**Journal of Management and Informatics (JMI)**
**Vol. 4 No. 3 December 2025**
E-ISSN: 2961-7731; P-ISSN: 2961-7472, Pages 981-997
*Publication Link: https://jmi.stekom.ac.id/index.php/jmi/issue/view/12*

# Human Error vs. System Security: Evaluating the Weakest Link in Digital Business Information Systems

Nguyen Thị Mai*[1], Iman Khalid[2]
Email: mai.nguyen@gmail.com
[1]*Vietnam National University, Hanoi, Vietnam*
[2]*Universiti Kuala Lumpur (UniKL), Kuala Lumpur, Malaysia*
*Corresponding Author

**Abstract**

*The perennial question in digital business cybersecurity concerns whether human error or technical system vulnerabilities constitute the greater threat to organizational information systems and thus should receive priority in security investment. This study empirically examines this issue by identifying the weakest link in contemporary digital business environments. The study offers a theoretical contribution by integrating Human Error Theory, Socio-Technical Systems Theory, and the ISO 27001 framework into a unified analytical model for evaluating organizational information security weaknesses. Using an explanatory sequential mixed-methods design, quantitative data were collected from 217 information technology professionals, complemented by 15 in-depth interviews and an analysis of security incident records. The results indicate that human error ($M = 3.82$) is significantly more prevalent than technical system vulnerabilities ($M = 2.94$), as confirmed by a paired t-test ($t(216) = 5.734$, $p < .001$). Structural Equation Modeling further reveals that workload pressure and insufficient practice-based training significantly contribute to human error ($\beta = 0.58$, $p < .001$). Qualitative findings highlight cognitive overload, training gaps, and social engineering as dominant contributing factors. The study demonstrates that human error should not be interpreted merely as individual negligence but as an outcome of more profound organizational and socio-technical weaknesses. These findings support a strategic shift toward human-centered and socio-technical cybersecurity approaches to enhance organizational digital resilience.*

**Keywords**: *Human Error, Digital Business Security, Socio-Technical Approach, Information Security Management Systems, Organizational Cyber Resilience.*
*Received in August 2025; Revised in September 2025; Accepted in October 2025; Published in December 2025.*

## I. INTRODUCTION

The rapid progression of digitalization has transformed contemporary business operations, compelling organizations to integrate advanced information systems into almost every functional domain (Ammirato et al., 2022). While this transformation enhances efficiency and scalability, it also broadens the cyberattack surface, making information security central to organizational sustainability (Saeed et al., 2023). Modern digital business ecosystems, ranging from fintech to e-commerce, represent complex socio-technical environments in which human actors and technical infrastructures are deeply interconnected (Baroni et al., 2021). Within this environment, a fundamental and recurring question persists: what constitutes the weakest link in the security chain? Despite substantial investments in sophisticated technical safeguards such as intrusion detection systems and firewalls (Repetto et al., 2021), growing empirical evidence suggests that the human element continues to represent an unpredictable and potent source of vulnerability

DOI: https://doi.org/10.51903/jmi.v4i3.305

(Amoresano & Yankson, 2023). Accordingly, the central challenge of cybersecurity today is no longer merely the construction of stronger technical defenses but the understanding of how human behavior interacts with these defenses in producing security failures (Florackis et al., 2020).

The existing information security literature has predominantly emphasized technical system vulnerabilities and corresponding mitigation strategies. Prior research has examined the resilience of digital business architectures (Ammirato et al., 2022) the implementation of international standards such as ISO 27001 in technological risk management, and the continuous development of cybersecurity risk assessment models aimed at strengthening technical infrastructure (Ekstedt et al., 2023; Judijanto et al., 2023). At the same time, a growing body of studies has begun to foreground the human factor from the perspective of Human Error Theory. For example, analytical models such as the Systematic Human Error Reduction and Prediction Approach (SHERPA) have been employed to classify and predict errors across operational environments, underscoring their critical role in system failure (Ashour et al., 2022; Read et al., 2021). Collectively, these studies suggest that errors are not random occurrences but are deeply rooted in systemic organizational conditions.

However, a clear research gap remains: the lack of a direct, empirical, and systematic comparison between human error and technical system vulnerabilities as competing sources of security failure in contemporary digital business environments. Most prior studies have examined these two dimensions in isolation, either prioritizing technical fortification or, to a lesser extent, focusing on behavioral failure. What remains critically underexplored is an integrated evaluation that empirically weighs the relative dominance of human error versus system vulnerability in real-world security incidents. This gap is particularly salient given the socio-technical character of modern organizations, in which human behavior and technology are mutually constitutive (Cameron & Rahman, 2022; Herrmann et al., 2022). This comparative approach is essential to identify not only technical weaknesses but also systemic behavioral risks that traditional cybersecurity models often overlook. Moreover, previous studies have not yet adequately combined the theoretical foundations of human failure, such as Reason's Swiss Cheese Model, with socio-technical systems theory and mature information security management paradigms to form a coherent analytical framework for digital business security.

The theoretical contribution of this study lies in its original integration of Human Error Theory, Socio-Technical Systems Theory, and the ISO 27001 framework into a unified analytical model that transcends purely technical or purely behavioral explanations of cybersecurity failure. From a practical standpoint, the findings offer evidence-based guidance for managers and IT security professionals in designing more resilient security strategies. By identifying the most probable

points of failure, organizations can allocate resources more effectively, strengthen training programs, refine security protocols, and cultivate a security-conscious organizational culture that complements technological investment. The remainder of this paper is structured as follows: Section 2 presents the literature review and theoretical framework; Section 3 outlines the research methodology; Section 4 reports the findings; and Section 5 concludes with implications and recommendations.

## II. LITERATURE REVIEW

This chapter establishes the conceptual and theoretical foundations for examining the interaction between human error and system security in digital business environments through a hypothesis-driven analytical structure. The discussion progresses from core theoretical perspectives to empirical evidence, culminating in the articulation of the research gap addressed in this study. Three principal theoretical pillars underpin this research: Human Error Theory, Socio-Technical Systems Theory, and the ISO 27001 standard. Each theory is explicitly linked to the development of the study's hypotheses to ensure conceptual coherence and empirical testability. The chapter then critically synthesizes prior empirical findings by identifying conceptual overlaps, methodological limitations, and unresolved gaps that motivate the present study.

### *A. Theoretical foundations*

The theoretical understanding of human error has evolved from viewing error as individual negligence to recognizing it as a systemic consequence of latent organizational conditions. James Reason's Swiss Cheese Model conceptualizes failure as the alignment of latent conditions and active failures across multiple defensive layers Reason, 1990 and (Read et al., 2021). Within this study, the Swiss Cheese Model provides the direct theoretical basis for Hypothesis 2, which links active human failures to latent organizational causes such as time pressure and inadequate training. This model has demonstrated broad applicability across domains, including healthcare (Ashour et al., 2022) and business operations (Torres et al., 2021). In digital business contexts, an active failure, such as clicking a phishing link, can bypass multiple technical safeguards when reinforced by latent conditions, such as weak security awareness. Empirical evidence confirms that human error remains a persistent feature across technological environments, including accounting systems (Al-Hattami, 2024) and e-business platforms (Handoko et al., 2025).

Socio-Technical Systems Theory posits that organizational outcomes emerge from the interdependence between social subsystems (people, culture, skills) and technical subsystems (technology, tasks, processes). This theory rejects the assumption that optimizing one subsystem in isolation leads to optimal system performance (Cameron & Rahman, 2022; Masili et al., 2024). In this study, Socio-Technical Systems Theory provides the foundational logic for Hypotheses 1

and 3 by framing cybersecurity risk as a systemic outcome of interactions between organizational units, human behavior, and technical controls. In cybersecurity, advanced technical defenses may be undermined by weak security culture, resistance to policy compliance, or fragmented communication across departments (Yang & Zhang, 2023). Applications of socio-technical evaluation heuristics further demonstrate the necessity of incorporating organizational and human considerations into system design (Herrmann et al., 2022). This perspective is increasingly salient in digital business ecosystems (Ammirato et al., 2022) characterized by rapidly evolving cyber threats (Havryliuk et al., 2023)**.**

The ISO/IEC 27001 standard provides a structured, risk-based framework for implementing an Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of organizational information assets (Fakiha, 2021). Prior studies demonstrate its effectiveness in structuring organizational cybersecurity governance (Ekstedt et al., 2023; Judijanto et al., 2023). In this research, ISO 27001 serves as the operational framework for Hypothesis 3, defining how security policies, controls, and procedures are implemented and evaluated in practice. However, while ISO 27001 formally acknowledges the human factor through its awareness and training controls, its operationalization remains predominantly procedural and technological. This limitation motivates integrating ISO 27001 with Human Error Theory and Socio-Technical Systems Theory to more comprehensively capture behavioral and organizational risk dynamics.

*B. Empirical Studies and Previous Research*

Technical cybersecurity research has primarily focused on the continuous development of threat assessment and defense architectures. (Ekstedt et al., 2023) critically reviewed cybersecurity assessment frameworks and identified persistent challenges in achieving holistic threat coverage. (Judijanto et al., 2023; Repetto et al., 2021) similarly emphasized technical resilience through architectural and business-oriented cybersecurity solutions. However, these studies largely conceptualize human factors as contextual variables rather than principal drivers of system failure.

Conversely, human-centered cybersecurity research has shown that human error is a frequent cause of security breaches. (Amoresano & Yankson, 2023) showed that behavioral failures were the primary contributors to data breaches in educational institutions. (Ashour et al., 2022) applied the SHERPA method to systematically predict and classify human error, offering methodological tools for proactive risk mitigation. Nevertheless, these studies remain sector-specific and do not statistically compare the dominance of human versus technical causes across broader digital business contexts. Usability research further indicates that poor interface design and system complexity significantly increase the probability of user error (Hamid et al., 2022). Socio-

technical studies remain limited but promising, as demonstrated by (Baroni et al., 2021), who showed how interface "dark patterns" can structurally induce human error, and by (Saeed et al., 2023), who advocated for balanced technological and human-centered digital resilience strategies. Across these empirical streams, a clear conceptual overlap exists between technical vulnerability, human fallibility, and organizational design; however, their interdependencies are rarely modeled in an integrated empirical framework. Methodologically, most prior studies rely on single-method designs, sector-specific samples, or unidimensional explanatory models, thereby limiting generalizability and causal inference. To synthesize these disparate empirical contributions and highlight the gaps they collectively reveal, Table 1 provides a consolidated summary of key studies, their methods, principal findings, and contextual limitations.

**Table 1. Summary of Key Empirical Studies**

| Researcher(s) | Method | Key Findings | Limitations / Context |
|---|---|---|---|
| (Ekstedt et al., 2023) | Framework Analysis | Proliferation of technical risk frameworks persists, but holistic coverage remains challenging. | Focus is predominantly on technical assessment, with human factors as a secondary variable. |
| (Amoresano & Yankson, 2023) | Case Study | Human error is a critical, often dominant, factor in data breaches within educational institutions. | Single-sector focus (education); lacks broad comparative analysis with technical causes. |
| (Ashour et al., 2022) | SHERPA Application | Human errors can be systematically predicted and classified to inform proactive mitigation. | Applied in a healthcare context, it requires validation in digital business environments. |
| (Saeed et al., 2023) | Literature Review | Effective cybersecurity resilience requires balancing technological and human-centric strategies. | A high-level conceptual review; it lacks empirical testing of the proposed integrated model. |

### *C. Research Gap and Conceptual Framework*

The synthesis of theoretical and empirical literature reveals a critical gap: the absence of a direct, comparative, and integrated empirical evaluation of human error and technical system vulnerability in digital business security. Most existing studies, as summarized in Table 1, prioritize either the technical or the human dimension, with the alternative treated merely as a background condition. For instance, (Amoresano & Yankson, 2023) identify human error as a dominant breach factor but do not statistically compare its relative contribution against technical system failures. Accordingly, the present study addresses this unresolved gap by integrating Human Error Theory, Socio-Technical Systems Theory, and ISO 27001 into a unified conceptual framework. This integrative combination is original in that it simultaneously explains security failure through behavioral mechanisms (human error), systemic-organizational interactions (socio-technical dynamics), and formalized security governance structures (ISO 27001). The framework posits that cybersecurity in digital business environments is an emergent property of

multi-level socio-technical interactions rather than a purely technical outcome. It formally advances the proposition that latent organizational conditions and active human failures collectively exert a stronger influence on security incidents than technical vulnerabilities alone.

### *D. Developing Hypotheses*

After establishing the theoretical logic and identifying empirical limitations, the following hypotheses are formulated:

H1: Human error contributes more to the occurrence of security events in digital business information systems than technical system weaknesses. (Derived from Socio-Technical Systems Theory and validated through comparative empirical testing.)

H2: The frequency of occurrence of specific types of human error (e.g., decision-based, skill-based slips) is increased by latent organizational causes (e.g., time pressure, inadequate training). (Directly derived from the Swiss Cheese Model's distinction between latent and active errors.)

H3: An integrated socio-technical security mitigation model will be assessed as more effective in reducing cybersecurity risk by IT professionals than models based purely on technical controls. (Operationalized through ISO 27001 as the policy and control framework combined with socio-technical principles.)

This chapter has established the theoretical pillars and critically reviewed empirical findings to demonstrate that, although each component has been well studied independently, the integrated and comparative empirical examination of their integration remains limited. The conceptual framework and hypotheses articulate how this study directly addresses this gap. The next chapter presents the mixed-methods research design employed to operationalize these constructs and empirically test the proposed hypotheses.

## III. RESEARCH METHOD

### *A. Research Design*

The study employs an explanatory sequential mixed-methods design, collecting and analyzing quantitative data in the first phase, followed by qualitative data to explain and contextualize the statistical findings. This design is appropriate for simultaneously testing the dominance of human error over technical vulnerability (H1–H2) and for developing a socio-technical mitigation framework grounded in practitioner experience (H3). The quantitative phase addresses the "what" and "how much," while the qualitative phase explains the "why" and "how." This sequential logic ensures both statistical rigor and contextual depth without unnecessary procedural complexity. This research process is illustrated in Figure 1.

Journal of Management and Informatics (JMI)
**Vol. 4 No. 3 December 2025**
E-ISSN: 2961-7731; P-ISSN: 2961-7472, Pages 981-997

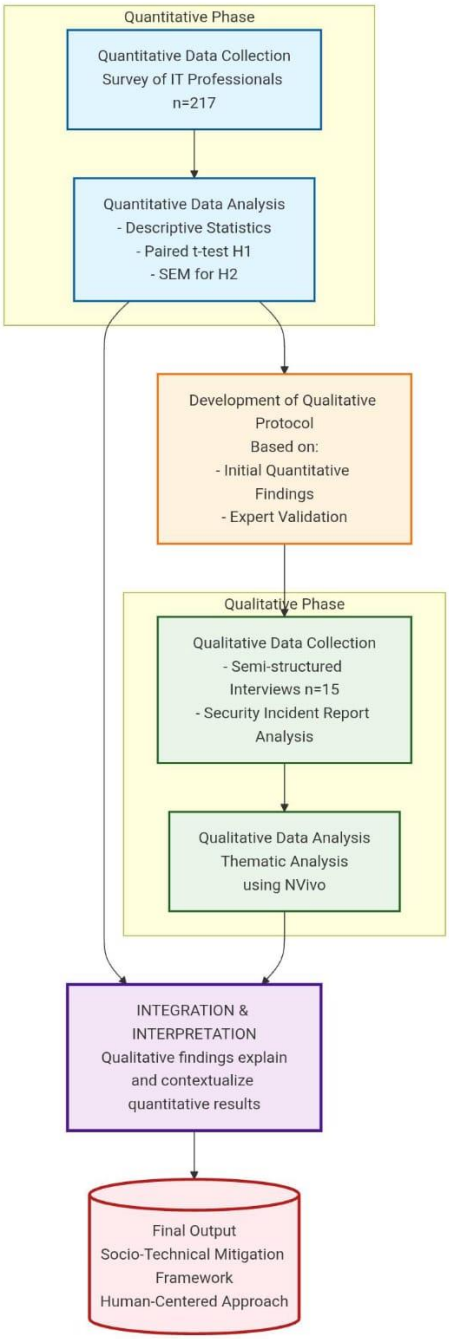


**Figure 1. Explanatory Sequential Mixed-Methods Research Design**

*B. Population, Sample, and Sampling Technique*

The population of this study consists of organizations operating in the digital business sector in Indonesia, including fintech, e-commerce, and platform-based service companies. Indonesia was selected as the research context because it represents one of the fastest-growing digital economies in Southeast Asia, characterized by rapid growth in internet penetration, digital payments, and online transactions, which simultaneously increases organizational exposure to cybersecurity

risks (Saeed et al., 2023). The sampling frame was constructed using professional IT networks and industry directories. A purposive sampling strategy was used to recruit respondents with direct knowledge of cybersecurity incidents, such as IT security managers, network administrators, and compliance officers. A total of 217 valid questionnaires were obtained for the quantitative phase. This sample size exceeds the minimum recommended threshold for Partial Least Squares–SEM, which follows the "10-times rule" requiring at least 10 respondents per structural path, thereby ensuring adequate statistical power for model estimation. For the qualitative phase, 15 participants were selected using stratified purposive sampling to represent variations in organizational size and incident experience.

### *C. Sources and Data Collection Techniques*

Data were obtained from both primary and secondary sources for triangulation. Primary quantitative data were collected through a structured online survey distributed via professional networks. Primary qualitative data were generated through semi-structured online interviews lasting approximately 45–60 minutes. Secondary data consisted of anonymized organizational security incident reports submitted by participating firms. This triangulated approach strengthens the validity of the findings by cross-verifying perceptual data with organizational records. To provide a clear overview of the multi-phase data strategy and the instruments employed, Table 2 presents a detailed data collection matrix summarizing sources, methods, and focal variables.

**Table 2. Data Collection Matrix**

| Phase | Data Source | Instrument | Variables / Focus | Administration |
|---|---|---|---|---|
| Quantitative | IT Professionals (n=217) | Structured Questionnaire | Human error types, frequency, latent conditions, system vulnerability metrics | Online survey (Google Forms) |
| Qualitative | IT/Security Staff (n=15) | Semi-structured Interview Guide | Root causes of incidents, organizational culture, perceived effectiveness of controls | Online interviews (Zoom), transcribed |
| Qualitative | Participating Organizations | Security Incident Reports | Objective data on incident cause (human vs. system), impact, resolution | Document analysis |

### *D. Variables and Operational Definitions*

The study examines four main constructs: Human Error Contribution, Technical Vulnerability Contribution, Latent Organizational Conditions, and Perceived Effectiveness of Socio-Technical Mitigation. All constructs were operationalized using multi-item Likert-type scales adapted from prior validated studies in human error and information security research (Ashour et al., 2022; Read et al., 2021; Saeed et al., 2023). The detailed operationalization is presented in Table 3.

**Table 3. Operationalization of Variables**

| Construct | Type | Operational Definition | Measurement Scale & Sample Indicator |
|---|---|---|---|
| Human Error Contribution | Dependent | The perceived frequency and impact of security incidents are primarily due to employee actions or inactions. | 5-point Likert (1=Very Low to 5=Very High); e.g., "In the past year, what proportion of security incidents were initiated by human error?" |
| Technical Vulnerability Contribution | Dependent | The perceived frequency and impact of security incidents primarily caused by flaws in software, hardware, or network design. | 5-point Likert (1=Very Low to 5=Very High); e.g., "In the past year, what proportion of incidents were due to unpatched system vulnerabilities?" |
| Latent Organizational Conditions | Independent | Underlying workplace factors that increase the likelihood of human error, such as workload, training adequacy, and clarity of procedures. | 5-point Likert (1=Strongly Disagree to 5=Strongly Agree); e.g., "Employees receive regular and effective cybersecurity awareness training." (Reverse-coded) |
| Perceived Effectiveness of Socio-Technical Mitigation | Dependent | The degree to which IT professionals believe an integrated human-technology approach would reduce cybersecurity risk. | 5-point Likert (1=Very Ineffective to 5=Very Effective); e.g., "How effective would a framework that equally addresses both user behavior and technical controls be?" |

### *E. Research Instrument and Validity/Reliability*

The questionnaire was developed based on established instruments in human error analysis and information security management. A two-stage pilot test was conducted: expert validation for content and structure, followed by field testing with 30 IT professionals. The pilot test resulted in a Cronbach's Alpha of 0.89, indicating high internal consistency. These procedures ensured that the instrument met accepted standards of psychometric robustness prior to full deployment. The qualitative interview guide was similarly peer-reviewed to reduce measurement bias.

### *F. Data Analysis Techniques*

Quantitative data were analyzed using SPSS v.28 and SmartPLS 4.0. Descriptive statistics were used to summarize respondent profiles and key variables. H1 was tested using a paired-samples t-test to compare the means of the contributions of human error and technical vulnerability. H2 was examined through SEM to assess the structural relationship between latent organizational conditions and human error. The use of SEM is justified by its suitability for simultaneously modeling latent constructs and testing complex causal relationships within a single analytical framework. Qualitative data were analyzed using thematic analysis following systematic coding and pattern identification procedures (Cao et al., 2021; Herrmann et al., 2022) , supported by NVivo software. The qualitative findings were used to contextualize the SEM results and refine the socio-technical mitigation model for H3.

### *G. Ethical Considerations*

All participants received detailed information regarding the study's objectives and procedures prior to participation. Informed consent was obtained electronically for the survey and verbally at the beginning of each interview. Confidentiality and anonymity were ensured through pseudonymization and the removal of identifying organizational information. All digital data were securely stored on encrypted, password-protected institutional servers with access limited to the core research team. Participation was voluntary, and respondents retained the right to withdraw at any stage without consequence.

## IV. RESULT

The empirical findings from the sequential quantitative and qualitative analyses are presented separately to ensure a clear distinction between statistical outcomes and their substantive interpretation. The presentation begins with the respondents' demographic profile, then presents hypothesis testing, and concludes with thematic findings from the qualitative phase. This structure ensures that the results section focuses strictly on empirical evidence without interpretative overlay. Such separation is intended to enhance analytical transparency and prevent premature theoretical inference at this stage.

### *A. Descriptive Statistics and Sample Profile*

The quantitative phase obtained 217 valid responses from IT professionals working in Indonesia's digital business environment. The demographic characteristics of these respondents, as tabulated in Table 4, indicate a well-distributed sample across key organizational functions and firm sizes. This distribution enhances the study's external validity. The majority of respondents were directly involved in information security management, strengthening the credibility of incident-related assessments.

**Table 4. Demographic Profile of Survey Respondents (N=217)**

| Characteristic | Category | Frequency | Percentage |
|---|---|---|---|
| Primary Role | IT Security Manager | 78 | 35.9% |
| Network/Systems Admin | 65 | 30.0% | |
| Risk/Compliance Officer | 45 | 20.7% | |
| Other IT Staff | 29 | 13.4% | |
| Company Size | Large (>500 employees) | 92 | 42.4% |
| Medium (50-500 employees) | 87 | 40.1% | |
| Small (<50 employees) | 38 | 17.5% | |
| Industry | Fintech/Payment Services | 101 | 46.5% |
| E-commerce & Retail | 76 | 35.0% | |
| Digital Services/Platforms | 40 | 18.4% | |

### *B. Hypothesis Testing: Human Error vs. System Vulnerabilities*

To test H1, a paired-samples t-test was conducted to compare the perceived contributions of human error and technical system vulnerabilities. The results in Table 5 indicate a statistically significant difference between the two mean values. Human error recorded a significantly higher mean score (M = 3.82) than technical vulnerability (M = 2.94), with t(216) = 5.734, p < .001. This result provides direct statistical support for H1.

**Table 5. Paired-Samples T-Test: Human Error and System Vulnerability Contribution**

| Variable | Mean | Std. Deviation | t-value | df | p-value |
|---|---|---|---|---|---|
| Human Error Contribution | 3.82 | 0.91 | 5.734 | 216 | .000 |
| System Vulnerability Contribution | 2.94 | 0.87 | | | |

To test H2, Structural Equation Modeling (SEM) was used to examine the effect of latent organizational conditions on the prevalence of human error. The structural model exhibited acceptable goodness-of-fit indices. The path coefficient indicates a strong, statistically significant positive relationship between latent conditions and the occurrence of human error. This finding statistically confirms that human failures are structurally embedded in organizational environments rather than emerging solely from individual behavior. Thus, H2 is supported.

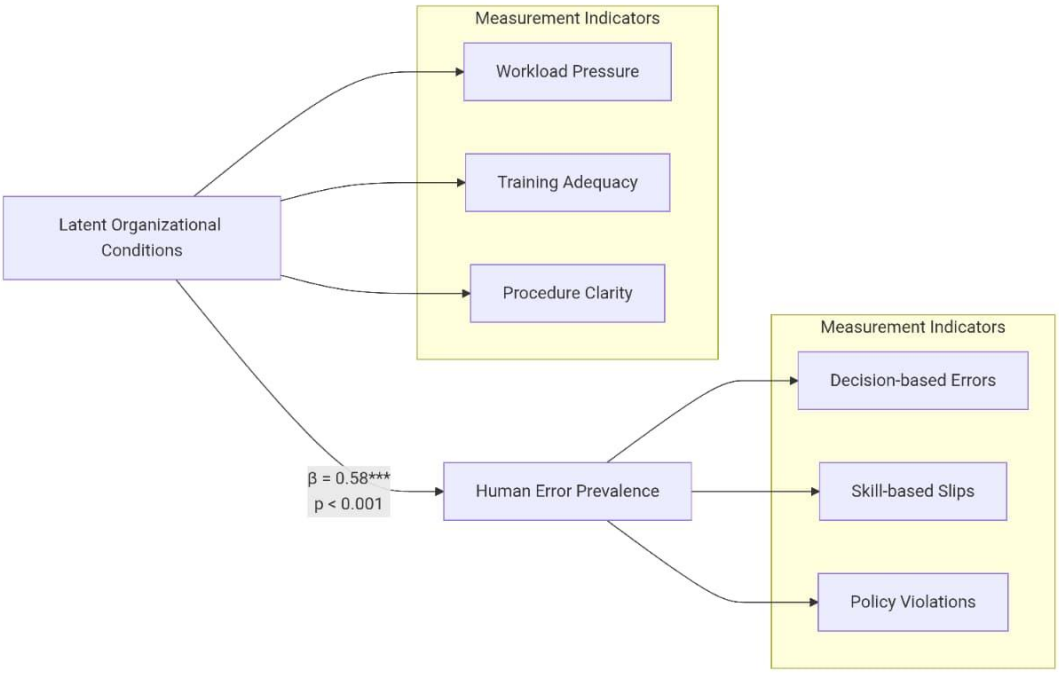


**Figure 2. Structural Model (SEM) for H2: Latent Conditions' Influence on Human Error**

### *C. Thematic Analysis: Opening Up the Black Box of the Human Factor*

Thematic analysis of interview transcripts and security incident reports generated three dominant themes that explain the human contribution to cybersecurity failures. These themes provide qualitative depth that reinforces the quantitative SEM and t-test findings. The themes illustrate

how latent organizational conditions become manifested in daily operational security behavior. This qualitative layer strengthens the explanatory power of the statistical models (Miklosik et al., 2021).

**Theme 1: Cognitive Overload from Complex Security Procedures.** Respondents consistently reported that high procedural complexity under operational pressure triggered procedural workarounds. One IT manager noted: "We use multi-step authentication, but during peak hours people rush and approve prompts without fully verifying the source." This theme empirically illustrates how workload pressure activates skill-based slips. This finding aligns with prior research on technology-induced cognitive strain in security-intensive environments (Gibbs et al., 2023).

**Theme 2: The Gap between Formal Training and Practical Threats.** Participants emphasized that compliance-based training did not adequately prepare staff for evolving phishing tactics. One respondent stated: "Annual security training is too generic. It does not prepare employees for targeted phishing." This finding empirically supports the SEM path linking training inadequacy to heightened human error. It is consistent with earlier evidence that generic cybersecurity education often fails to transfer into situational threat awareness (Ashour et al., 2022; Read et al., 2021).

**Theme 3: Social Engineering as the Primary Attack Vector.** Incident records consistently showed that phishing and pretexting were the dominant causes of breaches. This confirms that attackers deliberately prioritize psychological manipulation over technical exploitation. This qualitative evidence strengthens the quantitative dominance of human error over system vulnerability found in H1. The result also echoes broader threat intelligence findings that social engineering remains the most adaptive attack vector in digital ecosystems (Saeed et al., 2023).

## V. DISCUSSION

Unlike the Results section, this Discussion section focuses on theoretical integration, practical implications, and contribution to knowledge. The findings demonstrate that human error constitutes a more dominant contributor to digital security breaches than technical vulnerabilities. This aligns with prior studies emphasizing behavioral risk in cybersecurity (Amoresano & Yankson, 2023; Read et al., 2021) but significantly extends them by providing direct statistical comparison supported by qualitative explanation. Thus, this study moves beyond conceptual assertion toward empirical hierarchy of risk sources.

By empirically confirming H1, this study advances existing cybersecurity theory by quantifying the relative dominance of human error rather than merely asserting its importance. The

prominence of social engineering further demonstrates that contemporary cyber threats systematically target behavioral rather than technical weaknesses. This shifts the security paradigm from perimeter defense to human-centered risk management. It also helps explain why purely technology-driven security investments often fail to curb breach incidents in practice (Saeed et al., 2023; Ulven & Wangen, 2021).

The confirmation of H2 provides strong theoretical support for Reason's Swiss Cheese Model in digital business security. Latent organizational conditions particularly workload pressure and inadequate training are shown to be systemic precursors of active human failures rather than isolated personal negligence. This interpretation is strengthened through alignment with Socio-Technical Systems Theory, which explains how misalignment between human and technological subsystems produces compounded organizational risk (Cameron & Rahman, 2022; Herrmann et al., 2022) . Accordingly, security breaches emerge as systemic failures rather than individual misconduct.

The most significant theoretical contribution of this study lies in its integrated application of Human Error Theory, Socio-Technical Systems Theory, and ISO 27001 within a single empirical framework. Unlike earlier studies that examine these perspectives in isolation, this research demonstrates their structural complementarity: Human Error Theory explains what fails, Socio-Technical Systems Theory explains why it fails, and ISO 27001 provides guidance on how it can be systematically controlled. This integration represents an original analytical synthesis that bridges behavioral, organizational, and governance-based research in cybersecurity. As such, it extends the theoretical maturity of cybersecurity from a fragmented to a systemic discipline.

### *A. Managerial and Organizational Implications*

From a managerial standpoint, the findings call for a fundamental recalibration of cybersecurity strategy, moving away from a technology-dominant model toward a human-centered, socio-technical security approach. First, organizations should adopt usability-oriented security design to reduce cognitive overload during high-pressure operations. Second, security training must transition from generic compliance programs to adaptive, threat-driven simulations. Third, organizations should institutionalize continuous social engineering testing as part of operational risk governance. Together, these measures directly target the latent conditions statistically shown to amplify human error.

At the organizational level, these measures reposition employees from being perceived as the weakest link to becoming the first adaptive layer of cyber defense. This shift supports stronger cybersecurity culture, improved resilience, and more effective alignment between technical investments and human capability development. In the long term, such alignment strengthens

organizational cyber resilience and reduces the probability of cascading socio-technical failures. It also reinforces accountability structures under ISO 27001 by embedding human risk directly into operational control systems.

### *B. Theoretical and Practical Contributions*

This study makes a distinct theoretical contribution by integrating Human Error Theory, Socio-Technical Systems Theory, and ISO 27001 into a single empirical framework. Unlike previous research that treats these perspectives separately, our study demonstrates their complementarity: Human Error Theory identifies the failure phenomenon, Socio-Technical Systems Theory explains the systemic causes, and ISO 27001 provides structured guidance for mitigation. This integrated approach represents a novel analytical synthesis that advances both theoretical understanding and applied cybersecurity research. First, the study empirically confirms that human error is a more dominant contributor to digital security breaches than technical vulnerabilities, thereby reinforcing and extending Reason's Swiss Cheese Model in modern digital business environments. Latent organizational conditions such as cognitive overload and insufficient contextual training have been shown to systematically trigger human errors, highlighting the importance of analyzing failures at the socio-technical level rather than attributing them solely to individual mistakes.

Second, the research provides clear practical implications for cybersecurity management. Organizations are encouraged to prioritize human-centered security strategies, including: Reducing cognitive load through usability-focused design of security processes and tools. Implementing context-driven and threat-relevant training programs instead of generic compliance exercises. Conducting ongoing social engineering simulations to strengthen human defenses as part of operational risk governance. Finally, these findings emphasize the strategic value of employees as active participants in cybersecurity, rather than as the perceived weakest link. By embedding human risk management within organizational control structures aligned with ISO 27001 standards companies can foster a resilient cybersecurity culture, enhance operational alignment between technology and personnel, and mitigate cascading failures in socio-technical systems. This positions human-centered approaches as a foundational complement to technical controls, with both theoretical and practical relevance for contemporary digital enterprises.

## VI. CONCLUSION AND RECOMMENDATION

This study confirms that human error constitutes the primary contributor to digital business security failures, yet these errors are predominantly rooted in latent organizational conditions rather than isolated individual faults. The combined sequential quantitative and qualitative analyses revealed that excessive workload, inadequate contextual training, and complex security

procedures systematically induce skill-based slips and behavioral vulnerabilities, while social engineering exploits these weaknesses as strategic attack vectors (Amoresano & Yankson, 2023; Gibbs et al., 2023; Read et al., 2021; Saeed et al., 2023). The study contributes theoretically by integrating Human Error Theory, Socio-Technical Systems Theory, and ISO 27001 into a single framework, demonstrating that security is an emergent property of human, organizational, and technological interactions (Cameron & Rahman, 2022; Herrmann et al., 2022; Kirkegaard et al., 2023). Practically, it advocates a human-centered approach: usability-focused system design to reduce cognitive load, adaptive threat-driven training, and continuous social engineering simulations to empower employees as the first adaptive layer of cyber defense. Figure 3 presents a simplified socio-technical framework illustrating how human, technical, and organizational factors interact to produce security outcomes. Despite the study's robust methodological design, limitations include its geographic focus on Indonesia and cross-sectional nature, which constrains generalizability and temporal inference. Future research should employ longitudinal, experimental, or quasi-experimental designs across varied cultural and industrial contexts to test causal mechanisms of human-centered interventions, including AI-assisted predictive controls and adaptive training programs. These directions would enable organizations to refine socio-technical security strategies by integrating human and technical risk mitigation into operational and strategic planning to improve resilience and reduce cascading failures.

## REFERENCES

Al-Hattami, H. M. (2024). The influence of accounting information system on management control effectiveness: The perspective of SMEs in Yemen. *Information Development*, *40*(1), 75–93. https://doi.org/10.1177/02666669221087184

Ammirato, S., Felicetti, A. M., Linzalone, R., & Carlucci, D. (2022). Digital business models in cultural tourism. *International Journal of Entrepreneurial Behaviour and Research*, *28*(8), 1940–1961. https://doi.org/10.1108/IJEBR-01-2021-0070

Amoresano, K., & Yankson, B. (2023). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA – Journal of Business and Public Administration*, *14*(1), 110–132. https://doi.org/10.2478/hjbpa-2023-0007

Ashour, A., Phipps, D. L., & Ashcroft, M. (2022). Predicting dispensing errors in community pharmacies: An application of the Systematic Human Error Reduction and Prediction Approach (SHERPA). *PLoS ONE*, *17*(1 January). https://doi.org/10.1371/journal.pone.0261672

Baroni, L. A., Puska, A. A., De Castro Salgado, L. C., & Pereira, R. (2021, October 18). Dark Patterns: Towards a Socio-technical Approach. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3472301.3484336

Cameron, L. D., & Rahman, H. (2022). Expanding the Locus of Resistance: Understanding the Co-constitution of Control and Resistance in the Gig Economy. *Organization Science*, *33*(1), 38–58. https://doi.org/10.1287/ORSC.2021.1557

Cao, X., Ali, A., Pitafi, A. H., Khan, A. N., & Waqas, M. (2021). A socio-technical system approach to knowledge creation and team performance: evidence from China. *Information Technology and People*, *34*(7), 1976–1996. https://doi.org/10.1108/ITP-10-2019-0536

Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security*, *22*(6), 1713–1729. https://doi.org/10.1007/s10207-023-00713-y

Fakiha, B. (2021). Business organization security strategies to cyber security threats. *International Journal of Safety and Security Engineering*, *11*(1), 101–104. https://doi.org/10.18280/ijsse.110111

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2020). *Nber Working Paper Series Cybersecurity Risk*. http://www.nber.org/papers/w28196

Gibbs, M., Mengel, F., & Siemroth, C. (2023). Work from Home and Productivity: Evidence from Personnel and Analytics Data on Information Technology Professionals. *Journal of Political Economy Microeconomics*, *1*(1), 7–41. https://doi.org/10.1086/721803

Hamid, K., Iqbal, M. W., Abdul, H., Muhammad, B., Fuzail, M. Z., Waseem Iqbal, M., Fuzail, Z., Tabassum Ghafoor † † † † †, Z., & Ahmad, S. (2022). Usability Evaluation of Mobile Banking Applications in Digital Business as Emerging Economy. *IJCSNS International Journal of Computer Science and Network Security*, *22*(2), 250. https://doi.org/10.22937/IJCSNS.2022.22.2.32

Handoko, M., Yulianto, A. R., Jatinurcahyo, R., Subariyanti, H., Nikmah, W., Adawia, P. R., Yulianto, & Armaniah, H. (2025). Implementation of MIS (Management InformationSystem) to Improve Efficiency and Security of Interbank transactions Using BCA Mobile (Case Study at Bank BCA Tbk). *Journal of Management and Informatics*, *4*(2), 791–806. https://doi.org/10.51903/jmi.v4i2.201

Havryliuk, O., Yakushev, O., Petchenko, M., Zachosova, N., Bielialov, T., & Kozlovska, S. (2023). Cyber Security And Artificial Intelligence In The Context Of Ensuring Business Security In Wartime. *Financial and Credit Activity: Problems of Theory and Practice*, *6*(53), 451–459. https://doi.org/10.55643/fcaptp.6.53.2023.4130

Herrmann, T., Jahnke, I., & Nolte, A. (2022). A problem-based approach to the advancement of heuristics for socio-technical evaluation. *Behaviour and Information Technology*, *41*(14), 3087–3109. https://doi.org/10.1080/0144929X.2021.1972157

Judijanto, L., Hindarto, D., Wahjono, S. I., & Djunarto. (2023). Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386–396. https://doi.org/10.35870/ijsecs.v3i3.1816

Kirkegaard, J. K., Rudolph, D. P., Nyborg, S., Solman, H., Gill, E., Cronin, T., & Hallisey, M. (2023). Tackling grand challenges in wind energy through a socio-technical perspective. In *Nature Energy* (Vol. 8, Issue 7, pp. 655–664). Nature Research. https://doi.org/10.1038/s41560-023-01266-z

Masili, G., Binci, D., Cerruti, C., Appolloni, A., & Giraldi, L. (2024). Agility in virtual environments: the socio-technical approach of distributed agile teams. *Management Research Review*, *47*(13), 69–86. https://doi.org/10.1108/MRR-03-2023-0219

Miklosik, A., Evans, N., & Qureshi, A. M. A. (2021). The Use of Chatbots in Digital Business Transformation: A Systematic Literature Review. In *IEEE Access* (Vol. 9, pp. 106530–106539). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3100885

Read, G. J. M., Shorrock, S., Walker, G. H., & Salmon, P. M. (2021). State of science: evolving perspectives on 'human error.' In *Ergonomics* (Vol. 64, Issue 9, pp. 1091–1114). Taylor and Francis Ltd. https://doi.org/10.1080/00140139.2021.1953615

Repetto, M., Carrega, A., & Rapuzzi, R. (2021). An architecture to manage security operations for digital service chains. *Future Generation Computer Systems*, *115*, 251–266. https://doi.org/10.1016/j.future.2020.08.044

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. In *Sensors* (Vol. 23, Issue 15). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s23156666

Torres, Y., Nadeau, S., & Landau, K. (2021). Classification and quantification of human error in manufacturing: A case study in complex manual assembly. *Applied Sciences (Switzerland)*, *11*(2), 1–23. https://doi.org/10.3390/app11020749

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. In *Future Internet* (Vol. 13, Issue 2, pp. 1–40). MDPI AG. https://doi.org/10.3390/fi13020039

Yang, J., & Zhang, M. (2023). Beyond structural inequality: a socio-technical approach to the digital divide in the platform environment. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-02326-1