et al. (2009) confirm that up to 80% of major security failures stem from poor employee behavior rather than technical flaws. These findings underscore the need to embed security values into organizational culture, rather than relying solely on policy enforcement.

Van Niekerk (2010) introduces the concept of cultural elasticity, suggesting that employee behavior is shaped by the balance between management expectations, shared assumptions, and organizational knowledge. When security demands increase without corresponding support, behavior becomes unpredictable and compliance deteriorates. Schlienger & Teufel (2003) reinforce that security culture must be continuously evaluated and adapted to remain effective. Organizational culture evolves over time, and so must the security subculture within it.

In summary, human factors represent both a vulnerability and an opportunity in cybersecurity risk management. By understanding the psychological, behavioral, and cultural dimensions of security behavior, organizations can move beyond reactive controls and toward proactive, resilient strategies that align with the realities of modern work environments.

2.8 Gaps in Current Literature and Future Research Directions

Despite increasing scholarly attention to human-centered cybersecurity, the literature remains fragmented in its treatment of behavioral, cultural, and organizational dimensions. While technical safeguards are well-documented, the human factors that shape security behavior—such as stress, trust, leadership, and organizational culture—are often examined in isolation or through static models.

Mikołajczyk (2024) highlights that managerial digital wellbeing is frequently studied separately from cybersecurity behavior, resulting in limited understanding of how fatigue, emotional resilience, and leadership presence influence threat response. This disconnect limits the development of integrated frameworks that accurately reflect the realities of hybrid work environments, where psychological safety and digital overload coexist.

Przybyszewski et al. (2024) identify key cyberrisk factors in hybrid workforce settings, yet their analysis reveals a lack of longitudinal depth. Most studies rely on cross-sectional surveys, leaving a gap in tracking behavioral evolution, adaptation, and burnout over time. Without such data, organizations struggle to design proactive interventions that align with employee needs and threat dynamics.

Leadership and trust are frequently cited as enablers of cybersecurity culture, but few studies link specific leadership competencies to measurable security outcomes. Jokinen (2005) and Anderson et al. (2022) explore global leadership traits and emotional intelligence, yet the literature lacks models that connect these traits to reduced incident rates or improved compliance. Moreover, the role of HRM in cultivating leadership credibility and embedding security into organizational routines remains underexplored (Alnatheer, 2015; Triplett, 2022).

Ethical considerations related to behavioral monitoring and digital wellbeing interventions remain underexplored in current literature. As organizations adopt nudging strategies, analytics, and self-regulation technologies (Roffarello & Russis, 2022), questions of autonomy, consent, and surveillance emerge. Interdisciplinary research is needed to balance behavioral influence with ethical integrity, especially in environments where psychological safety is critical to reporting and compliance.

Another overlooked dimension is the elasticity of security culture. Van Niekerk (2010) argues that employee behavior (artifacts) is shaped by the balance between management expectations, shared assumptions, and knowledge. When security demands increase without corresponding support, cultural equilibrium is lost, and behavior becomes unpredictable. This insight calls for research into cultural elasticity and organizational maturity as predictors of security effectiveness.

Finally, the literature often treats information security culture as a static construct, whereas Veiga & Eloff (2002) and Schlienger & Teufel (2003) emphasize its dynamic nature. Culture must be continuously evaluated, maintained, and adapted to organizational goals and evolving threats. Yet few studies examine how security culture evolves over time or how interventions can sustain it across organizational levels.

In light of these gaps, future research should aim to address the following priorities:

- Longitudinal studies on security behavior and cultural adaptation in hybrid teams.
- Integration of wellbeing metrics into cybersecurity governance.
- Sector-specific analyses of leadership impact on compliance and resilience.
- Development of ethical frameworks for behavioral monitoring and nudging.
- Exploration of cultural elasticity and organizational readiness as success factors.

Addressing these gaps will enable researchers and practitioners to advance a more holistic and resilient cybersecurity paradigm—one that fully incorporates the complexity of human factors and adapts to the evolving nature of modern work environments.

3 Research Methodology

3.1 Research Philosophy and Approach

This study adopts a pragmatic research philosophy, reflecting its applied orientation and its focus on real-world challenges in cybersecurity culture. Pragmatism is particularly suitable for research that seeks actionable insights and practical tools, especially in complex domains where human behavior, organizational dynamics, and digital environments intersect. Rather than adhering strictly to a single epistemological stance, the pragmatic approach allows for methodological flexibility and the integration of both quantitative and qualitative perspectives.

In the context of cybersecurity culture, individual perception plays a central role in shaping secure behavior and organizational resilience. By focusing on how employees personally experience and evaluate cultural dimensions such as Leadership, HRM Involvement, and Digital Wellbeing, the study embraces a constructivist view of knowledge — one that acknowledges the subjective and context-dependent nature of human experience. At the same time, the research seeks to generate generalizable patterns and comparative insights through structured data collection and statistical analysis, aligning with a post-positivist orientation.

This dual perspective supports the development and application of the Cybersecurity Culture Maturity Index (CCMI) as a flexible, empirically grounded tool for assessing cultural maturity at the individual level. The index is designed not as a fixed or universal measure, but as a dynamic framework that can be adapted to different organizational contexts and analytical needs. By combining theoretical foundations with field data, the study aims to produce knowledge that is both academically rigorous and practically relevant — enabling organizations to better understand, benchmark, and enhance their cybersecurity culture from the ground up.

3.2 Research Design: Individual-Level Strategy

To address the complexity of cybersecurity culture in hybrid work environments, this study employs a quantitative research design centered on individual-level data collection and analysis. The goal is to capture structured indicators of how employees perceive cultural maturity across five thematic domains: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration.

The central instrument is the Cybersecurity Culture Maturity Index (CCMI), a modular framework designed to assess individual perceptions of cybersecurity culture. Each participant completes a standardized questionnaire consisting of 20 Likert-scale items (four per pillar), reflecting their personal experience within their organizational context. The questionnaire is uniform across roles and sectors, enabling comparative analysis while preserving consistency in measurement.

Unlike traditional organizational assessments, the CCMI is applied at the individual level, allowing for cross-sectional insights without requiring multiple responses from the same organization. This design supports the aggregation of individual scores to identify broader trends, while also enabling stratified analysis based on demographic variables such as role, sector, company size, and the presence or absence of key functions (e.g., CISO, HR department).

The study does not include a behavioral quiz component, as the focus is exclusively on perception-based maturity. However, the scoring model retains flexibility, allowing for future integration of behavioral data if needed. The CCMI score is calculated using a baseline arithmetic model, with each pillar contributing equally to the final index. Additional scoring models (e.g., geometric mean, threshold-based) are discussed in Chapter 4 but are not applied in this version of the study.

This individual-level design enables the identification of cultural strengths and weaknesses as experienced by employees, offering a scalable and inclusive approach to cybersecurity culture assessment. It also supports benchmarking across organizational types and strategic roles, providing actionable insights for leadership, HR, and GRC professionals seeking to enhance cultural resilience.

3.3 Data Collection

The data collection strategy is designed to capture structured, perception-based indicators of cybersecurity culture maturity at the individual level. To achieve this, the study utilizes a single standardized instrument: the CCMI questionnaire. This tool consists of 20 Likert-scale items, evenly distributed across five thematic pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration.

Each participant completes the questionnaire digitally and anonymously, providing responses based on their personal experience within their current organizational environment. Prior to answering, participants are asked to indicate whether key organizational roles—such as a dedicated CISO or HR department—exist in their organization. This contextual information is used to support stratified analysis and interpretive depth, but does not alter the scoring algorithm in this version of the study.

Demographic data is also collected, including role, sector, company size, and years of experience. These variables enable comparative analysis across different organizational profiles and professional backgrounds. The estimated completion time for the questionnaire is approximately 8–10 minutes, ensuring accessibility and minimizing respondent fatigue.

No behavioral quiz or scenario-based component is included in this version of the study, as the focus remains exclusively on perception-based maturity. All responses are stored securely and processed in compliance with GDPR and institutional ethical standards. No personally identifiable information is recorded, and participation is entirely voluntary.

This data collection approach supports a scalable and inclusive assessment of cybersecurity culture, enabling the aggregation of individual insights into broader trends while preserving the integrity of personal experience.

3.4 Sample Selection and Recruitment

The credibility and analytical depth of this study depend on a carefully designed sampling strategy that reflects the diversity of organizational contexts and professional roles. Since the CCMI is applied at the individual level, the sample is composed of professionals from various sectors, company sizes, and functional areas, allowing for comparative analysis across demographic and structural variables.

Participants are recruited from both public and private organizations, with representation from various roles including managers, HR professionals, IT/security staff, etc. This role-based structure supports the study's objective of capturing how different professional perspectives influence the perception of cybersecurity culture. Additionally, participants are asked to indicate whether their organization includes specific functions such as a dedicated CISO or HR department, enabling stratified analysis based on organizational structure.

All participants must be currently employed in one of the following work arrangements: Hybrid, Remote, or Flexible On-Site (primarily on-site with occasional fieldwork or remote work when required). This ensures that the study captures perspectives from professionals actively engaged in modern, digitally enabled work environments.

Recruitment is conducted through professional networks, LinkedIn outreach, alumni groups, and direct invitations. Participation is voluntary and anonymous, and all respondents are informed of the study's purpose, ethical safeguards, and data handling procedures prior to engagement.

This sampling strategy supports the study's goal of developing a flexible and inclusive framework for cybersecurity culture assessment, grounded in individual experience and applicable across a wide range of organizational profiles.

3.5 Data Analysis Techniques

The analysis of collected data is structured to support both descriptive interpretation and comparative evaluation of cybersecurity culture maturity at the individual level. Given the perception-based nature of the study, the analysis focuses on identifying trends, patterns, and differences across roles, sectors, and organizational characteristics.

Responses from the CCMI questionnaire are analyzed using descriptive statistics to explore central tendencies (mean, median), variability (standard deviation), and distribution patterns across the five cultural pillars. Each item is scored on a five-point Likert scale, and pillar-level scores are calculated by averaging the four items associated with each domain. Each pillar contributes a maximum of 20 points, resulting in a total CCMI score out of 100.

The overall CCMI score for each participant is computed using a baseline arithmetic model, where all five pillars are weighted equally. This score serves as a proxy for the individual's perception of their organization's cybersecurity culture maturity. While alternative scoring models (e.g., geometric mean, threshold-based, dynamic weighting) are discussed in Chapter 4, only the arithmetic model is applied in this version of the study.

To explore relationships between variables, inferential statistical techniques such as t-tests, ANOVA, and correlation analysis (e.g., Pearson or Spearman) are used. These tests assess whether significant differences exist in CCMI scores across demographic groups (e.g., role, sector, company size) and whether specific cultural dimensions are associated with higher or lower overall maturity perceptions.

All data is processed using statistical software (e.g., Python and R Programming), and results are interpreted in light of the study's research questions and conceptual framework. The analysis aims not only to validate the CCMI as a measurement tool but also to generate actionable insights into how different organizational and individual factors shape cybersecurity culture perception.

3.6 Ethical Considerations

This study places strong emphasis on ethical integrity, particularly given its focus on individual perceptions, workplace experiences, and organizational culture. All research activities are conducted in accordance with institutional guidelines and established ethical standards in social science research, including GDPR compliance and data protection protocols.

Prior to participation, individuals receive a clear explanation of the study's purpose, procedures, and their rights as participants. Informed consent is obtained digitally, and participation is entirely voluntary. Individuals retain the right to withdraw at any stage without consequence or justification.

To ensure anonymity and confidentiality, all questionnaire responses are anonymized. No personally identifiable information is collected, and demographic data is used solely for stratified analysis. Any organizational metrics provided are aggregated and reported without reference to specific companies or individuals. All collected data is stored securely on encrypted devices or password-protected platforms, accessible only to the researcher and academic supervisor. Data is retained only for the duration necessary to complete the research and is deleted in accordance with institutional policies.

Care is taken to minimize any psychological discomfort or reputational risk to participants. Questions are framed neutrally, and participants are reminded that they may skip any item or decline to answer without penalty. The questionnaire is designed to assess perceptions, not to evaluate individual competence or organizational performance.

Ethical approval is obtained from the relevant academic ethics committee prior to data collection. Any modifications to the research protocol are communicated to ensure continued compliance. By adhering to these principles, the study aims to uphold the dignity, privacy, and autonomy of all participants while ensuring the integrity and credibility of the research process.

3.7 Limitations of the Methodology

While the research design aims to provide a structured and inclusive exploration of cybersecurity culture maturity, certain methodological limitations must be acknowledged. These constraints may affect the generalizability, interpretive depth, and scalability of the findings.

First, the study relies exclusively on self-reported data, which introduces the potential for response bias. Participants may overstate positive perceptions or underreport challenges, particularly in areas related to leadership, HR involvement, or organizational support. Although anonymity and neutral phrasing are used to mitigate this risk, the subjective nature of perception-based data remains a limitation.

Second, the absence of a behavioral component (e.g., scenario-based quiz) means that the study does not capture actual security behavior or decision-making under pressure. As a result, the CCMI score reflects perceived maturity rather than demonstrated competence. Future research may address this gap by integrating behavioral assessments to compare perception with action.

Third, the cross-sectional design provides a snapshot of cybersecurity culture at a single point in time. It does not account for cultural evolution, organizational change, or the impact of interventions. Longitudinal studies would be required to track shifts in perception and maturity over time.

Fourth, while the sample includes participants from diverse sectors and roles, it may not fully represent the broader workforce. Recruitment through professional networks and voluntary participation may result in a sample skewed toward individuals with higher awareness or interest in cybersecurity topics.

Finally, the study does not incorporate external organizational metrics such as incident rates, audit outcomes, or compliance scores. These data could enrich the analysis and support validation of the CCMI, but are excluded due to access constraints and the need to preserve participant anonymity.

Despite these limitations, the methodology is designed to balance rigor with feasibility and to generate insights that are both academically meaningful and practically relevant. Transparency in design and analysis helps ensure that the findings contribute constructively to the evolving discourse on human-centered cybersecurity culture.

4 Development of the Cybersecurity Culture Maturity Index (CCMI)

4.1 Conceptual Framework of the CCMI

The Cybersecurity Culture Maturity Index (CCMI) is a multidimensional framework designed to assess the human-centered aspects of cybersecurity culture as perceived by individual employees. Unlike traditional models that evaluate organizational maturity through aggregated metrics or technical indicators, the CCMI focuses on how each person experiences and interprets the cultural environment surrounding cybersecurity within their workplace.

The conceptual foundation of the CCMI is built upon five core pillars, each representing a distinct domain of influence. These pillars were derived from interdisciplinary literature in cybersecurity governance, organizational psychology, human resource management, and digital wellbeing. Together, they form a holistic model that reflects the complexity of modern work environments, especially those operating under hybrid or remote conditions:

- **Leadership & Trust:** This pillar examines the role of organizational leaders in shaping cybersecurity culture. It includes constructs such as ethical leadership, psychological safety, and the extent to which leaders model secure behavior

and foster open communication. Leadership is treated as a cultural amplifier that can reinforce or undermine security norms.

- **HRM Involvement:** This dimension focuses on the contribution of human resource practices to cybersecurity culture. It encompasses onboarding procedures, training programs, policy communication, and the integration of security values into performance management and employee development.
- **Digital Wellbeing:** Digital wellbeing refers to the psychological and emotional impact of digital work environments. It includes factors such as technostress, digital fatigue, work–life boundaries, and perceived autonomy. In hybrid settings, digital wellbeing becomes a critical determinant of security behavior.
- **Security Awareness & Behavior:** This pillar evaluates individual and collective practices related to cybersecurity. It includes knowledge of policies, compliance behavior, incident reporting, and risk perception. The emphasis is placed on the translation of awareness into consistent, proactive behavior.
- **Hybrid Work Integration:** This domain assesses how flexible work models affect cultural cohesion, communication, and policy clarity. It considers the challenges and opportunities presented by remote collaboration, decentralized teams, and digital-first workflows.

Each pillar is assessed through a standardized questionnaire, with no behavioral component included in this version of the study. The CCMI is calculated using an arithmetic scoring model, where each pillar contributes equally to a total score out of 100. This structure allows for benchmarking across individuals and groups, while preserving the integrity of personal experience.

The framework is designed to be scalable, adaptable, and context-sensitive. It enables organizations and researchers to identify cultural strengths and vulnerabilities from the perspective of those who live and work within the system. By centering the individual, the CCMI offers a more inclusive and actionable approach to understanding cybersecurity culture maturity.

4.2 Questionnaire Design

The CCMI questionnaire is designed to capture structured, perception-based data across five core dimensions of cybersecurity culture. It serves as the primary instrument for assessing how individual employees experience and evaluate cultural maturity within their organizational environment. The questionnaire is built to be both conceptually rigorous and practically scalable, allowing for consistent administration across roles, sectors, and organizational sizes.

The instrument consists of 20 standardized items, with four items assigned to each of the five pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. Each item is measured on a five-point Likert scale, ranging from “Strongly Disagree” (1) to “Strongly Agree” (5). This format enables nuanced responses and supports statistical analysis of central tendencies, variability, and internal consistency.

All participants respond to the same set of items, ensuring comparability across roles and organizations. Prior to completing the survey, participants are asked to indicate whether key roles (e.g., CISO, HR department) exist within their organization. This contextual information is used for stratified analysis but does not affect the scoring algorithm in this version of the study.

The questionnaire is administered digitally and anonymously. Participants are informed of the study’s purpose and their rights before beginning, and no personally identifiable information is collected. Estimated completion time is approximately 8–10 minutes, balancing depth with respondent engagement.

Each pillar contributes a maximum of 20 points to the overall CCMI score, resulting in a total score out of 100. The questionnaire is designed to support this arithmetic scoring model, while also allowing for future integration with alternative models if needed. By capturing structured perceptions across key cultural domains, the CCMI questionnaire provides a robust foundation for evaluating cybersecurity culture maturity from the individual’s point of view.

4.3 Scoring Model and Index Calculation

The Cybersecurity Culture Maturity Index (CCMI) is calculated through a structured scoring model that integrates perception-based data across five cultural dimensions: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. Each dimension is assessed through four Likert-scale items, scored from 1 to 5. The average score per pillar is multiplied by 4, resulting in a maximum of 20 points per pillar and a total CCMI score out of 100.

For this study, the arithmetic scoring model was selected. In this model, all five pillars are weighted equally, and the final score is computed as the sum of the five pillar scores. This approach emphasizes simplicity, transparency, and interpretability, making it suitable for comparative analysis across individuals, roles, and organizational contexts. It also avoids introducing complexity or bias through differential weighting.

During the design of the CCMI, three alternative scoring models were considered:

- **Geometric Mean Model:** This model calculates the multiplicative average of the five pillar scores. It penalizes imbalance across dimensions, meaning that low performance in one area significantly reduces the overall score. This

approach is useful when consistency across cultural domains is considered essential for maturity.

- **Threshold-Based Model:** This model introduces minimum score requirements per pillar for classification into higher maturity levels. For example, an individual must score at least 70/100 in each pillar to be classified as “Advanced.” This prevents strong performance in some areas from masking weaknesses in others.
- **Dynamic Weighting Model:** Designed for versions of the CCMI that include both perception and behavioral components, this model adjusts the influence of each component based on divergence between them. Since this study does not include behavioral data, the dynamic weighting model is not applicable.

While these models offer valuable perspectives and may be applied in future research, the arithmetic model was chosen for its clarity and suitability to the individual-centric design of this study. It enables straightforward benchmarking and supports the classification of participants into four maturity levels:

- 0–49: Low Maturity
- 50–64: Moderate Maturity
- 65–84: High Maturity
- 85–100: Advanced Maturity

These categories provide a meaningful framework for interpreting results and identifying areas for cultural development. By centering the scoring process on individual perception, the CCMI offers a flexible and inclusive tool for assessing cybersecurity culture in diverse organizational settings.

4.4 CCMI Application Examples

To illustrate the interpretive depth and practical utility of the Cybersecurity Culture Maturity Index (CCMI), this section presents hypothetical examples of how the index can be applied across different individual profiles and organizational contexts. These examples demonstrate how the scoring model adapts to variations in role, sector, and structural characteristics, and how the results can be used to identify cultural strengths and areas for improvement.

Example A: Employee in a Small Private Firm (No CISO or HR Department)

- Role: General staff
- Sector: Private
- Company size: ~30 employees
- Reported absence of CISO and formal HR function)

- CCMI scores by pillar:
 - Leadership & Trust: 12/20
 - HRM Involvement: 8/20
 - Digital Wellbeing: 14/20
 - Security Awareness & Behavior: 10/20
 - Hybrid Work Integration: 13/20
- Total CCMI Score: 57/100 → Moderate Maturity

Interpretation: The participant perceives moderate cultural maturity overall, with relatively strong digital wellbeing and hybrid work support, but limited HR involvement and inconsistent leadership visibility. These results suggest that even in lean organizations, targeted improvements in onboarding and leadership communication could enhance cultural resilience.

Example B: Manager in a Medium-Sized Public Entity (HR Present, No CISO)

- Role: Team leader
- Sector: Public
- Company size: ~120 employees
- HR department present; no dedicated CISO
- CCMI scores by pillar:
 - Leadership & Trust: 15/20
 - HRM Involvement: 17/20
 - Digital Wellbeing: 13/20
 - Security Awareness & Behavior: 14/20
 - Hybrid Work Integration: 15/20
- Total CCMI Score: 74/100 → High Maturity

Interpretation: The participant reports high cultural maturity, with strong scores in leadership and HRM involvement. The absence of a CISO does not appear to negatively impact perception, possibly due to effective cross-functional coordination and visible support from management. This profile reflects a well-integrated culture with room for further development in digital wellbeing.

Example C: IT Security Professional in a Large Corporation (Full Structure)

- Role: Security analyst
- Sector: Private
- Company size: ~600 employees
- CISO and HR department present
- CCMI scores by pillar:
 - Leadership & Trust: 18/20
 - HRM Involvement: 19/20
 - Digital Wellbeing: 15/20

- Security Awareness & Behavior: 17/20
- Hybrid Work Integration: 16/20
- Total CCMI Score: 85/100 → Advanced Maturity

Interpretation: The participant perceives an advanced mature cybersecurity culture, with strong leadership, structured HR practices, and high awareness. This profile reflects a well-resourced organization with embedded cultural norms and strategic alignment. It serves as a benchmark for best practices in cybersecurity culture development.

4.5 Validation Strategy

The credibility and usefulness of the Cybersecurity Culture Maturity Index (CCMI) depend not only on its conceptual soundness but also on its empirical reliability and interpretive validity. Within the scope of this study, a multi-layered validation strategy is adopted to assess the robustness of the tool, recognizing that further refinement may be required through future applications.

To evaluate internal consistency, reliability analysis is conducted using Cronbach's alpha for each of the five questionnaire pillars. A threshold of $\alpha \geq 0.70$ is considered acceptable, indicating that the items within each dimension measure a coherent construct. Where alpha values fall below this threshold, item-level diagnostics are performed to identify and revise problematic questions. This process ensures that each pillar reflects a stable and interpretable domain of cybersecurity culture.

Construct validity is supported through the conceptual alignment of questionnaire items with established literature in cybersecurity governance, organizational psychology, and human resource management. Items are derived from validated instruments where appropriate and are reviewed for clarity, relevance, and neutrality. Pilot testing is conducted to assess engagement and comprehension, and expert feedback is sought from professionals in cybersecurity, HRM, and organizational development.

While criterion validity is difficult to establish due to the absence of a gold standard for cybersecurity culture, the study explores correlations between CCMI scores and contextual variables such as organizational size, role distribution, and sector type. These relationships offer preliminary evidence of the index's sensitivity to structural and cultural variation.

The scoring model itself contributes to interpretive robustness. By presenting results on a 0–100 scale and classifying individuals into four maturity levels, the CCMI enables clear and actionable interpretation. The equal weighting of pillars ensures transparency and avoids bias, while the option to analyze pillar-level scores supports targeted insights.

Finally, the CCMI is designed to be scalable and adaptable. While the current study applies the index to a cross-sectional sample, future research may extend its validation through longitudinal studies, sector-specific modules, and integration with behavioral or performance metrics. The goal is to develop a tool that is not only statistically sound but also meaningful and actionable for organizations seeking to strengthen their cybersecurity culture.

5 Data Analysis and Findings

5.1 Overview of Respondents

This section provides a demographic overview of the 100 individuals who participated in the CCMI survey. The sample was drawn from a diverse range of sectors, roles and organizational contexts, ensuring a broad representation of cybersecurity-culture perceptions across different environments. Because we retained only the first 100 fully completed questionnaires for the analysis, every person in the set answered all of the demographic items, giving us a complete dataset that does not require imputation or case deletion.

The distribution of respondents across key demographic categories is summarized below:

- **Age Group:** 6% of participants are under 25, 47% fall between 25–34, 31% between 35–44, and 16% between 45–54. This spread across generations is important because familiarity with technology, attitudes towards risk, and patterns of working behaviour can differ with age. Recognizing the generational makeup of the sample helps interpret variation in cybersecurity culture maturity along the continuum of life-stage and experience.
- **Gender:** The sample is 64% male and 36% female. Recording the gender composition is not only a matter of completeness but also speaks to the potential influence of culturally shaped attitudes and workplace dynamics on cybersecurity practices. Any systematic differences that emerge in the analysis can be situated against this backdrop of representation.
- **Work Arrangement:** 80% of respondents operate in hybrid settings, 14% work flexible on-site, and 6% work fully remotely. The predominance of hybrid patterns reflects contemporary modes of organizing labour and suggests that questions of remote access, blended supervision, and the maintenance of a coherent security ethos across physical boundaries are especially pertinent for understanding the culture we measure.
- **Tenure in Current Organization:** Half (50%) of the respondents report being with their organization for more than three years, 30% for one to three years,

13% for six to twelve months, and 7% for less than six months. This distribution signals that both long-established incumbents and more recent arrivals are represented. Length of service can influence exposure to formal training, socialization into the company's norms, and investment in its security practices.

- **Organization Size:** 46% of the sample come from organizations with 1,000+ employees, 27% from organizations of 251–1,000, 14% from those of 51–250, and 13% from the smallest band of 1–50. Because the scale of an organization shapes its formal structures, resources, and complexity of communication, this gradient allows us to explore how cybersecurity culture maturity may correlate with organizational scale.
- **Sector:** The private sector predominates (87% of the sample), with the public sector accounting for 10% and “Other” for 3%. Sectoral affiliation is relevant because regulatory regimes, mission imperatives, and stakeholder pressures differ across sectors, potentially influencing how security is governed and enacted.
- **Presence of a Dedicated HR Department:** 83% of respondents report that their employer has a dedicated HR function, 13% report that none exists, and 4% are unsure. The high incidence of formal human-resources infrastructures points to organisational maturity on a human-capital dimension. The presence (or absence) of HR may influence the extent to which training, accountability mechanisms, and people-centred policies are in place to support a security-minded culture.
- **Presence of a Dedicated CISO or Cybersecurity Team:** 52% confirm the existence of a CISO or cybersecurity team, 42% report that no such specialised function exists, and 6% are unsure. The roughly even split on this structural feature sets up a natural contrast for subsequent analyses. Formalised security leadership and dedicated personnel are often regarded as hallmarks of a mature security culture, so differences between these groups in later results will be particularly illuminating. This structural feature sets up a natural contrast for later group comparisons.

Because every case contributes information on all of these characteristics, the proportions for each category sum to 100% and no ad hoc deletions or imputations are required at this stage. The portrait of the sample that emerges—heterogeneous in age, gender, work arrangement, tenure, size, sector, and formal organisational features (HR/CISO provision)—establishes a firm base for the analyses that follow. This diversity both enriches the scope of our findings and ensures that comparisons between subgroups rest on adequately populated categories, allowing us to speak meaningfully

about the ways in which the maturity of cybersecurity culture may vary across different types of individuals and organisational contexts.

5.2 Descriptive Statistics and Reliability

Before subjecting the survey responses to inferential tests and multivariate procedures, it is essential to characterise the basic shape of the numerical data that underpin the Cybersecurity Culture Maturity Index (CCMI) and its constituent dimensions. Descriptive statistics provide a foundational summary of central tendencies, dispersion, and observed ranges, allowing us to frame subsequent results against the scale on which respondents answered. In parallel, reliability analysis evaluates the internal consistency of each pillar, ensuring that the aggregated scores represent coherent constructs suitable for further interpretation.

Descriptive Statistics

The table below summarises the key descriptive measures for the overall CCMI score and each of the five pillars:

Table 1: Descriptive Statistics of CCMI and Pillars

Dimensi on	Count (Respon ders)	Mean	Median	Std Dev	Min	Max
CCMI	100	63.10	65.00	17.57	24	97
Leadership & Trust	100	14.03	14.00	3.40	6	20
HRM Involvement	100	11.74	12.00	4.44	4	20
Digital Wellbeing	100	11.68	12.00	2.57	6	19
Security Awareness & Behavior	100	13.38	13.50	4.17	4	20
Hybrid Work Integration	100	12.27	13.00	4.60	4	20

The overall CCMI score averages 63.10 out of a possible 100, with a median of 65.00 and a standard deviation of 17.57. This suggests that, on average, respondents perceive their organizations to be moderately mature in terms of cybersecurity culture, though with considerable variation across the sample.

Among the pillars, Leadership & Trust shows a relatively high mean (14.03 out of 20), indicating generally positive perceptions of leadership commitment and trust dynamics. HRM Involvement and Digital Wellbeing score lower on average (11.74 and 11.68 respectively), suggesting that human resource practices and wellbeing initiatives may be less consistently embedded across organizations. Security Awareness & Behavior (13.38) and Hybrid Work Integration (12.27) reflect moderate levels of maturity, with wide ranges indicating variability in how these dimensions are experienced.

Importantly, none of the distributions exhibit extreme clustering at either end of the scale, and the alignment between means and medians suggests that the data are not severely skewed. The standard deviations confirm meaningful differentiation between respondents, supporting the validity of subsequent comparative and correlational analyses.

Reliability Analysis

To assess the internal consistency of each pillar, Cronbach's alpha was calculated for the four items comprising each dimension. The results are presented below:

Table 2: Reliability Analysis (Cronbach's Alpha per Pillar)

Dimension	Cronbach's Alpha
Leadership & Trust	0.92
HRM Involvement	0.94
Digital Wellbeing	0.75
Security Awareness & Behavior	0.92
Hybrid Work Integration	0.93

All five pillars demonstrate strong internal consistency, with alpha values exceeding the commonly accepted threshold of 0.70. Four of the five dimensions exceed 0.90, indicating excellent reliability. Even the lowest value, for Digital Wellbeing (0.75), remains well within acceptable bounds. These results confirm that the items within each pillar cohere as unidimensional constructs and justify the aggregation of item scores into composite measures.

Conclusion

Together, the descriptive and reliability findings establish a robust foundation for the analyses that follow. The data exhibit appropriate variability, well-behaved distributions, and psychometric integrity across all dimensions. With confidence in the measurement structure and internal coherence of the CCMI framework, we now proceed to examine how cybersecurity culture maturity varies across demographic groups and organisational contexts.

5.3 Group Comparisons

In addition to the univariate description of the five dimensions of the Cybersecurity Culture Maturity Index (CCMI) and the overall index presented elsewhere in this chapter, the sample was partitioned along a number of respondent-characteristic dimensions in order to explore how perceptions of culture maturity vary across identifiable groups. Eight categorical variables recorded on the questionnaire were used as the grouping factors: Age, Gender, Work arrangement, Tenure in current organization, Organization size, Sector, Presence of a dedicated HR department, Presence of a dedicated CISO or cybersecurity team.

For each of these factors, respondents were assigned to the appropriate category and the arithmetic mean of their CCMI score was computed. All statistics in this section are calculated on the 100 valid questionnaires returned (rows 2–101 of the spreadsheet). No cases were excluded due to missing data.

The group means were computed using Python with the following procedure:

```
df_resp = df.iloc[0:100].copy()
group_means = {}
for col in demographic_columns:
    gm = df_resp.groupby(col)['CCMI'].agg(['count', 'mean']).sort_values('mean', ascending=False)
    group_means[col] = gm
```

Table 3: Mean CCMI by Age Group

Age Group	Count	Mean CCMI
Under 25	6	68.33
35-44	31	64.19
45-54	16	63.81
25-34	47	61.47

Table 4: Mean CCMI by Gender

Gender	Count	Mean CCMI
Male	64	66.83
Female	36	56.47

Table 5: Mean CCMI by Work Arrangement

Work Arrangement	Count	Mean CCMI
Fully Remote	6	78.83
Hybrid	80	65.16
Flexible On-site	14	46.71

Table 6: Mean CCMI by Tenure

Tenure	Count	Mean CCMI
Less than 6 months	7	84.43
More than 3 years	50	66.10
6-12 months	13	56.92
1-3 years	30	55.80

Table 7: Mean CCMI by Organization Size

Organization Size	Count	Mean CCMI
1000+	46	72.83
251-1000	27	62.78
51-250	14	52.36
1-50	13	40.92

Table 8: Mean CCMI by Sector

Sector	Count	Mean CCMI
Other	3	70.33
Private	87	64.57
Public	10	48.10

Table 9: Mean CCMI by HR Department Presence

HR Department	Count	Mean CCMI
Not Sure	4	74.25
Yes	83	65.81
No	13	42.38

Table 10: Mean CCMI by CISO Presence

CISO Presence	Count	Mean CCMI
Yes	52	76.46
Not Sure	6	62.50
No	42	46.64

The tables above reveal systematic differences in perceived cybersecurity culture maturity across demographic and organizational categories:

- **Age:** Younger respondents (Under 25) report the highest CCMI scores, suggesting a more positive perception of cybersecurity culture among newer workforce entrants.

- **Gender:** Males report higher CCMI scores than females, indicating potential differences in how security culture is experienced or communicated.
- **Work Arrangement:** Fully remote workers score highest, followed by hybrid and on-site workers. This may reflect better digital infrastructure or autonomy in remote settings.
- **Tenure:** Employees with less than 6 months tenure report the highest CCMI, possibly due to onboarding effects or initial optimism.
- **Organization Size:** Larger organizations (>1000 employees) show higher CCMI scores, consistent with literature suggesting that scale supports formalized culture and governance.
- **Sector:** Private sector respondents report higher CCMI than public sector ones, aligning with known challenges in public sector digital transformation.
- **HR Department:** Presence of a dedicated HR department correlates with higher CCMI, supporting the role of HR in shaping culture.
- **CISO Presence:** Organizations with a CISO or cybersecurity team show significantly higher CCMI scores, reinforcing the importance of formal leadership in security.

These comparisons are descriptive and do not imply causality. Further statistical testing (e.g. ANOVA) and longitudinal designs would be needed to establish causal relationships. Some categories (e.g. “Other” sector, “Not Sure” responses) have small sample sizes and should be interpreted with caution.

5.4 Correlation Analysis

To understand how the different components of cybersecurity culture maturity relate to one another, we examined the linear associations between the five CCMI pillars and the overall index score. This analysis helps reveal whether strong performance in one area tends to coincide with strength in others, and whether the index behaves as a coherent whole.

We calculated the Pearson correlation coefficient for each pair of variables using the responses from the 100 participants. The coefficient ‘r’ quantifies the degree of linear relationship between two variables and ranges from -1 to +1. Values close to +1 indicate a strong positive relationship, values near -1 indicate a strong negative relationship, and values near 0 suggest no linear association. To assess the statistical significance of these relationships, we also computed p-values for each correlation.

The Pearson correlation coefficient r is defined as:

$$r_{XY} = \frac{\text{cov}(X, Y)}{\sigma_X \sigma_Y} = \frac{\sum_i (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_i (X_i - \bar{X})^2} \cdot \sqrt{\sum_i (Y_i - \bar{Y})^2}}$$

Values range from -1 to +1:

- $r \approx +1$: strong positive linear relationship
- $r \approx -1$: strong negative linear relationship
- $r \approx 0$: no linear relationship

The results of this analysis are presented in the following tables:

Table 11: Pearson Correlation Matrix

	Leadership & Trust	HRM Involvement	Digital Wellbeing	Security Awareness & Behavior	Hybrid Work Integration	CCMI
Leadership & Trust	1.00	0.87	0.70	0.77	0.82	0.91
HRM Involvement	0.87	1.00	0.74	0.75	0.81	0.92
Digital Wellbeing	0.70	0.74	1.00	0.71	0.75	0.83
Security Awareness & Behavior	0.77	0.75	0.71	1.00	0.94	0.92
Hybrid Work Integration	0.82	0.81	0.75	0.94	1.00	0.96
CCMI	0.91	0.92	0.83	0.92	0.96	1.00

Table 12: Corresponding p-Values

	Leadership & Trust	HRM Involvement	Digital Wellbeing	Security Awareness & Behavior	Hybrid Work Integration	CCMI
Leadership & Trust	0.00e+00	2.41e-31	5.49e-16	3.13e-21	5.88e-26	3.32e-40
HRM Involvement	2.41e-31	0.00e+00	7.16e-19	3.40e-19	4.22e-24	4.59e-41
Digital Wellbeing	5.49e-16	7.16e-19	0.00e+00	1.72e-16	3.89e-19	5.94e-27
Security Awareness & Behavior	3.13e-21	3.40e-19	1.72e-16	0.00e+00	2.37e-46	6.61e-43
Hybrid Work Integration	5.88e-26	4.22e-24	3.89e-19	2.37e-46	0.00e+00	3.88e-54
CCMI	3.32e-40	4.59e-41	5.94e-27	6.61e-43	3.88e-54	0.00e+00

These results reveal several important insights:

- All correlations are positive and strong, with values ranging from 0.70 to 0.96, indicating that the five pillars are highly interrelated.
- The strongest correlation is between Hybrid Work Integration and Security Awareness & Behavior ($r = 0.94$), suggesting that employees who feel well-supported in hybrid work environments also tend to exhibit strong security behaviors.
- Each pillar correlates strongly with the overall CCMI score ($r = 0.83$ to 0.96), confirming that all dimensions contribute meaningfully to the overall perception of cybersecurity culture maturity.
- The extremely low p-values (many $< 10^{-20}$) confirm that these correlations are statistically significant, and unlikely to have occurred by chance.

These findings support the socio-technical framework outlined in Chapter 2, where Leadership, HR practices, Digital Wellbeing, Security Behavior, and Hybrid Work are seen as interdependent components of a mature cybersecurity culture. The data suggest that improvements in one area are likely to positively influence others, reinforcing the need for holistic interventions rather than isolated efforts.

However, it is important to note that these results are based on cross-sectional data, and while they demonstrate strong associations, they do not imply causality. Future research using longitudinal or experimental designs would be necessary to determine the direction of these relationships.

5.5 Analysis of Variance Across Groups

To determine whether individuals from different demographic or organizational backgrounds perceive cybersecurity culture maturity differently, we conducted a one-way Analysis of Variance (ANOVA) on the CCMI scores across eight categorical variables. This statistical test evaluates whether the means of multiple groups differ significantly by comparing the variance between groups to the variance within groups.

The ANOVA results are summarized in the following tables. Table 13 presents the number of groups, degrees of freedom, F-statistics, and p-values for each factor. Table 14 provides the mean CCMI scores for each category within those factors.

Table 13: Summary of One-Way ANOVAs for CCMI

Factor	k	df1	df2	F	p-value	Significance
Age Group	4	3	96	0.35	0.786	Not significant
Gender	2	1	98	8.62	0.004	p < 0.01
Work Arrangement	3	2	97	9.01	0.00026	p < 0.001
Tenure	4	3	96	7.38	0.00017	p < 0.001
Organization Size	4	3	96	21.72	8.04×10^{-11}	p < 0.001
Sector	3	2	97	4.50	0.0135	p < 0.05
HR Presence	3	2	97	13.57	6.36×10^{-6}	p < 0.001

CISO/Cyber Team Presence	3	2	97	101.07	1.90×10^{-24}	p < 0.001
--------------------------	---	---	----	--------	------------------------	---------------------

Note: “k” is the number of groups with at least two observations. “df1” and “df2” are the degrees of freedom for the between-group and within-group variances, respectively.

Table 14: Group Means for CCMI

Factor	Categories and Mean CCMI Scores
Age Group	<ul style="list-style-type: none"> ▪ Under 25: 68.33 ▪ 35–44: 64.19 ▪ 45–54: 63.81 ▪ 25–34: 61.4
Gender	<ul style="list-style-type: none"> ▪ Female: 56.47 ▪ Male: 66.83
Work Arrangement	<ul style="list-style-type: none"> ▪ Flexible on-site: 46.71 ▪ Hybrid: 65.16 ▪ Fully remote: 73.83
Tenure	<ul style="list-style-type: none"> ▪ <6 months: 84.43 ▪ 6–12 months: 56.92 ▪ 1–3 years: 55.80 ▪ >3 years: 66.10
Organization Size	<ul style="list-style-type: none"> ▪ 1–50: 40.92 ▪ 51–250: 52.36 ▪ 251–1000: 62.78 ▪ 1000+: 72.83
Sector	<ul style="list-style-type: none"> ▪ Public: 48.10 ▪ Private: 64.57 ▪ Other: 70.33
HR Department Presence	<ul style="list-style-type: none"> ▪ No: 42.38 ▪ Not sure: 74.25 ▪ Yes: 65.81
CISO/Cybersecurity Team Presence	<ul style="list-style-type: none"> ▪ No: 46.64 ▪ Not sure: 62.50 ▪ Yes: 76.46

These results show that all factors except age group exhibit statistically significant differences in CCMI scores across their categories. For example:

- **Gender:** Male respondents report significantly higher CCMI scores than female respondents.
- **Work Arrangement:** Fully remote workers report the highest maturity, followed by hybrid, with on-site workers reporting the lowest.
- **Tenure:** New employees (<6 months) report the highest CCMI, while those with 1–3 years of tenure report the lowest.

- **Organization Size:** Larger organizations consistently report higher CCMI scores, suggesting that scale may support more mature security cultures.
- **Sector:** Public sector organizations lag behind private and other sectors in perceived maturity.
- **HR and CISO Presence:** Organizations with dedicated HR departments or cybersecurity teams show significantly higher CCMI scores.

These findings reinforce the descriptive trends observed in Section 5.3 and provide statistical confirmation that many demographic and organizational characteristics are associated with meaningful differences in how individuals perceive cybersecurity culture maturity.

5.6 Principal Component Analysis

To explore whether a simpler underlying structure exists within the five CCMI pillars, we conducted a Principal Component Analysis (PCA). This technique helps identify latent dimensions that explain the variance in the data and assesses whether the five pillars reflect a single dominant factor or multiple distinct constructs.

The five pillar scores were first standardized (mean = 0, standard deviation = 1) to ensure comparability. PCA was then applied to the standardized data, producing orthogonal components that successively explain the maximum possible variance.

The results are summarized below:

Table 15: Eigenvalues and Explained Variance

Component	Eigenvalue	% Variance	Cumulative %
1	4.19	82.95%	82.95%
2	0.35	6.95%	89.90%
3	0.32	6.42%	96.32%
4	0.13	2.53%	98.85%
5	0.06	1.15%	100.00%

These results show that the first principal component alone explains approximately 83% of the total variance, indicating a strong general factor underlying the five pillars. According to the Kaiser criterion (eigenvalues > 1), only the first component would be retained, supporting the validity of using a single index like the CCMI.

The component loadings (i.e., the contribution of each pillar to each component) are shown below:

Table 16: Component Loadings

Pillar	Comp 1	Comp 2	Comp 3	Comp 4	Comp 5
Leadership & Trust	0.45	0.01	0.56	0.70	-0.06
HRM Involvement	0.45	0.25	0.49	-0.70	-0.08
Digital Wellbeing	0.42	0.71	-0.54	0.15	-0.03
Security Awareness & Behavior	0.45	-0.53	-0.34	-0.07	-0.63
Hybrid Work Integration	0.47	-0.38	-0.20	0.07	0.77

- **Component 1** loads positively and relatively equally on all five pillars, reinforcing the idea of a unified maturity construct. However, the second and third components reveal subtler contrasts.
- **Component 2** distinguishes Digital Wellbeing (positive loading) from Security Awareness and Hybrid Work Integration (negative loadings), suggesting a latent tension between personal wellbeing and organizational security practices.
- **Component 3** contrasts Leadership & HRM (positive) with Digital Wellbeing and Security Behavior (negative), hinting at a divide between institutional support and individual experience.

These secondary components, while explaining less variance, offer valuable insights into the multidimensional nature of cybersecurity culture. They suggest that while a single index like CCMI is statistically justified, targeted interventions may benefit from considering these nuanced dimensions—especially when addressing specific organizational challenges such as aligning wellbeing initiatives with security behavior or balancing leadership visibility with HR engagement.

In summary, the PCA confirms that the CCMI is a statistically coherent and conceptually valid index. It captures a dominant maturity factor while also preserving interpretable substructures that reflect the complexity of individual experiences within organizational cybersecurity culture.

5.7 Cluster Analysis

To investigate whether individuals naturally group into distinct profiles based on their cybersecurity culture maturity, we applied K-means clustering to the standardized scores of the five CCMI pillars. This method helps identify latent respondent segments that share similar perceptions across the dimensions of Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration.

After standardizing the data (mean = 0, standard deviation = 1), we tested cluster solutions for $k = 2$ to 6. The inertia (within-cluster sum of squares) and silhouette scores (a measure of cluster separation) indicated that $k = 2$ and $k = 3$ were the most interpretable and statistically sound options.

Table 17: Cluster Evaluation Metrics

k	Inertia	Silhouette Score
2	189.19	0.527
3	126.25	0.465
4	107.67	0.427
5	94.51	0.343
6	84.05	0.379

The highest silhouette score was observed at $k = 2$, suggesting a clear separation between two respondent groups. However, $k = 3$ offered richer interpretive value while maintaining acceptable separation.

Table 18: Cluster Profiles ($k=3$)

Cluster	Size	Leadership & Trust	HRM Involvement	Digital Wellbeing	Security Awareness & Behavior	Hybrid Work Integration
0	40	10.68	7.58	9.35	9.45	7.58
1	43	15.49	13.02	12.40	14.91	14.16
2	17	18.24	18.29	15.35	18.76	18.53

These clusters can be interpreted as:

- **Cluster 0 – Low Maturity:** Respondents with consistently low scores across all pillars.
- **Cluster 1 – Moderate Maturity:** Respondents with above-average scores, indicating a reasonably mature culture.
- **Cluster 2 – High Maturity:** Respondents with very high scores, reflecting strong leadership, HR engagement, digital wellbeing, and security behavior.

The k = 2 solution also revealed a clear split:

- **Cluster 0 (n = 41):** Lower scores across all pillars.
- **Cluster 1 (n = 59):** Higher scores across all pillars.

This segmentation supports the idea that cybersecurity culture maturity is not uniformly distributed across individuals. Instead, respondents fall into distinct maturity profiles, which can inform targeted interventions. For example, organizations may prioritize foundational improvements for Cluster 0, while refining specific dimensions for Clusters 1 and 2.

As with previous analyses, this clustering is descriptive, not causal. Future studies could validate these clusters using longitudinal data or more advanced modeling techniques.

5.8 Integrated Interpretation of Findings

Bringing together the results from descriptive statistics, correlation analysis, group comparisons, ANOVA, PCA, and cluster analysis, a coherent picture emerges of how individuals perceive cybersecurity culture maturity within their organizations. These findings directly address the research questions posed in Chapter 1 and align with the socio-technical framework developed in Chapter 2.

The descriptive statistics revealed a moderately mature culture overall (mean CCMI ≈ 63), with substantial variation across individuals. Differences in average scores were observed across gender, work arrangement, tenure, organization size, sector, and the presence of formal structures like HR and CISO functions.

The correlation analysis confirmed strong interdependencies among the five pillars, with coefficients ranging from 0.70 to 0.96 and extremely low p-values. This validates the CCMI as a coherent index and supports the idea that cybersecurity culture operates as an integrated system.

The ANOVA results provided statistical confirmation of group-level differences. All factors except age showed significant variation in CCMI scores, reinforcing the notion

that demographic and organizational context shapes individual perceptions of culture maturity.

The Principal Component Analysis revealed a dominant latent dimension—explaining 83% of the variance—interpreted as a general maturity factor. Secondary components highlighted nuanced contrasts, such as the tension between digital wellbeing and security behavior, or between institutional support and personal experience.

The cluster analysis identified three distinct respondent profiles: low, medium, and high maturity. These clusters aligned with demographic patterns and echoed the findings from ANOVA and PCA, suggesting that individuals experience cybersecurity culture in stratified ways.

Taken together, these findings support a holistic understanding of cybersecurity culture maturity. The CCMI captures a unified construct, but also preserves meaningful subdimensions that reflect the complexity of individual experience. The results encourage both integrated interventions and tailored strategies for specific groups, while also highlighting the need for further research using longitudinal or experimental designs to explore causality.

5.9 Summary

This chapter presented the empirical findings of the study, based on 100 individual responses to the Cybersecurity Culture Maturity Index (CCMI) questionnaire. Through a structured sequence of analyses—descriptive statistics, correlation analysis, group comparisons, ANOVA, principal component analysis, and cluster analysis—we explored how individuals perceive cybersecurity culture maturity within their organizations and how these perceptions vary across demographic and organizational contexts.

The results revealed a moderately mature cybersecurity culture on average, with significant variation across individuals. Strong interdependencies among the five CCMI pillars confirmed the internal coherence of the index, while group-level differences highlighted the influence of factors such as gender, work arrangement, tenure, organization size, sector, and the presence of HR or CISO functions.

The PCA demonstrated that a single dominant component captures the majority of variance, validating the use of the CCMI as a unified index. However, secondary components revealed subtle contrasts that enrich our understanding of how different aspects of culture interact. The cluster analysis further segmented the sample into distinct maturity profiles, offering practical insights for targeted interventions.

Together, these findings provide a comprehensive and nuanced view of cybersecurity culture maturity from the individual's perspective. They support the theoretical framing of culture as a socio-technical system, emphasize the value of context-

sensitive strategies, and lay the groundwork for the discussion and recommendations that follow in the next chapters.

6 Discussion

6.1 Revisiting the Research Questions

This study set out to explore the concept of cybersecurity culture maturity from the perspective of individual employees, with the aim of developing and validating a Cybersecurity Culture Maturity Index (CCMI). The research was guided by the following key questions:

- How can cybersecurity culture maturity be conceptualized and measured at the individual level?
- What are the key dimensions that constitute a mature cybersecurity culture from the employee's perspective?
- Do individual perceptions of cybersecurity culture maturity vary across demographic and organizational factors?
- Can meaningful patterns or profiles of cybersecurity culture maturity be identified among employees?

The findings presented in Chapter 5 provide clear and comprehensive answers to these questions:

- The first question was addressed through the development and application of the CCMI, a structured instrument comprising five theoretically grounded pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. The index was shown to be both conceptually coherent and statistically robust, with high internal consistency and strong inter-pillar correlations.
- The second question was answered through the validation of these five dimensions. Each pillar was found to contribute meaningfully to the overall maturity construct, as evidenced by high correlations with the total CCMI score and strong loadings on the first principal component in the PCA.
- The third question was explored through group comparisons and ANOVA. The results demonstrated that perceptions of cybersecurity culture maturity do indeed vary significantly across several demographic and organizational variables, including gender, work arrangement, tenure, organization size, sector, and the presence of HR and CISO functions. These findings highlight the

importance of context in shaping individual experiences of cybersecurity culture.

- The fourth question was addressed through cluster analysis, which revealed distinct maturity profiles among respondents. These clusters—low, medium, and high maturity—reflected meaningful differences in how individuals perceive their organizational culture, and were associated with specific demographic and organizational characteristics.

In summary, the research questions have been thoroughly examined and answered through a combination of theoretical development and empirical analysis. The next sections of this chapter will delve deeper into the implications of these findings for theory, practice, and future research.

6.2 Interpretation of Key Findings

The results presented in Chapter 5 offer a rich and multi-layered understanding of how individuals perceive cybersecurity culture maturity within their organizations. Several key findings stand out, each contributing to a deeper interpretation of the CCMI and its practical relevance.

First, the strong internal consistency and high inter-pillar correlations confirm that the five dimensions of the CCMI—Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration—are not isolated constructs. Instead, they form a coherent and interdependent system, reflecting the socio-technical nature of cybersecurity culture. This validates the theoretical foundation laid out in Chapter 2 and supports the use of a single aggregated index to represent overall maturity.

Second, the group-level differences observed across demographic and organizational variables underscore the contextual sensitivity of cybersecurity culture. Factors such as gender, work arrangement, tenure, organization size, sector, and the presence of formal HR or cybersecurity structures significantly influence how individuals experience and evaluate their organizational culture. These findings suggest that cybersecurity culture is not uniformly distributed, but rather shaped by the structural and social environment in which individuals operate.

Third, the Principal Component Analysis revealed a dominant latent dimension that captures the majority of variance in the data. This “general maturity” factor reinforces the idea that the CCMI measures a unified construct. However, the presence of secondary components—highlighting tensions between wellbeing and security behavior, or between institutional support and personal experience—adds nuance to the interpretation. These latent dimensions suggest that while overall maturity can be

summarized in a single score, the qualitative experience of culture may differ across individuals and contexts.

Fourth, the cluster analysis identified distinct maturity profiles among respondents. The segmentation into low, medium, and high maturity groups provides a practical framework for targeted interventions. Organizations can use these profiles to tailor their strategies, focusing foundational efforts on low-maturity groups and refining practices for those already exhibiting higher levels of maturity. The demographic composition of these clusters further reinforces the findings from the ANOVA and group comparisons, offering a holistic view of how cybersecurity culture is experienced across the workforce.

Taken together, these findings paint a picture of cybersecurity culture maturity as a complex, multidimensional, and context-dependent phenomenon. The CCMI proves to be a valid and insightful tool for capturing this complexity, offering both a high-level summary and the ability to drill down into specific dimensions and respondent profiles. The next sections will explore the theoretical and practical implications of these findings, as well as the limitations and opportunities for future research.

6.3 Theoretical Implications

The findings of this study contribute meaningfully to the theoretical understanding of cybersecurity culture, particularly when viewed through the lens of individual experience. Several key implications emerge that reinforce, extend, and nuance existing frameworks discussed in the literature review (Chapter 2):

- **Cybersecurity Culture as a Socio-Technical System:** The strong interdependencies among the five CCMI pillars—confirmed through correlation analysis and principal component analysis—support the conceptualization of cybersecurity culture as a socio-technical system. This aligns with the view that culture is shaped not only by technological infrastructure and formal governance, but also by human behavior, psychological wellbeing, and organizational dynamics. The coherence of the CCMI as a unified construct validates this integrated perspective and suggests that interventions targeting one domain are likely to influence others.
- **Individual-Level Measurement of Culture:** By operationalizing cybersecurity culture maturity at the individual level, this study addresses a gap in the literature, which has traditionally focused on organizational or departmental assessments. The CCMI offers a scalable and perception-based tool that captures how employees experience culture in their daily work. This approach complements existing models and provides a more inclusive and granular understanding of maturity, especially in hybrid and decentralized work environments.

- **The Role of Leadership and HRM:** The prominence of Leadership & Trust and HRM Involvement in both the PCA and cluster analysis reinforces their foundational role in shaping culture. These findings echo theoretical work on transformational leadership, psychological safety, and HR-driven cultural alignment, suggesting that visible, trustworthy leadership and structured HR practices are critical enablers of cybersecurity maturity. The data also support the idea that culture is not only top-down but also experienced through interpersonal and procedural interactions.
- **Digital Wellbeing and Hybrid Work as Cultural Dimensions:** The inclusion of Digital Wellbeing and Hybrid Work Integration as pillars of the CCMI reflects an evolution in how cybersecurity culture is theorized. These dimensions are often overlooked in traditional models, yet the findings show they are statistically and conceptually integral to the maturity construct. This supports emerging literature that positions wellbeing and work modality as security-relevant factors, especially in post-pandemic organizational contexts.
- **Multidimensionality and Latent Structure:** The PCA revealed that while a dominant maturity factor exists, secondary components capture latent tensions and contrasts—such as between wellbeing and security behavior, or between institutional support and personal experience. This suggests that cybersecurity culture is not monolithic, but rather composed of interrelated subdimensions that may vary in salience across individuals and contexts. Theoretical models should therefore account for this multidimensionality, allowing for both holistic and targeted interpretations.

In summary, the study reinforces the theoretical framing of cybersecurity culture as a complex, dynamic, and context-sensitive phenomenon. It validates the CCMI as a theoretically grounded instrument and encourages future models to integrate psychological, behavioral, and structural elements in a unified framework.

6.4 Practical Implications

The findings of this study offer several actionable insights for organizations seeking to assess, understand, and improve their cybersecurity culture maturity. The Cybersecurity Culture Maturity Index (CCMI), developed and validated through this research, provides a scalable, perception-based tool that can be used to benchmark maturity, identify vulnerabilities, and guide strategic interventions:

- **Benchmarking and Diagnosis:** Organizations can use the CCMI to benchmark their cybersecurity culture maturity at the individual level. By aggregating scores across departments, roles, or demographic groups, leaders can identify areas of strength and weakness. The five-pillar structure allows for granular

diagnosis, enabling targeted improvements in leadership visibility, HR engagement, digital wellbeing, security behavior, or hybrid work integration.

- **Tailored Interventions:** The group comparisons and cluster analysis revealed that not all employees experience culture equally. For example, on-site workers, mid-tenure employees, women, and staff in small or public-sector organizations tend to report lower maturity scores. These insights support the design of tailored interventions that address the specific needs of different employee segments. Rather than applying one-size-fits-all solutions, organizations can prioritize resources where they are most needed.
- **Leadership and HR Strategy:** The strong influence of Leadership & Trust and HRM Involvement on overall maturity underscores the importance of visible leadership commitment and structured HR practices. Organizations should invest in leadership development, psychological safety, onboarding programs, and continuous training to reinforce cultural norms. HR departments play a critical role in embedding cybersecurity values into recruitment, performance management, and employee engagement.
- **Digital Wellbeing and Hybrid Work:** The inclusion of Digital Wellbeing and Hybrid Work Integration as core dimensions of the CCMI reflects the evolving nature of work. Organizations must recognize that wellbeing and work modality are security-relevant factors. Providing tools, support, and clear policies for remote and hybrid work can enhance both employee satisfaction and security behavior. Initiatives that reduce technostress and promote autonomy may indirectly strengthen the overall culture.
- **Strategic Planning and Policy Development:** The CCMI can inform strategic planning, helping organizations align cybersecurity culture with broader governance, risk, and compliance (GRC) objectives. By integrating CCMI results into policy development, internal audits, and risk assessments, organizations can move beyond compliance checklists toward a resilient, human-centered security posture.
- **Continuous Improvement and Monitoring:** Because CCMI is perception-based and easy to administer, it can be used for ongoing monitoring of cultural maturity. Organizations can track changes over time, evaluate the impact of interventions, and adjust strategies accordingly. This supports a continuous improvement mindset, where culture is treated as a dynamic asset rather than a static condition.

In summary, the CCMI offers a practical framework for organizations to measure, understand, and improve their cybersecurity culture. It enables both high-level

strategic alignment and targeted operational action, making it a valuable tool for leaders, HR professionals, and security teams alike.

6.5 Limitations of the Study

While the findings of this study offer valuable insights into cybersecurity culture maturity from the individual perspective, several limitations must be acknowledged. These limitations pertain to the study's design, methodology, and scope, and should be considered when interpreting the results and applying them in practice:

- **Cross-Sectional Design:** The study employed a cross-sectional survey design, capturing perceptions at a single point in time. While this approach is effective for identifying associations and patterns, it does not allow for the examination of causal relationships or changes over time. Longitudinal studies would be needed to assess how cybersecurity culture evolves and how interventions impact maturity.
- **Self-Reported Data:** All data were collected through self-reported questionnaires, which are inherently subject to response biases such as social desirability, recall bias, and subjective interpretation. Although anonymity was preserved to encourage honest responses, the absence of behavioral or observational data limits the ability to validate perceptions against actual practices.
- **Sample Size and Representativeness:** The sample consisted of 100 respondents, which is sufficient for exploratory analysis but may not be representative of all sectors, roles, or organizational types. Certain subgroups (e.g., "Other" sector, "Not sure" responses) were small, limiting the reliability of comparisons. Future studies should aim for larger and more diverse samples to enhance generalizability.
- **Lack of Behavioral and Organizational Metrics:** The study focused exclusively on individual perceptions, without incorporating objective organizational metrics such as incident rates, compliance records, or audit outcomes. While the CCMI captures subjective experience effectively, integrating behavioral data would provide a more comprehensive view of cybersecurity culture maturity.
- **Instrument Scope and Structure:** The CCMI was designed with equal weighting across five pillars, and each pillar was measured using four Likert-scale items. While this structure supports simplicity and comparability, it may oversimplify complex constructs or overlook nuances within each domain. Future iterations of the instrument could explore alternative scoring models, expanded item sets, or adaptive formats.

- **Interpretation of Statistical Models:** The use of statistical techniques such as PCA and cluster analysis provides valuable insights but should be interpreted with caution. These methods are descriptive, not inferential, and their results depend on the specific sample and assumptions made. Replication and validation in other contexts are necessary to confirm the robustness of the latent structures and respondent profiles identified.

In summary, while the study offers a strong foundation for understanding cybersecurity culture maturity at the individual level, its limitations highlight the need for ongoing refinement, methodological triangulation, and broader empirical validation. These considerations will inform the recommendations and future research directions outlined in the next section.

6.6 Directions for Future Research

This study lays the groundwork for a deeper understanding of cybersecurity culture maturity from the individual perspective, but it also opens several promising avenues for future research. One of the most immediate opportunities lies in adopting longitudinal designs that can track changes in cybersecurity culture over time. Such studies would allow researchers to move beyond static snapshots and begin to explore causal relationships—for example, whether improvements in leadership visibility or HR engagement lead to measurable shifts in security behavior or digital wellbeing. Longitudinal data would also enable the evaluation of specific interventions and organizational changes, providing a dynamic view of cultural evolution.

Complementing the perception-based nature of the CCMI with behavioral and qualitative data would further enrich future studies. Incorporating metrics such as incident reports, compliance records, or system usage logs could help validate self-reported perceptions against observable behavior. Similarly, interviews or focus groups could uncover the lived experiences behind the survey responses, offering a more holistic and nuanced understanding of cybersecurity culture.

Another important direction involves testing the CCMI across diverse organizational contexts. Applying the index in different industries, geographic regions, and cultural settings would help assess its generalizability and reveal sector-specific or culturally influenced variations in how cybersecurity culture is perceived and enacted. This would also support the development of localized or industry-specific adaptations of the CCMI.

Refining the instrument itself is another area for exploration. Future iterations of the CCMI could experiment with alternative scoring models, expanded item sets, or adaptive formats that respond to organizational priorities or individual roles. For example, weighting certain pillars more heavily in high-risk environments or

introducing behavioral anchors could enhance the instrument's diagnostic power and relevance.

The cluster analysis conducted in this study revealed distinct maturity profiles among respondents, suggesting that segmentation-based strategies may be effective. Future research could design and test targeted interventions for each cluster, evaluating their impact on shifting individuals toward higher maturity. This approach could lead to more efficient and impactful culture-building efforts, tailored to the specific needs of different employee groups.

Finally, integrating the CCMI into broader organizational governance, risk, and compliance frameworks presents a valuable opportunity. Future studies could explore how cultural maturity assessments can inform strategic planning, risk management, and performance evaluation processes. This would elevate cybersecurity culture from a peripheral concern to a core organizational capability, aligned with long-term resilience and human-centered security practices.

In summary, future research should aim to deepen, broaden, and operationalize the insights gained from this study. By expanding the methodological toolkit, validating the instrument across contexts, and linking culture to organizational outcomes, researchers can continue to advance the field and contribute to more adaptive, inclusive, and effective cybersecurity strategies.

7 Proposed Framework

7.1 Purpose and Scope of the Framework

The purpose of the proposed framework is to translate the empirical insights gained from the development and application of the Cybersecurity Culture Maturity Index (CCMI) into a practical, actionable model that organizations can use to assess, interpret, and improve their cybersecurity culture. While the CCMI provides a robust measurement tool, the framework presented in this chapter goes a step further by offering strategic guidance on how to interpret results, identify maturity levels, and implement targeted interventions.

This framework is designed to be individual-centric, reflecting the core premise of the study: that cybersecurity culture is experienced and shaped at the level of the individual. It recognizes that employees are not passive recipients of organizational policies but active participants in shaping and sustaining security culture. By focusing on individual perceptions, the framework enables organizations to uncover hidden vulnerabilities, understand cultural dynamics, and foster more inclusive and resilient security practices.

The scope of the framework is intentionally broad yet adaptable. It is suitable for organizations of varying sizes, sectors, and maturity levels, and can be integrated into existing governance, risk, and compliance (GRC) structures, HR processes, and security awareness programs. Whether used for benchmarking, strategic planning, or continuous improvement, the framework provides a structured pathway for organizations to move from reactive compliance toward proactive cultural resilience.

In the sections that follow, the framework will be presented in detail, including its design principles, maturity levels, application scenarios, and implementation guidelines. The goal is to equip organizations with a comprehensive and flexible toolset for cultivating a cybersecurity culture that is not only technically sound but also psychologically safe, behaviorally consistent, and organizationally embedded.

7.2 Design Principles

The proposed framework is built on a set of guiding principles that reflect both the theoretical foundations of cybersecurity culture and the practical realities of organizational life. These principles ensure that the framework is not only conceptually sound but also usable, scalable, and adaptable across diverse contexts.

At its core, the framework is individual-centric. It recognizes that cybersecurity culture is experienced at the level of the employee, and that meaningful change must begin with understanding how individuals perceive, internalize, and act upon cultural signals. This principle is embedded in the structure of the CCMI itself, which captures personal perceptions across five key domains.

The framework is also designed to be scalable and sector-agnostic. Whether applied in a small startup, a multinational enterprise, or a public-sector institution, the framework accommodates varying levels of organizational complexity. It does not assume the presence of specific roles or structures, but rather adapts to the realities of each organization, making it suitable for both mature and emerging cybersecurity environments.

Another key principle is integration. The framework is intended to complement existing governance, risk, and compliance (GRC) systems, HR processes, and security awareness programs. Rather than operating in isolation, it can be embedded into strategic planning, performance management, and organizational development efforts, enhancing alignment between cybersecurity and broader organizational goals.

The framework emphasizes actionability. It is not merely a diagnostic tool but a strategic instrument that guides decision-making. By linking maturity levels to specific indicators and interventions, it enables organizations to move from insight to impact. The structure supports both high-level benchmarking and targeted action, making it useful for executives, HR professionals, and security teams alike.

Finally, the framework is adaptive. It acknowledges that cybersecurity culture is dynamic and context-sensitive. Organizations evolve, technologies change, and employee needs shift. The framework is designed to accommodate these changes, supporting continuous improvement and iterative refinement over time.

Together, these design principles ensure that the proposed framework is not only grounded in research but also ready for real-world application. In the next section, the framework itself will be presented in detail, including its structure, components, and operational logic.

7.3 The Cybersecurity Culture Maturity Framework (CCMF)

The Cybersecurity Culture Maturity Framework (CCMF) is the practical embodiment of the insights gained through the development and application of the CCMI. It provides a structured model that organizations can use to interpret CCMI results, assess their current cultural maturity, and plan targeted improvements. The framework is designed to be both diagnostic and developmental—helping organizations understand where they stand and how they can progress.

At its foundation, the CCMF is built around the five pillars of the CCMI:

- Leadership & Trust
- HRM Involvement
- Digital Wellbeing
- Security Awareness & Behavior
- Hybrid Work Integration

Each pillar represents a distinct domain of cybersecurity culture, and together they form a comprehensive view of how individuals experience and engage with security-related values, behaviors, and structures in their organization.

The CCMF introduces a four-level maturity model, which maps the aggregated and pillar-specific CCMI scores to qualitative descriptors of cultural maturity. These levels are:

- **Low Maturity:** Characterized by fragmented leadership, limited HR engagement, low awareness, poor digital wellbeing, and minimal support for hybrid work. Security is perceived as reactive and compliance-driven.
- **Moderate Maturity:** Some structures and practices are in place, but inconsistencies exist. Leadership is visible but not fully trusted, HR involvement is procedural, and awareness is present but not embedded. Hybrid work and wellbeing are acknowledged but under-supported.

- **High Maturity:** Leadership is trusted and proactive, HR is engaged in culture-building, awareness is widespread and behaviorally consistent, digital wellbeing is actively supported, and hybrid work is well-integrated. Security culture is strategic and inclusive.
- **Advanced Maturity:** Culture is deeply embedded across all levels. Employees feel psychologically safe, empowered, and aligned with organizational values. Security is seen as a shared responsibility and a source of resilience. Continuous improvement is institutionalized.

The CCMF allows organizations to map their current state based on CCMI scores and identify which pillars require attention. It also supports pillar-specific maturity tracking, enabling targeted interventions in areas such as leadership development, HR integration, wellbeing programs, or hybrid work policy refinement.

In its visual form, the CCMF can be represented as a matrix or radar chart, showing each pillar's maturity level and the overall cultural profile. This visualization helps communicate findings to stakeholders and supports strategic planning.

The framework is designed to be iterative and adaptable. Organizations can use it for one-time assessments or integrate it into ongoing culture audits. It complements existing GRC and HR tools, and can be embedded into onboarding, training, and performance management systems.

In the next sections, we will define the maturity levels in more detail, explore application scenarios, and provide implementation guidelines to help organizations operationalize the CCMF effectively.

7.4 Maturity Levels and Progression Pathways

The Cybersecurity Culture Maturity Framework (CCMF) defines four distinct levels of maturity that organizations can use to interpret their CCMI results and guide their development efforts. These levels reflect increasing degrees of cultural integration, behavioral consistency, and strategic alignment across the five pillars of cybersecurity culture.

Each level is characterized by specific attributes that describe how individuals experience leadership, HR involvement, digital wellbeing, security behavior, and hybrid work integration. The progression from one level to the next represents a shift from reactive, fragmented practices toward proactive, embedded cultural norms.

The four maturity levels are:

- **Level 1 - Low Maturity:** At this stage, cybersecurity culture is underdeveloped. Leadership may be absent or distrusted, HR involvement is minimal, and security awareness is low or inconsistent. Employees may feel unsupported in

hybrid work environments and experience digital fatigue or technostress. Security is perceived as a compliance burden rather than a shared responsibility.

- **Level 2 - Moderate Maturity:** Organizations at this level have begun to establish cultural foundations. Leadership is visible but not fully trusted, HR processes exist but are not strategically aligned, and awareness programs are present but not behaviorally embedded. Hybrid work and wellbeing are acknowledged but inconsistently supported. Culture is emerging but lacks cohesion.
- **Level 3 - High Maturity:** Cybersecurity culture is well-integrated across the organization. Leadership is trusted and proactive, HR is engaged in culture-building, and employees demonstrate consistent security behavior. Digital wellbeing is actively supported, and hybrid work is seamlessly integrated into daily operations. Security is seen as a strategic enabler and part of the organizational identity.
- **Level 4 - Advanced Maturity:** At this level, cybersecurity culture is deeply embedded and continuously evolving. Employees feel psychologically safe, empowered, and aligned with organizational values. Leadership and HR work in tandem to reinforce norms, and security behavior is second nature. Digital wellbeing and hybrid work are optimized, and the organization fosters a culture of resilience, adaptability, and continuous improvement.

Organizations can use these maturity levels to map their current state, identify gaps, and define progression pathways. For example, a company scoring in the Moderate Maturity range may focus on strengthening leadership visibility, aligning HR practices with security goals, and improving support for hybrid work. Progression is not linear or uniform—different pillars may evolve at different rates, and interventions should be tailored accordingly.

By linking CCMI scores to these maturity levels, the framework provides a clear roadmap for cultural development. It enables organizations to move from fragmented practices to strategic resilience, guided by a structured understanding of what cybersecurity culture looks like at each stage.

7.5 Application Scenarios

The Cybersecurity Culture Maturity Framework (CCMF) is designed to be versatile and applicable across a range of organizational contexts. Its structure allows for both strategic and operational use, making it a valuable tool for leaders, HR professionals, cybersecurity teams, and organizational development practitioners. Below are several key scenarios in which the framework can be effectively applied:

- Organizations can use the CCMF for self-assessment and benchmarking, either as a standalone exercise or integrated into broader governance, risk, and compliance (GRC) processes. By administering the CCMI across departments, roles, or business units, organizations can generate a cultural maturity profile that highlights strengths and vulnerabilities. This enables internal benchmarking and supports cross-functional dialogue about cultural alignment and improvement priorities.
- The framework also supports strategic planning. Leadership teams can use CCMI results to inform cybersecurity strategy, align cultural initiatives with business objectives, and allocate resources more effectively. For example, if Digital Wellbeing scores are consistently low across the organization, this may signal the need for investment in employee support programs, workload management, or digital ergonomics.
- Another valuable application is in tailored interventions. The cluster analysis conducted in Chapter 5 revealed distinct maturity profiles among employees. Organizations can use these profiles to design targeted programs for specific groups—such as onboarding enhancements for new hires, leadership development for mid-level managers, or hybrid work support for on-site staff. This segmentation-based approach ensures that interventions are relevant, efficient, and impactful.
- The CCMF can also be used for policy development and refinement. By mapping CCMI results to maturity levels, organizations can identify gaps in existing policies and practices. For instance, low scores in Hybrid Work Integration may prompt a review of remote work policies, communication protocols, or digital collaboration tools. The framework provides a structured lens through which to evaluate whether policies are aligned with cultural maturity goals.
- In training and awareness programs, the CCMF can guide content development and delivery. Security awareness initiatives can be tailored to the maturity level of the audience, ensuring that messaging resonates and drives behavior change. For example, employees in low-maturity clusters may benefit from foundational training, while those in high-maturity clusters may be ready for advanced simulations or peer-led workshops.
- Finally, the framework supports continuous improvement and monitoring. Organizations can re-administer the CCMI periodically to track progress, evaluate the impact of interventions, and adjust strategies as needed. This creates a feedback loop that reinforces cultural development and embeds cybersecurity culture into the rhythm of organizational life.

In all these scenarios, the CCMF serves as a strategic enabler, helping organizations move from reactive compliance to proactive cultural resilience. It translates individual perceptions into organizational insight and provides a roadmap for building a cybersecurity culture that is inclusive, adaptive, and aligned with long-term goals.

7.6 Implementation Guidelines

To ensure that the Cybersecurity Culture Maturity Framework (CCMF) delivers practical value, organizations must approach its implementation with clarity, structure, and commitment. The following guidelines outline a recommended process for deploying the framework effectively, from initial assessment to continuous improvement:

- The first step is to administer the CCMI questionnaire across the organization. This can be done digitally and anonymously to encourage honest responses. It is important to ensure broad participation across departments, roles, and demographics to capture a representative view of the culture. The questionnaire should be accompanied by a clear explanation of its purpose and how the results will be used.
- Once responses are collected, the next step is to analyze the data. This involves calculating individual and aggregate scores for each of the five pillars, as well as the overall CCMI score. Organizations may choose to segment the data by role, tenure, location, or other relevant factors to identify patterns and disparities. Visualization tools such as radar charts or heatmaps can help communicate findings to stakeholders.
- With the scores in hand, organizations can map results to the CCMF maturity levels. This involves interpreting both the overall score and the pillar-specific scores to determine where the organization stands and which areas require attention. The maturity level descriptors provided in Section 7.4 serve as a reference for this mapping.
- Based on the maturity profile, organizations should prioritize interventions. For example, low scores in Leadership & Trust may prompt leadership development programs, while gaps in Digital Wellbeing may call for initiatives to reduce technostress or improve work-life balance. Interventions should be tailored to the specific needs of the organization and its employee segments, as identified through cluster analysis or group comparisons.
- To support long-term cultural development, organizations should establish a process for monitoring progress over time. This may involve re-administering the CCMI at regular intervals (e.g., annually or biannually), tracking changes in scores, and evaluating the impact of interventions. Embedding the CCMF into

existing HR, GRC, or organizational development cycles can help institutionalize this process.

- Finally, it is essential to communicate findings and actions transparently. Sharing results with employees, explaining the rationale behind interventions, and inviting feedback fosters trust and engagement. Cybersecurity culture is not built through mandates alone—it requires participation, dialogue, and shared ownership.

By following these guidelines, organizations can move from measurement to meaningful change. The CCMF provides the structure; successful implementation depends on leadership commitment, cross-functional collaboration, and a willingness to engage with culture as a strategic asset.

7.7 Benefits and Strategic Value

The Cybersecurity Culture Maturity Framework (CCMF) offers organizations a structured, evidence-based approach to understanding and improving their cybersecurity culture. Its benefits extend beyond measurement, providing strategic value across multiple dimensions of organizational life:

- One of the most immediate benefits is clarity. The framework translates abstract concepts of culture into tangible, measurable components. By breaking down cybersecurity culture into five pillars and mapping them to maturity levels, organizations gain a clear view of where they stand and what needs attention. This clarity supports informed decision-making and helps align security initiatives with broader organizational goals.
- The CCMF also enhances strategic alignment. By integrating cybersecurity culture into governance, risk, and compliance (GRC) processes, HR strategies, and leadership development, the framework ensures that culture is not treated as a siloed concern. Instead, it becomes a cross-functional priority that supports resilience, trust, and performance across the organization.
- Another key benefit is targeted action. The framework enables organizations to move beyond generic awareness campaigns and design interventions that are tailored to specific maturity levels, employee segments, or cultural gaps. This improves the efficiency and effectiveness of security programs, ensuring that resources are directed where they will have the greatest impact.
- The CCMF supports continuous improvement. Its structure allows for periodic reassessment, enabling organizations to track progress, evaluate the impact of interventions, and adapt strategies over time. This fosters a culture of learning and responsiveness, where cybersecurity is seen not as a static goal but as an evolving capability.

- Importantly, the framework promotes employee engagement. By centering the individual experience, it encourages organizations to listen to their people, understand their needs, and build culture from the ground up. This can lead to greater buy-in, stronger behavioral alignment, and a more inclusive approach to security.
- Finally, the CCMF contributes to organizational resilience. In an era of increasing digital complexity and threat exposure, a mature cybersecurity culture is a strategic asset. It enables organizations to anticipate risks, respond effectively to incidents, and maintain trust with stakeholders. The framework helps embed this culture into the fabric of the organization, making security a shared responsibility and a source of competitive advantage.

In summary, the CCMF is more than a diagnostic tool—it is a strategic enabler. It empowers organizations to understand their culture, act on insights, and build a cybersecurity posture that is resilient, adaptive, and aligned with their values and mission.

8 Conclusions and Recommendations

8.1 Summary of the Study

This study set out to explore how cybersecurity culture maturity can be conceptualized, measured, and interpreted through the lens of the individual. Recognizing that cybersecurity culture is often treated as an organizational abstraction, the research aimed to bring the individual experience to the forefront—capturing how employees perceive, engage with, and contribute to the cultural dimensions of cybersecurity within their workplace.

To achieve this, the study developed the Cybersecurity Culture Maturity Index (CCMI), a structured instrument composed of five pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. These pillars were grounded in a socio-technical framework and informed by an extensive literature review.

The CCMI was administered to a sample of 100 respondents, and the resulting data were analyzed using a range of statistical techniques. Descriptive statistics revealed a moderately mature culture overall, with significant variation across individuals. Correlation analysis confirmed strong interdependencies among the pillars, validating the coherence of the index. Group comparisons and ANOVA demonstrated that perceptions of maturity vary meaningfully across demographic and organizational factors. Principal Component Analysis identified a dominant latent dimension of maturity, while cluster analysis revealed distinct respondent profiles.

Building on these insights, the study introduced the Cybersecurity Culture Maturity Framework (CCMF)—a practical model that organizations can use to interpret CCMI results, assess their current maturity level, and plan targeted interventions. The framework defines four maturity levels and provides progression pathways, application scenarios, and implementation guidelines.

Together, the CCMI and CCMF offer a comprehensive approach to understanding and improving cybersecurity culture from the individual perspective. They bridge the gap between theory and practice, enabling organizations to move from reactive compliance to proactive cultural resilience.

8.2 Contributions to Knowledge

This study makes several important contributions to the academic and practical understanding of cybersecurity culture, particularly by shifting the focus toward the individual experience of culture maturity. Through the development and validation of the Cybersecurity Culture Maturity Index (CCMI), and the introduction of the Cybersecurity Culture Maturity Framework (CCMF), the research advances both conceptual clarity and applied methodology in the field.

One of the most significant contributions is the individual-centric measurement of cybersecurity culture. While previous models have often assessed culture at the organizational or departmental level, this study demonstrates that meaningful insights can be gained by examining how employees perceive and engage with cultural elements in their daily work. This approach offers a more inclusive and granular understanding of maturity, especially in hybrid and decentralized environments.

The study also contributes a novel measurement instrument—the CCMI—which operationalizes cybersecurity culture across five empirically and theoretically grounded pillars: Leadership & Trust, HRM Involvement, Digital Wellbeing, Security Awareness & Behavior, and Hybrid Work Integration. The instrument was shown to be internally consistent, statistically coherent, and conceptually valid, offering a reliable tool for future research and organizational assessment.

In addition, the research introduces the Cybersecurity Culture Maturity Framework (CCMF), a practical model that translates CCMI results into actionable insights. The framework defines four maturity levels and provides progression pathways, application scenarios, and implementation guidelines. It bridges the gap between measurement and strategic action, enabling organizations to move from reactive compliance to proactive cultural development.

The study also contributes to the theoretical discourse by reinforcing the view of cybersecurity culture as a socio-technical system. The findings support the idea that culture is shaped by the interplay of leadership, HR practices, individual behavior,

psychological wellbeing, and work modality. The identification of latent dimensions and maturity profiles adds nuance to this understanding, suggesting that culture is both unified and multidimensional.

Finally, the research offers a methodological contribution through its use of mixed statistical techniques—including correlation analysis, ANOVA, PCA, and cluster analysis—to explore the structure and variability of cybersecurity culture maturity. These methods provide a robust analytical foundation for future studies and demonstrate how quantitative data can be used to uncover meaningful cultural patterns.

In sum, this study advances the field by providing a validated instrument, a strategic framework, and a set of empirical insights that deepen our understanding of cybersecurity culture from the individual perspective. It lays the groundwork for future research, policy development, and organizational practice aimed at building more resilient, inclusive, and adaptive security cultures.

8.3 Recommendations for Organizations

Based on the findings of this study and the development of the Cybersecurity Culture Maturity Index (CCMI) and Framework (CCMF), several practical recommendations can be made for organizations seeking to assess and improve their cybersecurity culture maturity:

- First, organizations should consider adopting the CCMI as a regular assessment tool. By administering the questionnaire across departments and roles, organizations can gain a detailed understanding of how cybersecurity culture is perceived at the individual level. This enables targeted diagnostics and supports strategic planning.
- Second, organizations should use the CCMF to interpret CCMI results and guide interventions. Mapping scores to maturity levels across the five pillars allows for a nuanced understanding of strengths and weaknesses. This supports prioritization of resources and the design of tailored programs that address specific cultural gaps.
- Third, leadership teams should invest in visible and trustworthy leadership practices. The study showed that Leadership & Trust is a foundational pillar of culture maturity. Leaders should model security-conscious behavior, communicate openly about risks and expectations, and foster psychological safety.
- Fourth, HR departments should be actively involved in embedding cybersecurity culture into organizational processes. This includes integrating security values into recruitment, onboarding, training, performance

management, and employee engagement initiatives. HRM Involvement was shown to be a strong predictor of overall maturity.

- Fifth, organizations should recognize Digital Wellbeing and Hybrid Work Integration as security-relevant domains. Supporting employees in managing digital fatigue, maintaining work-life boundaries, and navigating hybrid work environments contributes to a healthier and more secure culture. These areas should be addressed in both policy and practice.
- Sixth, organizations should design interventions based on maturity profiles and cluster segmentation. Employees in low-maturity clusters may benefit from foundational training and support, while those in high-maturity clusters may be ready for advanced engagement or peer leadership roles. This segmentation-based approach ensures relevance and efficiency.
- Finally, organizations should treat cybersecurity culture as a dynamic capability, not a static attribute. Regular reassessment using the CCMI, combined with iterative use of the CCMF, supports continuous improvement. Embedding culture assessment into broader governance and development cycles ensures that cybersecurity remains aligned with organizational evolution.

By following these recommendations, organizations can move beyond compliance and toward a culture of shared responsibility, resilience, and strategic alignment in cybersecurity.

8.4 Recommendations for Policymakers and Regulators

The findings of this study have implications not only for individual organizations but also for policymakers, regulators, and sectoral bodies responsible for shaping cybersecurity standards and practices at a broader level. As cybersecurity threats continue to evolve, the importance of fostering a resilient and adaptive culture across industries and public institutions becomes increasingly clear.

Policymakers should consider promoting individual-centric approaches to cybersecurity culture assessment. Traditional compliance frameworks often focus on organizational structures and technical controls, overlooking the lived experience of employees. The CCMI offers a scalable and validated tool for capturing individual perceptions, which can complement existing standards and provide a more holistic view of cultural maturity.

Regulatory bodies may also explore integrating CCMI-like instruments into sectoral guidelines or certification schemes. For example, maturity assessments could be included as part of cybersecurity audits, risk assessments, or organizational readiness evaluations. This would encourage organizations to move beyond checkbox compliance and engage with culture as a strategic asset.

In sectors where cybersecurity is critical—such as healthcare, finance, energy, and government—regulators could mandate periodic culture assessments to ensure that organizations are not only technically secure but also culturally prepared. These assessments could inform policy development, resource allocation, and incident response planning.

Policymakers should also support research and innovation in cybersecurity culture measurement, including the development of behavioral indicators, longitudinal tracking tools, and sector-specific adaptations of the CCMI. Funding and collaboration opportunities could accelerate the refinement and adoption of culture-focused methodologies.

Finally, regulators can play a role in raising awareness about the importance of cybersecurity culture. By including culture in national strategies, public campaigns, and professional development programs, they can help shift the narrative from reactive compliance to proactive resilience—where culture is recognized as a cornerstone of cybersecurity readiness.

In summary, policymakers and regulators have an opportunity to elevate cybersecurity culture as a strategic priority. By embracing individual-centric tools like the CCMI and encouraging their integration into standards and practices, they can help build more secure, adaptive, and human-centered digital environments.

8.5 Final Reflections

This thesis began with a simple yet profound question: how do individuals experience cybersecurity culture, and how can that experience be meaningfully measured and improved? In answering this question, the study has moved beyond traditional, top-down conceptions of culture and embraced a more inclusive, bottom-up perspective—one that recognizes the central role of the individual in shaping and sustaining secure organizational environments.

The development of the Cybersecurity Culture Maturity Index (CCMI) and the accompanying Cybersecurity Culture Maturity Framework (CCMF) represent a step forward in both theory and practice. They offer a way to quantify what has often been considered intangible, and to translate that understanding into actionable strategies. By focusing on individual perceptions, the study has illuminated the human side of cybersecurity—where trust, wellbeing, leadership, and daily behavior intersect with policy, technology, and risk.

Perhaps most importantly, the findings underscore that cybersecurity culture is not a static attribute or a compliance checkbox. It is a dynamic, evolving system that reflects the values, structures, and lived experiences of people within an organization. It is shaped by leadership, reinforced by HR, influenced by work environments, and

enacted through everyday behaviors. As such, it demands continuous attention, thoughtful design, and inclusive engagement.

This research has laid a foundation, but it is only the beginning. There is much more to explore—across sectors, cultures, and time. As organizations continue to navigate the complexities of digital transformation, the need for resilient, human-centered cybersecurity cultures will only grow. The tools and insights presented here are intended to support that journey, offering a compass for those who seek to build not just secure systems, but secure communities.

9 Appendices

9.1 Appendix A: CCMI Questionnaire

The CCMI questionnaire consists of two sections:

- Section A: Demographic and Organisational Context
- Section B: Cybersecurity Culture Perception Items (CCMI)

All responses are anonymous and based on the participant's personal experience within their current organisation.

Section A: Demographic and Organisational Context

1	What is your current job role?				
	General Employee	Manager / Team Leader	HR Professional	IT / Security Professional	Other
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	How many years have you worked in your current organization?				
	Less than 6 months	6-12 months	1-3 years	More than 3 years	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	What is your age group?				
	Under 25	25–34	35–44	45–54	55+
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	What is your gender?				
	Male	Female	Prefer not to say		Other
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

5	What is the size of your organization?	Small (1-50 employees) <input type="checkbox"/>	Medium (51-250 employees) <input type="checkbox"/>	Large (251+ employees) <input type="checkbox"/>	Huge (1000+ employees) <input type="checkbox"/>
6	Does your organization have a dedicated HR department?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Not sure <input type="checkbox"/>	
7	Does your organization have a dedicated Cybersecurity Officer (CISO) or cybersecurity team?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Not sure <input type="checkbox"/>	
8	What sector does your organization operate in?	Public <input type="checkbox"/>	Private <input type="checkbox"/>	Non-profit / NGO <input type="checkbox"/>	Other <input type="checkbox"/>
9	What is your current work arrangement?	Flexible on-site <input type="checkbox"/>	Hybrid <input type="checkbox"/>	Fully remote <input type="checkbox"/>	

The CCMI questionnaire is a standardized instrument designed to assess the maturity of cybersecurity culture from the perspective of individual employees. It consists of 20 items, each rated on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The items are grouped into five thematic pillars, with four items per pillar.

Participants are asked to indicate their level of agreement with the following statements:

Section B: CCMI – Cybersecurity Culture Perception Items

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
Leadership & Trust					
1	I feel psychologically safe when reporting cybersecurity concerns to my manager or supervisor.				
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2	Organizational leaders consistently model secure behavior in their daily practices.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Leadership visibly integrates cybersecurity priorities into strategic decisions and communications.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	I trust that leadership takes cybersecurity risks seriously and acts transparently when incidents occur.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HRM Involvement						
5	Cybersecurity responsibilities are clearly communicated during onboarding and role transitions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	HR policies promote secure digital behavior and are reinforced through regular awareness initiatives.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	The organization provides regular, role-relevant cybersecurity training coordinated by HR.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	HR actively promotes a culture of security through recognition, feedback, and collaboration with other departments.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Digital Wellbeing						
9	I am able to maintain healthy boundaries between work and personal life when working digitally.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	The digital tools I use support my productivity without causing unnecessary stress or distraction.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	My organization provides resources or guidance to help manage digital fatigue and screen time.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	My organization actively supports emotional resilience in digitally demanding work conditions.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Awareness & Behavior						

13	I can recognize common indicators of phishing, social engineering, and suspicious digital activity.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	I understand the organization's cybersecurity policies and how they apply to my role.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	I know the appropriate steps to take when encountering a potential security threat.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	I apply secure practices consistently, even under time pressure or competing priorities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hybrid Work Integration						
17	I receive clear instructions on how to securely access systems and data when working remotely.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18	My organization regularly updates cybersecurity protocols to reflect hybrid work realities.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	I feel confident using secure communication tools when collaborating across locations.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	I feel confident identifying and mitigating cybersecurity risks specific to hybrid work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

This instrument provides a structured and scalable foundation for evaluating cybersecurity culture maturity, enabling organizations to identify strengths, address gaps, and benchmark progress across multiple scoring models.

Bibliography

Abeebe, M. (2020). Digital wellbeing as a dynamic construct. *Communication Theory*, 31. <https://doi.org/10.1093/ct/qtaa024>

Alexei, A., & Alexei, A. (2023). The difference between cyber security vs information security. *Journal of Engineering Science*, 29, 72–83. [https://doi.org/10.52326/jes.utm.2022.29\(4\).08](https://doi.org/10.52326/jes.utm.2022.29(4).08)

Alexander, A., De Smet, A., Langstaff, M., & Ravid, D. (2021). *What employees are saying about the future of remote work*. McKinsey & Company.

Alasoini, T., Hirvonen, S., & Käsälä, M. (2025). *Hybrid work model as a success factor: Guide to the opportunities and challenges of hybrid work*. Finnish Institute of Occupational Health. ISBN 978-952-391-198-7

Alhogail, A., & Mirza, A. (2014). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*. <https://doi.org/10.1109/WCCAIS.2014.6916579>

Alnatheer, M. A. (2015). Information security culture critical success factors. In *2015 12th International Conference on Information Technology – New Generations (ITNG)* (pp. 731–735). <https://doi.org/10.1109/ITNG.2015.124>

Anderson, A. B., Ahmad, A., & Chang, S. (2022). Competencies of cybersecurity leaders: A review and research agenda. *ICIS 2022 Proceedings*, 9.

Auffret, J.-P., Snowdon, J., Stavrou, A., Katz, J., Kelley, D., Rahman, R., Stein, F., Sokol, L., Allor, P., & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, 17, 1740001. <https://doi.org/10.1142/S0219265917400011>

Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research* (6/2016).

Büchi, M. (2024). Digital well-being theory and research. *New Media & Society*, 26(1), 172–189. <https://doi.org/10.1177/14614448211056851>

Critical success factors for cyber security leaders: Not just technical competence. (n.d.). *People + Strategy*, 39.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4, 13–21. <https://doi.org/10.22215/timreview/835>

Edegbeme-Beláz, A., Krasznay, C., & Mihály, S. (2020). Cybersecurity strategy and leadership management issues.

Flores, M. F. (2019). Understanding the challenges of remote working and its impact to workers. *International Journal of Business Marketing Management*, 4, 40–44.

Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., & Toscano, F. (2021). Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement, and stress. *Journal of Occupational and Environmental Medicine*, 63, e426–e432. <https://doi.org/10.1097/JOM.0000000000002236>

Handoko, B. L., Riantono, I. E., & Gani, E. (2020). Importance and benefit of application of governance risk and compliance principle. *Systematic Reviews in Pharmacy*, 11(9), 510–513.

Henke, J., Jones, S., & O'Neill, T. (2022). Skills and abilities to thrive in remote work: What have we learned. *Frontiers in Psychology*, 13. <https://doi.org/10.3389/fpsyg.2022.893895>

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13, 247–255. <https://doi.org/10.1016/j.istr.2008.10.010>

Jokinen, T. (2005). Global leadership competencies: A review and discussion. *Journal of European Industrial Training*, 29, 199–216. <https://doi.org/10.1108/03090590510591085>

Krajčák, M., Schmidt, D., & Barath, M. (2023). Hybrid work model: An approach to work–life flexibility in a changing environment. *Administrative Sciences*, 13, 150. <https://doi.org/10.3390/admsci13060150>

Knapp, K., Marshall, T., & Ford, F. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14, 24–36. <https://doi.org/10.1108/09685220610648355>

Lim, J., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. *Australian Information Security Management Conference*.

Mikołajczyk, K. (2024). Digital well-being of managers in the hybrid workplace. *International Journal of Contemporary Management*, 60. <https://doi.org/10.2478/ijcm-2024-0006>

Mira da Silva, M. (2011). A conceptual model for integrated governance, risk and compliance. In *Lecture Notes in Business Information Processing* (Vol. 6741, pp. 199–213). https://doi.org/10.1007/978-3-642-21640-4_16

Nicho, M., Khan, S., & Rahman, M. S. M. K. (2017). Managing information security risk using integrated governance risk and compliance. In *Proceedings of COMAPP* (pp. 56–66). <https://doi.org/10.1109/COMAPP.2017.8079741>

Papazafeiropoulou, A., & Spanaki, K. (2015). Understanding governance, risk and compliance information systems (GRC IS): The experts' view. *Information Systems Frontiers*, 18. <https://doi.org/10.1007/s10796-015-9572-3>

Piggin, R. S. H. (2014). Governance, risk and compliance: Impediments and opportunities for managing operational technology risk in industrial cybersecurity and safety. In *9th IET International Conference on System Safety and Cyber Security (2014)* (pp. 1–8). <https://doi.org/10.1049/cp.2014.0982>

Popovici, V., & Popovici, A.-L. (2020). Remote work revolution: Current opportunities and challenges for organizations. *Ovidius University Annals, Economic Sciences Series*, 20(1), 468–472.

Przybyszewski, K., Małagocka, K., & Przymus, Z. (2024). Identifying cyber-risk factors in hybrid workforce environments.

Reyes-Quezada, F. A. (2025). Digital well-being in hybrid work: Risks, resilience, and strategies for sustainable performance. *SSRN*. <https://doi.org/10.2139/ssrn.4567890>

Roffarello, A., & Russis, L. (2022). Achieving digital wellbeing through digital self-control tools: A systematic review and meta-analysis. *ACM Transactions on Computer-Human Interaction*, 30. <https://doi.org/10.1145/3571810>

Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *South African Computer Journal*, 31, 46–52.

Taherdoost, H. (2022). Cybersecurity vs. information security. *Procedia Computer Science*, 215, 483–487. <https://doi.org/10.1016/j.procs.2022.12.050>

Thangavel, S. (2025). Cybersecurity consciousness in hybrid work: The dominant role of organizational and technological support.

Triplett, W. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2, 573–586. <https://doi.org/10.3390/jcp2030029>

van der Ham, J. (2021). Towards a better understanding of “cybersecurity.” *Digital Threats: Research and Practice*, 2. <https://doi.org/10.1145/3442445>

van Niekerk, J. (2010). Information security culture: A management perspective. *Computers & Security*, 29, 476–486. <https://doi.org/10.1016/j.cose.2009.10.005>

van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>

Veiga, A., & Eloff, J. (2002). Information security culture. In *IFIP TC11, 17th International Conference on Information Security (SEC2002)* (pp. 203–214). https://doi.org/10.1007/978-0-387-35586-3_16