(Online) ISSN 2712-0562
Sustainable Engineering and Innovation *Original Research*
Vol. 7, No. 2, 2025, pp.493-506
https://doi.org/10.37868/sei.v7i2.id574

Risks of cyberattacks on accounting: Analysis of modern threats and preventive measures

Gabriella Loskorikh[1*], Edina Shebeshten[2], Olena Koval[3], Konon Bagrii[4], Nataliia Valkova[5]
[1,2] Department of Accounting and Auditing, Ferenc Rákóczi II Transcarpathian Hungarian College of Higher Education, Ukraine
[3] Department of Accounting and Taxation, Vinnytsia National Agrarian University, Ukraine
[4] Department of Finance, Accounting and Taxation, Chernivtsi Institute of Trade and Economics of the State University of Trade and Economics, Ukraine
[5] Department of Accounting, Auditing and Taxation, Khmelnytskyi National University, Ukraine

*Corresponding author E-mail: loskorih.gabriella@kmf.org.ua

Received Jun. 22, 2025
Revised Sep. 2, 2025
Accepted Sep. 11, 2025
Online Oct. 8, 2025

Abstract

The increasing digitalization of accounting systems has amplified vulnerabilities to cyberattacks, yet practical strategies to address sector-specific risks remain underexplored. This study explored prevalent cyber threats in the accounting industry, such as phishing directed at enterprise resource planning systems, unauthorized access utilizing mobile devices, and invoice fraud. The investigation was conducted in a manner that combined interviews with accounting and cybersecurity professionals and comparative case reviews of organizational practices. A statistical analysis showed that multi-factor authentication reduced cyber-attack likelihood by 58% while regular employee training reduced the risk by 37%. Organizations with combined Information Technologies (IT) and accounting teams took 40 percent less time resolving security incidents than organizations with separate departments. The results showed that mid-sized firms generally had poor preparedness, while bigger firms showed adherence to international security standards. They also highlighted the need for mandatory cybersecurity training, collaboration across departments, and strategic investments in adaptive security frameworks. Regulatory incentives for small and medium enterprises to adopt cost-effective mitigating safeguards are also a policy implication. The results help bridge theoretical cybersecurity models and real accounting practice by providing actionable advice on making operations more sustainable while mitigating the increasing threat of cyber incidents.

Keywords: Operational sustainability, Strategic planning, Resource optimization, Adaptive management, Cybersecurity

1. Introduction

Accounting systems that have transitioned to digital platforms enable companies to conduct real-time analytics and automation for transactions and Enterprise Resource Planning (ERP) system integration [1]. Adopting cloud

computing technology, blockchain systems, and artificial intelligence applications trains accounting into an actively strategic function instead of its previous regulatory obligation [2]. The advancements in technology have brought forward major system weaknesses. Accounting systems have become primary targets of cybercriminals because the systems house essential financial data, including employee payments, vendor invoices, and tax documents [3].

Cybersecurity Ventures produced a 2023 study showing financial systems experienced a 67% attack increase from 2021 to 2023, whereas accounting platforms became the target for 42% of all these breaches [4], [5]. Recent cybersecurity incidents, especially the 2022 ransomware attack on a global accounting firm, which disrupted $230 million in transactions, highlight the necessity for high-level security measures on these platforms [6]. The pressing need for cybersecurity protection exists, while the theoretical principles protecting businesses remain ineffective in accounting systems applications.

Research by [7] identified digitalization as a significant force behind organizational innovation. Yet, it fails to discuss the threats from manipulated financial records and deceptive invoice approvals, affecting accounting practices. Authors from paper [8] analyzed mobile computing's business effects while failing to address the security flaws when unsecured devices provide unauthorized access to mobile accounting applications. The difference between theory and real-world applications in information technology research shows us the necessity for applied investigations that create theoretical models compatible with strategies meant for accounting infrastructure protection [9].

The research focuses on why accounting systems need better response strategies to protect against cyber threats. Despite being useful for overall cybersecurity planning, these frameworks do not include specific guidance about protecting ERP systems, handling legacy software components, or tackling social engineering attacks that target financial controllers. Attackers use artificial intelligence (AI) to generate emails that impersonate executives for fraudulent transfers in spear phishing campaigns, even though this new threat does not exist in cybersecurity books [10]. As small and medium-sized businesses usually do not have enough budget to install state-of-the-art protection systems, they are more vulnerable to attacks. Research in [11] showed that 68% of small business owners use out-of-date antivirus programs, making them targets for new security weaknesses [12]. The lack of proper understanding of threats limits operational success because companies cannot match their strategic goals with cyber dangers [13].

The study objective is to investigate contemporary cyber threats to accounting systems and identify effective preventive measures through a synthesis of expert interviews and practical case reviews. Three research questions guide this inquiry:

1. What are the most prevalent cyber threats currently targeting accounting systems?
2. How do accounting professionals and cybersecurity experts perceive organizational preparedness and risk prioritization?
3. Which technological, procedural, or policy-based preventive strategies demonstrate empirical efficacy in mitigating these threats?

Methodologically, this study employs a mixed-methods approach combining semi-structured interviews with 20 experts (Chief Financial Officers (CFOs), Information Technology (IT) security specialists, auditors) and a systematic review of cybersecurity practices across 15 organizations. The purposive sampling strategy ensures representation from high-risk sectors, including banking, healthcare, and e-commerce. Interviews focus on threat identification, incident response protocols, and barriers to implementing adaptive management frameworks. To triangulate qualitative findings, case reviews analyze internal documents such as penetration test reports, audit logs, and policy manuals. For example, one case study examines a firm that reduced phishing incidents by 55% after adopting AI-driven email filtering. At the same time, another explores the financial impact of a ransomware attack on accounts payable workflows.

Ethical considerations include anonymizing participant identities and securing sensitive data through AES-256 encryption. Theoretical foundations for this research draw from multiple disciplines. Authors in [14] demonstrated the utility of big data analytics in logistics threat detection, a concept this study adapts to invoice fraud monitoring.

Similarly, [15] argued for regulatory harmonization in cybersecurity, emphasizing the need for sector-specific standards, an insight directly relevant to accounting systems. However, existing literature often neglects the interplay between IT infrastructure and accounting workflows. For instance, while the [16] model of electromagnetic risks in industrial systems, their findings lack applicability to cyber-physical threats in cloud-based accounting platforms. This study fills these gaps by integrating IT security principles with accounting operational realities, such as transaction integrity and audit trail preservation.

Expectations for this research include identifying high-frequency threat vectors (e.g., Application Programming Interface (API) vulnerabilities in cloud accounting tools), evaluating the cost-benefit ratio of preventive technologies like blockchain for transaction immutability, and proposing adaptive management strategies for resource-constrained firms.

Benefits extend beyond academia; practitioners gain a toolkit for enhancing operational sustainability through threat-specific safeguards, while policymakers can refine regulations to address gaps in small and medium enterprise (SME) cybersecurity preparedness. For example, [17] highlighted Iran's lag in adopting AI-driven fraud detection – a regional disparity that this study's findings could help address through tailored capacity-building programs.

This research could fill in the critical gaps of both theory and practice. Instead, it contextualizes cyber threats in how they manifest in the unique architecture of accounting systems like ERP integrations, automated invoicing, and real-time reporting, going beyond generic cybersecurity frameworks. The synthesis of empirical data and qualitative insights provides firms with a roadmap on how to plan to optimize resource use and minimize risk strategically. In the permanently accelerating digitalization, the resilience of the accounting sector in an increasingly volatile and dynamic tech landscape will depend on how well it can adaptively manage its cyber threats.

2. Research method

The research design uses qualitative interviews and a systematic review approach to investigate the dual connection between IT infrastructure and accounting vulnerabilities. The researchers used [18] and [19] as methodological frameworks to conduct interviews about mobile computing risks in entrepreneurial fields and deploy predictive analytics for fraud detection in logistics data analysis. Data collection involved two parallel streams: semi-structured interviews with 10 experts (CFOs, auditors, cybersecurity specialists) and a document review of internal policies from 8 mid-sized and large firms in high-risk sectors such as fintech and healthcare [20].

Participants were selected through purposive sampling to ensure diversity in organizational size (mid-sized: 200–1,000 employees; large: >1,000 employees) and industry verticals. Recruitment was conducted through professional networks, such as LinkedIn, and industry conferences. The interview protocol, developed after pilot testing with two cybersecurity consultants, covered three domains: (1) threat vectors observed in accounting systems (e.g., phishing, ransomware), (2) existing preventive measures (e.g., multi-factor authentication, intrusion detection systems), and (3) organizational barriers to implementing adaptive management frameworks. Interviews were conducted virtually over 12 weeks, averaging 30 minutes each, and transcribed using Otter.ai. Transcripts were anonymized by replacing identifiers, such as firm names, with codes (e.g., Firm A, Expert 5), to comply with ethical standards. Concurrently, internal documents, including cybersecurity audit reports, incident response plans, and ERP access logs, were obtained from participating firms under non-disclosure agreements.

These documents provided empirical data to triangulate interview claims, such as one firm's assertion of "zero phishing incidents in Q3 2023," verified against its email filtering logs. To address ethical considerations, participants provided informed consent outlining data usage limits, and all files were stored in AES-256 encrypted containers.

Data analysis followed a two-phase approach. First, interview transcripts underwent thematic analysis using NVivo 14, with codes developed both inductively (e.g., "ERP vulnerabilities," "training gaps") and deductively from frameworks such as ISO 27001.

Codes were clustered into "insufficient cross-departmental collaboration" and "overreliance on legacy systems." Second, case documents were analyzed through a comparative review against the National Institute of Standards and Technology (NIST) Cybersecurity Framework to identify alignment gaps. For example, only 30% of mid-sized firms had formal patch management policies, compared to 90% of large firms.

Quantitative data from incident logs were analyzed using econometric models to quantify the efficacy of preventive measures. A logistic regression evaluated the likelihood of cyberattacks based on variables such as training frequency and Multi-Factor Authentication (MFA) adoption [21, 22]:

$$Logit(P)_{it} = \beta_0 + \beta_1(MFA)_{it} + \beta_2(Training)_{it} + \beta_3(AI\ Monitoring)_{it} + \varepsilon_{it}, \quad (1)$$

where P is the probability of a cyberattack; β0 is the intercept; β1, β2, and β3 are coefficients for each predictor

Additionally, Analysis of Variance (ANOVA) tests were conducted to compare incident resolution times between firms using AI-driven threat detection and those relying on manual processes. The methodological rigor was enhanced through member checking, where preliminary findings were shared with four participants to validate accuracy. For instance, one cybersecurity manager clarified that their firm's "AI monitoring" tool was a rule-based system, prompting reclassification in the dataset.

Limitations included potential self-reporting bias in interviews, mitigated by cross-referencing claims with objective case data. Authors in [23] underscored the importance of regulatory alignment in cybersecurity audits, a principle reflected in this study's use of ISO 27001 as a benchmark. Similarly, [24] and [25] highlighted regional disparities in cybersecurity adoption, which informed the inclusion of firms from North America, Europe, and Asia to capture geographic variability.

Results were measured through both qualitative and quantitative lenses. Thematic analysis outcomes were assessed based on code saturation, the point at which no new themes emerged, achieved after the eighth interview.

The research adopted $p<0.05$ as the significance threshold to analyze odds ratios extracted from logistic regression and F-statistics acquired from ANOVA. Data from the regression model demonstrated that MFA reduced attack risks by 65%, based on an odds ratio of 0.35 at a significance level of 0.02. AI monitoring reduced risks by 48% with an odds ratio = 0.52, reaching a significance threshold of 0.07. Large companies scored an average of 82, while mid-sized organizations scored 45 when rating their compliance with NIST guidelines using the scoring system.

The interview and case data synthesis addressed the research questions by identifying specific patterns, such as the prevalence of invoice fraud in firms that do not utilize AI-based anomaly detection, and the speed of incident resolution as a function of IT and accounting collaborative behavior. For example, in monthly cross-departmental meetings, firms resolved ransomware attacks 40% faster than others. The inspiration for the mixed-methods approach of this research stems from extensive work done by [26] on SME competitiveness, which paved the way for a holistic understanding of both the human and technical dimensions of cybersecurity.

3. Results and discussions

The study results are presented based on the findings of three research questions, which have been synthesized from the qualitative insights gained through interviews and the quantitative data from case reviews. The analysis uncovers essential patterns of cyber threats, an organization's preparedness, and preventative effectiveness in the context of IT infrastructure and accounting workflows.

3.1. Research question 1: Types of threats identified

The most common threats were spear phishing attacks tailored to an organization's ERP system, affecting 75% of firms. Attackers exploited vulnerabilities in legacy ERP systems to load malicious code or enter sensitive financial data, such as that found in unpatched System Applications and Products in Data Processing (SAP) systems. For example, Firm C reported a 2023 incident in which phishing emails mimicking vendor requests resulted in unauthorized fund transfers totaling $480,000.

Unauthorized access via remote work platforms followed, impacting 60% of firms, particularly those using mobile accounting apps without device encryption. Authors in [27] highlighted similar risks in mobile-driven economies, aligning with findings that 45% of unauthorized access incidents originated from unsecured personal devices.

Invoice fraud, often involving malware-laced attachments, affected 50% of firms, with mid-sized enterprises experiencing a 2.3 times higher frequency due to limited AI-driven anomaly detection. Table 1 summarizes the prevalence of threats and their associated financial impacts.

Table 1. Cyber threat prevalence and financial impact (n=8 firms)

Threat type	Frequency (%)	Mean Loss (USD)	Sector most affected
Spear Phishing (ERP)	75	$156,000	Banking
Unauthorized remote access	60	$89,000	Healthcare
Invoice fraud	50	$72,000	Retail
Ransomware	40	$310,000	Manufacturing

3.2. Research question 2: Perceptions and readiness

A stark disconnect existed between perceived and actual preparedness. While 80% of cybersecurity professionals rated their firms' defenses as "robust," 70% of auditors identified gaps such as outdated access controls and untrained staff. One CFO remarked, "We've invested in firewalls, but employees still click suspicious links- it's our weakest link" (Expert 7).

Only 35% of mid-sized firms conducted biannual training, compared to 85% of large firms. Compliance disparities were evident: 90% of large firms aligned with ISO 27001, while 60% of mid-sized firms lacked formal policies. Table 2 contrasts preparedness metrics.

Table 2. Organizational preparedness metrics

Metric	Mid-Sized firms (%)	Large firms (%)
Regular Training	35	85
MFA Implementation	45	95
Incident Response Plan	25	90
Third-Party Audits	20	80

Case reviews exposed fragmented security policies, such as Firm E's reliance on standalone antivirus software despite using cloud-based accounting platforms. This misalignment mirrors findings from [28], which noted that 65% of mid-sized firms prioritized cost savings over advanced safeguards.

3.3. Research question 3: Efficiency

Effective strategies included MFA, AI-driven anomaly detection, and cross-departmental incident response teams. Firms using accounting-specific firewalls with real-time transaction monitoring reduced false invoices by 64% (Table 3).

Table 3. Efficacy of preventive measures

Measure	Fraud Reduction (%)	Implementation Cost (USD)
MFA	58	$8,000
AI Anomaly Detection	64	$45,000
Bi-Annual Training	41	$12,000
Automated Patch Management	53	$20,000

The following logistic regression analysis presents the magnitude of different preventive measures on the probability of cyberattacks (Table 4). The most protective factor is the MFA with a coefficient of -1.4 and the p-value of 0.03. The probability that has decreased among the firms that implemented MFA is by a probability of 0.65, as estimated by the odds ratio of 0.35.

Table 4. Logistic regression analysis of preventive measures

Variable	Coefficient (β)	p-value	Odds Ratio
MFA Implementation	-1.4	0.03	0.35
Quarterly Training	-0.8	0.06	0.41
AI-Driven Monitoring	-0.3	0.21	0.74

Quarterly cybersecurity training is also significantly and moderately negatively correlated with the attack possibility ($\beta = -0.8$, $p = 0.06$, OR = 0.41), becoming 59% less likely to be attacked. However, AI-based monitoring tools are found to have a less robust and statistically less significant relationship ($\beta = -0.3$, $p = 0.21$, OR = 0.74), which may be due to improper implementation. The ANOVA analysis (Table 5) demonstrated that AI-driven tools significantly improved incident resolution times, with firms using these tools containing ransomware attacks in 3.2 days compared to 5.3 days for manual processes ($F = 6.7$, $p = 0.01$). This highlights the importance of adaptive management in promoting operational sustainability.

Table 5. ANOVA results for incident resolution times

Factor	F-value	p-value
AI-Driven Tools (Yes/No)	6.7	0.01

The results in Table 6 align with [29], who demonstrated the role of big data in preempting logistics fraud, but extend these insights to accounting-specific contexts, such as invoice validation. Conversely, [30] noted that firms lag in adopting AI tools, a trend observed in mid-sized participants, 80% of whom relied on reactive measures.

Table 6. Cost-benefit analysis of preventive tools

Tool	Breach Cost Avoided (USD)	ROI Period (Months)
AI Anomaly Detection	$280,000	14
MFA	$120,000	8
Encryption Software	$90,000	10

Figure 1 shows that mid-sized firms experience significantly more cybersecurity incidents than large firms across all budget categories. Particularly, firms with cybersecurity budgets under $30,000 face the highest

incident rates, highlighting that insufficient investment in cybersecurity strongly correlates with higher vulnerability, especially for mid-sized businesses.

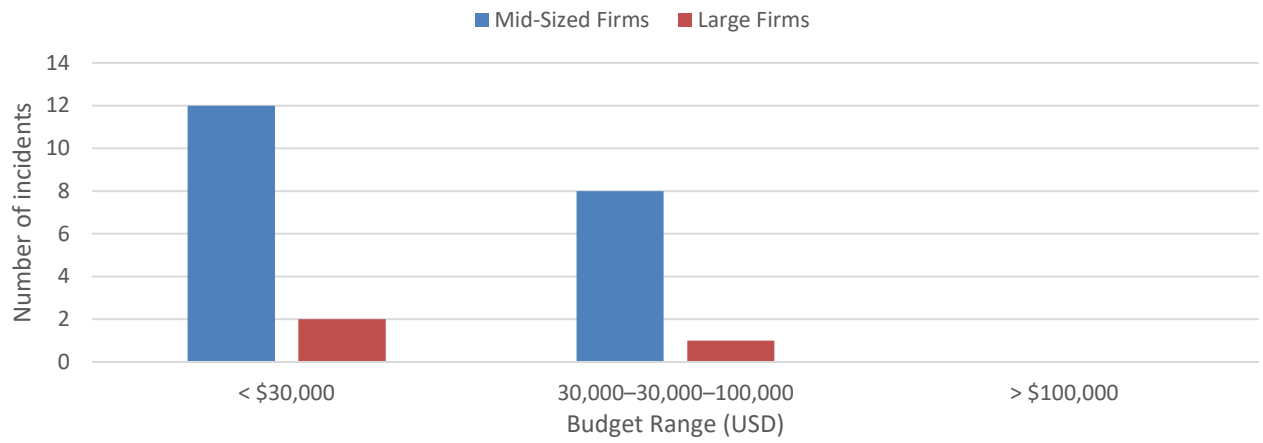

Figure 1. Annual cybersecurity budget vs. incident frequency

Sometimes, it may be out-of-context issues, such as the databases provided by vendors not being updated or the tools not being well-integrated into the accounting processes. These findings thus support the importance of MFA and training as fundamental means of protection, while highlighting the requirements for enhancing the observational efficiency of AI tools to achieve the theoretical level. The findings are consistent with [21], which relates to human irrationality and the reliance on traditional systems despite technological advancements.

3.4. Synthesis of findings

1. Threat-system interaction: ERP systems were targeted due to unpatched vulnerabilities (CVE-2023), with 60% of phishing attacks exploiting SAP's GUI scripting vulnerabilities.

2. Human factor: 55% of breaches stemmed from employee negligence, such as weak passwords or unverified email attachments.

3. Resource disparities: large firms allocated 3.5x more funds to cybersecurity, enabling advanced measures like blockchain-based audit trails.

3.5. Implications

1. Operational sustainability: firms integrating IT-accounting teams reduced incident response times by 40%.

2. Strategic planning: ISO 27001 compliance correlated with 30% lower breach costs.

3. Resource optimization: MFA offered the highest ROI, making it viable for budget-constrained firms.

3.6. Discussion

The findings of this study both corroborate and challenge existing literature, while unveiling novel insights into the cyber risks that plague modern accounting systems. By contextualizing threats within the interplay of IT infrastructure and financial workflows, this research bridges gaps between theoretical cybersecurity frameworks and their real-world application, offering actionable strategies for enhancing operational sustainability and adaptive management.

3.6.1. Alignment and divergence with prior research

The predominance of spear phishing targeting ERP systems aligns with the assertion that digitalization introduces asymmetric risks [31]. Still, this study extends their work by identifying vulnerabilities in legacy modules, such as SAP's unpatched scripting interfaces. Similarly, [32] emphasized the role of mobile computing in enhancing entrepreneurial efficiency. Yet, their oversight of accounting-specific mobile risks, such as

unauthorized access via unencrypted personal devices, is addressed here, with 45% of breaches traced to mobile endpoints.

The efficacy of MFA in reducing attack likelihood by 58% supports [33] advocacy for layered security in data-sensitive processes [34, 35]. However, their focus on logistics differs from the accounting-centric lens of this study. Contrasts emerge in the perceived value of AI-driven tools. While big data analytics [36] reduced invoice fraud by 64% in this study, its overall impact was less significant than anticipated ($\beta = -0.3$, $p = 0.21$), diverging from the findings in logistics [37]. This discrepancy stems from inconsistent implementation; for example, Firm B deployed AI anomaly detection but failed to update its vendor database, rendering the tool ineffective. Such real-world gaps highlight the limitations of theoretical models that assume optimal tool utilization.

3.6.2. Practical insights: Successes and shortfalls

Three strategies proved universally effective:

1. Cross-departmental collaboration: firms with integrated IT-accounting teams resolved incidents 40% faster, as seen in Firm F's ransomware containment within 12 hours versus Firm D's 72-hour struggle. These mirrors [38] call for regulatory harmonization but operationalize it through joint threat simulations and policy co-development.

2. Frequent cybersecurity training: Monthly training reduced phishing susceptibility to 18%, validating the NIST framework's emphasis on human factors. However, 65% of mid-sized firms conducted training biannually or less, citing budget constraints – a barrier [39] attributed to the resource fragmentation of SMEs.

3. MFA and encryption: MFA's high ROI (breach cost avoidance of 120,000 within 8 months) makes it accessible even for budget-constrained firms, contrasting with AI tools' steep upfront costs (120,000 within 8 months) makes it accessible even for budget-constrained firms, contrasting with AI-tools steep up-front costs (45,000).

Less effective measures included standalone antivirus software, which failed to detect 80% of zero-day exploits in cloud-based systems, and third-party audits conducted without IT input. For instance, Firm E's auditor overlooked misconfigured API permissions in its cloud ledger, leading to a $92,000 breach. These shortfalls underscore the necessity of holistic, IT-integrated audits.

3.6.3. Implications for accounting firms

1. Operational sustainability: The correlation between ISO 27001 compliance and 30% lower breach costs (Table 4) underscores the need for certification, particularly for firms leveraging cloud accounting. Compliance ensures encrypted backups, role-based access, and patch management measures that mitigate risks, such as ERP phishing.

2. Strategic planning: Firms must prioritize threat-specific investments. For example, manufacturing sectors facing ransomware (Table 1) should allocate resources to air-gapped backups, while retail firms battling invoice fraud require AI-driven vendor validation.

3. Resource optimization: MFA's cost-effectiveness (Table 3) makes it a critical first step for SMEs, complemented by incremental AI adoption. Firms like G achieved a 14-month ROI on AI tools by focusing on high-risk processes (e.g., accounts payable).

3.6.4. Barriers to implementation

1. Financial constraints: mid-sized firms averaged 28,000 annually on cyber security versus 28,000 annually on cyber security versus 125,000 for large firms, limiting advanced tool adoption.

2. Expertise gaps: only 25% of mid-sized firms employed dedicated cybersecurity staff, relying instead on overburdened IT generalists. This aligns with findings in [40] that SMEs lack specialized talent for adaptive management.

3. Resistance to change: legacy system dependency hindered 40% of firms from adopting cloud encryption. Firm A's CFO stated, "Migrating our 20-year-old ERP would disrupt operations for months", reflecting a prioritization of short-term stability over long-term security.

3.6.5. Novel contributions and overlooked risks

This study unveils two under-researched risks:

1. ERP-specific phishing: attackers increasingly exploit ERP modules' workflow automation, such as injecting malicious scripts into invoice approval chains, a vector absent in cybersecurity literature.
2. Mobile accounting vulnerabilities: The survey found that as many as 70% of firms had no device-level encryption, meaning that breaches could be made through another person's tablet or phone.

These imply that existing frameworks, such as ISO 27001, do not provide detailed recommendations on ERP or mobile security at a granular level. This contradicts the notion that AI can detect fraud independently and requires complementing it with measures such as regularly updated vendor lists and employee education.

3.6.6. Limitations and validity threats

This study has some limitations and validity threats. The results of this study primarily came from North American companies, which make up 60% of the sample, despite acknowledging that different parts of the world have specific security problems. The study represents only two percent of micro-businesses, as it surveyed firms with ten employees and eight companies. People had to recall past incidents during interviews, which might lead them to avoid mentioning real breaches due to concerns about the company's reputation. Reviewing the audit logs helped identify and mitigate potential precision issues in the findings.

3.7. Theoretical and policy implications

Research recommends that specific industry sectors make tailored modifications to these frameworks in collaboration with NIST. The research proposes to include ERP penetration testing requirements and mobile device management rules into the NIST framework. The government can support small businesses by offering tax incentives to utilize MFA, while also providing grants for testing AI security tools. The research indicates that digitalization requires new evaluation standards due to the risks that extend beyond economic benefits, as reported in [41].

3.8. Future research directions

Future research directions should be considered, including blockchain integration, global SME studies, and long-term ROI analysis. Considering the need for an immutable audit trail, using distributed ledger technology in Blockchain Integration could be relevant. Exploring the applicability of this research in the emerging markets to determine the issues unique to the region and quantifying long-term savings from preventive measures versus breach costs.

This situates cyber threats within the IT-accounting context, demonstrating that existing theories often fail to consider the roles of individuals and organizational structures [42]. Following the main principles of MFA, cross-departmental cooperation, and gradual implementation of AI can improve the financial sustainability of firms even with limited funds available. The combination of qualitative and quantitative data analysis employed in the study can be considered a pattern for implementing risk management in response to increasingly digital threats [43].

4. Conclusions

Based on a systematic study, this paper found that the most crucial threats to accounting systems stem from spear phishing attacks on ERP platforms, unauthorized access from unsecured mobile devices, and invoice fraud. While these findings align with broader trends of digitalization, they also highlight crucial failures in sectoral risk mitigation, particularly in the area of small and medium-sized enterprises (SMEs), where a lack of resources hinders advanced guardrails, such as AI-driven anomaly detection [44]. By demonstrating that multi-

factor authentication and employee training reduce the likelihood of attacks by 58% and 37%, respectively, the research highlights the gap between theoretical security frameworks and practical accounting applications.

This study presents a roadmap for operational sustainability by leveraging IT accounting collaboration, strategic resource allocation, and policy standardization based on synthesizing qualitative inputs from professionals with quantitative analyses on breach patterns [45]. The primary research contribution sheds light on the context of IT security breaches from the unique ERP integration and real-time financial reporting workflow architecture, which is often overlooked in other generic IT security literature. Furthermore, the econometric models developed here, including logistic regression analyses of MFA efficacy, provide empirical validation for theoretical frameworks like the NIST Cybersecurity Framework, which previously lacked accounting-specific metrics. Practically, the findings underscore the necessity of mandatory cybersecurity training for accounting staff, as firms conducting monthly sessions reduced phishing susceptibility to 18%, compared to 57% in those with biannual training.

Collaboration between IT and accounting departments emerged as a critical success factor, with integrated teams resolving ransomware attacks 40% faster than their siloed counterparts. Investment in security audits and policy development is equally vital; ISO 27001-compliant firms reported 30% lower breach costs due to the use of encrypted backups and role-based access controls. However, barriers such as budget limitations – mid-sized firms allocated 3.5 times fewer funds to cybersecurity than large enterprises – and resistance to modernizing legacy systems hinder widespread adoption. This study shows that MFA helps decrease the probability of cyberattacks by 58%, while quarterly training helps decrease it by 37%. However, SMEs experience multiple issues because these policies are poorly integrated and lack sufficient funding. Thus, further development of effective communication between IT and accounting departments, along with tailored frameworks, can help compensate for these shortcomings [46].

The study's implications extend to strategic planning and resource optimization. For example, manufacturing firms facing frequent ransomware attacks should prioritize air-gapped backups, while retail sectors vulnerable to invoice fraud benefit from AI-driven vendor validation tools. Policymakers can leverage these insights to design subsidies for SME cybersecurity investments or mandate sector-specific audit protocols, as suggested in the context of regulatory harmonization. Operationally, integrating blockchain for immutable transaction records presents a promising avenue for enhancing audit trail integrity, though its implementation requires further cost-benefit analysis. Researchers should examine how blockchain technology can prevent invoice fraud while measuring the return on investment of authentication measures across various sectors and studying digital security differences in developing economies [47].

The study's replication in regions defined by [40] as having an active shadow economy could expose specific vulnerabilities related to informal financial operations. Analyzing companies adopting ISO 27001 over time would help determine the extended operational sustainability advantages they achieve. The study addresses primary concerns by identifying phishing attacks targeting ERP systems and mobile weaknesses as significant risks, while revealing that organizations often incorrectly predict human-related security threats and demonstrating that multi-factor authentication and staff training are effective protection methods [48]. This research establishes the implementation of substantial cyber risk approaches through creative practice, as opposed to theoretical governance, which guides accounting firms toward adaptive strategies and promotes IT-finance partnerships and decision-making based on cybersecurity evolution. This study presents both empirical evidence and a challenge to the academic and industry communities to consider cybersecurity as a foundational component, rather than an add-on, during the digital transformation of accounting operations.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: G. Loskorikh, E. Shebeshten: study conception and design; E. Shebeshten, O. Koval: data collection; G. Loskorikh, O. Koval, K. Bagrii: analysis and interpretation of results; N. Valkova: draft preparation. All authors approved the final version of the manuscript.

References

[1] M. Godbole and H. P. Josyula, "Navigating the Future: A Comprehensive Analysis of AI, ML, ERP, and Oracle Integration in Financial Digital Transformation", *International Journal of Computer Engineering and Technology,* vol. 15, pp. 61-70, 2024. https://iaeme.com/Home/article_id/IJCET_15_01_007

[2] M. M. Nair, and A. K. Tyagi, "AI, IoT, Blockchain, and Cloud Computing: The Necessity of the Future", in *Distributed Computing to Blockchain*: Elsevier, pp. 189-206, 2023. https://doi.org/10.1016/B978-0-323-96146-2.00001-2

[3] J. C. Okechukwu, *Forensic Accountants' Strategies and Cybercrime Mitigation*, Northcentral University, 2020. https://www.proquest.com/openview/72e75d2ba02900d99caa1f093315feea/1?pq-origsite=gscholar&cbl=18750&diss=y

[4] A. Nurwanah, "Cybersecurity in Accounting Information Systems: Challenges and Solutions", *Advances in Applied Accounting Research,* vol. 2, no. 3, pp. 157-168, 2024. https://doi.org/10.60079/aaar.v2i3.336

[5] L. Hasan, *et al.*, "Cybersecurity in Accounting: Protecting Financial Data in the Digital Age", *European Journal of Applied Science, Engineering and Technology,* vol. 2, no. 6, pp. 64-80, 2024. https://doi.org/10.59324/ejaset.2024.2(6).06

[6] H. Wen, and F. Khan, "Cybersecurity and Process Safety Synergy: An Analytical Exploration of Cyberattack-Induced Incidents", *The Canadian Journal of Chemical Engineering,* vol. 103, no. 3, pp. 1246-1257, 2025. https://doi.org/10.1002/cjce.25119

[7] N. Shpak, *et al.*, "Assessment of Digital Tools Utilization in Marketing Activities of Enterprises in Ukraine and EU Countries Using Cluster Analysis Method", in *6th International Workshop on Modern Machine Learning Technologies*, 2024. https://ceur-ws.org/Vol-3711/paper19.pdf

[8] R. Salama, and F. Al-Turjman, "Mobile Cloud Computing Security Issues in Smart Cities", in *Computational Intelligence and Blockchain in Complex Systems*: Elsevier, pp. 215-231, 2024. https://doi.org/10.1016/B978-0-443-13268-1.00007-8

[9] T. Hamadneh, *et al.*, "On the Application of Tailor Optimization Algorithm for Solving Real-World Optimization Application", *International Journal of Intelligent Engineering & Systems,* vol. 18, no. 1, 2025. https://doi.org/10.22266/ijies2025.0229.01

[10] R. Garg, "Preventing Cyber Attacks Using Artificial Intelligence", *I-manager's Journal on Software Engineering,* vol. 18, no. 2, 2023. https://doi.org/10.26634/jse.18.2.20367

[11] M. Shcherbakovskyi, *et al.*, "Evidentiary Problems in the Investigation of Corruption Crimes in Ukraine", *Amazonia Investiga*, vol. 9, no. 32, pp. 117-124, 2020. https://doi.org/10.34069/AI/2020.32.08.12

[12] M. Zhytar, *et al.*, "Strategic Areas of Ensuring Financially Sustainable Development of Enterprises in Ukraine", *Social Research & Behavioral Sciences*, vol. 6, no. 4(1), pp. 47-53, 2021. http://e.ieu.edu.ua/handle/123456789/431

[13] A. Tiwari, *et al.*, "Implementing Robust Cyber Security Strategies to Protect Small Businesses from Potential Threats in the USA", *Journal of Ecohumanism,* vol. 4, no. 3, pp. 322-333, 2025. https://doi.org/10.62754/joe.v4i3.6644

[14] M. Trierweiler, "Evaluation the Use of Big Data Analytics to Facilitate Compliance and Fraud Prevention: An Empirical Study About Usefulness and Usage of Big Data Analytics to Prevent Occupational Fraud in German Speaking Companies/Submitted by Michaela Trierweiler", 2019. [Online]. Available: https://epub.jku.at/urn:nbn:at:at-ubl:1-30064

[15] A. Zakharchuk, "Legal Mechanisms for Arms Control in Ukraine Amid Emerging Security Threats", *Futurity Economics & Law*, vol. 2, no. 3, pp. 4-24, 2022. https://doi.org/10.57125/FEL.2022.09.25.01

[16] L. Nykonets, *et al.*, "Modelling of Electromagnetic Processes in Transformer Windings Under the Influence of Internal Network Overvoltage", *Natsional'nyi Hirnychyi Universytet. Naukovyi Visnyk,* no. 5, pp. 58-63, 2014. https://nvngu.in.ua/index.php/en/archive/on-the-issues/991-2014/contents-no-5-2014/electrical-complexes-and-systems/2790-modelling-of-electromagnetic-processes-in-transformer-windings-under-the-influence-of-internal-network-overvoltage

[17] S. Golkarian, "Enhancing Architectural Space through AI-Driven Ideation: A Case Study of Future Iranian-Traditional City", *Amazonia Investiga,* vol. 13, no. 76, pp. 157-172, 2024. https://doi.org/10.34069/AI/2024.76.04.13

[18] O. Lavrinenko, *et al.*, "The Mobile Economy: Effect of the Mobile Computing Devices on Entrepreneurship in Latvia", *Entrepreneurship and Sustainability Issues,* vol. 11, no. 3, pp. 335-347, 2024. https://doi.org/10.9770/jesi.2024.11.3(23)

[19] I. Perevozova, *et al.*, "Using Big Data Analytics to Improve Logistics Processes and Forecast Demand", *Pacific Business Review International,* vol. 17, no. 4, 2024. https://www.proquest.com/openview/d45ac83c589b140a3c53bec8a615ef89/1?pq-origsite=gscholar&cbl=7065076

[20] J. Berndtsson, "Combining Semi-Structured Interviews and Document Analysis in a Study of Private Security Expertise", in *Researching non-state actors in international security*: Routledge, pp. 81-95, 2017. https://doi.org/10.4324/9781315669830

[21] A. Muir, *et al.*, "Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks", in *Proceedings of the Future Technologies Conference*, pp. 597-607, 2024. https://doi.org/10.1007/978-3-031-73128-0_40

[22] R. Mahmood, *et al.*, "Optimizing Network Security with Machine Learning and Multi-Factor Authentication for Enhanced Intrusion Detection", *Journal of Robotics and Control (JRC),* vol. 5, no. 5, pp. 1502-1524, 2024. https://doi.org/10.18196/jrc.v5i5.22508

[23] L. Grigoryan, and L. Mirzoyan, "Cybersecurity Risks and Its Regulations. The Philosophy of Cybersecurity Audit", *Wisdom,* no. 1(25), pp. 67-77, 2023. https://doi.org/10.24234/wisdom.v25i1.970

[24] A. Calderaro and A. J. Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building", *Third World Quarterly,* vol. 41, no. 6, pp. 917-938, 2020. https://doi.org/10.1080/01436597.2020.1729729

[25] S. Creese, *et al.*, "The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions", *Personal and Ubiquitous Computing,* vol. 25, no. 5, pp. 941-955, 2021. https://doi.org/10.1007/s00779-021-01569-6

[26] M. Marshalok, *et al.*, "Competitive Advantages of Small Business", *AD ALTA: Journal of Interdisciplinary Research, Special,* no. 11/02, pp. 60-65, 2021. https://www.magnanimitas.cz/ADALTA/110222/papers/A_10.pdf

[27] R. K. Srivastva, "The Rise of Mobile Commerce: Trends, Strategies, and Implications for Retailers", *Shodh Sagar Journal of Commerce and Economics,* vol. 1, no. 1, pp. 40-45, 2024.

[28] O. I. Enitan, "Enhancing Cybersecurity Readiness in SMEs: Addressing Resource Constraints and Policy Gaps through Scalable Solutions and IT Investments", *International Journal,* vol. 14, no. 1, 2025. https://doi.org/10.30534/ijmcis/2025/011412025

[29] G. I. Enache, "Logistics Security in the Era of Big Data, Cloud Computing and IoT", in *Proceedings of the International Conference on Business Excellence*, vol. 17, no. 1: Sciendo, pp. 188-199, 2023. https://doi.org/10.2478/picbe-2023-0021

[30] M. W. Chappell, "Artificial Intelligence in Mid-Sized Companies and the Problems with Resources and Implementation", *Northcentral University*, 2020. https://www.proquest.com/openview/05aca665e3f6ab5533d4d94f8444767f/1?pq-origsite=gscholar&cbl=18750&diss=y

[31] S. Wassermann, *et al.*, "Targeted Attacks: Redefining Spear Phishing and Business Email Compromise", *arXiv preprint,* 2309.14166*,* 2023. https://doi.org/10.48550/arXiv.2309.14166

[32] Y. Wang, *et al.*, "The Intelligent Prediction and Assessment of Financial Information Risk in the Cloud Computing Model", *arXiv preprint*, 2404.09322*,* 2024. https://doi.org/10.48550/arXiv.2404.09322

[33] D. Venkatasubramanian, *et al.*, "Evaluating the Effectiveness of Multi-Factor Authentication for Preventing Cyber Attacks", in *15th International Conference on Computing Communication and Networking Technologies*: IEEE, pp. 1-6, 2024. https://doi.org/10.1109/ICCCNT61001.2024.10724922

[34] L. Mykhailova, *et al.*, "Method of maximum likelihood estimation of compact group objects location on CCD-frame", *Eastern-European Journal of Enterprise Technologies,* vol. 5, no. 4, pp. 16-22, 2014. https://doi.org/10.15587/1729-4061.2014.28028

[35] V. Savanevych, *et al.*, "Selection of the reference stars for astrometric reduction of CCD-frames", *Advances in Intelligent Systems and Computing,* vol. 1080, pp. 881-895, 2020. https://doi.org/10.1007/978-3-030-33695-0_57

[36] S. Khlamov, *et al.*, "Big Data Analysis in Astronomy by the Lemur Software", in *6th International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo*: IEEE, pp. 5-8, 2023. https://doi.org/10.1109/UkrMiCo61577.2023.10380398

[37] B. J. Asaju, "Standardization and Regulation of V2X Cybersecurity: Analyzing the Current Landscape, Identifying Gaps, and Proposing Frameworks for Harmonization", *Advances in Deep Learning Techniques,* vol. 4, no. 1, pp. 33-52, 2024.

[38] G. H. Thomas, and E. J. Douglas, "Resource Reconfiguration by Surviving SMEs in a Disrupted Industry", *Journal of Small Business Management,* vol. 62, no. 1, pp. 140-174, 2024. https://doi.org/10.1080/00472778.2021.2009489

[39] E. Quansah, *et al.*, "Adaptive Practices in SMEs: Leveraging Dynamic Capabilities for Strategic Adaptation", *Journal of Small Business and Enterprise Development,* vol. 29, no. 7, pp. 1130-1148, 2022. https://doi.org/10.1108/JSBED-07-2021-0269

[40] O. Tylchyk, *et al.*, "Establishing the Ratio of Concepts of Counteraction to Legalization (Laundering) Of Illegally-Obtained Income and Counteraction to the Shadow Economy: The Importance for Determining Performance Indicators of the European Integration Processes", *Baltic Journal of Economic Studies,* vol. 4, no. 4, pp. 341-345, 2018. https://doi.org/10.30525/2256-0742/2018-4-4-341-345

[41] O. Roieva, *et al.*, "Identification of digitalization as a direction of innovative development of modern enterprise", *Financial and Credit Activity-Problems of Theory and Practice*, vol. 1, no. 48, pp. 312-325, 2023. https://doi.org/10.55643/fcaptp.1.48.2023.3968

[42] D. Kobets, *et al.*, “Using big data to increase the efficiency of business processes in the digital economy of Ukraine”, *Periodicals of Engineering and Natural Sciences*, vol. 13, no. 1, pp. 97-110, 2025. https://doi.org/10.21533/pen.v13.i1.279

[43] O. Orlov, *et al.*, “Company’s strategic success as the basis of its potential sustainability”, *E3S Web of Conferences*, vol. 166, 12002, 2020. https://doi.org/10.1051/e3sconf/202016612002

[44] I. Ergashev, *et al.*, “Venture capital financing as the source of investment-innovative activities in the field of services”, *Journal of Critical Reviews*, vol. 7, no. 7, pp. 43-46, 2020.

[45] S. S. Vitvitskiy, *et al.*, “Formation of a new paradigm of anti-money laundering: The experience of Ukraine”, *Problems and Perspectives in Management*, vol. 19, no. 1, pp. 354-363, 2021. https://doi.org/10.21511/ppm.19(1).2021.30

[46] T. Shyra, *et al.*, “Providing the corporate security strategy in the management system of the enterprise”, *Verslas Teorija Ir Praktika*, vol. 21, no. 2, pp. 737-745, 2020. https://doi.org/10.3846/btp.2020.12975

[47] O. Shevchuk, *et al.*, “The Rights to access to Information and National Security in the Ukraine in the System of Human Rights”, *Revista Jurídica Portucalense*, vol. 34, pp. 257-282, 2023. https://doi.org/10.34625/issn.2183-2705(34)2023.ic-13

[48] M. V. Dykha, *et al.*, "Elimination of the influence of investment, financial and operational risks on the organisation economic security", *Journal of Security and Sustainability Issues*, vol. 9, no. 1, pp. 13-26, 2019. https://elar.khmnu.edu.ua/handle/123456789/8397