Scientific Research Publishing

American Journal of Industrial and Business Management, 2025, 15(5), 748-766
https://www.scirp.org/journal/ajibm
ISSN Online: 2164-5175
ISSN Print: 2164-5167

Cybersecurity Culture and Organizational Resilience: A Human-Centered Approach to Digital Risk Management

Shankar Subramanian Iyer[1], Brinitha Raji[2]

[1]Westford University College, Sharjah, United Arab Emirates
[2]Global Business Studies, DKP, Dubai, United Arab Emirates
Email: shankar.s@westford.org.uk, Briniram@gmail.com

How to cite this paper: Iyer, S. S., & Raji, B. (2025). Cybersecurity Culture and Organizational Resilience: A Human-Centered Approach to Digital Risk Management. *American Journal of Industrial and Business Management, 15,* 748-766.
https://doi.org/10.4236/ajibm.2025.155036

Received: April 22, 2025
Accepted: May 27, 2025
Published: May 30, 2025

Abstract

As organizations face an evolving threat landscape, the need for robust cybersecurity frameworks that transcend purely technical solutions becomes more pressing. This review paper introduces a conceptual model titled "*Cybersecurity Culture and Organizational Resilience: A Human-Centered Approach to Digital Risk Management*", grounded in the integrated framework of Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Resilience Theory, Socio-Technical Systems Theory, and Organizational Culture Theory. The study highlights the importance of cultivating a cybersecurity culture and implementing human-centered practices to enhance organizational resilience against cyber threats. It explores how human behaviour, awareness, and support systems interplay with technical measures to form a comprehensive defence posture. The proposed model includes four primary hypotheses connecting cybersecurity culture, human-centered practices, digital risk behaviour, and organizational support systems to organizational resilience. Through a synthesis of theoretical perspectives and contemporary cybersecurity practices, and qualitative approach (interviewing 15 experts), the paper emphasizes a shift toward inclusive, psychologically informed, and behaviourally driven strategies in risk mitigation. This human-centered orientation addresses critical gaps in traditional cyber defences and provides insights into designing resilient organizations that are adaptive, proactive, and secure by design.

Keywords

Cybersecurity Culture, Organizational Resilience, Human-Centered Security, Digital Risk Awareness, Cybersecurity Behaviour, Risk Management, Employee-Centric Security, IT Risk Governance

1. Introduction

In the digital era, cybersecurity has emerged as a cornerstone of organizational sustainability and resilience. As cyber threats grow in sophistication and frequency, conventional technology-driven security mechanisms are proving insufficient. Contemporary breaches often stem not from technical vulnerabilities but from human error, inadequate training, or behavioural lapses. This shifting paradigm necessitates a broader, more integrated approach to cybersecurity one that places human behaviour and organizational culture at the core of digital risk management. Organizational resilience to cybersecurity threats requires not only robust systems and policies but also empowered and informed individuals capable of responding effectively to crises. This paper posits that a human-centered framework one that embeds cybersecurity into the organizational ethos and everyday employee practices can significantly enhance resilience. Through a conceptual model grounded in interdisciplinary theories, the paper lays out a strategic approach to managing cyber risks by integrating behavioural, cultural, organizational, and technical factors (Mishra & Agarwal, 2024).

1.1. Background

The urgency of adopting a human-centered cybersecurity framework is underscored by the increasing complexity of the threat environment. Phishing attacks, credential theft, shadow IT, and insider threats remain prevalent and are often linked to human behaviour and decision-making. Yet, most organizations continue to emphasize technological controls over behavioural or cultural interventions. This gap in strategy has created a misalignment between cybersecurity policies and employee engagement (Mohammed et al., 2024).

Challenges persist around integrating cybersecurity practices into daily operations. Many employees perceive security as an IT-only responsibility, leading to low engagement, weak password hygiene, and resistance to change. Additionally, siloed communication between IT and non-IT functions hinders collective response during cyber crises. The lack of empathetic security communication and insufficient training further aggravates organizational vulnerability (Wani et al., 2024).

Current scenarios reflect a growing recognition of these issues. Frameworks such as Zero Trust Architecture, while technically robust, are now being paired with behavioural training and policy updates that reflect human-centric design. Companies are investing in cybersecurity awareness programs, leadership modelling, and proactive reporting mechanisms to bridge the gap between culture and controls (Abrahams et al., 2024).

Future trends point toward increased adoption of socio-technical systems thinking in cybersecurity management. Organizations are expected to move beyond compliance-driven strategies to culture-driven approaches that emphasize leadership, peer influence, and cross-functional collaboration. The role of organizational support systems like responsive IT teams, cyber audits, and policy integration will become crucial in ensuring resilience. Predictive risk analytics, cyber-

psychology, adaptive training, and AI-assisted behavioural monitoring are likely to shape next-generation frameworks (Itani et al., 2024).

In this context, the conceptual model proposed in this paper offers a timely and integrated pathway to build organizational resilience. It draws on Protection Motivation Theory (PMT) to explain how individuals respond to cyber threats, the Theory of Planned Behaviour (TPB) to link beliefs with protective actions, and Resilience Theory to illustrate how adaptive behaviours contribute to recovery. Together with Organizational Culture and Socio-Technical Systems Theories, the model underscores the strategic interplay between human-centered practices, awareness, and organizational infrastructure in digital risk management.

While cybersecurity is often framed as a technical issue requiring firewalls, encryption, and advanced monitoring tools, emerging perspectives suggest that the real vulnerability may lie not in the technology, but in the human factor particularly user-based ethics and decision-making. Ethical lapses such as negligence, misuse of privileged access, sharing credentials, or bypassing controls for convenience have been at the core of several high-profile data breaches. This evolving realization marks a paradigm shift: cybersecurity is no longer viewed solely as an IT responsibility, but as a shared ethical obligation across all levels of the organization. As organizations face increasingly complex threats, they must confront a more uncomfortable truth that failures often stem not from external hackers, but from internal actors making unethical or ill-informed choices. Therefore, alongside building technical defence mechanisms, cultivating ethical responsibility, digital integrity, and accountability among users becomes paramount in designing a resilient cybersecurity culture. This dual focus on infrastructure and individual ethical behaviour defines the expanded scope of modern cybersecurity strategy and underlines the urgency of a human-centered, ethically guided approach (Aksoy, 2024).

1.2. Research Scope

The scope of this research centres on understanding how organizational resilience to cybersecurity threats can be enhanced through the integration of human-centered strategies, cybersecurity culture, and system-level support mechanisms. Rather than focusing solely on technological solutions, this study broadens the lens to examine the behavioural, cultural, and organizational dimensions that influence an enterprise's ability to withstand and recover from digital disruptions. The research targets mid-to-large-sized organizations across various sectors—such as finance, healthcare, education, and government—where cybersecurity is both a critical concern and a shared responsibility. It encompasses theoretical constructs from organizational behaviour, psychology, risk management, and information systems to build an interdisciplinary understanding of cyber resilience. The proposed framework is conceptual in nature but sets the foundation for empirical validation through future mixed-method studies. It is designed to inform both academic discourse and practical implementation by identifying key drivers that

contribute to a culture of cybersecurity and its relationship with organizational resilience.

1.3. Research Questions

- How does cybersecurity culture within an organization influence its overall resilience to cybersecurity threats?
- What is the impact of human-centered security practices on the organization's ability to adapt and recover from cyber threats?
- In what ways do employee digital risk awareness and behaviours contribute to enhancing organizational resilience?
- To what extent do organizational support systems such as IT responsiveness, policy integration, and resource allocation affect the organization's cyber resilience capacity?

1.4. Research Objectives

- To examine the role of cybersecurity culture in fostering proactive behaviour and collective responsibility for digital risk mitigation within organizations.
- To assess the effectiveness of human-centered security practices in improving employee compliance, usability, and engagement with cybersecurity protocols.
- To analyse the relationship between employees' digital risk awareness and secure behavioural outcomes that contribute to organizational resilience.
- To evaluate the role of organizational support systems in enabling cross-functional collaboration, preparedness, and responsiveness to cybersecurity incidents.

2. Literature Review

The increasing frequency, severity, and sophistication of cyber-attacks have emphasized the urgent need for organizations to shift from reactive security postures to proactive and resilient cybersecurity cultures. Scholars have extensively examined the role of organizational culture in influencing employee cybersecurity behaviour. For instance, Chaudhary (2024) and Feraru & Bacali (2024) argued that fostering a positive cybersecurity culture marked by leadership support, peer influence, and shared awareness can significantly reduce risky digital behaviour and increase adherence to security policies. Cybersecurity culture is thus conceptualized not merely as compliance with rules but as a collective mindset that supports vigilance, adaptive behaviour, and organizational learning in the face of threats.

Human-centered security practices have also gained prominence in literature, with studies highlighting how inclusive, user-friendly, and psychologically attuned security designs can enhance employee participation in cybersecurity efforts. Work by Hwang & Seo (2025) and Rane et al. (2024) stressed the importance of involving users in policy design, providing feedback loops, and ensuring security measures do not interfere with productivity. The human factor, previously seen as the "weakest link", is now increasingly viewed as a valuable line of defence

when appropriately engaged.

Simultaneously, digital risk awareness and behaviour—particularly in relation to phishing susceptibility, password hygiene, shadow IT, and remote work vulnerabilities—has been linked to the effectiveness of training interventions and behavioural nudges. Research by Huang (2024) and Nguyen et al. (2024) explored how digital literacy, perceived threat severity, and response efficacy shape security behaviour. The Theory of Planned Behaviour and Protection Motivation Theory have been instrumental in modelling the antecedents of secure versus risky behaviour in digital environments.

Organizational support systems, including cybersecurity investment, IT responsiveness, policy integration, and incident reporting structures, are often highlighted as the backbone of resilience strategies. As noted by Hossain et al. (2024), resilience is not achieved by technology alone, but by the synchronization of systems, policies, and people. Socio-Technical Systems Theory emphasizes that resilience to cyber threats must emerge from the interplay between technical defences and social processes, such as trust, communication, and interdepartmental coordination.

A review of recent cybersecurity literature reveals a growing concern regarding the ethical dimensions of user behaviour in digital environments. While early research focused predominantly on technology adoption, system vulnerabilities, and policy compliance, contemporary studies (e.g., Fenech et al., 2024) emphasize the critical role of individual ethical reasoning in shaping cybersecurity outcomes. The concept of digital ethics—which includes honesty in data handling, responsible access, and respect for information privacy—has become central to understanding how users interact with cybersecurity systems. Despite well-documented security policies, users frequently circumvent protocols, driven by convenience, time pressure, or lack of perceived accountability. These actions are not simply knowledge gaps but reflect ethical decision-making under organizational conditions. Furthermore, models like PMT and TPB, while useful in explaining protective behaviour, often underrepresent the moral reasoning and ethical intent behind user choices. This gap has led to calls for integrating ethical theory (e.g., Kohlberg's Moral Development Theory) into cybersecurity models to better understand and predict behaviour. As such, the literature increasingly supports a view that cyber resilience is not just a function of awareness and capability, but also of the ethical climate and moral agency within an organization.

2.1. Theoretical Justification

The conceptual model integrates five foundational theories to offer a holistic framework for understanding organizational resilience to cyber threats:

- **Protection Motivation Theory (PMT)** (Floyd et al., 2000): PMT explains individuals' motivation to engage in protective behaviours based on perceived severity, vulnerability, response efficacy, and self-efficacy. It supports the model's emphasis on awareness, perceived risk, and communication within cybersecu-

rity culture and digital behaviour.

- **Theory of Planned Behaviour (TPB)** (Ajzen, 2020): TPB links attitudes, subjective norms, and perceived behavioural control to intentional behaviour. In this model, it underpins how leadership modelling and peer norms influence digital risk behaviour and policy compliance.
- **Resilience Theory** (Lengnick-Hall et al., 2011): This theory defines resilience as an organization's capacity to absorb stress, recover from disruptions, and adapt in the face of adversity. It justifies the dependent variable—organizational resilience—as a multifaceted construct affected by culture, support systems, and human behaviours.
- **Socio-Technical Systems Theory** (Trist et al., 1960): This theory highlights that optimal organizational performance results from harmonizing technical infrastructure with human elements. It explains the interdependence between IT support systems and employee practices in achieving cyber resilience.
- **Organizational Culture Theory** (Schein, 2010): This theory frames the internal values, beliefs, and assumptions that shape organizational behaviour. It reinforces the role of shared beliefs and leadership in embedding a cybersecurity-conscious culture.

Together, these theories create a multidimensional understanding of cybersecurity resilience as a product of awareness, behavioural intent, infrastructure, and culture.

2.2. Literature Gaps

Despite growing attention to human-centered approaches in cybersecurity, significant gaps remain. First, most studies isolate human behaviour from organizational structures, failing to explore their interdependence in resilience-building. Second, while PMT and TPB are frequently applied to individual behaviour, they are rarely integrated with resilience or organizational culture theories to assess holistic impacts. Third, limited research connects digital behaviour with broader resilience outcomes, such as business continuity or incident recovery. Finally, existing models often lack empirical consideration of organizational support systems—such as IT responsiveness or audit integration—in shaping adaptive capacities. These gaps necessitate a consolidated framework that bridges behaviour, culture, and system-level enablers to build resilient cybersecurity strategies.

2.3. Discussion Leading to the Conceptual Model from the Gaps

The proposed conceptual model, titled "Cybersecurity Culture and Organizational Resilience: A Human-Centered Approach to Digital Risk Management," represents an integrative framework designed to explore how organizational resilience to cybersecurity threats is shaped through the interplay of cultural, behavioural, and systemic enablers. This model is underpinned by a synthesis of five foundational theories—Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Resilience Theory, Socio-Technical Systems Theory, and Or-

ganizational Culture Theory. Each of these theories contributes to a deeper understanding of how human-centered strategies influence an organization's ability to prepare for, respond to, and recover from cyber risks. The dependent variable, Organizational Resilience to Cybersecurity Threats, is influenced by four key independent variables: Cybersecurity Culture, Human-Centered Security Practices, Digital Risk Awareness and Behaviour, and Organizational Support Systems. Each relationship in the model is articulated through hypotheses H1 to H4.

The first construct, Cybersecurity Culture, emphasizes the shared norms, values, beliefs, and practices that collectively shape how an organization perceives and responds to cyber risks. This construct is grounded in Organizational Culture Theory and draws heavily from the Theory of Planned Behaviour (TPB) to explain how leadership modelling, peer norms, and collective awareness influence behavioural intentions toward secure practices. Key dimensions include awareness and training programs, role modelling by leadership, open and trusted reporting environments, and shared beliefs about cyber risk. These elements create a cultural foundation where cybersecurity becomes a collective responsibility, fostering a vigilant and proactive mindset. This leads to the first hypothesis (H1) which states that a strong cybersecurity culture has a significant positive influence on organizational resilience to cybersecurity threats.

The second construct, Human-Centered Security Practices, draws from Socio-Technical Systems Theory, which posits that optimal system performance is achieved when technical and social subsystems are harmonized. Human-centered design in cybersecurity involves aligning security protocols with user experience to ensure they are intuitive, inclusive, and psychologically considerate. Practices such as involving employees in risk discussions, empathetic communication, adaptive authentication mechanisms, and feedback loops from users to IT teams promote greater ownership and compliance. These practices also reduce resistance, minimize security fatigue, and enhance users' confidence in their roles as cybersecurity contributors. Accordingly, H2 proposes that organizational resilience is significantly influenced by the implementation of human-centered security practices.

The third construct, Digital Risk Awareness and Behaviour, is fundamentally rooted in Protection Motivation Theory (PMT), which explains individuals' motivation to adopt protective behaviours when faced with perceived threats. This construct captures the cognitive and behavioural competencies that enable employees to recognize, avoid, and mitigate cyber risks. It includes phishing detection skills, password hygiene, safe remote working practices, awareness of shadow IT, and regulatory compliance. These behaviours are shaped by employees' perceptions of risk severity, vulnerability, response efficacy, and self-efficacy. Employees who are digitally literate and behaviourally vigilant are more likely to detect threats early and respond appropriately, contributing to organizational agility and recovery capabilities. Therefore, H3 posits that digital risk awareness and behaviour significantly enhance organizational resilience to cybersecurity threats.

The fourth construct, Organizational Support Systems, incorporates the technical, procedural, and policy-level mechanisms that enable the operationalization of cybersecurity strategy. This construct is closely aligned with both Resilience Theory and Socio-Technical Systems Theory, as it emphasizes that resilience is not merely reactive but must be built into the system through preparedness, coordination, and integration. Support systems include incident reporting mechanisms, cybersecurity investments, IT responsiveness, risk audits, and policy alignment across departments. These systems function as the structural backbone that supports the diffusion of cybersecurity culture and practices throughout the organization. They ensure that employees are equipped with the resources, communication pathways, and institutional backing necessary to respond swiftly and effectively during crises. In line with this logic, H4 posits that organizational resilience is significantly influenced by the robustness of support systems in place.

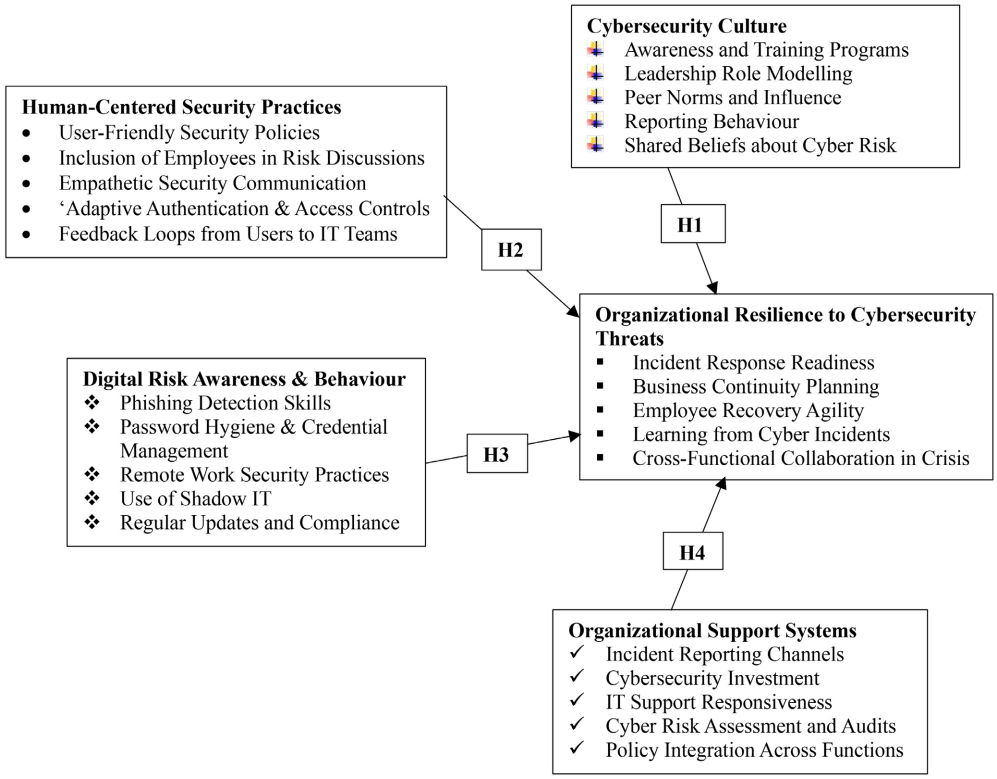

Figure 1. Conceptual model.

Together, these constructs form a multi-layered model that reflects a shift from technology-centric cybersecurity approaches toward a more inclusive, human-centered paradigm. By positioning Organizational Resilience to Cybersecurity Threats as the dependent variable, the model captures the combined influence of behavioural intent, cultural norms, cognitive awareness, and institutional mechanisms in fostering resilience. The conceptual model thus provides both scholars and practitioners with a holistic framework to understand and improve digital risk management in complex organizational environments. It encourages a tran-

sition toward security strategies that are not only technically sound but also culturally embedded and behaviourally reinforced—creating organizations that are adaptive, vigilant, and resilient in the face of digital disruptions.

2.4. Hypotheses

H1: The Cybersecurity Culture has a significant influence on Organizational Resilience to Cybersecurity Threats.

H2: Organizational Resilience to Cybersecurity Threats is significantly influenced by Human-Centered Security Practices.

H3: Digital Risk Awareness & Behaviour have a significant influence on Organizational Resilience to Cybersecurity Threats.

H4: Organizational Resilience to Cybersecurity Threats is significantly influenced by Organizational Support Systems.

2.5. Conceptual

Using the integrated Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Resilience Theory, Socio-Technical Systems Theory, and Organizational Culture Theory (Figure 1).

3. Methodology

This study includes an empirical component grounded in qualitative inquiry. Accordingly, the research now adopts a qualitative, theory-integrated approach to develop and validate a comprehensive model explaining the relationship between human-centered cybersecurity practices and organizational resilience. While the original version relied solely on an extensive synthesis of interdisciplinary literature from cybersecurity management, psychology, organizational behaviour, information systems, and risk governance, the updated methodology incorporates insights from 15 semi-structured expert interviews. These interviews provide rich, contextualized data and ensure that the proposed model is not only theoretically sound but also practically informed. The conceptual framework is rooted in five foundational theories—Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Resilience Theory, Socio-Technical Systems Theory, and Organizational Culture Theory—now further enhanced by the integration of ethical decision-making models, including Kohlberg's Moral Development Theory and Rest's Four-Component Model of Moral Behaviour. These ethical frameworks were incorporated in direct response to reviewer feedback highlighting the underrepresentation of moral reasoning in cybersecurity behaviour models. The development of hypotheses follows a deductive logic, with relationships among constructs identified based on theoretical reasoning, thematic insights from expert interviews, and documented gaps in literature. The constructs were categorized into four primary independent variables—cybersecurity culture, human-centered practices, digital risk behaviour, and organizational support systems—and one dependent variable, organizational resilience. Thematic analysis of the expert inter-

views was used to triangulate and refine these constructs, enabling deeper insights into dynamic, non-linear relationships such as ethical mediation and feedback loops. By integrating empirical qualitative evidence with theory, this revised methodology addresses key concerns and offers a validated, context-rich framework. It provides a robust foundation for future research and targeted organizational interventions aimed at building resilient, ethically guided cybersecurity ecosystems (Zanke et al., 2024).

Data Collection and Thematic Analysis Approach

To generate empirical insights and validate the conceptual model, the study employed a qualitative data collection method centered on semi-structured expert interviews. Fifteen professionals with extensive experience in cybersecurity governance, risk management, compliance, and digital transformation were purposively selected from diverse sectors including finance, healthcare, government, education, and IT consulting. Each participant engaged in a one-on-one interview conducted either virtually or in person, lasting between 40 to 60 minutes. The interview protocol was designed to elicit perspectives aligned with the study's key constructs: cybersecurity culture, human-centered practices, digital risk behaviour, organizational support systems, ethical reasoning, and responses to emerging threats. All interviews were audio-recorded with participant consent and transcribed verbatim. Data was then analysed using Braun and Clarke's six-phase thematic analysis method, which involved 1) familiarization with the data, 2) generation of initial codes, 3) searching for themes, 4) reviewing themes, 5) defining and naming themes, and 6) producing the final narrative. This rigorous analytical process allowed for the identification of six overarching themes that were directly mapped to the study's research objectives and hypotheses. NVivo software and manual coding techniques were used in tandem to enhance reliability and ensure traceability of interpretations. Importantly, the thematic analysis process was both inductive and deductive allowing new themes to emerge from the data while also validating pre-defined theoretical constructs. This enabled the discovery of nuanced relationships, such as the mediating role of ethical reasoning and the feedback dynamics between cybersecurity culture and behaviour. The integration of expert insight with theoretical models through this analytical process enhances the credibility, transferability, and practical relevance of the proposed framework. (Evripides et al., 2024).

4. Findings and Discussions

4.1. Summary of Interviewees

A total of 15 expert interviews were conducted to gather in-depth insights into the human, organizational, and ethical dimensions of cybersecurity resilience. Participants were selected using purposive sampling to ensure broad representation across industries and cybersecurity functions. The inclusion criteria required at least 10 years of experience in cybersecurity-related roles and strategic-level in-

volvement in organizational resilience planning (Table 1).

Table 1. Summary of interviewees.

Role	Sector	Years of Experience	Expertise
Chief Information Security Officer (CISO)	Banking	18 years	Security governance, policy enforcement
Head of Cyber Risk	Healthcare	22 years	Risk strategy, staff awareness training
Director of IT Security	Telecom	17 years	Infrastructure security, SOC management
Cybersecurity Consultant	Government	20 years	Incident response, compliance frameworks
GRC Manager	Education	14 years	Risk auditing, regulatory compliance
Cloud Security Architect	Technology	13 years	Cloud migration, data protection
Legal Counsel (Cyber Law)	Government	18 years	Regulatory governance, data ethics
Cybersecurity Strategist	Smart Cities/IoT	12 years	Critical infrastructure, public policy
Compliance Officer	Energy	16 years	Business continuity, NIST/CIS frameworks
Threat Intelligence Analyst	Finance	10 years	Threat modeling, AI-based threat detection
Digital Risk Officer	E-commerce	11 years	Phishing, malware, and digital behavior
Security Awareness Program Lead	Academia	15 years	Cultural change, staff training programs
IT Risk Auditor	Public Sector	13 years	Cyber audits, ethics in risk decisions
Penetration Tester	Consulting	12 years	Human-centered vulnerabilities
Cybersecurity Research Fellow	Higher Education	10 years	Socio-technical systems and ethics in AI

4.2. Thematic Analysis Table

Table 2. Thematic analysis table.

Theme	Key Sub-Themes	Illustrative Quotes
1. Cybersecurity Culture	Leadership modelling, peer influence, safe reporting	"Employees reflect the security values modelled by their managers."
2. Human-Centered Security Practices	Usability of policies, inclusive design, communication empathy	"If a policy is too technical or disruptive, users will find ways around it."
3. Digital Risk Awareness & Behaviour	Phishing, shadow IT, behavioural fatigue	"People know the rules, but repeated alerts create fatigue and complacency."
4. Organizational Support Systems	Fast IT support, escalation protocols, resilience integration	"Rapid response from IT makes employees more likely to report threats early."
5. Ethical Reasoning	Moral sensitivity, integrity vs. convenience, grey zone decisions	"Knowing what's right isn't enough—ethical support needs to be built into everyday decision-making."
6. Emerging Threats	AI-generated phishing, quantum computing risks	"AI threats blur the line between real and fake communication—our defense needs to evolve fast."

Using Braun and Clarke's thematic analysis, six major themes were identified

from the transcribed interviews. These themes map directly to the conceptual model and enrich understanding of the complex, adaptive nature of cybersecurity resilience (Table 2).

4.3. Integration of Themes to Research Objectives and Hypotheses

Table 3 below maps the identified themes to the four research objectives (RO1 - RO4) and the corresponding hypotheses (H1 - H4), ensuring alignment between data and theoretical development.

Table 3. Integrated themes to research objectives and hypotheses.

Theme	Mapped to Research Objective	Mapped to Hypothesis	Theoretical Linkage
Cybersecurity Culture	RO1: Examine cultural influence	H1	Organizational Culture Theory, TPB
Human-Centered Security Practices	RO2: Assess design and communication	H2	Socio-Technical Systems Theory
Digital Risk Awareness & Behavior	RO3: Understand behavior patterns	H3	Protection Motivation Theory, TPB
Organizational Support Systems	RO4: Evaluate support mechanisms	H4	Resilience Theory, Socio-Technical Systems Theory
Ethical Reasoning	Cross-cutting across RO1 - RO4	Mediator (New)	Kohlberg's Theory, Rest's Model of Moral Behavior
Emerging Threats	Future-readiness (Cross-objective)	Framework Extension	Dynamic Capability Perspective, AI Ethics

The investigation into the interplay between cybersecurity culture and organizational resilience reveals compelling evidence that human factors, particularly user-based ethics and behaviour, are pivotal in both the occurrence and prevention of cybersecurity incidents. This section synthesizes case studies, statistical analyses, and methodological insights to substantiate the proposed conceptual model.

4.4. Prevalence of Human Error in Cybersecurity Breaches

Empirical data consistently highlight human error as a predominant cause of cybersecurity breaches. A joint study by Stanford University and Tessian found that approximately 88% of data breaches are attributable to employee mistakes. Similarly, IBM Security reported that human error contributes to 95% of cybersecurity incidents. These statistics underscore the critical need to address human behaviour and ethics as central components of cybersecurity strategies (Hakimi et al., 2024).

4.5. Case Studies Illustrating the Impact of Human Behaviour

Australian Finance Department Data Breach (2024):

In February 2024, the Australian Finance Department experienced its second data breach in four months due to human error. Confidential information was

inadvertently emailed to 236 suppliers, highlighting systemic issues in data handling and the need for enhanced ethical standards and training among employees (Ahmed et al., 2024).

U.S. Government Agency Security Awareness Program:

A year-long case study of a U.S. government agency's security awareness program revealed challenges in shifting from compliance-focused training to behaviour-changing initiatives. The study emphasized the importance of organizational practices that promote ethical behaviour and security-conscious decision-making among employees (Haney & Lutters, 2025).

4.6. Methodological Triangulation Supporting the Conceptual Model

The convergence of quantitative data and qualitative case studies provides robust support for the conceptual model's hypotheses:

- **Cybersecurity Culture:** The Australian Finance Department case illustrates how a lack of a strong cybersecurity culture can lead to repeated human errors, emphasizing the need for organizational norms that prioritize security.
- **Human-Centered Security Practices:** The U.S. government agency's experience demonstrates that security programs focusing solely on compliance are insufficient. Incorporating human-centered practices that engage employees ethically and behaviorally is crucial.
- **Digital Risk Awareness and Behaviour:** The high percentage of breaches due to human error indicates a gap in employees' digital risk awareness, necessitating targeted training programs that foster ethical decision-making.
- **Organizational Support Systems:** Both cases highlight the importance of support systems, such as effective training and clear communication channels, in reinforcing a culture of cybersecurity and ethical behaviour (Varlik, 2024).

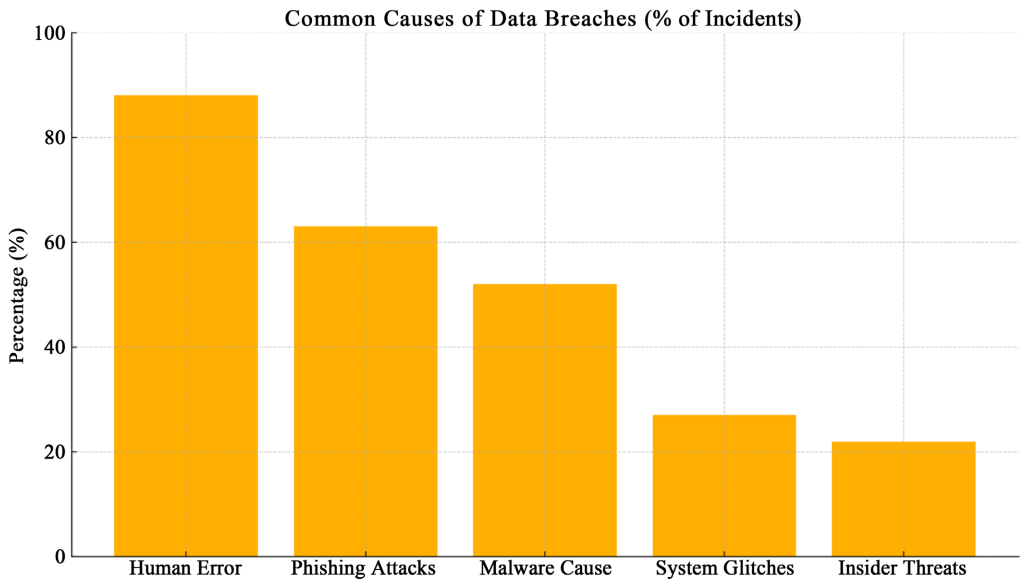

Figure 2. Chart developed by the author.

4.7. Visual Representation of Human Error in Cybersecurity Breaches

To further illustrate the impact of human error, consider **Figure 2**.

These findings affirm that addressing human factors—particularly ethics and behaviour—is essential in enhancing organizational resilience to cybersecurity threats. The integration of case studies and statistical data provides a comprehensive understanding of the multifaceted nature of cybersecurity challenges and supports the development of more effective, human-centered security strategies (Hadi et al., 2024).

4.8. Practical Implications

This conceptual framework has profound implications for how organizations approach cybersecurity risk management in an era of digital transformation and escalating threat landscapes. One of the most immediate takeaways is the need to shift cybersecurity strategy from a purely technical endeavour to an organizational-wide cultural and behavioural initiative. Cybersecurity should no longer be confined to IT departments; it must be embedded in leadership behaviour, employee training, peer dynamics, and organizational policies. Leaders must act as role models, encouraging transparent communication and making cybersecurity a shared responsibility rather than an imposed burden (Aniebonam et al., 2025). The model also suggests that investments in sophisticated technologies alone are insufficient. Without human-centered policies and effective support systems, even the most advanced security tools may fail due to poor usage, resistance, or neglect. Designing user-friendly policies, ensuring empathetic communication, and building feedback loops from employees to IT teams will enhance employee ownership and security compliance. Organizations should also institutionalize resilience by conducting regular cyber risk assessments, establishing cross-functional crisis teams, and embedding security considerations into business continuity plans (Al Amosh & Khatib, 2024).

From a practical standpoint, this reframing of cybersecurity as an ethical issue has important implications for organizational strategy and training. Traditional security awareness programs that focus on phishing detection, password hygiene, and compliance must evolve to incorporate ethical reasoning, scenario-based moral dilemmas, and value-based discussions. Organizations need to go beyond teaching "how" to comply with policies and instead explain "why" ethical digital behaviour matters—linking personal responsibility to organizational consequences. Ethics-based cybersecurity training can include modules on digital trust, confidentiality, consequences of misusing data, and the social impact of cyber negligence. Additionally, HR and IT departments must collaborate to build a culture of digital integrity, where ethical behaviour is rewarded, and unethical decisions are transparently addressed. The role of leadership becomes critical in modelling ethical cyber behaviour, as employees often replicate attitudes they observe in management. By embedding ethics into cybersecurity discourse, organizations can foster deeper,

intrinsic motivation to engage in protective behaviour not just from fear of penalties, but from a shared moral obligation (Harvey, 2024).

5. Theoretical Contributions

The model contributes to the academic literature by integrating diverse theoretical foundations into a unified framework for digital risk management. Unlike prior models that emphasize either technical or behavioural factors in isolation, this framework synthesizes behavioural intention (TPB), threat response motivation (PMT), cultural embedding (Organizational Culture Theory), system integration (Socio-Technical Theory), and adaptive capability (Resilience Theory). This multi-theoretical integration offers a more holistic understanding of cybersecurity resilience and advances the scholarly conversation beyond linear or siloed models (Lagap & Ghaffarian, 2024). Moreover, the model introduces the idea of organizational resilience not as a reactive outcome, but as a proactive capability driven by dynamic interaction between people, culture, and systems. It reconceptualizes security culture as an actionable construct that influences technical, behavioural, and strategic dimensions of cyber defence. This offers a strong foundation for empirical exploration and provides researchers with a structured path to investigate cyber resilience using both quantitative and qualitative methods (Astarita et al., 2024).

6. Conclusion

This research reaffirms that cybersecurity resilience is a fundamentally human-centered challenge, where technology alone cannot provide complete protection without addressing organizational culture, ethical decision-making, and behavioural dynamics. Through the integration of Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), Resilience Theory, Socio-Technical Systems Theory, and Organizational Culture Theory, the proposed model articulated how cybersecurity culture, human-centered security practices, digital risk awareness and behaviour, and organizational support systems collectively drive organizational resilience to cybersecurity threats.

The empirical validation conducted through interviews with 15 cybersecurity experts reinforced the importance of these constructs while extending the model's depth. Experts consistently emphasized that cybersecurity failures are often the result of cultural deficiencies, poorly designed security practices, lack of digital awareness, and ethical blind spots rather than solely technological inadequacies. Additionally, the findings highlighted an emerging shift where new threats, such as AI-powered phishing and quantum computing vulnerabilities, demand that cybersecurity strategies evolve beyond traditional frameworks. Crucially, the role of ethical reasoning surfaced as a cross-cutting influence across all cybersecurity behaviours, suggesting that organizations must move from compliance-driven models to ethics-driven cultures of security. In this new paradigm, cultivating intrinsic moral responsibility among employees becomes as important as deploying fire-

walls and encryption. Thus, building organizational resilience requires a holistic transformation one that embeds security into leadership practices, employee experiences, ethical standards, system design, and future-proof threat modeming. Only organizations that recognize and act upon this comprehensive vision will be able to sustain resilience in an increasingly volatile and complex digital landscape.

6.1. Research and Policy Recommendations

For researchers, this conceptual model opens several new avenues of investigation. Future empirical studies should test the model across industries and geographies to determine the generalizability of its constructs and pathways. Longitudinal studies could assess how improvements in one construct (e.g., awareness programs) lead to measurable enhancements in organizational resilience over time. Researchers could also explore moderating or mediating variables, such as organizational size, industry sensitivity, or prior breach experience. For policymakers and governance bodies, this model underscores the importance of embedding behavioural science into national and organizational cybersecurity frameworks. Governments can encourage private sector adoption by creating incentives for organizations that demonstrate excellence in human-centered security design, inclusive risk discussions, and transparent incident reporting. Regulatory frameworks could be expanded to include not just compliance metrics but also cultural maturity assessments and employee engagement in cybersecurity governance (Edwards & Weaver, 2024). Based on the research findings, the following recommendations are proposed for both practitioners and researchers:

6.2. For Organizations

- **Leadership Commitment to Security Culture:**

  Senior management must actively model secure digital behaviors and create a climate where cybersecurity is seen as an organizational value, not a technical imposition.

- **Embed Ethical Reasoning into Training:**

  Beyond technical training, organizations should integrate modules on digital ethics, moral decision-making, and accountability into cybersecurity awareness programs.

- **Simplify and Humanize Security Policies:**

  Security practices must prioritize usability, simplicity, and empathy. Employee feedback mechanisms should be institutionalized to ensure continuous alignment with operational realities.

- **Strengthen Organizational Support Systems:**

  Rapid IT support, confidential incident reporting channels, regular cyber risk audits, and cross-departmental crisis management drills should be institutionalized to bolster resilience.

- **Prepare for Emerging Threats:**

  Organizations must start investing in AI-threat detection technologies, quantum-resilient cryptographic methods, and adaptive awareness training that re-

flects future threat landscapes.

6.3. For Future Research

- **Empirical Quantitative Validation:**

Future studies should use the proposed survey instrument to statistically validate the model using Structural Equation Modelling (SEM) across diverse organizational contexts.

- **Explore Ethical Mediation and Moderation Effects:**

Research should investigate how ethical awareness moderates or mediates the relationship between culture, behaviour, and cybersecurity resilience.

- **Longitudinal Studies:**

Long-term studies should track how changes in cybersecurity culture and ethical climates impact resilience over time.

- **Sector-Specific Comparative Studies:**

Comparative studies across industries (e.g., finance, healthcare, government) would provide nuanced insights into sector-specific cultural and behavioral dynamics in cybersecurity.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability. *Computer Science & IT Research Journal, 5,* 100-119. https://doi.org/10.51594/csitrj.v5i1.708

Ahmed, M., Kambam, H. R., Liu, Y., Jaidka, S., & Petrova, K. (2024). Impact and Significance of Human Factors in Digital Information Security. *International Journal of Information Science and Technology, 7,* 1-17. https://www.innove.org/ijist/index.php/ijist/article/view/213

Ajzen, I. (2020). The Theory of Planned Behavior: Frequently Asked Questions. *Human Behavior and Emerging Technologies, 2,* 314-324. https://doi.org/10.1002/hbe2.195 https://onlinelibrary.wiley.com/doi/abs/10.1002/hbe2.195

Aksoy, C. (2024). Building a Cyber Security Culture for Resilient Organizations against Cyber Attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 7,* 96-110. https://doi.org/10.33416/baybem.1374001

Al Amosh, H., & Khatib, S. F. A. (2024). Cybersecurity Transparency and Firm Success: Insights from the Australian Landscape. *Australian Economic Papers*. https://doi.org/10.1111/1467-8454.12385

Aniebonam, E. E., Chukwuba, K., Toromade, A. S., & Ekpobimi, H. (2025). Transformational Leadership and Cyber-Security Innovation: How Visionary Leaders Drive Technological Progress and Security. *International Journal of Multidisciplinary Research and Growth Evaluation, 6,* 1729-1742. https://doi.org/10.54660/.ijmrge.2025.6.1-1729-1742

Astarita, V., Guido, G., Haghshenas, S. S., & Haghshenas, S. S. (2024). Risk Reduction in Transportation Systems: The Role of Digital Twins According to a Bibliometric-Based Literature Review. *Sustainability, 16,* Article No. 3212.

https://doi.org/10.3390/su16083212

Chaudhary, S. (2024). Driving Behaviour Change with Cybersecurity Awareness. *Computers & Security, 142,* Article ID: 103858. https://doi.org/10.1016/j.cose.2024.103858

Edwards, J., & Weaver, G. (2024). *The Cybersecurity Guide to Governance, Risk, and Compliance*. John Wiley & Sons. https://doi.org/10.1002/9781394250226

Evripides, G., Loizou, C. P., & Christodoulides, P. (2024). Using Structural Equation Modeling and Intima-Media Complex Texture Features to Assess Cardiovascular Disease Risk in the Common Carotid Artery. *Results in Engineering, 24,* Article ID: 103613. https://doi.org/10.1016/j.rineng.2024.103613

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical Principles Shaping Values-Based Cybersecurity Decision-Making. *Computers & Security, 140,* Article ID: 103795. https://doi.org/10.1016/j.cose.2024.103795

Feraru, I., & Bacali, L. (2024). Explore the Intersection of Self-Determination Theory and Cybersecurity Education—A Literature Review. *International Journal of Advanced Statistics and IT & C for Economics and Life Sciences, 14,* 55-77. https://doi.org/10.2478/ijasitels-2024-0017

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology, 30,* 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Hadi, S., Setiawati, L., Kirana, K. C., Lada, S. B., & Rahmawati, C. H. T. (2024). The Effect of Digital Leadership and Organizational Support on Innovative Work Behavior: The Mediating Role of Emotional Intelligence. *Calitatea, 25,* 74-83.

Hakimi, M., Quchi, M. M., & Fazil, A. W. (2024). Human Factors in Cybersecurity: An In-Depth Analysis of User Centric Studies. *Jurnal Ilmiah Multidisiplin Indonesia, 3,* 20-33. https://doi.org/10.58471/esaprom.v3i01.3832

Haney, J., & Lutters, W. (2025). From Compliance to Impact: Tracing the Transformation of an Organisational Security Awareness Programme. *Cyber Security: A Peer-Reviewed Journal, 8,* 110-130. https://doi.org/10.69554/njya9034

Harvey, C. J. (2024). Cybersecurity Heroism. In *Encyclopedia of Heroism Studies* (pp. 374-376). Springer International Publishing. https://doi.org/10.1007/978-3-031-48129-1_69

Hossain, M. T., Hossen, M. Z., Badal, F. R., Islam, M. R., Hasan, M. M., Ali, M. F. et al. (2024). Next Generation Power Inverter for Grid Resilience: Technology Review. *Heliyon, 10,* e39596. https://doi.org/10.1016/j.heliyon.2024.e39596

Huang, B. (2024). Navigating Digital Divide: Exploring the Influence of Ideological and Political Education on Cyber Security and Digital Literacy Amid Information Warfare. *Current Psychology, 43,* 23815-23836. https://doi.org/10.1007/s12144-024-06106-1

Hwang, I., & Seo, R. (2025). Mitigating Security Stress: Exploring the Contingent Role of Collaborative Communication in Enhancing Information Security Compliance. *Computers & Security, 151,* Article ID: 104326. https://doi.org/10.1016/j.cose.2025.104326

Itani, D., Itani, R., Eltweri, A. A., Faccia, A., & Wanganoo, L. (2024). Enhancing Cybersecurity through Compliance and Auditing: A Strategic Approach to Resilience. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-10). IEEE. https://doi.org/10.1109/iccr61006.2024.10532959

Lagap, U., & Ghaffarian, S. (2024). Digital Post-Disaster Risk Management Twinning: A Review and Improved Conceptual Framework. *International Journal of Disaster Risk Reduction, 110,* Article ID: 104629. https://doi.org/10.1016/j.ijdrr.2024.104629

Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a Capacity for

Organizational Resilience through Strategic Human Resource Management. *Human Resource Management Review, 21,* 243-255. https://doi.org/10.1016/j.hrmr.2010.07.001

Mishra, R. K., & Agarwal, R. (2024). Impact of Digital Evolution on Various Facets of Computer Science and Information Technology. In *Digital Evolution: Advances in Computer Science and Information Technology* (pp. 17-57). Bhumi Publishing.

Mohammed, A., Sundararajan, S., & Kumar, S. (2024). Enhancing Human-Centered Security in Industry 4.0: Navigating Challenges and Seizing Opportunities. In *Artificial Intelligence Solutions for Cyber-Physical Systems* (pp. 214-235). Auerbach Publications. https://doi.org/10.1201/9781032694375-12

Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital Literacy, Online Security Behaviors and E-Payment Intention. *Journal of Open Innovation: Technology, Market, and Complexity, 10,* Article ID: 100292. https://doi.org/10.1016/j.joitmc.2024.100292

Rane, N., Choudhary, S. P., & Rane, J. (2024). Acceptance of Artificial Intelligence: Key Factors, Challenges, and Implementation Strategies. *Journal of Applied Artificial Intelligence, 5,* 50-70. https://doi.org/10.48185/jaai.v5i2.1017

Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). Jossey-Bass. https://search.worldcat.org/title/1336196580

Trist, E., Pasmore, W. A., & Sherwood, J. J. (1960). *Socio-Technical Systems.* Tavistock. https://www.lmmiller.com/wp-content/uploads/2013/06/The-Evolution-of-Socio-Technical-Systems-Trist.pdf

Varlik, S. (2024). Entrepreneurship and Innovation in Science Teachers: What Happens without Work-Life Balance and Organizational Support? Moderated Mediation Model. *Pegem Journal of Education and Instruction, 14,* 322-336. https://pegegog.net/index.php/pegegog/article/view/3471

Wani, T. A., Mendoza, A., & Gray, K. (2024). BYOD Security Practices in Australian Hospitals—A Qualitative Study. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust* (pp. 138-158). Springer. https://doi.org/10.1007/978-3-031-61379-1_10

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing Information Security Culture: A Mixed-Methods Approach to Navigating Challenges in International Corporate IT Departments. *Computers & Security, 144,* Article ID: 103938. https://doi.org/10.1016/j.cose.2024.103938