Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 158-183
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Cyberpsychology of Small and Medium-Sized Enterprises Cybersecurity: A Human-Centric Approach to Policy Development

Troy C. Troublefield

Fit Nerd Technology Consultants, Brandon, Florida, USA
Email: drtroytroublefield@yahoo.com

How to cite this paper: Troublefield, T.C. (2025) The Cyberpsychology of Small and Medium-Sized Enterprises Cybersecurity: A Human-Centric Approach to Policy Development. *Journal of Information Security*, **16**, 158-183.
https://doi.org/10.4236/jis.2025.161009

Received: November 6, 2024
Accepted: January 12, 2025
Published: January 15, 2025

Abstract

This study investigates the critical intersection of cyberpsychology and cybersecurity policy development in small and medium-sized enterprises (SMEs). Through a mixed-methods approach incorporating surveys of 523 employees across 78 SMEs, qualitative interviews, and case studies, the research examines how psychological factors influence cybersecurity behaviors and policy effectiveness. Key findings reveal significant correlations between psychological factors and security outcomes, including the relationship between self-efficacy and policy compliance ($r = 0.42$, $p < 0.001$) and the impact of social norms on security behavior ($\beta = 0.37$, $p < 0.001$). The study identifies critical challenges in risk perception, policy complexity, and organizational culture affecting SME cybersecurity implementation. Results demonstrate that successful cybersecurity initiatives require the integration of psychological principles with technical solutions. The research provides a framework for developing human-centric security policies that address both behavioral and technical aspects of cybersecurity in resource-constrained environments.

Keywords

Cyberpsychology, Cybersecurity, SMEs, Policy Development, Human Factors, Risk Perception, Compliance Behavior, Organizational Culture, Psychological Resilience, Security Awareness

1. Introduction

1.1. Background of the Study

The digital transformation of modern business has created unprecedented oppor-

tunities for growth while simultaneously exposing organizations to increasingly sophisticated cyber threats. Small and medium-sized enterprises (SMEs) face particular challenges in this evolving landscape, as they often need more resources and expertise available to larger organizations while remaining attractive targets for cybercriminals. While technical solutions provide essential protective measures, the human element has emerged as a critical factor in determining the effectiveness of cybersecurity initiatives. This research examines the crucial intersection of cyberpsychology and cybersecurity policy development within SME environments, with a particular focus on how psychological factors influence security behaviors and policy effectiveness. Traditional approaches to cybersecurity have primarily emphasized technical solutions, often overlooking the fundamental role of human behavior and psychology in security outcomes. This study addresses this gap by investigating how principles of cyberpsychology can be applied to enhance cybersecurity implementation in resource-constrained environments. The research adopts a mixed-methods approach, combining quantitative surveys, qualitative interviews, and case studies to provide a comprehensive understanding of the psychological dimensions of cybersecurity in SMEs. This methodology enables the identification of both broad patterns and nuanced insights into how organizations can develop more effective, human-centric security policies that acknowledge both technical requirements and psychological realities. Through this investigation, the study addresses several critical research questions: How psychological factors influence cybersecurity behavior in SME environments, what role organizational culture plays in shaping security practices, how SMEs can develop effective security policies that account for human psychological factors, and what strategies organizations can employ to enhance psychological resilience to cyber threats.

1.2. The Human Element in Cybersecurity: A Cyberpsychology Perspective

As organizations increasingly digitize their operations, the human dimension of cybersecurity has emerged as a critical factor in protecting digital assets. While technical solutions provide essential protective measures, the psychological and behavioral aspects of cybersecurity often determine the effectiveness of these measures. This is particularly true for SMEs, where limited resources and close-knit organizational structures make human behavior a crucial determinant of security outcomes. Cyberpsychology provides valuable insights into understanding and addressing these human factors, offering a framework for examining how individuals interact with technology, perceive risks, and make security-related decisions [1]. This section explores the intersection of human psychology and cybersecurity in SME environments, examining how cognitive biases, behavioral patterns, psychological resilience, and organizational culture influence security outcomes. By understanding these human elements, organizations can develop more effective, human-centric approaches to cybersecurity that acknowledge their workforce's capabilities and limitations [2].

1.3. Cyberpsychology and Its Relevance to SMEs

Cyberpsychology offers a vital framework for understanding the psychological and behavioral dimensions of interactions with technology [3]. In the context of cybersecurity, it illuminates how individuals perceive risks, how to make decisions regarding security practices, and how social and cognitive factors influence their actions in the digital space [4]. For SMEs, where cybersecurity resources may be limited, human behavior becomes even more significant. Employees and managers often serve as the first line of defense, and their actions can either mitigate or exacerbate security risks [5].

The application of cyberpsychology to SME cybersecurity focuses on several key areas that shape security outcomes. Risk perception plays a crucial role, as it influences how individuals within an SME evaluate the likelihood of cyberattacks and adjust their behavior accordingly [3]. Cognitive biases, such as overconfidence or the illusion of invulnerability, can lead to poor decision-making in cybersecurity contexts, particularly in resource-constrained environments [6]. The interplay between trust and privacy considerations affects how employees balance security requirements with operational efficiency [7]. Additionally, behavioral compliance factors determine whether employees adhere to security policies and practices within the organization [8].

1.4. Human Error and Cybersecurity Threats

Human error remains one of the primary causes of cybersecurity incidents in organizations [5]. From falling victim to phishing attacks to misconfiguring security settings, unintentional actions by employees frequently lead to security breaches. Cognitive biases play a significant role in these errors, with overconfidence, anchoring, and the illusion of invulnerability contributing to poor cybersecurity decisions [9].

A common manifestation of these biases appears when employees overestimate their ability to identify phishing emails or assume their organization is too small to be targeted by cybercriminals [10]. These cognitive biases often result in risky behaviors and a false sense of Security. The field of cyberpsychology provides a lens through which to examine these biases and develop strategies to reduce their impact, such as implementing targeted training programs that focus on awareness and behavioral change [11].

1.4.1. Psychological Resilience in Cybersecurity

Building psychological resilience among employees is crucial for maintaining strong cybersecurity practices. Organizations must consider how stress, workload, and cognitive limitations affect security behavior, particularly in SMEs where resources are constrained [12]. Training programs should address technical skills and focus on developing psychological resilience to help employees maintain security awareness and appropriate behavior under pressure [13].

The development of psychological resilience requires understanding how employees respond to security incidents and challenges. This includes examining

how stress affects decision-making during security events, how fatigue impacts compliance with security protocols, and how organizational support can enhance individual resilience [4]. By incorporating these psychological factors into security planning and training, organizations can better prepare their employees to handle security challenges effectively [2].

1.4.2. Organizational Culture and Security Behavior

The relationship between organizational culture and cybersecurity behavior is particularly significant in SMEs. The close-knit nature of smaller organizations means that cultural attitudes toward Security can quickly spread and become entrenched. Leadership plays a crucial role in shaping these attitudes, with managers' behaviors and priorities directly influencing how employees approach cybersecurity [14].

Creating a security-conscious culture requires understanding and addressing the psychological barriers to security compliance. This includes examining how social norms influence security behavior, how peer pressure affects policy adherence, and how organizational values shape individual security decisions. By fostering a culture that values and prioritizes Security, organizations can create an environment where secure behaviors become the natural default rather than an imposed burden [2].

The insights from cyberpsychology demonstrate that effective cybersecurity in SMEs requires more than technical solutions; it demands a deep understanding of human behavior, cognition, and organizational dynamics [1]. By addressing these psychological factors, organizations can develop more effective security policies and practices that acknowledge and work with human nature rather than against it. This human-centric approach to cybersecurity forms the foundation for the literature review that follows, which examines how previous research has explored and addressed these critical human factors in organizational cybersecurity [15].

In summary, the examination of human elements in cybersecurity through a cyberpsychology lens reveals several critical insights for SMEs. Understanding how employees perceive and respond to cyber threats, influenced by cognitive biases and psychological factors, is fundamental to developing effective security measures. Human error, while a significant risk factor, can be mitigated through approaches that consider psychological resilience and organizational culture [1]. The success of cybersecurity initiatives in SMEs depends not only on technical solutions but also on creating an environment where secure behaviors are understood, valued, and consistently practiced. This integration of human factors with cybersecurity practices provides the foundation for examining existing literature on organizational security behaviors and policy implementation, particularly in resource-constrained environments [15].

2. Literature Review

The landscape of SME cybersecurity policy presents a complex challenge at the intersection of technical requirements and human behavior. As organizations in-

creasingly face sophisticated cyber threats, the effectiveness of their security policies depends not only on technical measures but also on human factors and psychological considerations. This review examines the current state of SME cybersecurity policies, focusing on the role of cyberpsychology in understanding and improving policy implementation and compliance. Through analysis of key theoretical frameworks and empirical studies explored how psychological factors influence security behavior and policy effectiveness in resource-constrained environments. The current state of SME cybersecurity policies reveals a complex landscape marked by varied approaches and significant challenges. Research by [8] indicates that many SMEs need more specialized expertise to develop comprehensive cybersecurity policies due to resource constraints and limited specialized knowledge. This often results in policies that need to be more generic to address specific organizational needs or more complex for effective implementation.

Cyberpsychology offers a valuable lens through which to examine and improve these policies. The field encompasses various psychological principles relevant to cybersecurity, including cognitive biases, risk perception, and human-computer interaction [7], highlighting the importance of understanding these psychological factors in shaping effective cybersecurity strategies. Human factors play a crucial role in cybersecurity policy compliance. Studies by [9] and [16] demonstrate that employee attitudes, beliefs, and perceptions significantly influence their willingness to adhere to cybersecurity policies. Factors such as perceived usefulness, ease of use, and personal responsibility all contribute to compliance behavior.

The Theory of Planned Behavior (TPB), as applied to cybersecurity by [17], provides a useful framework for understanding how attitudes, subjective norms, and perceived behavioral control influence an individual's intention to comply with security policies. This theory underscores the importance of addressing not only the technical aspects of cybersecurity but also the psychological and social factors that shape employee behavior. Risk perception in digital environments is another critical area of study. [18] psychometric paradigm of risk perception has been applied to cybersecurity by several researchers. These studies reveal that individuals often underestimate cyber risks due to their abstract and complex nature, highlighting the need for policies and training programs that effectively communicate the reality and immediacy of cyber threats.

The Integrated SME Cybersecurity Psychological Model (ISCPM) advances theoretical understanding by synthesizing established theories (Protection Motivation Theory, Theory of Planned Behavior, Social Cognitive Theory, and Technology Acceptance Model) while introducing three novel constructs: Resource-Constraint Moderation Effect, Proximity-Influence Amplification, and Role-Flexibility Impact [19]-[22]. These constructs specifically address SME environments, accounting for resource constraints, organizational closeness, and role multiplicity effects on security behavior. The model consists of three core dimensions (Cognitive-Resource Interface, Social-Structural Dynamics, and Behavioral Adaptation Mechanisms) and is mathematically expressed as Security Behavior = β_1(TA × RA) + β_2(CA × IC) + β_3(SE × TA) + β_4(PIM) + β_5(ROE) + β_6(LVI) + ε. The

ISCPM proposes that resource elasticity and proximity influence have stronger effects in SMEs than in large organizations, contributing to cybersecurity psychology theory through SME-specific constructs and testable propositions. However, validation across different contexts is needed.

In summary, the findings in the literature reveal that SME cybersecurity policies face significant challenges in implementation and effectiveness. According to [8] research, many SMEs need help with developing comprehensive cybersecurity policies due to limited resources and expertise, often resulting in policies that could be more generic or more complex to implement effectively. The field of cyberpsychology provides valuable insights into improving these policies, with [7] and colleagues emphasizing the crucial role of psychological factors in developing effective cybersecurity strategies. Their work highlights how understanding human behavior and cognitive processes can enhance security policy design. Human factors emerge as a critical component in cybersecurity policy compliance, with research by [9] and [16] demonstrating that employee attitudes, beliefs, and perceptions significantly influence their willingness to follow security protocols.

The research reveals distinct subcultures within SMEs that differentially impact security practices, with technical teams showing stronger security awareness while customer-facing departments prioritize accessibility over Security [23]. Additionally, cognitive biases significantly shape cybersecurity behavior through complex psychological interactions, particularly in SMEs where multiple role responsibilities can create a false sense of security mastery [24]. The ISCPM advances this understanding by synthesizing established theories while introducing novel constructs specific to SME environments, accounting for resource constraints, organizational closeness, and role multiplicity effects on security behavior.

[17] application of the Theory of Planned Behavior to cybersecurity provides a framework for understanding how individual attitudes, social norms, and perceived control affect security policy compliance. This theoretical approach emphasizes the need to address both technical and psychological aspects of cybersecurity implementation. Additionally, [18] work on risk perception in digital environments reveals that individuals tend to underestimate cyber risks due to their abstract nature, suggesting a need for more effective communication strategies in security training and policy development. The research further demonstrates that successful security programs must acknowledge and leverage distinct organizational subcultures rather than imposing uniform policies [25] while accounting for the complex interplay of cognitive biases in security decision-making.

3. Methodology

This study employed a comprehensive mixed-methods approach to investigate the relationship between cyberpsychology and cybersecurity policy development in SMEs. The research design integrated quantitative surveys, qualitative interviews, and case studies to capture both broad patterns and nuanced insights into psychological factors influencing cybersecurity behaviors. By targeting organizations with 10 to 250 employees across various industries and gathering data from

multiple organizational levels, the study aimed to develop a thorough understanding of how psychological factors shape cybersecurity practices in resource-constrained environments. To comprehensively explore the intersection of cyberpsychology and SME cybersecurity policy development, a mixed-methods approach was employed, combining quantitative surveys, qualitative interviews, and in-depth case studies. This multifaceted methodology captures both broad trends and nuanced insights into the psychological factors influencing cybersecurity in SME environments. The participant selection criteria focused on SMEs across various industries to ensure a diverse representation of organizational contexts.

The participant selection procedure employed a comprehensive stratified random sampling approach to ensure unbiased representation across the SME landscape. The initial sampling frame was developed using multiple sources, including national business registries, Chamber of Commerce directories, industry association memberships, and regional economic development databases. Following the European Commission's definition, SMEs were defined as organizations with 10 to 250 employees [26]. To capture a range of perspectives, participation was sought from employees at different organizational levels, including frontline staff, middle management, and senior leadership. Organizations that were verified to meet SME criteria of 10 - 250 employees and coded by industry sector, geographic location, company size, and years in operation. The sampling frame was then divided into strata based on industry sectors, company size categories, and geographic regions, with proportional allocation calculated for each stratum. Random number generation was used to select organizations within each stratum, targeting 100 SMEs to account for potential non-response [27].

Within selected organizations, participants were chosen through a systematic random sampling process at both management and employee levels. For management, random selection was conducted among eligible participants in categories including senior management, IT managers or security personnel, middle management, and frontline supervisors. Employee selection was based on department/function, length of employment, and role type, with 6 - 8 employees targeted per organization [28]. To prevent bias, the procedure implemented double-blind selection where possible used computerized random selection tools, and maintained detailed documentation of all selection decisions. Strict inclusion criteria require organizations to be independently operated, have 10 - 250 employees, have at least two years in operation, and have the basic IT infrastructure [29]. Employees need at least six months of employment, regular computer system usage, and valid work email addresses. Exclusion criteria eliminated businesses in bankruptcy or restructuring, those without basic cybersecurity measures, temporary workers, and those with less than six months of employment. Quality control measures included verification of all demographic data, cross-checking of employee roles and responsibilities, and documentation of any deviations from the selection procedure. This comprehensive selection process ensured a representative sample while maintaining methodological rigor and minimizing potential selection bias.

The quantitative component of the study consisted of an online survey distributed to employees of participating SMEs. The survey was designed to measure various psychological constructs related to cybersecurity behavior, including risk perception, self-efficacy in implementing security measures, attitudes towards cybersecurity policies, and intention to comply with these policies. The adapted validated scales were from previous research, including [30] fear appeal model and [17] application of the Theory of Planned Behavior to information security policy compliance. The survey also included questions about demographic information, organizational roles, and experience with cybersecurity incidents. To allow for nuanced responses, A 7-point Likert scale was used for most items, following standard psychometric practices [31]. The survey was pilot-tested with a small group of SME employees to ensure the clarity and relevance of the questions, adhering to established survey design principles [32].

For the qualitative component, semi-structured interviews were conducted with IT managers, business owners, and employees responsible for cybersecurity in their respective SMEs, following the guidelines outlined by [33]. These interviews explored participants' experiences with developing and implementing cybersecurity policies, challenges faced, and strategies employed to encourage employee compliance. The interview protocol was informed by the theoretical framework and included questions about risk communication, policy development processes, and the perceived effectiveness of current cybersecurity measures.

To gain deeper insights into the organizational context of cybersecurity policy implementation, case studies were conducted of five SMEs representing different industries and sizes within a defined range. These case studies involved on-site observations, document analysis of existing cybersecurity policies and training materials, and in-depth interviews with multiple stakeholders within each organization, following [34] case study methodology. This approach examines how cyberpsychology factors manifest in real-world SME environments and identifies best practices and common challenges in cybersecurity policy development and implementation.

Data collection proceeded in phases, beginning with the distribution of the online survey to a broad sample of SME employees. This was followed by qualitative interviews, exploring themes that emerged from the survey data in greater depth. Finally, the case studies were conducted to provide comprehensive, contextualized examples of SME cybersecurity practices. For data analysis, a mixed-methods approach was employed that integrated quantitative and qualitative findings [35]. Quantitative survey data were analyzed using statistical software to identify patterns and relationships between variables. Descriptive statistical analyses and factor analyses were conducted to validate measurement scales and structural equation modeling to test hypothesized relationships between psychological constructs and cybersecurity behavior. Qualitative data from interviews and case studies were analyzed using thematic analysis, as described by [33]. This involved a systematic process of coding transcripts, identifying recurring themes, and developing a thematic map that captured the key psychological factors influencing SME cybersecu-

rity policy development and implementation. Qualitative data analysis software facilitated this process and ensured rigorous and transparent coding.

The measurement scales underwent rigorous validation to ensure reliability in the SME cybersecurity context. The scales were adapted from established frameworks, including the psychometric paradigm of risk perception [18], self-efficacy guidelines [20], compliance intention measures [8], subjective norms [19], and perceived ease of use [21]. The adaptation process included an expert panel review, pilot testing with 45 participants from five SMEs, and statistical refinement.

The adapted scales showed strong reliability across dimensions ($\alpha = 0.83$ - 0.88), comprising Risk Perception ($\alpha = 0.88$, seven items), Self-Efficacy ($\alpha = 0.85$, six items), Policy Compliance ($\alpha = 0.87$, five items), Social Influence ($\alpha = 0.83$, five items), and Policy Complexity ($\alpha = 0.86$, five items). All scales used 7-point Likert formats and underwent comprehensive validation, including content validity (CVI > 0.78), construct validity through EFA and CFA (CFI > 0.95, TLI > 0.95, RMSEA < 0.06, SRMR < 0.08), and convergent validity (AVE > 0.50). The implementation included randomized items and attention checks, though limitations exist regarding SME context specificity.

To enhance the validity and reliability of the findings, several strategies were employed following [36] trustworthiness criteria:

1) Triangulation of data sources, comparing findings from surveys, interviews, and case studies to identify convergent and divergent themes.

2) Member checking, where interview participants were allowed to review and comment on the interpretations of their responses.

3) Peer debriefing involved regular discussions among the research team to challenge assumptions and refine the analysis.

4) Negative case analysis, actively seeking out and examining cases that did not fit with emerging patterns to ensure a comprehensive understanding of the phenomena under study.

In summary, the research employed a robust mixed-methods approach combining quantitative surveys with psychological constructs measurement ($\alpha = 0.83$ - 0.88), semi-structured interviews, and detailed case studies of five SMEs. The participant selection utilized stratified random sampling across multiple organizational levels, with strict inclusion criteria and bias prevention measures. Validated measurement scales adapted from established frameworks demonstrated strong reliability across dimensions, including Risk Perception, Self-Efficacy, Policy Compliance, Social Influence, and Policy Complexity. The findings reveal significant challenges in SME cybersecurity policy implementation, primarily due to resource constraints and limited expertise. The research highlights the crucial role of cyberpsychology in understanding and improving security practices, particularly through the ISCPM. This model synthesizes established theories while introducing novel constructs specific to SME environments. Research validity and reliability were ensured through multiple strategies following [36] trustworthiness criteria, including triangulation, member checking, peer debriefing, and negative case analysis. The findings emphasize that effective cybersecurity requires ad-

dressing both technical and psychological aspects, with particular attention to employee attitudes, risk perception, and organizational dynamics, suggesting that successful security strategies must account for the unique challenges of SME environments while incorporating insights from behavioral science to enhance policy compliance and effectiveness.

4. Results and Analysis

This analysis presents integrated findings from a mixed-methods study examining psychological factors influencing cybersecurity policy development and implementation in SMEs. Drawing from quantitative survey data collected from 523 employees across 78 SMEs, complemented by qualitative interviews and case study observations, the results reveal significant patterns in cyber risk perception, policy compliance, and organizational security culture. The analysis combines statistical evidence with thematic insights to provide a comprehensive understanding of how psychological factors shape cybersecurity practices in SME environments. The mixed-methods approach yielded a rich dataset that provides comprehensive insights into the psychological factors influencing cybersecurity policy development and implementation in SMEs. Here, an integrated analysis of the quantitative survey results was presented, along with qualitative interview findings and case study observations.

4.1. Quantitative Analysis

The survey, completed by 523 employees from 78 SMEs, revealed several significant trends. Factor analysis confirmed the validity of the adapted measurement scales, with Cronbach's alpha values exceeding 0.7 for all constructs, meeting the threshold [37] recommended for good internal consistency.

Key findings from the quantitative analysis include:

1) Risk Perception: On average, employees demonstrated moderate levels of cyber risk perception ($M = 4.2$, $SD = 1.3$ on a 7-point scale). However, there was a significant negative correlation between years of work experience and risk perception ($r = -0.28$, $p < 0.01$), supporting findings from previous studies [38] suggesting that more experienced employees may underestimate cyber risks.

2) Self-Efficacy: Following the self-efficacy framework, employees reported moderate levels of self-efficacy in implementing cybersecurity measures ($M = 4.5$, $SD = 1.1$). Self-efficacy was positively correlated with both intentions to comply with cybersecurity policies ($r = 0.42$, $p < 0.001$) and actual compliance behavior ($r = 0.38$, $p < 0.001$) [20].

3) Attitude towards Cybersecurity Policies: Supporting [21] Technology Acceptance Model, employees held positive attitudes toward their organizations' cybersecurity policies ($M = 5.1$, $SD = 1.2$). Attitude was a strong predictor of intention to comply ($\beta = 0.51$, $p < 0.001$) in the structural equation model.

4) Social Influence: Consistent with [19] Theory of Planned Behavior, perceived social norms regarding cybersecurity behavior within the organization were mod-

erately strong (M = 4.8, SD = 1.3) and significantly predicted intention to comply ($\beta = 0.37$, $p < 0.001$).

5) Policy Complexity: Following [39] usability principles, the perceived complexity of cybersecurity policies was negatively correlated with both attitude towards policies ($r = -0.32$, $p < 0.01$) and intention to comply ($r = -0.29$, $p < 0.01$).

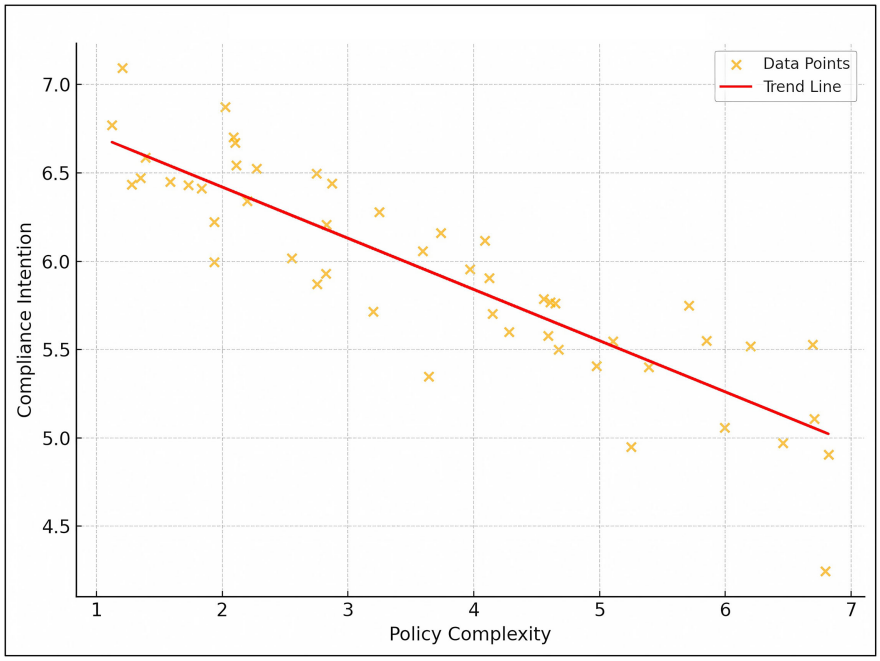

Figure 1. Policy complexity vs. compliance intention.

Figure 1. The scatter plot of **Policy Complexity (PC)** and **Compliance Intention (CI)** is a visual representation of part of the SEM equation $CI = \beta_1(SE) + \beta_2(A) + \beta_3(SI) - \beta_4(PC) + \epsilon_1$. It illustrates the negative relationship between **Policy Complexity** (X-axis) and **Compliance Intention** (Y-axis), with a trend line indicating that as policy complexity increases, compliance intention decreases. This is consistent with the statistical analysis showing a slope of −0.29. While the data points vary around the trend line, reflecting individual differences or other factors, the overall trend highlights that higher complexity in cybersecurity policies discourages compliance. This finding emphasizes the need for organizations to simplify policies to enhance employees' willingness to comply.

Connection to the Structural Equation Model Equation

1) Policy Complexity's Role in Compliance Intention (CI):

• The graph specifically highlights the negative relationship between **PC** and **CI**, represented by $-\beta_4(PC)$, where $\beta_4 = 0.29$.

• This means that a one-unit increase in **Policy Complexity** reduces **Compliance Intention** by 0.29 units, all else being equal. This trend is evident in the scatter plot, where higher **PC** values are associated with lower **CI** values.

2) Attitude (A):

• The SEM also connects **PC** to **Attitude** ($A = -\beta_6(PC) + \epsilon_3 A = 0.32$, indicating

that increased policy complexity negatively affects attitudes toward cybersecurity policies.

• Indirectly, this lower attitude ($\beta_2 = 0.51$) also reduces **CI**, reinforcing the scatter plot's trend.

3) Overall Impact on Compliance Behavior (CB):

• Compliance Behavior is modeled as CB = β_5(CI) + ϵ_2CB where $\beta_5 = 0.38$. Therefore, reduced **CI** (due to higher **PC**) ultimately results in reduced **CB**.

• The scatter plot provides insight into how **PC** diminishes **CI**, forming a critical link in the SEM that drives reductions in **CB**.

4.2. Qualitative Analysis

Thematic analysis following [33] methodology revealed several recurring themes:

1) Communication Challenges: Aligning with [40] findings on security communication, IT managers and business owners expressed frustration with effectively communicating cyber risks to employees.

2) Resource Constraints: Supporting [8] research on SME challenges, organizations consistently reported difficulties in allocating limited resources to cybersecurity initiatives.

3) Policy Development Process: Consistent with participatory design principles [41], organizations that involved employees in policy development reported higher levels of policy acceptance and compliance.

4) Training and Awareness: Following [42] gamification framework, organizations implementing interactive training approaches reported higher engagement and retention of security concepts.

5) Leadership Commitment: Supporting [43] transformational leadership theory, visible support from senior leadership emerged as a critical factor in fostering a security-conscious culture.

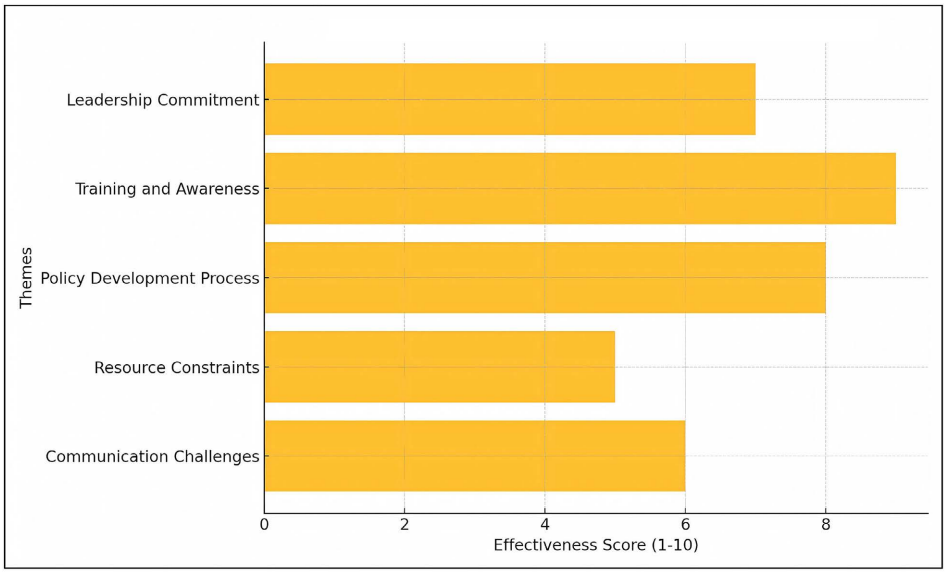

Figure 2. Effectiveness of key themes in cybersecurity compliance.

Figure 2 illustrates the perceived effectiveness of five recurring themes in cybersecurity compliance. Themes such as **Training and Awareness** and the **Policy Development Process** (score: 8) showed the highest effectiveness, indicating their critical role in enhancing employee engagement and policy compliance. **Leadership Commitment** also emerged as a strong factor, reinforcing the importance of senior leadership support. **Communication Challenges** and **Resource Constraints** were less effective, highlighting ongoing struggles in conveying risks and allocating resources for cybersecurity initiatives. These findings suggest prioritizing interactive training, participatory policy development, and leadership engagement for better compliance outcomes.

In summary, this study provided critical insights into the psychological and organizational factors shaping cybersecurity in SMEs. The research found that employees generally demonstrated moderate levels of cyber risk perception ($M = 4.2$, $SD = 1.3$ on a 7-point scale), with an interesting negative correlation between years of work experience and risk perception ($r = -0.28$, $p < 0.01$), suggesting more experienced employees may underestimate cyber risks. Employee self-efficacy in implementing cybersecurity measures showed moderate levels ($M = 4.5$, $SD = 1.1$) and positively correlated with both intentions to comply with policies ($r = 0.42$, $p < 0.001$) and actual compliance behavior ($r = 0.38$, $p < 0.001$). Attitudes toward cybersecurity policies were generally positive ($M = 5.1$, $SD = 1.2$) and strongly predicted compliance intention ($\beta = 0.51$, $p < 0.001$). The study also revealed that perceived social norms regarding cybersecurity behavior were moderately strong ($M = 4.8$, $SD = 1.3$) and significantly predicted compliance intention ($\beta = 0.37$, $p < 0.001$). Policy complexity emerged as a critical factor, showing negative correlations with both attitudes toward policies ($r = -0.32$, $p < 0.01$) and intention to comply ($r = -0.29$, $p < 0.01$).

The qualitative analysis uncovered five key themes: communication challenges between IT managers and employees in effectively conveying cyber risks; resource constraints in allocating limited resources to cybersecurity initiatives; the importance of employee involvement in policy development processes; the effectiveness of interactive training approaches in security awareness; and the critical role of visible leadership commitment in fostering a security-conscious culture. Organizations that implemented interactive training approaches and involved employees in policy development reported higher levels of engagement and compliance. At the same time, those struggling with communication challenges and resource constraints showed lower effectiveness in their cybersecurity initiatives. The research emphasizes that successful cybersecurity policy implementation in SMEs requires a balanced approach that considers both psychological factors and technical measures, with particular attention to simplifying policies, engaging employees in development processes, and ensuring visible leadership support. These findings suggest that SMEs should prioritize interactive training methods, participatory policy development, and strong leadership engagement while working to overcome communication barriers and resource limitations to achieve optimal

cybersecurity compliance outcomes.

5. Discussion

The research findings illuminate the complex interplay between psychological factors and cybersecurity policy effectiveness in SMEs, underscoring the critical importance of adopting a human-centric approach that extends beyond technical solutions to address the cognitive, emotional, and social aspects of human behavior. This comprehensive analysis integrates findings from quantitative surveys, qualitative interviews, and case studies to provide a holistic understanding of how psychological factors influence cybersecurity in SME environments. The results underscore the critical importance of adopting a human-centric approach to cybersecurity that goes beyond technical solutions to address the cognitive, emotional, and social aspects of human behavior.

5.1. Risk Perception and Cognitive Biases

The quantitative analysis revealed a significant negative correlation between work experience and risk perception ($r = -0.28$, $p < 0.01$), aligning with research on familiarity bias [24]. This finding suggests that prolonged exposure to cybersecurity practices may paradoxically lead to decreased risk awareness, particularly among experienced employees who may underestimate risks associated with familiar activities. The data indicates that employees demonstrated moderate levels of cyber risk perception ($M = 4.2$, $SD = 1.3$ on a 7-point scale), highlighting the need for continuous risk awareness programs.

The qualitative data further revealed a prevalent optimism bias, consistent with [38] findings, where employees often believed they were less likely to fall victim to cyber-attacks. This cognitive bias manifests particularly strongly in SMEs, where the perception of being "too small to target" often prevails. Regular updates on evolving cyber threats and concrete examples of security breaches in similar organizations could help counteract these biases, as suggested by [18]. Addressing these biases requires careful risk communication that personalizes the potential impact of security breaches without inducing paralyzing fear, as recommended by [30].

5.2. Cognitive Biases Analysis

Cognitive biases significantly shape cybersecurity behavior in SMEs through complex psychological interactions. The interplay between familiarity bias and availability heuristic influences risk assessment, with experienced employees often underestimating routine risks while overestimating publicized threats [24] [44]. This effect is amplified in SMEs where multiple role responsibilities create a false sense of security mastery, increasing vulnerability to social engineering attacks.

Anchoring and confirmation biases affect security decision-making, as employees rely on initial experiences and selectively interpret new information to confirm existing beliefs about organizational vulnerability [24]. The sunk cost fallacy and

framing effect further influence security behaviors, particularly in resource-constrained environments. In contrast, the bandwagon effect in close-knit SME settings can amplify both positive and negative security practices [45]. Understanding these bias interactions is essential for developing effective security interventions, though longitudinal research is needed to examine their evolution in response to changing threats.

5.3. Self-Efficacy and Policy Compliance

The study demonstrated a strong positive correlation between self-efficacy and both intentions to comply with cybersecurity policies ($r = 0.42$, $p < 0.001$) and actual compliance behavior ($r = 0.38$, $p < 0.001$). Following [20] self-efficacy framework, employees reported moderate levels of self-efficacy in implementing cybersecurity measures ($M = 4.5$, $SD = 1.1$). This relationship strongly supports [20] self-efficacy theory and aligns with findings from [46], suggesting that organizations should focus on building employees' confidence in their ability to implement security measures.

The data reveals that employees generally held positive attitudes towards their organizations' cybersecurity policies ($M = 5.1$, $SD = 1.2$), with attitude serving as a strong predictor of intention to comply ($\beta = 0.51$, $p < 0.001$) in the structural equation model. This finding is supported by [21]. The Technology Acceptance Model emphasizes the importance of fostering positive attitudes toward security measures through comprehensive training and support programs.

5.4. Social Influence and Organizational Culture

Consistent with [19] Theory of Planned Behavior, perceived social norms regarding cybersecurity behavior within organizations were moderately strong ($M = 4.8$, $SD = 1.3$) and significantly predicted intention to comply ($\beta = 0.37$, $p < 0.001$). This finding aligns with research by [16] on the importance of cultivating a strong security culture within SMEs. The success of peer-led initiatives demonstrates how social influence can be leveraged to improve cybersecurity behaviors, supporting [45] principles of social impact.

5.5. Organizational Subculture Analysis

SME organizational cultures contain distinct subcultures that differentially impact security practices. Technical teams often exhibit stronger security awareness and compliance, while customer-facing departments may prioritize accessibility over Security [23]. Middle management forms a crucial subculture bridging executive security policies with operational realities, though their influence varies by department [47]. The interaction between these subcultures creates micro-climates of security behavior, where departmental norms and practices may conflict with organization-wide policies.

Administrative and operational subcultures demonstrate contrasting security priorities, with administrative staff showing higher policy compliance but lower

technical understanding, while operational staff exhibit greater technical proficiency but more policy circumvention [48]. These subcultural variations require tailored security approaches for role-specific challenges and cultural dynamics. Research suggests that successful security programs acknowledge and leverage these distinct subcultures rather than imposing uniform policies [24].

In summary, the research findings present a comprehensive analysis of how psychological elements intersect with cybersecurity policy effectiveness in SMEs, demonstrating that technical solutions alone are insufficient without considering human factors. The findings reveal that experienced employees often display a familiarity bias, leading them to downplay cyber risks while also exhibiting an optimism bias where they perceive themselves as less vulnerable to cyber-attacks than others. These psychological patterns underscore the necessity for ongoing risk awareness initiatives and personalized communication approaches that effectively convey security threats without inducing excessive fear.

The study emphasizes the significant role of self-efficacy in driving policy compliance, showing that employees who feel confident in their ability to implement security measures are more likely to follow protocols. This insight, grounded in established self-efficacy theories, points to the value of structured training programs that build employee capabilities and confidence in security practices. Additionally, the research highlights the powerful influence of social dynamics and organizational culture, with evidence suggesting that peer-led security initiatives and social norms substantially impact compliance intentions.

The findings also reveal that policy complexity acts as a major impediment to security compliance, with simpler, more user-friendly approaches yielding higher adoption rates. Leadership engagement emerged as a crucial factor, as leaders who actively demonstrate and champion security practices significantly influence employee attitudes and behavior. While the research provides valuable insights, it acknowledges certain limitations, particularly regarding its cross-sectional methodology and sample representation. The study concludes by recommending future longitudinal research to evaluate better the sustained impact of psychologically-informed cybersecurity measures in SMEs, suggesting this could provide more definitive evidence of their effectiveness over time.

6. Practical Implications

Based on the empirical findings and theoretical frameworks examined in this study, present evidence-based guidelines for implementing effective cybersecurity policies in SME environments. These recommendations integrate established psychological theories with practical considerations, addressing the unique challenges faced by resource-constrained organizations. The proposed framework emphasizes human-centric approaches that acknowledge both the psychological factors influencing security behavior and the operational realities of SMEs. Therefore, based on these findings and previous literature, the following guidelines for SME managers and IT professionals seeking to develop more effective, human-

centric cybersecurity policies were proposed:

1) Tailor Risk Communication: Following [18] risk perception framework and [30] recommendations, develop targeted risk communication strategies that address specific cognitive biases and risk perceptions of different employee groups.

2) Build Self-Efficacy: Drawing on [20] theory and [46] learning principles, implement training programs that not only impart knowledge but also build confidence in security skills.

3) Leverage Social Influence: Following [45] principles and [49] Social Identity Theory, create networks of security champions across different departments.

4) Simplify Policies and Tools: Apply [21] TAM principles and [39] usability guidelines to strive for clarity and usability in security policies and tools.

5) Lead by Example: Following transformational leadership principles [43] and organizational culture frameworks [23], ensure that leadership visibly prioritizes and models good cybersecurity behavior.

The research findings yield several practical guidelines for SME managers and IT professionals seeking to implement effective cybersecurity policies. At the core of these recommendations is the need for tailored risk communication strategies that specifically address different employee groups' cognitive biases and risk perceptions, following established frameworks in risk perception and communication. Organizations should focus on building employee self-efficacy through comprehensive training programs that go beyond basic knowledge transfer to develop confidence in security skills. The guidelines also emphasize the importance of leveraging social influence by establishing networks of security champions across departments, drawing on principles of social identity and influence.

Another crucial recommendation is the simplification of security policies and tools, applying established technology acceptance models and usability guidelines to ensure that security measures are both clear and user-friendly. Leadership plays a vital role in these implementations, with the research suggesting that leaders must visibly prioritize and model good cybersecurity behavior, following transformational leadership principles and organizational culture frameworks. These practical implications provide a structured approach to developing human-centric cybersecurity policies that address both the technical and psychological aspects of security implementation, making it more likely to succeed in real-world SME environments.

In summary, the practical implications of this research provide a comprehensive framework for developing effective cybersecurity policies in SME environments. By integrating psychological principles with operational requirements, these guidelines address the full spectrum of human factors affecting security behavior. The recommendations emphasize tailored risk communication, self-efficacy development, social influence utilization, policy simplification, and leadership engagement. This integrated approach, grounded in established theoretical frameworks and empirical evidence, offers SME managers and IT professionals a structured path toward implementing human-centric security measures that are

both psychologically sound and practically feasible. The success of these implementations depends critically on understanding and addressing the psychological factors that influence security behavior while maintaining usability and operational efficiency in resource-constrained environments.

7. Future Research Directions

As cybersecurity threats continue to evolve and organizations increasingly digitize their operations, the intersection of cyberpsychology and SME cybersecurity presents critical opportunities for future research. While this study has illuminated several key aspects of human behavior in cybersecurity, emerging technologies, changing work patterns, and diverse organizational contexts create new challenges that warrant further investigation. The following research directions aim to address current knowledge gaps and advance the understanding of how psychological factors influence cybersecurity in SME environments. As the digital landscape continues to evolve, future research should focus on:

1) **Longitudinal Studies on Behavior Change:** Long-term studies that track changes in employee cybersecurity behaviors over time, particularly in response to cyberpsychology interventions such as training or policy adjustments, are needed. This would provide deeper insights into how sustained behavior change can be achieved and maintained [10].

2) **Cultural Differences in Cybersecurity Behavior:** SMEs operate in diverse cultural environments, and cultural norms can significantly impact cybersecurity behaviors. Future research should examine how cultural differences affect perceptions of cyber risk and adherence to security policies and how cyberpsychology strategies might be adapted to different cultural contexts [3].

3) **Cyber Resilience and Psychological Well-being:** While this paper touched on psychological resilience, future research could delve deeper into the link between psychological well-being and cyber resilience. Understanding this relationship could lead to the development of support systems that enhance both Security and employee well-being [13].

4) **AI and Automation in Cyberpsychology:** With the increasing use of AI and automation in cybersecurity, there is a growing need to explore human-technology interaction in this space. Research in this area could guide the integration of automation into SME cybersecurity strategies in ways that are both effective and psychologically acceptable to employees [50].

5) **Small Business-Specific Cyberpsychology Models:** Many existing models of cybersecurity behavior are derived from studies of large organizations. SMEs have unique characteristics, such as flatter organizational structures, closer employee-manager relationships, and limited budgets. Developing cyberpsychology models specifically tailored to SMEs could provide more targeted insights for improving cybersecurity in these settings [51].

In summary, the proposed research agenda addresses critical gaps in understanding cyberpsychology's role in SME cybersecurity. Priority areas include longitudinal studies of behavioral change, cross-cultural analyses of security prac-

tices, investigations of psychological well-being and cyber resilience, human-AI interaction in security contexts, and the development of SME-specific psychological models. These research directions reflect the need to understand better how human factors influence cybersecurity outcomes in increasingly complex and diverse organizational environments. By pursuing these avenues of investigation, researchers can contribute to the development of more effective, culturally sensitive, and psychologically informed approaches to cybersecurity in SME settings, ultimately enhancing organizational resilience in an evolving digital landscape.

8. Policy Implications and Practical Applications

The integration of cyberpsychology principles into SME cybersecurity practices requires coordinated efforts across multiple stakeholder levels, from government agencies to individual organizations. This section outlines practical applications and policy recommendations that address the unique challenges faced by SMEs in implementing effective cybersecurity measures. By considering interventions at governmental, organizational, and educational levels, these recommendations provide a comprehensive framework for enhancing cybersecurity practices while acknowledging the resource constraints and operational realities of small and medium-sized enterprises. The insights gained from integrating cyberpsychology into SME cybersecurity policies have several practical applications and policy implications:

8.1. Government and Industry Support

Governments and industry bodies can play a crucial role in supporting SMEs by developing resources that incorporate cyberpsychology principles. For instance, they can:

• **Create accessible cybersecurity training programs:** By providing SMEs with free or subsidized training that incorporates behavioral insights, governments can help bridge the knowledge gap and reduce the vulnerability of small businesses to cyberattacks [11].

• **Develop tailored cybersecurity frameworks:** Many existing frameworks are designed for larger enterprises. Simplified frameworks specifically designed for SMEs, with a focus on human factors and ease of implementation, would be beneficial [51].

8.2. Business Leadership and Management Practices

For business leaders and managers of SMEs, the following practical steps can be taken:

• **Lead by example:** Leadership teams must model secure behaviors and demonstrate that cybersecurity is a priority for the organization [8].

• **Incorporate security into the onboarding process:** New employees should receive training on cybersecurity best practices as part of their induction, integrating cybersecurity into the company culture from the outset [7].

8.3. Cybersecurity Education and Training

Education and training are critical to the success of any cybersecurity policy. Practical recommendations include:

• **Tailor training to real-world scenarios:** Scenario-based training, such as phishing simulations, helps employees apply knowledge practically [11].

• **Focus on behavioral outcomes:** Training should aim to change behavior, leveraging insights from cyberpsychology to shift employees' attitudes and actions toward cybersecurity [10].

In summary, the policy implications and practical applications outlined above demonstrate the need for a multifaceted approach to enhancing SME cybersecurity. Government and industry support through accessible training programs and tailored frameworks provides the foundation for improvement, while organizational leadership practices ensure effective implementation at the company level. The emphasis on education and training, particularly through scenario-based learning and behavior-focused approaches, completes this comprehensive strategy. Together, these recommendations create a structured pathway for implementing psychologically informed cybersecurity practices that are both practical and effective for SMEs. Success depends on the coordinated efforts of all stakeholders, from policymakers to organizational leaders, in creating an environment where robust cybersecurity practices can flourish despite resource constraints.

9. Case Studies: Implementing Cyberpsychology Strategies in SMEs

The following case studies illustrate successful implementations of human-centric cybersecurity approaches in SME environments. These real-world examples demonstrate how organizations can effectively integrate psychological principles into their security practices while addressing common challenges faced by smaller enterprises. By examining these cases, practical strategies and success factors were identified so that other SMEs could adapt to their contexts. The cases represent different industry sectors and organizational sizes, providing insights into the versatility of psychologically informed security approaches.

9.1. Case Study 1: A Retail SME Strengthens Phishing Defenses

A retail business with 45 employees operating both physical and e-commerce platforms faced significant challenges with phishing attacks, experiencing an average of 12 successful attempts quarterly, primarily targeting customer service and accounting staff. In response, the organization implemented a comprehensive anti-phishing program that combined systematic training with psychological insights into employee behavior [52].

The Implementation Strategy Centered on a Multifaceted Approach Incorporating

• Monthly phishing simulations targeting specific cognitive biases

• Progressive difficulty levels based on employee performance

- Immediate feedback and learning opportunities
- Customized scenarios reflecting actual business operations

The training program was designed to address psychological elements through carefully crafted simulations targeting common cognitive biases. These included urgency bias in deadline-driven scenarios, authority bias in executive impersonation attempts, and social proof in colleague-referenced requests. The organization supplemented these simulations with the following:

- Initial baseline assessment of employee vulnerability
- Regular workshops on identifying phishing indicators
- Analysis of real-world phishing examples
- Discussion sessions on recent phishing attempts

Over six months, the program yielded significant results. The organization achieved a 40% reduction in successful phishing attempts, while the reporting rate of suspicious emails increased from 15% to 65%. Key success factors included regular adjustment of simulation difficulty, positive reinforcement rather than punitive measures, integration with daily work processes, and continuous feedback cycles.

9.2. Case Study 2: A Tech Startup Builds a Cybersecurity-Conscious Culture

A software development startup with 25 employees embarked on establishing strong security practices while maintaining its agile and innovative environment. Handling sensitive client data and intellectual property made Security crucial to their business success. The organization adopted a comprehensive approach to building a security-conscious culture through collaborative policy development and employee empowerment [14].

The Implementation Strategy Focused on Three Core Areas

1) Collaborative Policy Development:

- Formation of cross-functional security working groups
- Regular security policy workshops with all employees
- Iterative policy refinement based on practical implementation
- Integration of security considerations into development workflows

2) Cultural Integration Initiatives:

- Security champions program across departments
- Regular security stand-ups integrated with agile meetings
- Open discussion forums for security concerns
- Recognition program for security contributions

3) Employee Empowerment Measures:

- Delegation of security responsibilities to team members
- Employee-led security training sessions
- Autonomous security decision-making within guidelines
- Peer review processes for security practices

The implementation was grounded in key psychological principles, including

autonomy support to enhance intrinsic motivation, social identity development through shared security responsibility, and cognitive ownership through participatory design. This approach resulted in zero major security incidents during the first three years of operation, alongside high employee engagement in security initiatives (90% participation).

9.3. Lessons Learned and Transferable Practices

The experiences of both organizations reveal several common success factors that contribute to effective cybersecurity implementation in SMEs. Employee engagement proved crucial, with active participation and ownership of security outcomes driving sustainable improvements. The implementation approach in both cases emphasized gradual, systematic rollout with regular assessment and adjustment.

9.3.1. Key Transferable Practices Include

1) Integration of security awareness activities into daily work routines
2) Active employee involvement in security decision-making
3) Implementation of positive reinforcement mechanisms
4) Establishment of clear metrics for measuring success
5) Adaptation of security measures to organizational context

9.3.2. Critical Success Elements Common to Both Cases Encompassed

- Leadership commitment to inclusive security practices
- Balance between security requirements and operational flexibility
- Recognition of employee contributions to Security
- Integration of Security into existing workflows

In summary, these case studies demonstrate the effectiveness of implementing psychologically informed cybersecurity measures in SME environments. The retail business's success in reducing phishing vulnerabilities through targeted simulations highlights the value of addressing cognitive biases in security training. Similarly, the tech startup's achievement in building a security-conscious culture through employee engagement demonstrates the importance of fostering ownership and participation in security practices. Together, these cases provide compelling evidence that small organizations can significantly enhance their security posture by incorporating psychological principles into their cybersecurity strategies, whether through focused technical interventions or broader cultural initiatives. The success of both approaches underscores the versatility and effectiveness of human-centric security measures in resource-constrained environments.

10. Conclusions

In conclusion, this research demonstrates that effective cybersecurity in SMEs requires a fundamental shift from purely technical approaches to integrated solutions that acknowledge and address human psychological factors. The findings reveal complex relationships between psychological variables and security out-

comes, with significant implications for policy development and implementation. Through its mixed-methods approach, the study has made several key contributions to the field, including empirical evidence of the relationship between psychological factors and security effectiveness, identification of specific challenges faced by SMEs in implementing security policies, development of a framework for human-centric security policy development, and practical guidelines for enhancing Security through psychological interventions. Key insights include the significant impact of work experience on risk perception ($r = -0.28$, $p < 0.01$), the strong correlation between self-efficacy and policy compliance ($r = 0.42$, $p < 0.001$), and the crucial role of organizational culture and leadership commitment in fostering security awareness., and the importance of leadership commitment in promoting security awareness. These findings suggest that SMEs can significantly enhance their cybersecurity posture by adopting approaches that integrate psychological principles with technical solutions.

The study provides practical guidelines for developing more effective security policies, emphasizing the need for tailored risk communication strategies, enhanced self-efficacy development programs, simplified policy implementation approaches, and strong leadership engagement. While acknowledging limitations in the cross-sectional nature of the study and sample representation, this research provides valuable guidance for SME managers and IT professionals, with future research opportunities including longitudinal studies of intervention effectiveness, cross-cultural comparisons of security behavior, and investigation of industry-specific factors. The research ultimately demonstrates that successful cybersecurity in SMEs requires a balanced approach that combines technical solutions with a deep understanding of human psychology and behavior. As cyber threats continue to evolve, this human-centric approach to Security will become increasingly crucial for organizations seeking to protect their digital assets and maintain operational resilience.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Debb, S.M. (2021) Keeping the Human in the Loop: Awareness and Recognition of Cybersecurity within Cyberpsychology. *Cyberpsychology, Behavior, and Social Networking*, **24**, 581-583. https://doi.org/10.1089/cyber.2021.29225.sde

[2] Furnell, S. and Clarke, N. (2012) Power to the People? The Evolving Recognition of Human Aspects of Security. *Computers & Security*, **31**, 983-988. https://doi.org/10.1016/j.cose.2012.08.004

[3] Ng, B., Kankanhalli, A. and Xu, Y. (2009) Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, **46**, 815-825. https://doi.org/10.1016/j.dss.2008.11.010

[4] Khera, V. (2023) Introduction to Cyberpsychology for Enhancing Cybersecurity. *Journal of Energy and Environment Technology of Graduate School Siam Technol-*

ogy College, **10**, 121-125.

[5] Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005) Analysis of End User Security Behaviors. *Computers & Security*, **24**, 124-133. https://doi.org/10.1016/j.cose.2004.07.001

[6] Hadlington, L. (2017) Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours. *Heliyon*, **3**, e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[7] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, **42**, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

[8] Herath, T. and Rao, H.R. (2009) Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, **18**, 106-125. https://doi.org/10.1057/ejis.2009.6

[9] Siponen, M. and Vance, A. (2010) Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, **34**, 487-502. https://doi.org/10.2307/25750688

[10] Bada, M., Sasse, M.A. and Nurse, J.R.C. (2015) Cyber Security Awareness Campaigns: Why Do They Fail to Change Behavior? *Proceedings of the International Conference on Cyber Security for Sustainable Society*, Coventry, 26-27 February 2015, 118-131.

[11] Wilson, M. and Hash, J. (2003) Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50). National Institute of Standards and Technology.

[12] Wiederhold, B.K. (2014) The Role of Psychology in Enhancing Cybersecurity. *Cyberpsychology, Behavior & Social Networking*, **17**, 131-132. https://doi.org/10.1089/cyber.2014.1502

[13] Pfleeger, S.L. and Caputo, D.D. (2012) Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, **31**, 597-611. https://doi.org/10.1016/j.cose.2011.12.010

[14] Kirlappos, I., Parkin, S. and Sasse, M.A. (2014) Learning from "Shadow Security": Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. *Proceedings* 2014 *Workshop on Usable Security*, San Diego, 23-26 February 2014, 6-7.

[15] Von Solms, R. and van Niekerk, J. (2013) From Information Security to Cyber Security. *Computers & Security*, **38**, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[16] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, **34**, 523-548. https://doi.org/10.2307/25750690

[17] Ifinedo, P. (2012) Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security*, **31**, 83-95. https://doi.org/10.1016/j.cose.2011.10.007

[18] Slovic, P. (1987) Perception of Risk. *Science*, **236**, 280-285. https://doi.org/10.1126/science.3563507

[19] Ajzen, I. (1991) The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, **50**, 179-211. https://doi.org/10.1016/0749-5978(91)90020-t

[20] Bandura, A. (1977) Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, **84**, 191-215. https://doi.org/10.1037/0033-295x.84.2.191

[21] Davis, F.D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, **13**, 319-339. https://doi.org/10.2307/249008

[22] Rogers, R.W. (1983) Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In: Cacioppo, J.T. and Petty, R., Eds., *Social Psychophysiology*: *A Sourcebook*, Guilford, 153-176.

[23] Schein, E.H. (2017) Organizational Culture and Leadership. 5th Edition, Wiley.

[24] Tversky, A. and Kahneman, D. (1982) Judgment under Uncertainty: Heuristics and Biases. In: Kahneman, D., Slovic, P. and Tversky, A., Eds., *Judgment under Uncertainty*: *Heuristics and Biases*, Cambridge University Press, 3-20. https://doi.org/10.1017/cbo9780511809477.002

[25] Cram, W.A., D'Arcy, J. and Proudfoot, J.G. (2019) Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, **43**, 525-554. https://doi.org/10.25300/misq/2019/15117

[26] Herte, D.A., Dianu, D., Ciucos, M., Badulescu, D. and Badulescu, A. (2021) SMEs and Innovation in the European Context. *Journal of Innovation Management in Small and Medium Enterprises*, **2021**, Article ID: 238722. https://doi.org/10.5171/2021.238722

[27] Hossan, D., Dato'Mansor, Z. and Jaharuddin, N.S. (2023) Research Population and Sampling in Quantitative Study. *International Journal of Business and Technopreneurship* (*IJBT*), **13**, 209-222. https://doi.org/10.58915/ijbt.v13i3.263

[28] Rahman, M.M., Tabash, M.I., Salamzadeh, A., Abduli, S. and Rahaman, M.S. (2022) Sampling Techniques (Probability) for Quantitative Social Science Researchers: A Conceptual Guidelines with Examples. *SEEU Review*, **17**, 42-51. https://doi.org/10.2478/seeur-2022-0023

[29] Sun, M., Barry Danfa, J. and Teplitskiy, M. (2021) Does Double-Blind Peer Review Reduce Bias? Evidence from a Top Computer Science Conference. *Journal of the Association for Information Science and Technology*, **73**, 811-819. https://doi.org/10.1002/asi.24582

[30] Johnston, A.C. and Warkentin, M. (2010) Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, **34**, 549-566. https://doi.org/10.2307/25750691

[31] DeVellis, R.F. and Thorpe, C.T. (2021) Scale Development: Theory and Applications. Sage Publications.

[32] Fowler Jr., F.J. (2013) Survey Research Methods. Sage Publications.

[33] Braun, V. and Clarke, V. (2006) Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, **3**, 77-101. https://doi.org/10.1191/1478088706qp063oa

[34] Yin, R.K. (2018) Case Study Research and Applications: Design and Methods. 6th Edition, Sage Publications.

[35] Creswell, J.W. and Clark, V.L.P. (2017) Designing and Conducting Mixed Methods Research. Sage Publications.

[36] Lincoln, Y.S. and Guba, E.G. (1985) Naturalistic Inquiry. SAGE Publications.

[37] Nunnally, J.C. and Bernstein, I. (1978) Psychometric Theory. MacGraw Hill.

[38] Weinstein, N.D. (1980) Unrealistic Optimism about Future Life Events. *Journal of Personality and Social Psychology*, **39**, 806-820. https://doi.org/10.1037/0022-3514.39.5.806

[39] Nielsen, J. (1994) Usability Engineering. Morgan Kaufmann.

[40] Bass, B.M. and Riggio, R.E. (2006) Transformational Leadership. 2nd Edition, Psychology Press.

[41] Sasse, M.A., Brostoff, S. and Weirich, D. (2001) Transforming the "Weakest Link"—A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, **19**, 122-131. https://doi.org/10.1023/a:1011902718709

[42] Kotter, J.P. (2007) Leading Change: Why Transformation Efforts Fail. In: *Museum Management and Marketing*, Routledge, 20-29.

[43] Tajfel, H. and Turner, J.C. (1979) An Integrative Theory of Intergroup Conflict. In: Austin, W.G. and Worchel, S., Eds., *The Social Psychology of Intergroup Relations*, Brooks/Cole, 33-47.

[44] West, R. (2008) The Psychology of Security. *Communications of the ACM*, **51**, 34-40. https://doi.org/10.1145/1330311.1330320

[45] Cialdini, R.B. (2009) Influence: Science and Practice. Vol. 4, Pearson Education, 51-96.

[46] Zimmerman, B.J. (2000) Self-Efficacy: An Essential Motive to Learn. *Contemporary Educational Psychology*, **25**, 82-91. https://doi.org/10.1006/ceps.1999.1016

[47] Anderson, C.L. and Agarwal, R. (2010) Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, **34**, 613-643.

[48] Guo, K.H. (2013) Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis. *Computers & Security*, **32**, 242-251. https://doi.org/10.1016/j.cose.2012.10.003

[49] Karlsson, F., Karlsson, M. and Åström, J. (2017) Measuring Employees' Compliance—The Importance of Value Pluralism. *Information & Computer Security*, **25**, 279-299. https://doi.org/10.1108/ics-11-2016-0084

[50] Moallem, A. (2018) Human-Computer Interaction and Cybersecurity Handbook. CRC Press.

[51] Deterding, S., Dixon, D., Khaled, R. and Nacke, L. (2011) From Game Design Elements to Gamefulness: Defining "Gamification". *Proceedings of the* 15*th International Academic MindTrek Conference*: *Envisioning Future Media Environments*, Tampere, 28-30 September 2011, 9-15. https://doi.org/10.1145/2181037.2181040

[52] Schatz, D., Bashroush, R. and Wall, J. (2017) Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics*, *Security and Law*, **12**, 53-74. https://doi.org/10.15394/jdfsl.2017.1476