Leadership Influence on Cybersecurity Culture Development

Hamdi Khamis

Year of publication 2026

Laurea University of Applied Sciences

Leadership Influence on Cybersecurity Culture Development

Hamdi Khamis

Master of business administration

Thesis

March, 2026

Laurea University of Applied Sciences **Abstract**

Leading Transformational change

Master of business administration

Hamdi Khamis

Leadership Influence on Cybersecurity Culture Development

Year 2026 Number of pages 73

This exploratory thesis examines how leadership approaches appear to influence the development of cybersecurity culture, and how organizational context may shape culture-building mechanisms. Using an exploratory mixed-methods design, the study integrates (1) a thematic literature review, (2) two illustrative documentary case studies (Princeton University and Liberty Mutual) based on published materials, and (3) an exploratory survey of 12 Chief Information Security Officers (CISOs) and senior security leaders administered between August 28, 2025 and September 3, 2025.

The case studies suggest how context shapes feasible leadership strategies: decentralized academic environments tend to require influence-based approaches that build trust and participation, while regulated corporate environments can embed secure behavior through formal management systems, structured communications, and reinforcement mechanisms. Survey findings indicate that transformational and adaptive leadership are the most frequently reported primary styles (33.3% each). Half of respondents (50.0%) reported a "Managed" level of cybersecurity culture maturity, while fewer reported "Optimizing" maturity (16.7%), suggesting that sustained continuous improvement remains difficult. The most frequently cited barrier to culture development was lack of executive support (33.3%), followed by competing priorities and resource constraints (25.0% each).

This thesis contributes a preliminary conceptual framework linking leadership approach, organizational levers, and culture maturity, and provides initial guidance for leaders seeking to move beyond compliance-oriented programmes toward sustained, human-centered secure behavior. Given the study's exploratory nature and methodological limitations—including the use of documentary case studies based on secondary sources and a small survey sample—the findings represent preliminary insights that require further validation through future research.

Keywords: Culture, Leadership, Organizational Change, Context-Sensitive Framework, CISO Survey, Exploratory Research

Author's Declaration on the Use of Artificial Intelligence

I, Hamdi Khamis, hereby declare that this thesis is the product of my own original research, analysis, and intellectual effort.

In the course of writing this document, I utilized generative Artificial Intelligence (AI) language models as a supportive tool. The use of these tools was strictly limited to the following auxiliary tasks:

- Editing and Proofreading: Assisting with grammar, spelling, punctuation, and sentence structure.
- Clarity and Readability: Suggesting alternative phrasing and reformatting sentences to improve flow and comprehension.
- Brainstorming and Idea Structuring: Helping to organize thoughts and structure arguments during the drafting process.

The core research, including the literature review, data collection, case study analysis, interpretation of findings, and the formulation of the final conclusions, was conducted entirely by the author. All sources have been appropriately cited, and the final text, including any AI-assisted revisions, has been critically reviewed and approved by the author to ensure it accurately reflects my own work and arguments. I take full responsibility for the academic integrity and originality of this thesis

Contents

1. Introduction

1.1 Background and Context

In an era defined by digital transformation, cyber threats pose significant challenges to organizations across all sectors and sizes. Organizations find themselves in a state of heightened vigilance against evolving cyber adversaries, with the financial and reputational consequences of breaches continuing to escalate. Traditional approaches to cybersecurity have emphasized technological controls and policy compliance, yet human factors remain implicated in the majority of security incidents.

The conventional view has long characterized employees as the weakest link in the security chain. However, contemporary thinking increasingly recognizes employees as potential assets in organizational defense. This perspective shift underpins the concept of cybersecurity culture—the collective mindset, shared assumptions, and behavioral norms that shape how organizational members approach security-related decisions and actions. Rather than viewing culture as a soft or peripheral concern, emerging research positions it as fundamental to organizational resilience against cyber threats.

This thesis explores the relationship between leadership and cybersecurity culture development within organizational contexts. It examines how leaders may influence the cultivation of security-conscious behavior and investigates how organizational context appears to shape the effectiveness of different leadership approaches. The research is grounded in the premise that cybersecurity culture is not an accidental outcome but can be deliberately fostered through intentional leadership practices adapted to specific organizational circumstances.

1.2 Problem Statement

Despite substantial investments in security technologies and comprehensive policy frameworks, many organizations continue to experience security breaches attributed to human factors. This persistent vulnerability suggests limitations in technology-centric approaches to cybersecurity. The challenge lies in recognizing that security is not solely a technical issue but involves complex interactions among individual psychology, group dynamics, and organizational culture. While policies can prescribe desired behaviors, they cannot by themselves instill the intrinsic motivation and situational awareness required to navigate the complexities of the modern threat landscape.

Leadership's influence on organizational culture is well-established in management literature, yet its specific application to cybersecurity culture development remains underexplored. There is a need to better understand how different leadership approaches may foster security consciousness and how these approaches might need to be adapted to different organizational contexts. Existing frameworks often present generic solutions that may not account for the significant variations in organizational structure, industry requirements, regulatory environments, and existing cultural norms.

This research addresses this gap by exploring the relationship between leadership and cybersecurity culture through multiple lenses: a synthesis of existing literature, illustrative case studies of contrasting organizational contexts, and preliminary survey data from security leaders. The goal is to develop initial insights that can inform both future research and practical approaches to culture development.

1.3 Research Objectives

This exploratory research examines the relationship between leadership and cybersecurity culture development within organizational contexts. It seeks to move beyond generic approaches by investigating how context may shape the effectiveness of different leadership strategies. The specific objectives are:

- To explore the relationship between leadership approaches and cybersecurity culture development within organizational contexts. This involves examining how different leadership styles—including transformational, transactional, servant, and adaptive leadership—appear to influence security-related attitudes and behaviors based on existing literature and illustrative cases.

- To investigate contextual factors that may influence leadership-driven cybersecurity culture change. This includes an initial examination of how factors such as organizational size, industry sector, regulatory environment, and pre-existing cultural norms appear to shape the relationship between leadership and culture, providing a foundation for future research on their potential may interact with.

- To develop a preliminary conceptual framework for context-sensitive cybersecurity culture development. This framework aims to synthesize insights from the literature review, case studies, and survey to propose a model that can

guide future research and offer initial guidance for practitioners seeking to diagnose their organizational context and select appropriate leadership strategies.

To provide initial, evidence-informed recommendations for leaders and organizations. These recommendations are intended to offer preliminary guidance for strengthening cybersecurity culture, acknowledging that further validation through future research will be necessary to establish their broader applicability.

1.4 Research Questions

At the heart of this research lies a central exploratory question:

- How do leadership approaches appear to influence the development of cybersecurity culture, and how might this relationship be shaped by organizational context? To address this central question, the research explores three supporting inquiries: What leadership styles and practices are reported or observed in organizations that have undertaken cybersecurity culture development initiatives, and what patterns emerge regarding their apparent effectiveness?

- In what ways do contextual factors—such as organizational structure, industry characteristics, and regulatory environment—appear to influence the relationship between leadership and cybersecurity culture?

- What strategies do leaders report using or are observed employing to cultivate cybersecurity culture, and how do these strategies appear to vary across different organizational contexts?

1.5 Significance of the Study

This exploratory research aims to contribute to both academic understanding and practitioner knowledge in the domain of cybersecurity culture. For the academic community, it offers a context-sensitive examination of the leadership-culture relationship in cybersecurity, addressing a gap in existing literature. The research provides a preliminary conceptual framework that can serve as a foundation for future empirical

studies and offers initial evidence supporting the importance of the human element in cybersecurity.

For practitioners, this research provides an alternative perspective to generic, one-size-fits-all approaches to security culture development. It offers a preliminary, evidence-informed guide for leaders seeking to understand how organizational context may shape the effectiveness of different culture-building strategies. By proposing a framework for diagnosing organizational context and considering appropriate leadership approaches, this research aims to support leaders in moving beyond purely compliance-based approaches toward more human-centered strategies for fostering security consciousness.

It is important to note that given the exploratory nature of this study and its methodological limitations, the findings should be viewed as preliminary insights that warrant further investigation rather than validated best practices.

1.6 Scope and Limitations

This study explores the relationship between leadership and cybersecurity culture within specific organizational contexts. The scope is intentionally focused on three complementary research activities: (1) a thematic synthesis of existing literature on leadership, organizational culture, and cybersecurity; (2) an illustrative analysis of two distinct organizational contexts through documentary case studies; and (3) an exploratory survey of senior security leaders to gather preliminary data on their perspectives and experiences.

Several important limitations must be acknowledged:

- Exploratory Nature: This research is exploratory and theory-building in orientation. It does not seek to establish causal relationships or produce statistically generalizable findings. Its primary aim is to develop a preliminary conceptual model and identify patterns that can inform future research.

- Documentary Case Study Methodology: The analysis of Princeton University and Liberty Mutual is based on previously published research and publicly available materials, not on primary data collected by the author. Consequently, the insights are filtered through the perspectives and research goals of the original authors. This approach, while suitable for the exploratory nature of this thesis and common in Master's-level research, restricts the depth of analysis and prevents the kind of

nuanced, firsthand understanding that could be achieved through direct interviews or observational research. The findings from these cases should therefore be considered illustrative examples rather than definitive evidence.

- Limited Survey Sample: The CISO survey includes 12 respondents, which is insufficient for statistical generalization. The survey data provides indicative patterns and preliminary insights rather than conclusive evidence. The findings represent the perspectives of a small group of security leaders and may not reflect the broader population.

- Organizational Focus: The study is confined to organizational contexts and does not extend to broader societal or national dimensions of cybersecurity culture. While the research examines contrasting organizational contexts (academic and corporate), it does not claim to cover all possible organizational environments.

- Preliminary Framework: The proposed framework is conceptual and preliminary. It synthesizes insights from multiple sources but has not been validated through longitudinal study or tested across a broad range of organizations. The framework should be interpreted as a starting point for discussion and future research rather than a validated model.

Consequently, the findings of this research should be interpreted as preliminary insights and proposed relationships that require further validation through future empirical work, not as established principles or generalizable conclusions.

1.7 Thesis Structure

This thesis is organized to progressively build understanding of the relationship between leadership and cybersecurity culture, with each chapter contributing to the development of a preliminary conceptual framework.

- Chapter 1: Introduction establishes the research context, articulates the problem statement, defines the research objectives and questions, discusses the study's significance, and acknowledges its scope and limitations.

- Chapter 2: Literature Review synthesizes existing knowledge on cybersecurity culture, leadership, and organizational change through a thematic approach. It critically examines key theories, frameworks, and empirical findings to establish

the theoretical foundation for this research and identify gaps that motivate the empirical components of the study.

- Chapter 3: Research Methodology provides a detailed account of the research design, explaining the rationale for the exploratory mixed-methods approach and describing the specific data collection and analysis methods employed in the literature review, case studies, and CISO survey.

- Chapter 4: Case Study Analysis presents an illustrative analysis of two organizations—Princeton University and Liberty Mutual—that have undertaken cybersecurity culture development initiatives. These documentary case studies, based on published research, offer contrasting examples of how leadership approaches and organizational context interact in practice.

- Chapter 5: CISO Survey Analysis presents the exploratory findings from the survey of 12 CISOs and senior security leaders, providing preliminary quantitative data to complement the qualitative insights from the literature and case studies.

- Chapter 6: Discussion and Recommendations synthesizes findings from all previous chapters to propose a preliminary conceptual framework for context-sensitive cybersecurity culture development. It offers initial, evidence-informed recommendations for leaders while acknowledging the need for further validation.

- Chapter 7: Conclusion summarizes the key findings and contributions of the research, discusses its practical implications, acknowledges its limitations, and identifies directions for future research in this domain.

2. Literature Review

2.1 Scope and Structure: A Thematic Synthesis

Cybersecurity culture has emerged as a central concern in both academic research and organizational practice. This prominence stems from a fundamental recognition: many cyber incidents are not caused by a lack of technological defenses, but rather by how individuals interpret risk and make decisions under the everyday pressures of organizational life. In this thesis, cybersecurity culture is understood as the collective tapestry of shared assumptions, unspoken norms, and ingrained practices that shape

how employees approach security-related decisions—particularly when they are busy, under pressure, or navigating trade-offs between productivity and protection.

Rather than offering a simple chronological summary of prior research, this chapter synthesizes the existing literature through five interconnected thematic lenses. This approach recognizes that in any real-world organization, culture, leadership, and behavior are inextricably intertwined. The five organizing categories are:

- Organizational Culture and Cybersecurity: Exploring how the overarching organizational culture sets the stage for security-related attitudes and actions.
- Leadership and Cybersecurity: Examining how leaders can effectively champion and embed a security-conscious mindset throughout the organization.
- Employee Behavior and Security Compliance: Investigating the complex factors that drive individual employees to either adhere to or circumvent security protocols.
- Context-Sensitive Approaches to Cybersecurity: Highlighting the need to tailor security strategies to the unique operational and cultural context of an organization.
- Cybersecurity Culture Assessment and Development: Detailing the methods for measuring the current state of a security culture and fostering its development over time.

Within each category, the discussion focuses on what the literature implies for managers and cybersecurity leaders: what to measure, where culture is likely to break down, and which levers are realistically available to influence behavior at scale. The chapter concludes with an integrated synthesis that connects these five streams into a conceptual model and identifies gaps that motivate the empirical portion of this study.

2.2 Organizational Culture and Cybersecurity

2.2.1 Organizational Culture as a Managerial Control System

Organizational culture is frequently described as a pattern of shared meanings that guides how members interpret situations and behave, particularly under ambiguity and time pressure. As Jerab and Mabrouk (2023) have argued, culture operates like an “invisible hand”—it shapes decision-making, coordination, and problem-solving, and leadership is

central to how values and norms are communicated and reinforced. From this perspective, culture is not simply a soft attribute of organizations; it is the behavioral infrastructure that stabilizes expectations and reduces the transaction costs of coordination. This is of paramount importance for cybersecurity because many protective actions are discretionary—reporting near misses, challenging unusual requests, pausing work to verify identity—and these behaviors are difficult to mandate through formal rules alone.

Culture-change research also frames leaders as cultural architects. Leaders send cultural signals through what they pay attention to, what they reward, and how they respond when things go wrong (Jerab & Mabrouk, 2023). This is especially relevant for cybersecurity because initiatives often rely on symbolic artifacts (policies, training modules, posters), while employees calibrate their behavior to lived incentives such as workload, deadlines, and managerial tolerance of workarounds. When leaders treat cybersecurity as a peripheral compliance requirement, employees learn that it can be traded off against more visible performance outcomes. Conversely, when leaders build cyber risk into operational priorities and resource allocation, they reduce the perceived conflict between getting the job done and doing it securely.

2.2.2 Defining Cybersecurity Culture and Distinguishing Adjacent Concepts

Cybersecurity culture is commonly defined as shared assumptions, values, and behavioral norms that influence how people protect organizational information and systems. Huang and Pearlson (2019) argue that culture sits behind the unwritten rules employees rely on in daily work, and that resilience is shaped by the routine choices made across the workforce rather than by specialist security teams alone. Willie (2023) similarly frames cybersecurity culture as an organizational capability that aligns people, processes, and technology around the protection of assets and continuity of operations, while recognizing that it is embedded in broader organizational culture. In combination, these definitions place cybersecurity in strategic and identity-based terrain, not as a technical add-on.

Information security culture (ISC) is sometimes used interchangeably with cybersecurity culture (CSC), but the literature implies subtle differences. ISC research has a strong tradition of operationalizing culture into measurable dimensions and tracking change over time(Da Veiga & Eloff, 2010); Da Veiga & Martins, 2015). CSC work tends to pay greater

attention to evolving threats, including social engineering and ecosystem risk, and to contemporary workplace conditions such as remote work, vendor reliance, and cross-functional communication (Huang & Pearlson, 2019) Osburn, 2025). Nasir et al. (2019) caution that definitional inconsistency persists because studies often adopt different boundaries and dimension sets without explaining why. For this thesis, the implication is that the concept of culture should be fit for purpose: broad enough to incorporate leadership, work design, and meaning making, yet specific enough to guide measurement and intervention.

2.2.3 Frameworks, Initiatives, and Continuous Improvement Cycles

Culture frameworks attempt to make a broad, abstract concept manageable by breaking it into components that can be assessed and influenced. Da Veiga and Eloff (2010) provide an influential example by proposing both a framework and an assessment instrument for information security culture. Their starting point is behavioral: information security success depends heavily on what employees do, so organizations need guidance to build a security-aware culture. The managerial contribution is practical. Culture is treated as a measurable condition that can be diagnosed, benchmarked, and improved through targeted interventions, rather than as something beyond managerial influence.

Da Veiga and Eloff's (2010) approach also highlights a key methodological choice: culture is operationalized through dimensions that can be observed through survey items and everyday organizational practices. This supports leadership action because it helps identify weak areas and prioritize resources. Longitudinal work further strengthens the link between diagnosis and improvement. Da Veiga and Martins (2015) show how repeated measurement, paired with implementation and monitoring actions, can support culture improvement over time.

Alhogail and Mirza (2014) extend the framework tradition by focusing explicitly on how culture change unfolds. Rather than assuming culture will follow automatically once policies and training exist, they position cultural transition as a change-management challenge that requires planning, stakeholder engagement, communication, and sustained reinforcement. This is particularly relevant to leadership because resistance, fear, and confusion are expected responses to new security expectations. Treating non-compliance as simple deviance overlooks the organizational work required to make new behaviors understandable, legitimate, and practically achievable.

2.2.4 Measuring Culture and Awareness as Governance Practices

A central managerial question is whether cybersecurity culture can be measured in ways that support governance decisions, rather than producing superficial scores. Da Veiga and Eloff (2010) argue that organizations need diagnostic capability to understand the state of their information security culture and to identify targeted improvement areas. Their assessment approach implies an iterative governance cycle: assess culture, interpret results, implement interventions, and reassess. In an MBA context, this resembles a management control cycle in which measurement informs resource allocation and accountability.

Da Veiga and Martins (2015) strengthen this assessment-to-governance link by showing how monitoring and implementation actions can improve culture over time. Their case study highlights that culture data can be used to prioritize developmental areas, with awareness and training programs as visible facets of improvement. The leadership implication is that measurement is not an end in itself. Meaningful improvement only occurs when there is genuine commitment to act on findings, provide necessary funding for interventions, and address underlying structural impediments such as ill-defined roles, ineffective communication channels, or misaligned incentives.

2.2.5 Practice-Based Mechanisms for Building Cybersecurity Culture

The literature on organizational culture also emphasizes that culture is built through repeated practices and rituals, not through policies alone. Alshaikh (2020) identifies concrete mechanisms for enhancing cybersecurity culture in Australian organizations: identifying and promoting key security behaviors, establishing networks of cybersecurity champions, cultivating a distinct brand for the internal security team, creating a centralized hub for security resources, and aligning awareness campaigns with broader organizational events. These initiatives provide managers with actionable pathways for translating abstract cultural goals into concrete, institutionalizable mechanisms.

The concept of a champion network is particularly powerful. By embedding security advocates within business units, these networks bridge the gap between central security teams and the day-to-day operational realities of the workforce. This serves as an antidote to the credibility problem that many CISOs experience. When security messages emanate exclusively from a central, often physically remote, security team, they can be dismissed as out of touch. However, when reinforced by peers and local champions, security

becomes more socially normalized and more responsive to the unique constraints of different organizational parts.

2.3 Leadership and Cybersecurity

2.3.1 The CISO Role, Organizational Credibility, and Cultural Constraints

Leadership influence in cybersecurity is frequently discussed through the Chief Information Security Officer (CISO) and related governance roles. A(Ashenden & Sasse, 2013) examine CISOs and organizational culture using interviews and organizational behavior theory. They show that CISOs often struggle to gain credibility and influence because of limited formal power, uncertainty about role identity, and difficulty engaging employees effectively. The study demonstrates that security leadership effectiveness is shaped as much by organizational structures and cultural expectations about authority as by technical expertise.

A strategic risk follows from this credibility problem. When CISOs lack authority, security initiatives can be experienced as external impositions rather than shared

organizational commitments, leading to superficial compliance alongside informal norms that prioritize local performance goals. The implication is that cybersecurity culture development requires distributed leadership. Middle managers and business leaders must reinforce expectations and build security into operational planning; otherwise, the CISO becomes symbolically accountable for security without being empowered to shape the everyday conditions that drive behavior.

2.3.2 Human Factors Leadership and Strategic Communication

(Triplett, 2022) focuses on the human factors challenges cybersecurity leaders face. The work highlights how vulnerabilities can emerge from organizational conditions such as weak strategic implementation, unsatisfactory execution, and poor alignment between plans and reality. This framing supports an important managerial interpretation: many incidents reflect systemic weaknesses in organizational design and leadership, not simply individual carelessness.

The human factors lens also implies that leadership effectiveness depends on cross functional collaboration. Cybersecurity leaders must work with HR, operations, and line management to shape behavioral expectations and reduce error likelihood through better design. In practice, this includes choosing communication strategies that resonate with different employee groups, acknowledging workload and cognitive burden, and ensuring

awareness initiatives are supported by usable tools. Human factors therefore reinforces the view that culture is a socio-technical outcome produced through interactions between people and work environments.

2.3.3 Transformational Leadership Mechanisms: Support, Identity, and Discretionary Effort

Transformational leadership is often proposed as a driver of cultural change because it shapes meaning, motivation, and identity. Dinc et al. (2022) examine transformational leadership in the banking sector and show how leadership dimensions such as inspirational motivation and individual consideration influence perceived organizational support, which then affects organizational identity. While this is not a cybersecurity study, the mechanisms are relevant because cybersecurity culture development depends on discretionary behaviors beyond formal compliance, such as reporting suspicious activity, helping colleagues adopt safer practices, and raising concerns that may slow work.

The mediating role of perceived organizational support is particularly important. When employees believe the organization values their contribution and cares about their wellbeing, they may be more willing to invest effort in protective behaviors that are not immediately rewarded by performance metrics (Dinc, 2022). Organizational identity matters for the same reason: security-first aspirations require employees to internalize security as part of “who we are” as an organization, not just what we do for auditors. This suggests leadership influences cybersecurity culture through psychological pathways that increase willingness to accept short-term inconvenience for long-term protection.

2.3.4 Transformational IT Leadership and Resilience Integration into Technical Governance

A distinctive contribution in the reviewed sources is the effort to integrate leadership principles into technical security practice. Eseryel et al. (2024) propose the PASTA-TITL framework, embedding Transformational IT Leadership principles into the PASTA threat modeling process. Their argument is that escalating threats require leadership engagement that bridges cybersecurity management and strategic decision-making. By incorporating leadership principles across threat modeling stages, the framework aims to reduce implementation complexity and to encourage proactive engagement in risk management across functions.

The PASTA-TITL proposal is relevant to culture because it treats technical governance as a site of cultural reinforcement (Eseryel, 2024). When leadership practices promote shared

vision, empowerment, and cross-functional participation, threat modeling becomes more than a technical exercise: it becomes a cultural practice that normalizes risk-informed decision making. This suggests leadership influence can be operationalized through participation in governance processes that shape how risk trade-offs are discussed, justified, and documented.

2.3.5 Leadership Shaping Education and Awareness Programmes in SMEs/SMBs

Education and awareness programmes remain the most visible organizational interventions aimed at improving security behavior. The literature, however, suggests that effectiveness depends on design choices that reflect organizational context and learner diversity. (Bada & Nurse, 2019)) propose a cybersecurity education and awareness programme for small and medium-sized enterprises (SMEs), noting that

SMEs often face limited resources, limited specialist staff, and informal processes. These constraints make comprehensive enterprise-style programmes unrealistic. Their approach therefore emphasizes practicality and prioritization, reinforcing the view that culture development must be scaled to organizational capacity.

The SME lens matters because it challenges assumptions that organizations can mandate extensive training, deploy sophisticated measurement tools, and maintain dedicated awareness teams. In many SMEs, leaders have closer contact with employees and can model behavior more visibly, but they may struggle to allocate time to structured governance. Bada and Nurse (2019) thus implicitly strengthen the leadership theme: in resource-constrained settings, leadership attention and role modeling may be a more powerful culture driver than formal controls because leaders can directly shape everyday priorities and norms.

2.3.6 Leadership for Culture Change: Resistance, Fairness, and Reinforcement

Across the reviewed literature, cybersecurity culture development repeatedly resembles organizational change rather than simple training delivery. Alhogail and Mirza (2014) propose a multistep framework for information security culture change grounded in change-management principles to address resistance and confusion.

The change-management framing also integrates fairness and reactance perspectives. If leaders implement controls in ways employees experience as disrespectful or purely controlling, resistance becomes likely (Lowry, Wilson, & Hafer, 2015). Culture-change leadership therefore includes constructing legitimacy: explaining the purpose of controls, demonstrating proportionality, and showing willingness to adapt policies to fit operational

realities. In this sense, cybersecurity culture development is partly political. Leaders have to negotiate trade-offs, align interests, and build shared meaning around protection and risk.

Taken together, the leadership-focused literature suggests that culture cannot be delegated to training teams or policy owners. Leadership influence operates through credibility, communication, prioritization, and the day-to-day governance mechanisms that signal what matters under pressure. In practical terms, leaders shape the conditions under which secure behavior is either supported and normalized —or quietly traded off.

2.4 Employee Behavior and Security Compliance

2.4.1 Rationality-Based Beliefs and the Economics of Compliance

Explaining policy compliance requires a behavioral lens that goes beyond awareness messages. Bulgurcu et al. (2010) develop a model of information security policy compliance that draws on rationality-based beliefs alongside information security awareness. Their findings suggest that compliance intention is shaped by perceived benefits, perceived costs, and beliefs about the effectiveness of policy requirements. This makes the managerial challenge clear: even when employees understand rules, they may judge compliance as costly in time, effort, or disruption, particularly under deadlines and customer-facing pressures.

This also clarifies why generic awareness campaigns often have limited effect. If employees already believe security matters but experience compliance as operationally difficult, additional messaging is unlikely to shift behavior. Leaders must instead reduce compliance costs by redesigning workflows, improving tool usability, and clarifying roles and responsibilities. In MBA terms, compliance often depends on perceived return on effort: when secure action is the path of least resistance, compliance becomes more likely and less dependent on individual heroism.

2.4.2 Protection Motivation and Deterrence as Complementary Explanations

Herath and Rao (2009) explain security policy compliance by combining protection motivation theory and deterrence theory. Protection motivation theory proposes that people are more likely to act protectively when they view a threat as serious, feel vulnerable to it, and believe they can respond effectively without excessive cost. Deterrence theory, by contrast, emphasizes perceived certainty and severity of sanctions

for non-compliance. Herath and Rao's (2009) combined framework is valuable because it mirrors the dual nature of organizational security governance: organizations try to motivate compliance through capability mechanisms (efficacy beliefs and self-confidence) and through control mechanisms (monitoring and sanctions).

The managerial implication is that deterrence without coping support is unlikely to produce sustained culture change. If employees feel threatened with sanctions but lack self-efficacy or face high response costs, they may comply superficially or conceal

non-compliance. Strong coping appraisal—confidence in one's ability to act securely, and belief that secure actions are effective—supports voluntary compliance and the internalization of security norms. Leaders therefore influence compliance by investing in training, resources, and practical support, not only by relying on punitive controls.

2.4.3 Fairness, Reactance, and the Risk of Backlash Following Policy Tightening

A key limitation of control-heavy approaches is that they can trigger resistance. Lowry et al. (2015) examine reactive computer abuse following stricter organizational security policies and explain behavior through fairness theory, psychological reactance, counterfactual reasoning, and organizational trust. Their results suggest that employees can experience policy tightening as a loss of freedom and respond with reactance that ranges from deliberate misuse to "getting back" at the organization. Crucially, perceptions of fairness and adequate explanation reduce reactance by increasing trust, indicating that policy legitimacy is a determinant of behavioral response.

For leadership-focused research, the study offers a clear warning: governance can become self-defeating when leaders treat employees as adversaries rather than stakeholders (Lowry, Wilson, & Hafer, 2015). Stricter controls introduced without credible communication can be interpreted as arbitrary or punitive, especially when they increase work friction. Leaders can mitigate this risk by giving advance notice, explaining the rationale, involving employees in implementation, and showing that policies are designed to protect both the organization and its members. This aligns with change-management principles in culture change frameworks (Alhogail & Mirza, 2014) and reinforces that trust is a protective factor in security outcomes.

2.4.4 Integrating Behavioral Theories into a Culture Perspective

Taken together, rationality-based beliefs, protection motivation, deterrence, and fairness/reactance perspectives provide a multi-layer behavioral foundation for understanding cybersecurity culture. Culture shapes how employees weigh the costs and benefits of compliance, what shortcuts are seen as acceptable, whether managers tolerate workarounds, and whether secure action is perceived as valued.

Culture also shapes threat appraisal through shared interpretations of risk and through organizational narratives about incidents. Finally, culture influences trust and

perceived fairness, which affect whether employees cooperate with security initiatives or resist them. In this sense, behavioral theories and culture frameworks are complementary: behavioral theories explain individual decision processes, while culture frameworks explain how leadership and organizational context create the conditions in which those decisions are made.

2.4.5 Everyday Cybersecurity Behavior, Trade-Offs, and the Normalization of Workarounds

Everyday cybersecurity behavior research helps explain why employees deviate from security expectations. Ertan et al. (2018) synthesize evidence for the UK Cabinet Office and argue that security behavior is best understood through daily organizational routines. Employees often face trade-offs between productivity and security, especially when security tasks add extra steps, delays, or cognitive load. In these conditions, deviations frequently represent adaptive responses to organizational pressures rather than malicious intent.

This perspective implies that culture development cannot rely on enforcement alone. Leaders need to identify where processes and incentives unintentionally encourage insecure behavior. When employees are rewarded for speed and penalized for delays, security requirements that slow work will predictably be bypassed. Workarounds then become normalized locally, creating a culture in practice that differs from the culture described in policy.

The everyday behavior lens also connects directly to rationality-based beliefs: perceived compliance cost is often structural, not merely personal (Bulgurcu, Cavusoglu, &

Benbasat, 2010). The managerial challenge is therefore to redesign work systems so that secure actions are integrated into normal work rather than experienced as exceptional burdens.

2.4.6 Empirical Links Between Culture, Leadership, and Social Engineering Awareness

Leadership and culture arguments are strengthened when they connect to domain specific cybersecurity outcomes.(Olaniyi, 2023) examine how organizational security culture and transformational leadership relate to social engineering awareness among bank employees. Their regression analysis indicates that both culture and transformational leadership are associated with variation in social engineering

awareness. The banking context is important because financial organizations face persistent social engineering threats and rely heavily on employee vigilance and verification as a frontline defense.

Although regression studies do not establish causality in the same way as experiments, Olaniyi et al. (2023) support the plausibility of leadership and culture as predictors of security-relevant capability. For an MBA thesis, the practical implication is that leadership and culture are not only conceptual ideals: they can be linked empirically to measurable outcomes. This strengthens the rationale for studying leadership actions and organizational conditions that help employees recognize and resist manipulation, particularly when attackers exploit trust, urgency, and hierarchy.

In summary, the employee behavior stream explains why security programs can succeed on paper but fail in practice: compliance depends on beliefs about effectiveness and effort, perceptions of fairness and legitimacy, and the practical realities of everyday work. A leadership-driven culture approach therefore needs to address not only knowledge gaps, but also work design, incentives, and trust.

2.5 Context-Sensitive Approaches to Cybersecurity

2.5.1 Security-First Culture as an Identity and Strategy Alignment Concept

The idea of a security-first culture emphasizes that cybersecurity should be treated as a primary organizational priority, built into decision-making rather than positioned as a secondary compliance obligation.(Willie, 2023) argues that achieving a security-first culture requires alignment between organizational values, leadership behavior, and

employee routines so that security is experienced as shared responsibility and part of professional identity. This matters because many risks are created at the boundary between business speed and procedural caution. When employees experience security as an obstacle imposed by outsiders, shortcuts become more attractive; when security is framed as protecting customers, colleagues, and organizational purpose, secure behavior can become a source of professional pride.

At the same time, a security-first message can become counterproductive if it remains rhetorical. Employees quickly detect gaps between leadership slogans and operational reality, for example when performance targets and time pressures implicitly reward

risky workarounds. Handri et al. (2024) identify success factors such as leadership commitment, clear communication, and practical integration of security into workflows, suggesting that security-first is achieved through consistent managerial action rather than branding alone. This aligns with broader organizational culture arguments that culture becomes real through repeated, observable patterns of attention and reinforcement (Jerab & Mabrouk, 2023).

2.5.2 Policies as Organizational Artifacts and Quality Criteria for Usability

Security policies formalize expectations, but policy documents do not automatically translate into secure practice. Karlsson et al. (2017) use practice-based discourse analysis to argue that policy quality should be assessed from the employee perspective. A central insight is that policies embed assumptions about work. When those assumptions do not match how tasks are actually performed, employees are pushed to interpret, adapt, or circumvent requirements in order to deliver their work.

Karlsson et al. (2017) also challenge a common simplification in governance: treating policy existence as a proxy for security. Following incidents, organizations often respond by adding more rules or increasing policy detail. Yet policy proliferation can raise ambiguity, create conflicts, and increase compliance costs. The discourse analysis lens shifts attention from policy quantity to policy usability. For leaders, this implies iterative design: policies should be written in actionable language, tested against workflows, and refined through feedback from end users, alongside providing the resources needed to comply.

2.5.3 From Compliance Metrics to Impact Metrics in Awareness Programmes

Debates about measurement connect directly to criticism of compliance-focused awareness programmes. Haney and Lutters (2023) trace how an organizational awareness programme shifted from compliance metrics (training completion rates) to objectives focused on behavior and attitudes.

Their longitudinal case study shows that this shift is not only a technical matter of choosing better indicators. It is also an organizational and cultural challenge. Awareness teams must manage stakeholder expectations, legacy compliance requirements, and the limited recognition of awareness work as a professional role. In other words, organizations have to value learning and behavioral change enough to reconfigure governance expectations.

From a leadership perspective, the compliance-to-impact shift changes what counts as accountability. When leaders demand simple completion metrics, awareness teams are pushed to optimize for training volume rather than behavioral relevance. When leaders ask for evidence of behavioral outcomes, they create incentives to experiment, tailor content by role, and embed awareness into everyday communication. This aligns with the assessment-to-action cycle in information security culture research (Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015) and reinforces the idea that culture development is a sustained managerial process rather than a one-off campaign.

Emphasis on everyday practice also changes how awareness is conceptualized. (Haney & Lutters, 2023)) show how awareness programmes can evolve from being training event driven to being embedded in organizational practices, communication channels, and professional roles. Their case study suggests that transformation requires new

ways of collaborating with business units, tailoring content to local contexts, and measuring success in terms of outcomes, not attendance. This reinforces a core culture argument: culture is sustained by repeated practices, not occasional interventions.

For leaders, the implication is that awareness is not a peripheral activity owned only by the security function. Programmes become more effective when they are built into managerial routines such as onboarding, team meetings, operational dashboards, and learning reviews after incidents. This aligns with the monitoring-and-implementation emphasis in information security culture improvement research (Da Veiga & Martins,

2015) and suggests that leadership influence is often exercised through institutionalizing practices that make secure behavior normal.

2.5.4 Third-Party Ecosystems, Narratives, and Sensemaking in Cybersecurity Culture

Cyber risk increasingly emerges from organizational ecosystems, not internal operations alone. Outsourcing, cloud services, software supply chains, and Internet of Things deployments create dependencies that extend the attack surface. In this context, cybersecurity culture must also cover how employees interpret and manage third-party risk through procurement decisions, vendor oversight, and day-to-day collaboration with external suppliers. Traditional information security culture frameworks often focus on internal compliance and awareness, but ecosystem realities require cultural capability for negotiation, coordination, and shared accountability.

Osburn (2025) extends cybersecurity culture research by examining narrative practices used to negotiate risk and establish culture in vendor contexts. Through ethnographic observation and interviews, the study analyzes interdisciplinary communication between IT and Facilities professionals working with Internet of Things vendors. The findings show that storytelling, sensemaking, and sensegiving help professionals develop shared interpretations of vendor risk and coordinate decisions. This is a distinctive contribution because it treats culture not only as attitudes or compliance, but as ongoing meaning-making through which organizations navigate uncertainty.

The managerial relevance of this narrative view is its emphasis on cross-functional communication. Vendor risk management involves actors with different professional languages and priorities: IT may focus on technical vulnerabilities, Facilities may focus on operational continuity, and procurement may prioritize cost and contractual terms. Narrative practices can help bridge these differences by creating shared reference points for what counts as risk and what trade-offs are acceptable (Osburn, 2025).

The narrative perspective also points to a leadership responsibility: creating organizational space for interdisciplinary dialogue. Where vendor security is treated as purely contractual or purely technical, important operational concerns can be missed, and accountability becomes diffuse. By supporting joint conversations and shared

learning, leaders can help teams build common ground on vendor expectations, responsibilities, and escalation routes.

More broadly, stories shape what employees perceive as normal, what they fear, and what they believe leaders value. If organizational narratives portray security as a barrier to progress, employees may treat security concerns as optional. If narratives portray security as essential for protecting customers and sustaining operations, employees are more likely to accept verification steps and reporting duties. Leaders therefore influence culture through communication, incident storytelling, and the framing of trade-offs, especially in complex ecosystem settings (Osburn, 2025).

2.5.5 Trends and Success Factors Across Contexts

Handri et al. (2024) contribute to the dimension debate by synthesizing trends and success factors in cybersecurity culture research. Their review indicates growing interest in culture as a determinant of cyber resilience, with repeated emphasis on

leadership commitment, employee engagement, and the integration of security into business processes. The success-factor lens is helpful for bridging academic and managerial concerns because it highlights the enabling conditions for implementation, such as resources, governance structures, and communication channels, rather than treating culture only as an attitudinal variable.

Handri et al. (2024) emphasize success factors such as integration of security into business processes, suggesting that interventions work best when they align with how an organization creates value. For leadership research, context sensitivity means leadership actions should be analyzed alongside operational constraints, governance structures, and strategic priorities, not in isolation.

A context-sensitive lens is especially important for leadership research because it discourages ‘copy-paste’ culture programmes. The literature repeatedly shows that the same control or message can be interpreted differently across roles, sectors, and working conditions, which means leaders must adapt interventions to local realities while still maintaining a coherent organizational direction.

2.6 Cybersecurity Culture Assessment and Development

2.6.1 Dimension Selection and Conceptual Fragmentation in Culture Assessment

A persistent challenge in culture research is the lack of agreement on which dimensions make up information security culture. Nasir et al. (2019) address this directly in a systematic review and show that dimension sets overlap across studies, while authors often provide little justification for why particular dimensions were selected.

This fragmentation is not only an academic concern. It affects comparability between studies and can undermine intervention design. If two organizations assess culture using different dimension sets, they may diagnose different problems and take incompatible actions, even when they face similar risks.

Nasir et al. (2019) also highlight that information security culture is associated with multiple organizational facets, including management support, communication,

awareness, and policy clarity. The broader implication is that culture is multi-causal: single-factor interventions (for example, training alone) are unlikely to be sufficient. A systems view is needed that includes leadership behaviors, organizational structures, and the design of work tasks. For MBA research, one practical response is a context sensitive measurement approach: select dimensions that are theoretically grounded and relevant to the organization's risk profile, and be explicit about why those dimensions were chosen.

2.6.2 Designing and Validating Assessment Instruments in Crisis Conditions

The need for context awareness is reinforced by Georgiadou et al. (2021), who design a cybersecurity culture assessment survey for critical infrastructures during the COVID- 19 crisis. Their framework is layered across organizational and individual levels and operationalized through multiple domains. Importantly, they recognize that external shocks such as pandemics can reshape working conditions, disrupt controls, and create new vulnerabilities. This supports the view that cybersecurity culture is not static: it is tested, and sometimes reshaped, during crises when employees work remotely, rely more on digital tools, and face higher cognitive load and uncertainty.

From a leadership perspective, the (Georgiadou, 2021)instrument highlights a pragmatic issue: measurement tools must reflect the reality of the operating environment. Critical infrastructures face different regulatory demands, risk tolerances, and operational constraints than many private-sector firms. Assessment instruments therefore need to be

adaptable while remaining conceptually coherent. Layered frameworks help because they separate organizational enablers (leadership, policies, resources) from individual behaviors (secure practices, reporting, vigilance).

The COVID-19 crisis illustrates how external shocks can test and reshape cybersecurity culture. Georgiadou et al. (2021) develop a survey instrument for critical infrastructures during the pandemic, recognizing that working conditions and risk exposure changed substantially. Remote work, altered communication patterns, and heavier reliance on digital systems can elevate vulnerability to phishing, credential theft, and misconfiguration. The crisis context underlines that culture is not only about stable norms, but also about how organizations adapt security practices under rapidly changing constraints.

For leaders, the implication is that culture development must include adaptive capacity. Policies and training designed for stable office environments may not

transfer directly to remote or hybrid work. Assessment tools therefore need to capture both organizational enablers (such as communication, support, and governance) and individual practices under new conditions. This reinforces the context-sensitive approach recommended by dimension reviews and success-factor syntheses (Nasir, Ali, & Jhanjhi, 2019)(Handri, 2024).

2.6.3 What Technology Cannot Fix: Modeling Organizational Cybersecurity Culture

Where information security culture frameworks often focus on assessment and improvement cycles, cybersecurity culture models increasingly propose causal pathways that link leadership and context to culture and behavior. Huang and Pearlson (2019) argue that what technology cannot fix is the organizational and human side of cybersecurity. They propose a managerial model that connects leadership attention, communication, and organizational practices to employee behavior. Their case-based analysis illustrates how leaders can intentionally cultivate a culture of data protection by aligning values, policy expectations, and everyday work practices.

A strength of Huang and Pearlson's (2019) model is its recognition that culture operates through both formal and informal channels. Formal mechanisms include policies, standards, and training. Informal mechanisms include peer norms, unwritten rules, and everyday decision heuristics. This aligns with socio-technical views that treat security outcomes as emerging from interactions between people, processes, and technology,

rather than from any single control. For leadership research, the implication is that leaders shape culture not only through messaging but through organizational design choices that reduce ambiguity and friction when employees try to act securely.

2.6.4 Mindset Change: From Human-as-Problem to Human-as Solution

A notable shift in contemporary cybersecurity discourse is the critique of the human as-problem framing. (Zimmermann & Renaud, 2019) use problematization to examine how government, industry, and hackers describe the cybersecurity problem. They argue that dominant narratives often treat humans as inherently risky or potentially malicious, encouraging solutions that focus on restricting behavior through additional controls and policies. The continued prevalence of breaches,

despite these approaches, suggests limits to this mindset and the need for a change in framing.

This critique matters for leadership because leadership choices often determine whether organizations pursue punitive, control-heavy strategies or supportive, enablement-focused strategies. Control-heavy approaches can raise response costs and increase the likelihood of reactance when employees experience controls as unfair or disrespectful (Lowry, Wilson, & Hafer, 2015).

By contrast, a human-as-solution perspective treats employees as contributors to security. When people are empowered and supported, they can spot anomalies, report issues, and help improve local practice. This aligns with protection motivation theory: strengthening self-efficacy and response efficacy improves coping appraisal and encourages protective behavior (Herath & Rao, 2009). Leaders therefore influence culture not only through control, but by enabling employees to succeed under real working conditions.

A human-centered approach implies that secure behavior should be built into systems and workflows rather than demanded as extra effort. Huang and Pearlson (2019) argue that technology cannot fix the organizational and human dimensions of cybersecurity, and that culture shapes the unwritten rules embedded in daily practice. When secure behavior is framed as a list of additional steps employees must remember under pressure, organizations create conditions for predictable failure. When secure behavior is embedded through usable tools, streamlined processes, and clear role expectations, employees can act securely without disproportionate cognitive burden. This reflects a

managerial principle of choice architecture: leaders can redesign environments so the safest option is also the easiest option.

From this perspective, culture development intersects with operational excellence. Friction such as complex authentication, unclear escalation routes, or conflicting policy requirements predictably leads to workarounds that become normalized(Ertan, 2018); (Karlsson, 2017) Human-centered culture development therefore treats incidents and workarounds as signals of system design problems, not merely compliance failures. It can also strengthen psychological safety, making employees more willing to report issues when they expect leaders to focus on improvement rather than blame.

2.6.5 Resilience Orientation and Integration of Culture into Risk Management Practice

Resilience-oriented cybersecurity focuses on the capacity to anticipate, withstand, recover from, and adapt to threats. Culture contributes to resilience because it influences how quickly employees detect anomalies, how willingly they escalate concerns, and how organizations learn from near misses. Eseryel et al. (2024) connect resilience and leadership by integrating transformational IT leadership principles into threat modeling through PASTA-TITL. The framework implies that resilience requires shared engagement in risk management rather than isolating risk decisions within technical teams. When leaders promote proactive participation across functions, risk management becomes a collective practice that reinforces culture.

Resilience thinking also complements the human-as-solution perspective. When organizations treat employees as partners in resilience, they invest in capabilities such as incident reporting, cross-functional collaboration, and continuous improvement. When organizations treat employees primarily as threats, they tend to invest in surveillance and restriction, which can encourage concealment and reduce learning.

2.6.6 The Role of Leadership in Changing Organizational Culture

Throughout the cybersecurity culture literature, leadership emerges as the critical variable in determining whether cultural initiatives succeed or stagnate. Leaders establish the vision, allocate resources, model desired behaviors, and create accountability mechanisms. Without sustained leadership commitment, even well designed interventions can falter. Conversely, when leaders genuinely prioritize cybersecurity culture as a strategic imperative, they create the conditions for meaningful and lasting

change. This is not a one-time effort but an ongoing commitment to reinforcing security values, addressing barriers to compliance, and celebrating progress.

2.7 Synthesis: Toward a Context-Sensitive Model of Leadership-Driven Culture

2.7.1 Core Propositions Emerging from the Literature

A synthesis of the literature reviewed in this chapter gives rise to several core propositions. First, cybersecurity culture is a manageable organizational capability, not an immutable trait. It can be diagnosed, developed, and matured through deliberate and sustained effort. Second, leadership is the primary driver of this cultural development. Leaders, through their words, actions, and allocation of resources, signal what truly matters within the organization, and it is these signals that shape the norms and behaviors of employees. Third, employee behavior is a product of both individual and organizational factors. While individual knowledge and motivation are important, they are often outweighed by the influence of the organizational context, including workload pressures, incentive structures, and the usability of security tools and processes. Finally, context is king. The effectiveness of any cultural intervention is contingent on its alignment with the organization's specific operational realities, risk profile, and strategic priorities.

2.7.2 Context Sensitivity and Transferability of Culture Interventions

The literature consistently cautions against a "one-size-fits-all" approach to cybersecurity culture. The same control, the same message, the same training module can be interpreted in vastly different ways across different roles, sectors, and working conditions. This means that leaders must be adept at adapting their interventions to local realities while still maintaining a coherent and consistent organizational direction. This is not to say that the principles of a strong security culture are not transferable, but rather that their application must be thoughtfully tailored to the specific context in which they are being implemented.

2.7.3 An Integrated Conceptual Model Linking Leadership, Culture Mechanisms, and Behavior

Drawing these threads together, we can propose an integrated conceptual model that links leadership, culture, and behavior. In this model, leadership actions are the primary input. These actions, which include everything from strategic communication

to the design of work processes, shape the organization's cybersecurity culture. This culture, in turn, influences the security-related behaviors of employees. These behaviors then lead to specific security outcomes, which can be measured and fed back into the system to inform future leadership actions. This model, which is grounded in the literature reviewed in this chapter, provides a framework for understanding the complex interplay of factors that contribute to an organization's overall security posture.

2.8 Research Gaps and Implications for This Thesis

While the existing literature provides a strong foundation for understanding the importance of leadership in shaping cybersecurity culture, there are still significant gaps in our knowledge. Much of the research is either conceptual or based on case studies of single organizations. There is a need for more large-scale empirical research that examines the relationship between specific leadership behaviors and measurable security outcomes across a range of organizational contexts. Furthermore, while the literature is replete with calls for a more context-sensitive approach, there is a lack of practical guidance for leaders on how to actually achieve this. This thesis seeks to address these gaps by empirically investigating the impact of different leadership styles on cybersecurity culture and by developing a practical, evidence-based framework for leadership-driven cultural change.

2.9 Summary and Link to Subsequent Chapters

In summary, this literature review has established that fostering a robust cybersecurity culture is a critical organizational imperative, and that leadership is the central catalyst in this endeavor. We have moved from a broad understanding of culture as an "invisible hand" to a more nuanced appreciation of its various dimensions, including the pivotal roles of leadership credibility, employee motivation, and contextual sensitivity. The review has synthesized diverse streams of research—from organizational behavior to human factors and socio-technical systems—to argue that effective security is not merely a matter of implementing the right technical controls, but of cultivating a human-centric ecosystem where secure behaviors are both valued and practical.

The subsequent chapters build directly on this foundation. Chapter 3 details the pragmatic mixed-methods design, including the documentary case study approach and the exploratory CISO survey. Chapter 4 presents two case studies (Princeton University and Liberty Mutual) to illustrate how leadership mechanisms interact with organizational context in real-world culture change efforts. Chapter 5 reports descriptive survey findings

from CISOs and senior security leaders, highlighting common leadership approaches, constraints, and measurement practices. Chapter 6 synthesizes insights across the literature, case studies, and survey results to develop a context-sensitive framework and practical recommendations. Chapter 7 concludes by summarizing contributions, acknowledging limitations, and identifying future research opportunities.

3. Research methodologies

3.1 A Pragmatic Approach to a Complex Problem

This research adopts a pragmatic philosophy, which is characterized by its focus on practical problem-solving and real-world applicability. This approach is particularly well-suited to the study of cybersecurity culture, as it allows for the integration of multiple perspectives and methodologies to address a complex and multifaceted problem. The pragmatic paradigm is not bound by a single, rigid set of epistemological or ontological assumptions, but rather embraces a more flexible and eclectic approach to inquiry.

3.2 A Mixed-Methods Research Design

In line with the pragmatic philosophy, this research employs a mixed-methods research design, combining qualitative and quantitative data collection and analysis techniques. This approach allows for a more comprehensive and nuanced understanding of the research topic than could be achieved through a single methodology alone. The qualitative component of the research provides rich, in-depth insights into the contextual factors that shape cybersecurity culture (Bada & Nurse, 2019), while the quantitative component provides statistical evidence of the relationships between key variables (Bulgurcu, Cavusoglu, & Benbasat, 2010). The research is structured in three distinct phases, each of which builds upon the last to provide a progressively more detailed and nuanced understanding of the research topic cybersecurity culture research because it addresses both theoretical understanding and practical implementation challenges faced by organizations.

1. Phase 1: Exploratory Literature Review: This phase involves a systematic and comprehensive review of the existing academic and practitioner literature on cybersecurity culture, leadership, and organizational change. The literature review serves as the theoretical foundation for the research, providing a conceptual framework for the subsequent phases of the study.

2. Phase 2: Qualitative Case Study Analysis: This phase involves an in-depth analysis of two organizations that have undertaken significant cybersecurity culture change initiatives. The case studies provide a rich and detailed understanding of the practical challenges and success factors of leadership-driven culture change in real-world settings.

3. Phase 3: Quantitative CISO Survey: This phase involves a survey of 12 Chief Information Security Officers (CISOs) and senior security leaders. The survey provides quantitative data on the relationships between leadership styles, culture maturity, and implementation barriers, allowing for the statistical testing of the hypotheses derived from the literature review and the case studies.

3.3 Data Collection Methods

3.3.1 Literature Review

The literature review was conducted using a systematic and comprehensive search strategy. A wide range of academic and industry databases were searched, including Google Scholar, Scopus, and the ACM Digital Library. The search terms included "cybersecurity culture," "information security culture," "leadership," "organizational change," and "human factors in security". The search was limited to English-language publications from the last 10 years to ensure the relevance and currency of the literature.

3.3.2 Case Studies

This thesis uses two documentary case studies to explore how leadership approaches shape cybersecurity culture in contrasting organizational contexts. The cases were selected purposely to provide variation in structure and operating environment: (1) a decentralized academic institution (Princeton University) and (2) a regulated corporate organization (Liberty Mutual).

The case study evidence is based on previously published and publicly available materials, including documented case research and organizational artefacts described in those sources. This approach enables in-depth qualitative examination of leadership actions, culture mechanisms, and reported outcomes without collecting primary interview data.

3.3.3 CISO Survey

The CISO survey was designed to gather quantitative data on the relationships between leadership styles, culture maturity, and implementation barriers. The survey was developed based on the findings of the literature review and the case studies, and it was pilot-tested with a small group of security professionals to ensure its clarity and validity. The survey was distributed to a targeted sample of CISOs and other senior security leaders through a professional networking platform. The survey was administered online, and the data was collected anonymously to encourage candid responses. A total of 12 completed surveys were received, representing a response rate of approximately 20%.

3.4 Data Analysis Approach

3.4.1 Literature Review

The data from the literature review was analyzed using a thematic synthesis approach. This involved identifying the key themes and concepts in the literature and organizing them into a coherent conceptual framework. The framework was then used to guide the subsequent phases of the research.

3.4.2 Case Studies

The case study analysis followed a structured qualitative template approach. Each case was analyzed using a consistent set of analytic categories: organizational context (sector, structure, constraints), leadership approach, culture mechanisms (communication, incentives, policies/processes, champions), implementation strategy, and reported outcomes. The analysis first produced within-case summaries and then conducted cross-case comparison to identify patterns and differences in how leadership strategies interacted with context. This pattern-matching approach strengthens analytical consistency across cases and supports the development of transferable propositions for the framework presented in Chapter 6.

3.4.3 CISO Survey

Survey data were analyzed using descriptive statistics to summarize patterns across respondents. Frequency counts and percentages were calculated for each question to identify the most commonly reported leadership approaches, contextual pressures, barriers, and measurement practices. Given the exploratory nature of the survey and the

small sample size (n=12), the analysis emphasizes interpretation of patterns rather than inferential statistical testing.

3.5 Ethical Considerations

A Commitment to Integrity This research was conducted in accordance with the highest ethical standards. For the CISO survey, all participants were provided with a clear and comprehensive explanation of the research and their rights as participants. Informed consent was obtained from all survey participants, and their responses were fully anonymized to protect their identity and that of their organizations. The two case studies presented in Chapter 4 are based on previously published, publicly available materials (Blum et al., 2021; Huang & Pearlson, 2019). As such, the organizations and individuals named in those sections are referenced in accordance with their original source documents.

4. Case Study Analysis

How does a cybersecurity plan on paper become a living, breathing part of an organization's culture? It’s a journey that goes far beyond installing new software or issuing new rules. It’s a story of leadership, influence, and changing the way people think, feel, and act when it comes to digital threats. This chapter explores two powerful real-world stories that show how it’s done.

First, we’ll visit Princeton University, a place where academic freedom and decentralization are paramount. Their story reveals how a culture of security can be nurtured from the ground up through a smart, empathetic awareness program. Then, we’ll turn to Liberty Mutual, a global financial giant, where researchers from MIT Sloan documented how leaders systematically embedded a “culture of data protection” using the core mechanics of the organization itself—from executive messaging to performance reviews.

Though one is an Ivy League university and the other a Fortune 100 company, their experiences converge on a single, powerful truth: a strong security culture isn’t installed like a firewall. It’s carefully and patiently built through leadership choices that connect high-level security goals to the everyday routines and values of the people on the ground.

4.1 Case Study 1: Princeton University - Balancing Tradition and Transformation

This case study is based on the published research by Blum, Sherry, and Schaufler (2021), which documents Princeton University's security culture transformation initiative

- The Challenge: Securing a City of Ideas

Imagine trying to secure an entire city—not with walls and gates, but with shared habits and a sense of collective responsibility. That was the challenge facing Princeton University. With its sprawling campus, thousands of independent-minded students and faculty, and a culture built on openness and intellectual curiosity, a traditional, top-down security mandate was destined to fail. The very spirit of collaboration that made Princeton a world-class research institution also made it vulnerable.

When David Sherry took the helm as Chief Information Security Officer (CISO) in 2016, he found an organization with no active security awareness program to speak of. The task wasn't just to plug technological gaps; it was to change mindsets. The Information Security Office (ISO) set out on a mission to make security both “programmatic and cultural,” recognizing that without the cultural piece, any policy or technology would ultimately fall short.

- Leadership in Action: A People-First Bet

So, where did Sherry start? Not with a new algorithm or a complex piece of hardware. His very first move—his “number one hire”—was to bring on a leader for security awareness and training. It was a bold, people-first statement: the greatest gains wouldn’t come from better machines, but from more engaged and aware people. Tara Schaufler, hired as the Awareness and Training Program Manager, delivered her first class within 90 days, signaling that this was not a long-term, abstract goal but an immediate and serious priority.

This philosophy even extended to hiring. The team recognized that to change a culture, you need expertise in communication and learning, not just technical credentials. By valuing the user’s perspective, they ensured the program would be built on a foundation of empathy and connection.

- How They Did It: A Strategy of Influence

Cutting Through the Noise: In the information-rich environment of a university, getting anyone's attention is a battle. The team had to become master marketers, creating content that was not only informative but worth consuming.

Building an Army of Allies: With a tiny team and a community of over 17,000, they couldn't go it alone. They smartly identified the campus computing support staff as their “force multipliers.” By equipping these trusted influencers with information and resources, they created a distributed network that carried the message of security into every corner of the university.

Earning the Right to Be Heard: The team knew that forcing mandatory training on a skeptical audience would backfire. Instead, they took a “low and slow” approach, focusing first on building relationships, establishing credibility, and explaining the “why” behind security. It was a strategic choice to win trust before making demands.

From “Weakest Link” to “Guardian”: In a brilliant psychological shift, the program reframed employees and students not as security liabilities, but as “guardians at the gate.” This wasn’t just clever branding; it was an invitation to be part of a shared defense, tapping into a sense of pride and ownership.

Making Security Stick: The program was designed to be engaging and relevant. Content was framed around personal impact (“How does this affect me?”), and threats were made real through tools like the “Phish Bowl” website. They even made it fun, using games like “Cyber Wheel of Fortune” to lower barriers and make learning about security a positive, social experience.

- The Payoff: A Culture in Motion

The results weren’t just abstract. They were visible in people’s actions:

Tools People Actually Used: A new password manager, LastPass, saw over 1,100 sign-ups in its first year, with most people using it regularly.

A Pull, Not Just a Push: Departments started requesting security training, a clear sign that the culture was shifting from resistance to proactive engagement.

A Sharper Eye for Threats: The Phish Bowl became a popular resource, and a “Danger Banner” on suspicious emails was widely accepted, showing that people were becoming more vigilant.

Outside Validation: Even the auditors, who once flagged awareness as a weakness, were now satisfied with the program's progress.

By tracking everything from the number of classes held to the attendance at each event, the team could prove their impact. The journey from a non-existent program to a thriving culture of awareness was well underway.

4.2 Case Study 2: Liberty Mutual – Engineering a Culture of Protection

This case study is based on research conducted by Huang and Pearlson (2019) at MIT Sloan, which examined how Liberty Mutual built a culture of data protection.

- The Challenge: High Stakes in a World of Risk

For a global insurance leader like Liberty Mutual, cybersecurity isn't just an IT issue—it's a fundamental matter of trust. Operating in a highly regulated industry with over 50,000 employees, the company faced a constant barrage of advanced threats. Researchers from MIT Sloan studied how Liberty Mutual's leadership went beyond technology to systematically build what they called a "culture of data protection."

This wasn't just about internal motivation. External pressures, like the stringent New York Department of Financial Services (NYDFS) Cybersecurity Regulation, made robust awareness training a legal requirement. In the world of finance and insurance, a reputation for security is a competitive advantage, making culture-building an urgent business imperative.

- Leadership in Action: A Deliberate Design

Where Princeton's approach felt organic and influence-based, Liberty Mutual's was more like precision engineering. The MIT research shows how leaders used the formal "organizational mechanisms"—the levers of management—to deliberately shape the culture.

- Key leadership moves included:

Making It a Top-Down Priority: Executives didn't just approve a budget; they made cybersecurity a visible strategic priority. The CISO became the public face of the campaign, using regular blog posts and communications to signal that this was a core business concern, not just an IT project.

Giving Culture a Home: In a critical structural decision, the CISO created a dedicated leadership role focused entirely on cybersecurity awareness and culture. This sent a powerful message: culture change is a full-time responsibility, not a side project.

Creating a Shared Identity: The company developed a common language with slogans like “Responsible Defender” and “Our Information. Our Responsibility.” This wasn’t just corporate jargon; it was a way to forge a collective identity and reinforce the idea that everyone was in it together. Phishing exercises became a topic of conversation, creating peer-to-peer reinforcement.

Translating expectations into simple behavioral guidance: Employees reported clarity in what to do through the "Pillars of Data Protection," a simple guideline set. Policies were also written to be more accessible and included "what this means to me" sections—turning formal rules into personally meaningful expectations. This approach reduced policy readability burden and supported internalization rather than superficial compliance.

Weaving Security into Performance: This is where the culture-building became deeply embedded. The company used organizational reinforcement to make security behaviors count. Employees who repeatedly failed phishing tests might see a note in their performance evaluation. Those who were vigilant were publicly praised. By linking security to accountability and recognition, leaders made it part of how success was measured.

- The Payoff: A Company of First Responders

The results were clear in the data: more employees were reporting suspicious emails, and fewer were clicking on malicious links. But the most powerful change was behavioral. The program encouraged “extra-role” behaviors, where employees acted like security “first responders,” proactively helping colleagues and flagging issues without fear of blame. This created a virtuous cycle of learning and collective defense, proving that the culture of data protection had truly taken root.

4.3 The Blueprint for Success: What Both Cases Teach Us

Looking at Princeton and Liberty Mutual side-by-side, we see a blueprint for building a successful cybersecurity culture. While their methods were tailored to their unique environments—one open and academic, the other corporate and regulated—the core principles of their success were remarkably similar.

Shared Keys to Success:

- Security as a Shared Identity: Both organizations moved away from blaming users. Instead, they invited everyone to be part of the solution, framing security as a collective responsibility and a source of pride.

- Leadership from the Front: In both cases, senior leaders were visible, committed, and vocal. Whether it was Princeton's CISO making a strategic first hire or Liberty Mutual's executives blogging about security, their participation gave the initiatives legitimacy and urgency.

- Making It Real and Relevant: Both programs succeeded by connecting security to people's daily lives and personal risks, not just abstract corporate policies. They answered the all-important question: "Why should I care?"

- A Multi-Channel, Continuous Effort: This wasn't a one-time training event. It was a continuous campaign, using everything from newsletters and games to formal training and performance metrics to keep the message alive.

Context is King:

The key difference lay in the how. Princeton, with its culture of autonomy, relied on influence, relationships, and a gradual, "low and slow" approach. Liberty Mutual, operating in a more structured corporate world, effectively used formal management systems to drive and reinforce change.

Ultimately, both stories prove the same fundamental point: building a strong cybersecurity culture is one of the most critical leadership challenges of the digital age. It requires a deep understanding of people, a clear vision, and a relentless commitment to turning that vision into a shared reality.

5. CISO Survey Analysis

This chapter presents the empirical findings from a structured survey of 12 Chief Information Security Officers (CISOs) and senior security leaders. The survey was designed to test and refine the central thesis of this research: that cybersecurity culture is profoundly shaped by its organizational context, and that effective leadership requires an adaptive approach tailored to that context. The survey was not intended to produce statistically generalizable results, but rather to provide a practice grounded view of the

challenges, constraints, and successes that security leaders experience in their efforts to cultivate a security-conscious culture.

5.1 Survey Design and Data Collection

The survey instrument was a 30-question, single-choice questionnaire designed to facilitate a comparative analysis of leadership patterns. The questions were structured around five key thematic areas:

1. Culture Maturity and Drivers: Assessing the current state of cybersecurity culture and the primary motivations for its development.

2. Industry and Organizational Context: Understanding the environmental and structural factors that shape the cultural landscape.

3. Leadership Approach and Influence Mechanisms: Identifying the dominant leadership styles and the tactics used to influence employee behavior.

4. Barriers and Constraints: Pinpointing the most significant obstacles to culture change.

5. Assessment and Measurement Practices: Examining how leaders track progress and measure the effectiveness of their initiatives.

The survey was administered online between August 28, 2025, and September 3, 2025. The data was collected anonymously to encourage candid responses, and a basic quality check was performed to ensure the integrity of the dataset.

5.2 Respondent Demographics

The 12 survey respondents represent a diverse cross-section of industries and organizational sizes, providing a rich dataset for contextual analysis. The majority of respondents (67%) were from large organizations with over 10,000 employees, and the most heavily represented industries were financial services, healthcare, and technology. The respondents were also highly experienced, with the majority (75%) having over 10 years of experience in the cybersecurity field.

5.3 Findings Theme 1: Organizational Context and Culture Maturity

This section explores the environmental and structural factors that shape the landscape of cybersecurity culture, including the reported level of maturity, the primary drivers of

culture work, the pressures of the industry context, and the influence of organizational characteristics.

5.3.1 Cybersecurity Culture Maturity: A Plateau of Progress

When asked to classify their organization's cybersecurity culture maturity, half of the respondents selected 'Managed,' indicating a mature security culture with measurable outcomes. This suggests that many organizations have successfully moved beyond the initial, ad-hoc stages of culture development and have implemented a more systematic and proactive approach. However, the fact that only a small minority (16.7%) selected 'Optimizing' suggests that the journey to continuous improvement and innovation in culture is a challenging one.

Table 1: Reported Cybersecurity Culture Maturity (n=12)

Response Option	Count	Percentage
Managed - Mature security culture with measurable outcomes	6	50.0%
Developing - Basic security policies in place with growing awareness	3	25.0%
Optimizing - Continuously improving security culture with innovation	2	16.7%
Defined - Established security culture with consistent practices	1	8.3%

This distribution suggests a 'maturity plateau,' where many organizations reach a point where security expectations are formalized and measurable, but struggle to make the leap to a truly 'Optimizing' culture. This transition requires a sustained commitment to high-quality measurement, a willingness to redesign processes to make secure behavior the path of least resistance, and a leadership team that is dedicated to continuous improvement.

5.3.2 The Drivers of Culture Work: Beyond the Breach

Contrary to the common assumption that major security incidents are the primary driver of culture work, the survey results indicate that customer and stakeholder expectations (41.7%) and regulatory compliance (33.3%) are the most significant motivators. This suggests that many leaders view cybersecurity culture not merely as a reactive measure to prevent breaches, but as a proactive strategy for maintaining external trust and legitimacy.

Table 2: Primary Driver for Cybersecurity Culture Development (n=12)

Response Option	Count	Percentage
Customer or stakeholder expectations	5	41.7%
Regulatory compliance requirements	4	33.3%
Previous security incidents or breaches	1	8.3%
Industry best practices and benchmarking	1	8.3%
Board or executive mandate	1	8.3%

This finding has important implications for leadership communication. If culture work is framed solely as a matter of compliance, employees may adopt a ‘checkbox’ mentality, focusing on avoiding mistakes rather than building resilient habits. However, if it is framed as a matter of customer trust and business continuity, the same security controls can be imbued with a greater sense of meaning and purpose.

5.4 Findings Theme 2: Leadership Approaches and Influence Mechanisms

This section delves into the leadership styles, communication strategies, and influence tactics that security leaders employ to shape cybersecurity culture.

5.4.1 The Dominance of Transformational and Adaptive Leadership

The survey results indicate that transformational and adaptive leadership are the two most common leadership styles among the respondents, with each being cited by 33.3% of the leaders. This suggests that many security leaders recognize the importance of inspiring a shared vision and of adapting their approach to the specific context of their organization.

Table 3: Primary Leadership Style Used (n=12)

Response Option	Count	Percentage
Transformational - Inspiring vision and motivating change	4	33.3%
Adaptive - Flexible approach based on situation and context	4	33.3%
Servant - Supporting and empowering employees	2	16.7%
Transactional - Clear expectations and performance management	2	16.7%

Transformational leadership is essential for creating a sense of meaning and urgency around cybersecurity, while adaptive leadership is crucial for tailoring interventions to the specific needs of different business units, roles, and maturity levels. The presence of servant and transactional leadership as complementary styles suggests that a blended approach, which combines inspiration with empowerment and clear expectations, is often the most effective.

5.4.2 The Barriers to Culture Change: A Triangle of Constraints

The survey results reveal a ‘constraint triangle’ of time pressure, sponsorship, and capacity as the most significant barriers to cybersecurity culture change. The lack of executive support and commitment was cited as the primary barrier by 33.3% of the respondents, followed by competing business priorities and time pressures (25.0%) and limited resources and budget constraints (25.0%).

Table 4: Primary Barrier to Cybersecurity Culture Development (n=12)

Response Option	Count	Percentage
Lack of executive support and commitment	4	33.3.%
Competing business priorities and time pressures	3	25.0%
Limited resources and budget constraints	3	25.0%
Resistance to change and cultural inertia	2	16.7%
Technical complexity and system limitations	0	0.0%

This finding underscores the critical importance of securing executive buy-in and of aligning cybersecurity initiatives with the broader strategic objectives of the

organization. Without a sustained commitment of time, resources, and leadership attention, even the most well-designed culture change initiatives are likely to fail.

6. Discussions and Recommendations

This chapter synthesizes the findings from the thematic literature review, documentary case study analysis, and exploratory CISO survey to develop a preliminary conceptual framework for context-sensitive cybersecurity culture development. Given the exploratory nature of this research and its methodological constraints—including reliance on secondary data for case studies and a small survey sample—the discussion focuses on emerging patterns, potential relationships, and initial insights rather than definitive conclusions or causal claims. The chapter presents a preliminary framework and offers initial recommendations that warrant further validation through future research.

6.1 The Importance of Context-Sensitive Leadership

A key pattern emerging from this exploratory research is the apparent importance of context-sensitive leadership in cybersecurity culture development. The documentary case studies of Princeton University and Liberty Mutual, as analyzed through published research materials, provide illustrative examples of this principle. At Princeton, the documented approach emphasized a transformational leadership style focused on collaboration and shared values, which appeared well-suited to the university's decentralized and intellectually autonomous environment. The Liberty Mutual case, as documented by researchers, illustrated how systematic integration of security into organizational processes and performance management aligned with a regulated corporate context.

The exploratory CISO survey findings offer preliminary support for this observation. Transformational and adaptive leadership were the two most frequently reported primary styles among the 12 respondents (each cited by 33.3%), suggesting that many security leaders recognize the value of adapting their approach to organizational context. While the small sample size precludes statistical generalization, the patterns in the survey data appear consistent with the case study insights regarding the potential importance of context-sensitive approaches.

It is important to note that these findings are indicative rather than conclusive. The reliance on documentary case studies means the analysis is filtered through the perspectives of the original researchers, and the small survey sample provides only preliminary evidence of practitioner perspectives. Future research with primary case study data and larger survey samples would be needed to validate these patterns.

6.2 The Potential Role of Transformational and Adaptive Leadership

While context sensitivity appears important, the findings of this exploratory research also suggest the potential value of transformational and adaptive leadership approaches in cultivating security-conscious culture. The CISO survey results indicate that these two styles are equally prominent among respondents (each cited by 33.3%), and the documentary case studies provide examples of how leaders employing these styles appeared to inspire and motivate employees toward more security-conscious behavior.

The literature review synthesized theoretical arguments suggesting that transformational leaders may function as "cultural architects" who shape organizational values and beliefs

by articulating compelling visions, communicating them effectively, and empowering employees to participate in realizing those visions. The case study examples appear consistent with this theoretical perspective, though the documentary nature of the cases limits the depth of insight into the actual mechanisms at work.

These preliminary findings suggest that transformational and adaptive leadership may be particularly relevant for cybersecurity culture development, but further empirical research would be needed to establish the conditions under which these approaches are most effective and to understand the specific mechanisms through which they influence culture.

6.3 A Preliminary Framework for Context-Sensitive Cybersecurity Culture Development

Based on the synthesis of findings from this exploratory research, this thesis proposes a preliminary conceptual framework for context-sensitive cybersecurity culture development. This framework is intended as a starting point for discussion and future research rather than a validated model. It synthesizes insights from the literature, illustrative case examples, and preliminary survey data, but has not been tested across diverse organizational settings or validated through longitudinal research.

The framework consists of four interconnected components:

1. Context Assessment

The first component involves assessing the organization's context to understand factors that may influence culture development approaches. This includes examining:

- Organizational structure (centralized vs. decentralized)
- Industry characteristics and regulatory environment
- Existing organizational culture and values
- Current cybersecurity maturity level
- Key stakeholder groups and their perspectives

The case studies suggest that context assessment is foundational, as Princeton's decentralized academic environment and Liberty Mutual's regulated corporate setting appeared to require quite different approaches.

2. Leadership Approach Selection

The second component involves considering which leadership approaches may be appropriate given the organizational context. This may involve:

- Selecting leadership styles (e.g., transformational, adaptive, servant) that align with organizational culture
- Ensuring authenticity—the approach should resonate with the leader's values
- Considering hybrid approaches that combine elements of different styles
- Recognizing that different contexts may call for different emphases

The survey data suggest that transformational and adaptive leadership are commonly employed, though the small sample size limits conclusions about their relative effectiveness.

3. Culture Change Initiatives

The third component involves designing initiatives tailored to the organizational context. Based on the case examples, this may include:

- Balancing top-down direction with bottom-up participation
- Integrating security into existing organizational processes
- Creating engaging, relevant communications and training
- Building networks of security champions
- Aligning security initiatives with business objectives

The case studies illustrate different approaches: Princeton emphasized awareness programs and relationship-building, while Liberty Mutual focused on integrating security into performance management and operational processes.

4. Measurement and Continuous Refinement

The fourth component involves establishing processes to assess progress and refine approaches over time. This includes:

- Defining appropriate metrics (both quantitative and qualitative)
- Establishing baseline measurements
- Regularly assessing culture maturity
- Using assessment data to inform strategy adjustments
- Recognizing culture development as an ongoing process

The survey findings indicate that measurement practices vary widely, with respondents reporting different maturity levels and barriers, suggesting this remains a challenging area for practitioners.

5. Framework Limitations and Future Validation Needs

- This framework should be interpreted as a preliminary conceptual model that synthesizes insights from limited empirical data. Key limitations include:
- The framework has not been validated through implementation and testing. It is based on only two illustrative case examples (analyzed through secondary sources)
- Survey data comes from a small, non-representative sample.
- The relationships between components are proposed rather than empirically established.
- Contextual factors may be more numerous and complex than captured here.

Future research should test this framework across diverse organizational settings, refine its components based on empirical evidence, and establish more specific guidance for how context should inform leadership and initiative selection.

6.4 Initial Recommendations for Leaders

This exploratory research offers preliminary, evidence-informed recommendations for leaders seeking to strengthen cybersecurity culture. These recommendations should be viewed as initial guidance that warrants further validation rather than as established best practices.

- For Organizations:

Consider Investment in Leadership Development. The case studies and survey data suggest that leadership may play a central role in culture development. Organizations might benefit from leadership development programs that help leaders understand different leadership approaches and how to adapt them to organizational context. However, the optimal design and content of such programs requires further research.

Foster Psychological Safety. The literature review and case examples suggest that psychological safety—where employees feel comfortable raising security concerns without fear of blame—may be important for effective culture development. Organizations might consider how to create environments that encourage reporting and learning from security incidents, though specific implementation approaches will vary by context.

Align Security with Business Objectives. The case studies suggest that framing security as an enabler of business objectives rather than a compliance burden may help secure executive support and employee engagement. However, the specific strategies for achieving this alignment likely depend on organizational context and industry.

- For Security Leaders:

Develop Contextual Awareness. The findings suggest that understanding organizational context—including structure, culture, and constraints—may be foundational to selecting effective approaches. Security leaders might benefit from developing skills in organizational diagnosis and stakeholder analysis.

Consider Multiple Leadership Approaches. The survey data indicate that transformational and adaptive leadership are commonly employed, and the case examples suggest these approaches may be valuable in certain contexts. Leaders might consider developing capabilities across multiple leadership styles to enable flexibility.

Build Cross-Functional Relationships. The case studies suggest that security culture development may require collaboration across organizational functions. Security leaders might consider strategies for building networks of security champions and engaging diverse stakeholders, though the specific approaches will depend on organizational structure and culture.

Establish Measurement Practices. The survey findings indicate variation in how organizations measure culture maturity. Leaders might benefit from establishing baseline measurements and ongoing assessment processes, recognizing that appropriate metrics may vary by organizational context and maturity level.

Important Caveat: These recommendations are based on limited empirical data and should be adapted to specific organizational circumstances. Organizations considering implementing these suggestions should do so thoughtfully, with attention to their unique context, and should evaluate outcomes to determine effectiveness in their setting.

7. conclusion

This exploratory research has examined the relationship between leadership and cybersecurity culture development, seeking to move beyond generic, technology-centric approaches toward a more context-sensitive, human-centered perspective. The findings, drawn from a thematic literature synthesis, documentary case study analysis, and an exploratory survey of security leaders, offer preliminary insights into how leadership and organizational context may interact to shape cybersecurity culture. While the methodological limitations of this study preclude definitive conclusions, the research provides a foundation for future empirical work and offers initial guidance for practitioners.

7.1 A Recapitulation of the Research Journey

This thesis began with the premise that cybersecurity culture—the collective mindset and behavioral norms that shape how employees approach security—is significantly influenced by leadership and organizational context. To explore this premise, the research employed a pragmatic exploratory mixed-methods approach integrating three components:

The thematic literature review synthesized existing knowledge on cybersecurity culture, leadership, and organizational change, identifying key concepts, theoretical frameworks, and gaps in current understanding. This provided the conceptual foundation for the empirical components.

The documentary case study analysis examined two contrasting organizational contexts—Princeton University and Liberty Mutual—through published research materials. While this approach limited the depth of analysis compared to primary case

research, it provided illustrative examples of how leadership approaches and organizational context may interact in practice.

The exploratory CISO survey gathered preliminary data from 12 senior security leaders on their leadership approaches, organizational maturity, barriers, and measurement practices. While the small sample size precludes statistical generalization, the survey provided initial evidence of practitioner perspectives that complemented the case study insights.

Together, these methods enabled a triangulated exploration of the research questions while maintaining appropriate caution about the generalizability and definitiveness of the findings.

7.2 The Key Findings: A New Understanding of Cybersecurity Culture

This exploratory research has identified several patterns and preliminary insights regarding cybersecurity culture development:

- Context Appears to Matter. The case studies and survey data suggest that organizational context—including structure, industry, regulatory environment, and existing culture—may significantly influence which leadership approaches and culture development strategies are most appropriate. The contrast between Princeton's decentralized academic environment and Liberty Mutual's regulated corporate setting illustrates how different contexts may call for different approaches. This finding challenges one-size-fits-all approaches to security culture.

- Leadership May Be Central. Across the literature, case studies, and survey data, leadership emerged as a potentially critical factor in shaping cybersecurity culture. The case examples suggest that leaders who articulate clear visions, align security with organizational values, and empower employees may be more successful in fostering security-conscious behavior. However, the documentary nature of the cases and the small survey sample limit conclusions about the specific mechanisms through which leadership influences culture.

7.3 The Knowledge Contributions

This exploratory research makes several preliminary contributions to understanding cybersecurity culture development:

- Preliminary Conceptual Framework. The research proposes a four-component framework linking context assessment, leadership approach selection, culture change initiatives, and measurement. While this framework requires validation through future research, it offers a starting point for thinking systematically about context-sensitive culture development.

- Synthesis of Multidisciplinary Literature. The thematic literature review integrates insights from cybersecurity, leadership, and organizational change literature, providing a foundation for understanding culture development as a multifaceted challenge requiring attention to technical, behavioral, and organizational factors.

- Illustrative Case Examples. The documentary case studies provide concrete examples of how different organizational contexts may call for different approaches, making abstract concepts more tangible for practitioners.

- Preliminary Practitioner Insights. The exploratory survey provides initial evidence of how security leaders think about their roles, the challenges they face, and the approaches they employ, offering a foundation for future research with larger, more representative samples.

- Initial Guidance for Practitioners. While acknowledging the need for further validation, the research offers preliminary recommendations that may help leaders think more systematically about how to approach culture development in their specific contexts.

7.4 The Practical Implications

It is essential to acknowledge the significant limitations of this research, which constrain the conclusions that can be drawn:

- Exploratory Nature. This research is exploratory and theory-building rather than confirmatory. It identifies patterns and proposes relationships but does not establish causal connections or test hypotheses statistically. The findings should be interpreted as preliminary insights requiring further investigation.

- Documentary Case Study Methodology. The case study analysis relies on published research materials rather than primary data collection. This approach, while appropriate for an exploratory Master's thesis, limits the depth of insight and means the findings are filtered through the perspectives and research goals of the

original authors. Primary case research with interviews and observations would provide richer, more nuanced understanding.

- Small Survey Sample. The survey includes only 12 respondents, which is insufficient for statistical generalization. The findings represent the perspectives of a small group of security leaders and may not be representative of the broader population. Larger-scale survey research would be needed to establish the prevalence of the patterns observed.

- Limited Organizational Diversity. The case studies examine only two organizations in specific contexts (academic and corporate financial services). The framework and recommendations may not apply equally well to other organizational types, industries, or cultural contexts.

- Cross-Sectional Data. The research captures perspectives and examples at specific points in time rather than tracking culture development longitudinally. Longitudinal research would be needed to understand how culture evolves over time and to assess the long-term effectiveness of different approaches.

- Self-Reported Data. The survey relies on self-reported data from security leaders, which may be subject to social desirability bias or limited awareness of organizational dynamics. Multi-source data including employee perspectives would provide a more complete picture.

These limitations mean that the findings should be viewed as indicative patterns and preliminary insights rather than established facts or generalizable conclusions. The proposed framework and recommendations require validation through future research before they can be considered evidence-based best practices.

7.5 A Vision for the Future: The Human-Centric Security Organization

This exploratory research identifies several important directions for future investigation:

- Primary Case Study Research. Future research should conduct primary case studies using interviews, observations, and document analysis to gain deeper understanding of how leadership influences culture development. Longitudinal

case studies tracking organizations over multiple years would be particularly valuable.

- Large-Scale Survey Research. Surveys with larger, more representative samples of security leaders and employees would help establish the prevalence of different leadership approaches, the relationship between leadership and culture maturity, and the most common barriers and success factors.

- Quantitative Testing of Relationships. With appropriate sample sizes, future research could test specific hypotheses about relationships between leadership styles, contextual factors, and culture outcomes using statistical methods.

- Framework Validation. The preliminary framework proposed in this research should be tested through implementation studies that track organizations as they apply the framework and assess whether it improves culture development outcomes.

- Expanded Contextual Factors. Future research should investigate additional contextual factors beyond those examined here, such as organizational age, geographic location, workforce characteristics, and technological infrastructure.

- Employee Perspectives. Research incorporating employee perspectives would provide important insights into how leadership actions are perceived and experienced at different organizational levels.

- Longitudinal Studies. Long-term studies tracking culture development over multiple years would help understand the dynamics of culture change and the sustained impact of different leadership approaches.

7.6 Concluding Reflections

This research has explored the complex relationship between leadership and cybersecurity culture development, emphasizing the importance of context sensitivity and human-centered approaches. While the methodological limitations preclude definitive conclusions, the findings suggest that effective cybersecurity culture development requires more than technical controls and policy compliance—it requires thoughtful leadership adapted to organizational context.

The vision that emerges from this research is of a security organization built not on fear and compliance but on trust, empowerment, and shared responsibility. In such an organization, every employee understands their role in protecting organizational assets, security is integrated into daily work rather than seen as a burden, and leaders create environments where people feel comfortable raising concerns and learning from mistakes.

The journey toward this vision will not be easy. It requires a fundamental shift in how many organizations think about cybersecurity—from a technical problem to be solved to a human challenge requiring ongoing attention, adaptation, and leadership. The findings of this exploratory research suggest that this shift is not only possible but essential. In an era of ever-increasing cyber threats, the human-centric security organization is not merely a competitive advantage but a strategic imperative.

However, realizing this vision will require continued research to validate and refine the preliminary insights offered here. This thesis should be viewed as a starting point—an initial exploration that raises questions and proposes directions for future investigation. It is hoped that future researchers will build on this foundation, conducting the rigorous empirical work needed to transform these preliminary insights into validated knowledge that can truly guide practice.

References

Alhogail, A., & Mirza, A., 2014. A framework of information security culture change, Journal of Theoretical and Applied Information Technology, 64(2), 540–549.

Alshaikh, M., 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective, Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

Ashenden, D., & Sasse, A., 2013. CISOs and organisational culture: Their own worst enemy?, Computers & Security, 39, 396–405. https://doi.org/10.1016/j.cose.2013.09.004

Bada, M., & Nurse, J. R. C., 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs), Information & Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Blum, D., Sherry, D., & Schaufler, T., 2021. Transforming Princeton's Security Culture Through Awareness, ISACA Journal, 1. https://www.isaca.org/resources/isaca-

journal/issues/2021/volume-1/case-study-transforming-princetons-security-culture-through-awareness

Bulgurcu, B., Cavusoglu, H., & Benbasat, I., 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, MIS Quarterly, 34(3), 523–548.

Da Veiga, A., & Eloff, J. H. P., 2010. A framework and assessment instrument for information security culture, Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N., 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study, Computers & Security, 49, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

Dinc, M. S., Zaim, H., Hassan, M., & Alzoubi, Y. I., 2022. The effects of transformational leadership on perceived organizational support and organizational identity, Human Systems Management, 41, 699–716. https://doi.org/10.3233/HSM-211563

Ertan, A., Crossland, G., Heath, C., Denney, D., & Jensen, R. B., 2018. Everyday Cyber Security in Organisations: Literature review, Royal Holloway, University of London.

Eseryel, U. Y., Killingsworth, B. L., Reed, A. H., & Furner, C. P., 2024. Strengthening cybersecurity resilience with transformational IT leadership: PASTA-TITL threat modeling framework, Journal of Leadership and Management (online published July 2024).

Georgiadou, A., Mouzakitis, S., & Askounis, D., 2021. Designing cyber-security culture assessment survey targeting critical infrastructures during COVID-19 crisis, International Journal of Network Security & Its Applications, 13(1), 33–50. https://doi.org/10.5121/ijnsa.2021.13103

Haney, J. M., & Lutters, W., 2023. From compliance to impact: Tracing the transformation of an organizational security awareness program, Working paper.

Handri, E. Y., Sensuse, D. I., & Lusa, S., 2024. Examining cybersecurity culture: Trends and success factors, Journal of Internet Services and Information Security, 14(3), 330–352. https://doi.org/10.58346/JISIS.2024.I3.020

Herath, T., & Rao, H. R., 2009. Protection motivation and deterrence: A framework for security policy compliance in organisations, European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Huang, K., & Pearlson, K., 2019. For what technology can't fix: Building a model of organizational cybersecurity culture, Proceedings of the 52nd Hawaii International Conference on System Sciences, 6398–6407. https://hdl.handle.net/10125/60074

Jerab, D., & Mabrouk, T., 2023. The role of leadership in changing organizational culture, SSRN working paper. https://ssrn.com/abstract=4574324

Karlsson, F., Hedström, K., & Goldkuhl, G., 2017. Practice-based discourse analysis of information security policies, Computers & Security, 67, 267–279. https://doi.org/10.1016/j.cose.2016.12.012

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust, Information Systems Journal, 25, 193–230. https://doi.org/10.1111/isj.12063

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S., 2019. An analysis on the dimensions of information security culture concept: A review, Journal of Information Security and Applications, 44, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

Olaniyi, O. O., Asonze, C. U., Ajayi, S. A., Olabanji, S. O., & Adigwe, C., 2023. A regressional study on the impact of organizational security culture and transformational leadership on social engineering awareness among bank employees: The interplay of security culture and transformational leadership, Asian Journal of Economics, Business and Accounting, 23(23), 128–143. https://doi.org/10.9734/AJEBA/2023/v23i231176

Osburn, L. D., 2025. Telling stories about vendors: Narrative practices to negotiate risk and establish an organizational cybersecurity culture, Journal of Cybersecurity, 11(1), tyae030. https://doi.org/10.1093/cybsec/tyae030

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T., 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

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

Willie, M. M., 2023. The role of organizational culture in cybersecurity: Building a security-first culture, Preprint. https://doi.org/10.13140/RG.2.2.14940.18560

Zimmermann, V., & Renaud, K., 2019. Moving from a human-as-problem to a human-as-solution cybersecurity mindset, International Journal of Human-Computer Studies, 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Tables

Appendices

Appendix A: CISO Survey Questionnaire

Leadership Influence on Cybersecurity Culture

This survey is designed to gather comprehensive insights into CISO perspectives on cybersecurity culture development within organizational contexts

1. How would you describe your organization's current cybersecurity culture maturity level?

   Mark only one oval.

   - ◯ Initial - Ad hoc security practices with limited awareness
   - ◯ Developing - Basic security policies in place with growing awareness
   - ◯ Defined - Established security culture with consistent practices
   - ◯ Managed - Mature security culture with measurable outcomes
   - ◯ Optimizing - Continuously improving security culture with innovation

2. What is the primary driver for cybersecurity culture development in your organization?

   Mark only one oval.

   - ◯ Regulatory compliance requirements
   - ◯ Previous security incidents or breaches
   - ◯ Board or executive mandate
   - ◯ Industry best practices and benchmarking
   - ◯ Customer or stakeholder expectations

3. How does your organization's industry context influence cybersecurity culture development?

Mark only one oval.

- ◯ Heavily regulated environment requiring strict compliance culture
- ◯ Competitive environment emphasizing innovation and agility
- ◯ High-risk environment with significant threat exposure
- ◯ Traditional environment with established security practices
- ◯ Emerging industry with evolving security requirements

4. What organizational characteristics most significantly impact cybersecurity culture development?

Mark only one oval.

- ◯ Company size and complexity
- ◯ Geographic distribution and remote work
- ◯ Technology infrastructure and legacy systems
- ◯ Organizational hierarchy and decision-making processes
- ◯ Employee demographics and technology literacy

5. How do you assess the current state of cybersecurity culture in your organization?

Mark only one oval.

- ◯ Formal culture assessment surveys and metrics
- ◯ Security incident analysis and trend monitoring
- ◯ Employee feedback and focus groups
- ◯ Compliance audit results and findings
- ◯ Informal observation and stakeholder discussions

6. What is the biggest challenge in developing cybersecurity culture within your organizational context?

   Mark only one oval.

   - ◯ Limited resources and budget constraints
   - ◯ Resistance to change and cultural inertia
   - ◯ Competing business priorities and time pressures
   - ◯ Lack of executive support and commitment
   - ◯ Technical complexity and system limitations

7. How does your organization's existing culture support or hinder cybersecurity culture development?

   Mark only one oval.

   - ◯ Strongly supports through risk-aware and compliance-oriented culture
   - ◯ Moderately supports with some alignment to security objectives
   - ◯ Neutral with mixed support depending on business unit
   - ◯ Moderately hinders due to efficiency and productivity focus
   - ◯ Strongly hinders through risk-taking and innovation-focused culture

8. What role does organizational structure play in cybersecurity culture development?

   Mark only one oval.

   - ◯ Hierarchical structure enables clear security directives and accountability
   - ◯ Flat structure promotes collaboration and shared security responsibility
   - ◯ Matrix structure creates complexity but enables cross-functional security integration
   - ◯ Decentralized structure allows for customized security approaches by unit
   - ◯ Structure has minimal impact on security culture development

9. How do external factors (regulations, threats, industry standards) influence your cybersecurity culture approach?

Mark only one oval.

- ◯ Heavily influence with strict adherence to external requirements
- ◯ Moderately influence with adaptation to organizational context
- ◯ Minimally influence with focus on internal business needs
- ◯ Influence varies by business unit and function
- ◯ External factors are secondary to internal culture considerations

10. What organizational capabilities are most critical for successful cybersecurity culture development?

Mark only one oval.

- ◯ Strong leadership and change management capabilities
- ◯ Effective communication and training capabilities
- ◯ Robust technology and security infrastructure
- ◯ Clear governance and policy development capabilities
- ◯ Employee engagement and feedback capabilities

11. Which leadership style do you primarily employ for cybersecurity culture development?

Mark only one oval.

- ◯ Transformational - Inspiring vision and motivating change
- ◯ Transactional - Clear expectations and performance management
- ◯ Servant - Supporting and empowering employees
- ◯ Authentic - Transparent and values-based leadership
- ◯ Adaptive - Flexible approach based on situation and context

12. How do you communicate cybersecurity culture importance to different organizational levels?

Mark only one oval.

- Consistent message across all levels with role-specific examples
- Tailored messages for executives, managers, and employees
- Technical focus for IT staff, business focus for other employees
- Compliance emphasis for regulated functions, risk focus for others
- Storytelling and narrative approaches across all levels

13. What strategies do you use to gain executive support for cybersecurity culture initiatives?

Mark only one oval.

- Business case development with ROI and risk quantification
- Regulatory compliance and audit requirement emphasis
- Industry benchmarking and competitive positioning
- Incident impact scenarios and potential business consequences
- Integration with existing business strategy and objectives

14. How do you engage middle management in cybersecurity culture development?

Mark only one oval.

- Training managers to incorporate security into team discussions
- Providing security culture metrics and performance indicators
- Creating security champion roles and recognition programs
- Integrating security culture into management performance evaluations
- Regular communication and feedback sessions with management

15. What approach do you take to influence employee cybersecurity behaviors?

Mark only one oval.

- ◯ Policy enforcement and compliance monitoring
- ◯ Education and awareness training programs
- ◯ Positive reinforcement and recognition programs
- ◯ Peer influence and social norm development
- ◯ Technology solutions that make secure behaviors easier

16. How do you handle resistance to cybersecurity culture change?

Mark only one oval.

- ◯ Address concerns through open communication and feedback
- ◯ Provide additional training and support for resistant individuals
- ◯ Use influence and persuasion techniques to build buy-in
- ◯ Implement gradual change with pilot programs and phased rollouts
- ◯ Enforce compliance through disciplinary measures when necessary

17. What role do you play in modeling cybersecurity behaviors for the organization?

Mark only one oval.

- ◯ Highly visible role modeling with consistent security practices
- ◯ Regular communication about personal security practices and experiences
- ◯ Participation in security training and awareness programs
- ◯ Transparent discussion of security challenges and lessons learned
- ◯ Focus on strategic leadership rather than personal behavior modeling

18. How do you measure the effectiveness of your leadership approach to cybersecurity culture?

Mark only one oval.

- Employee engagement and satisfaction surveys
- Security incident trends and behavior metrics
- Compliance audit results and regulatory feedback
- 360-degree feedback and leadership assessments
- Business impact metrics and risk reduction measures

19. What leadership challenges do you face in cybersecurity culture development?

Mark only one oval.

- Balancing security requirements with business operational needs
- Communicating technical security concepts to non-technical stakeholders
- Maintaining momentum and engagement over time
- Adapting leadership approach to different organizational contexts
- Managing competing priorities and resource constraints

20. How do you develop other leaders within the organization to support cybersecurity culture?

Mark only one oval.

- Formal leadership development programs with security culture components
- Mentoring and coaching relationships with emerging security leaders
- Cross-functional assignments and security culture project leadership
- External training and certification programs for security leadership
- Peer learning networks and security leadership communities

21. What is the most significant barrier to cybersecurity culture development in your organization?

Mark only one oval.

- ◯ Limited budget and resource allocation
- ◯ Competing business priorities and time constraints
- ◯ Lack of employee awareness and engagement
- ◯ Technical complexity and system limitations
- ◯ Organizational resistance to change

22. How do budget and resource constraints impact cybersecurity culture development?

Mark only one oval.

- ◯ Severely limit culture development initiatives and programs
- ◯ Require creative approaches and leveraging of existing resources
- ◯ Focus efforts on high-impact, low-cost culture initiatives
- ◯ Minimal impact due to culture being primarily about behaviors
- ◯ Drive innovation and efficiency in culture development approaches

23. How do regulatory requirements impact cybersecurity culture development?

Mark only one oval.

- ◯ Provide clear framework and motivation for culture development
- ◯ Create compliance focus that may undermine genuine culture change
- ◯ Require specific culture elements that may not fit organizational context
- ◯ Offer external validation and support for culture initiatives
- ◯ Have minimal impact on actual culture development efforts

24. How does organizational change readiness affect cybersecurity culture development?

Mark only one oval.

- ◯ High change readiness accelerates culture development significantly
- ◯ Low change readiness requires extended timeline and additional support
- ◯ Change readiness varies by department requiring tailored approaches
- ◯ Culture development can improve overall organizational change readiness
- ◯ Change readiness is less important than leadership commitment

25. How do performance measurement and incentive systems impact cybersecurity culture?

Mark only one oval.

- ◯ Aligned incentives strongly support culture development
- ◯ Misaligned incentives create significant barriers to culture change
- ◯ Individual incentives are less important than team and organizational recognition
- ◯ Incentive systems have minimal impact on security culture
- ◯ Performance measurement helps track progress but doesn't drive culture

26. How frequently do you assess cybersecurity culture in your organization?

Mark only one oval.

- ◯ Continuously through ongoing metrics and monitoring
- ◯ Annually through comprehensive culture assessments
- ◯ Quarterly through pulse surveys and key indicators
- ◯ After major incidents or significant organizational changes
- ◯ Irregularly based on available resources and priorities

27. How do you use cybersecurity culture assessment results?

Mark only one oval.

- Identify specific areas for improvement and targeted interventions
- Track progress over time and demonstrate culture development success
- Benchmark against industry standards and peer organizations
- Support business case development for additional security culture investment
- Inform strategic planning and resource allocation decisions

28. How do you validate the accuracy and reliability of culture assessment results?

Mark only one oval.

- Multiple assessment methods and data source triangulation
- External validation through third-party assessments
- Longitudinal tracking and trend analysis
- Comparison with objective security performance metrics
- Stakeholder feedback and result validation sessions

29. How do you communicate culture assessment results to different stakeholders?

Mark only one oval.

- Executive dashboards with high-level metrics and trends
- Detailed reports with specific findings and recommendations
- Department-specific feedback with relevant improvement areas
- Organization-wide communication highlighting progress and achievements
- Tailored presentations based on stakeholder interests and responsibilities

30. How do you ensure cybersecurity culture assessment leads to meaningful action?

Mark only one oval.

- ◯ Clear action planning process with specific improvement initiatives
- ◯ Assignment of accountability and ownership for culture improvement
- ◯ Integration with performance management and evaluation processes
- ◯ Regular follow-up and progress monitoring
- ◯ Resource allocation and budget support for identified improvements