E-ISSN: 2708-4523
P-ISSN: 2708-4515
Impact Factor (RJIF): 5.61
AJMC 2025; SP- 6(3): 154-158
© 2025 AJMC
www.allcommercejournal.com
Received: 17-07-2025
Accepted: 20-08-2025

Aishwarya Gajanan Panadi
Department of Commerce, Dr. D. Y. Patil Arts, Commerce and Science College, Pimpri, Pune, Maharashtra, India

Monika M. Jogdand
Department of Commerce, Dr. D. Y. Patil Arts, Commerce and Science College, Pimpri, Pune, Maharashtra, India

Corresponding Author:
Aishwarya Gajanan Panadi
Department of Commerce, Dr. D. Y. Patil Arts, Commerce and Science College, Pimpri, Pune, Maharashtra, India

Ensuring trust in transformation: Incident response and security readiness in next-gen accounting

Aishwarya Gajanan Panadi and Monika M Jogdand

DOI: https://www.doi.org/10.22271/27084515.2025.v6.i3Sa.813

Abstract

The accounting profession is changing rapidly as digital innovations shape how financial data is created, processed, and secured. While moving from manual bookkeeping and ledger reporting to software-based environments like Excel, enterprise resource planning (ERP) systems, and cloud environments has improved efficiency and accuracy, it has also introduced considerable cyber security risks. As accountants work with sensitive financial data, they are likely targets for cyber incidents from ransomware, phishing, illicit access, and data breaches. Although existing literature points to values of technologies like AI, block chain, cloud computing, and data analytics across the professional accounting landscape, research investigating the impacts of these systems on cyber security preparedness and resilience is lacking. There are key gaps related to process towards organizations understanding how accounting firms select, adopt and implement cyber security frameworks; how firms resolve skill deficits among their staff; and human factors with regard to behaviors and attitudes which can heighten cyber risk exposure. This study will apply a mixed-methods methodology implementing a combination of quantitative surveys and qualitative interviews. Auditors, chartered accountants, cost accountants and CPAs in a developing economy were purposively sampled through Google Forms and semi-structured interviews.

The quantitative portion measures the frequency of digital tools and the maturity of cyber security practices, while the qualitative portion examines lived experience of adopting digital technology, perceived vulnerabilities, and obstacles to adoption. Preliminary results indicate that while there has been an increase in AI and block chain adoption for audit efficiencies, fraud detection, and regulatory requirements, there has not been an adequate alignment of cyber security with employing those technologies. In fact, the study indicates that fraud reduction results become much better when AI is applied with maturity in applying cyber security practices. Large firms have reported as much as 25% speed up on audits because of AI. Human factors continue to be at risk: not many practitioners have sufficient cyber security awareness; and small to medium enterprises may not have the policies updated due to operating under tight budgets. Compliance with laws and regulations adds further strain on resources when you consider that laws and regulations change, staff training has to keep up - the practice doesn't have sufficient funds to adequately respond. In light of these findings, this study recommends the following: zero trust architecture, multi factor authentication, encryption strength (TLS 1.3, AES 256), annual penetration testing, employing AI for anomaly detection, clear written information security policy document, employee cyber security awareness training, vet third party integrations with the same cyber security standards, and to have clearly delineated incident response plans.

Keywords: Digital transformation, cyber preparedness, accounting cyber security, challenges, tools

1. Introduction

The accounting profession is experiencing a paradigm shift as technological advancements redefine the ways that financial data is collected, processed, and analyzed. The digital transformation of accounting throughout the years has progressed from paper based bookkeeping and reporting to today's highly automated cloud based programs and systems. These technologies also considerably lowering the time and costs of traditional accounting practices, and giving professionals the power to make better choices based on knowledge received in real-time from data inputted. Naturally, with the use of technology in current accounting practice comes accountability issues, and also security risk. Through their reliance on the technology, security of traditional accounting is now threatened through potential cyber-attacks and exploitations; for instance, data breaches, ransomware attacks, phishing, system intrusions, etc. Vulnerabilities to data security and security risks often become more critical considering accounting professionals often deal directly with personal or confidential financial client information, reporting business financial information, and preparing government regulatory reporting documents, all of which provide appealing opportunities for today's cyber criminals.

This research project will also assess risk of cyber security, cyber security frameworks employed, and their relevance in the digital environments of accounting and assess the degree of knowledge, training and awareness of accounting professions operating in the digital environment. Many studies have pointed out the positive aspects of digital technology and have discussed security risk but have not drawn definitive conclusions on the connections between technology adoption and action cyber security. The research will provide both practitioners and scholars with valuable contributions both in the form of specific recommendations to mitigate against cyber threats in digital environments of accounting and possible future directions for policy and training.

2. Literature review

2.1 Latul Hasan *et al.*, (2024) [1]

The research looks at the effect cyber security has on accounting practice with improvements in data integrity and client trust along with the need for continual training and cross disciplinary knowledge.

2.2 S. Sairam *et al.*, (2025) [3]

The study discusses critical areas where innovation has created a disruption in traditional practices, including ledger maintenance, auditing, taxation, and financial reporting. The research mentions key challenges of organizations faced when updating accounting practices with modern systems such as security concerns regarding data, changes in slow adapting firms and the lack of professionals in the labor market.

2.3 Yousif Hameed Nayyef (2024) [4]

This research investigates accounting transformations, considering the understanding, insights and challenges they cause. The research conclude that transformative technology has created a reconceptualization of traditional accounting practices that has changed and speedup accounting practices regarding the gathering and analysis of financial data.

2.4 D. Rajagopal, (2022) [5]

This research is designed to show how recent technologies have altered old ways of DOIng things. In particular, old ways only required to upgrading manually, one hour of being in a room, with (in most cases) no visual aid.

2.5 Dhimas Surya *et al.*, (2024) [7]

This research examines the existing literature on cyber-attacks against accounting information systems, concentrating on the causes, impacts and mitigation factors. Effective mitigation demands a multi-layered strategy combining strong technical safeguards (e.g., authentication, patching, backups), continuous staff training and governance, and advanced tools

3. Research Gap

Despite a growing body of academic literature that documents the digitalization of accounting the research attempting to empirically examine the evolution of cyber security risks as organisational practices have progressed through the digital adoption spectra is still very limited. Most of the existing research has focused on theorising the extensive potential benefits of broader risks associated with virtualised tools such as artificial Intelligence, block chain and cloud computing without a comprehensive evaluation of secure implementations, or whether organisations were adequately prepared to implement them. New research needs to look at how accounting firms, select and implement cyber security frameworks, and their engagement with skills gaps to ensure appropriate protections and level of adaptability against attacks focused on design-based outcomes on Al-driven, and cloud-based systems. Additionally, research should examine cyber security plans specifically tailored for accountants as well as how organisations are using block chain technology to secure the protection and management of financial data. There is an absolute need for mixed-method, real-world research of implementation of frameworks, human factors, and emerging technologies specific cyber security measures. This future agenda encompasses the shared priorities of: accounting firms, SMEs, framework adoption, skill gaps, block chain, AI, cloud**,** and program effectiveness**.**

4. Research methodology

This research utilizes both quantitative and qualitative studies. This approach allows for a holistic view of the technical, organizational, and human aspect of digital transformation in accounting. The research quantified auditors, accountants and academician's perception on used of digitalized accounting application on the accounting function. This research also employed, a quantitative method, to examine the relationships between digital transformation, and the cyber safety practices in the accounting profession. To obtain data on technology usage, cyber safety, and the risk management practices of accountancy professionals a precise questionnaire (also refer to, as a survey), was developed. The survey was developed from Digital transformation in accounting. A purposive sampling arrangement was used with accounting professionals. Primary data was collected through semi-structured interviews with Chartered accountants, Cost accounts, certified public accounts and structured surveys. The data was captured in Google Forms to capture the Quantitative data; it assisted in data gathering data from 80-100 people about digital transition in accounting, currently used tools adapting to the need of market structure, and future tools line OCR & ASN simplify processes. Qualitative data was collected through interviews of 8-10 people that incorporated more practical data related to the challenges faced by the organization in the transformation to the digital age and the associated benefits from upgrading to new technology. Secondary data was collected by the user of `legacy`, or previous tools of accounting like ERP, Tally Prime, Microsoft excel, Zoho software etc. Also from other academic and academic ad articles.

Table 1: High risk, low awareness, satisfied

Tools	Cyber-Risk Exposure	Cyber security Awareness	Satisfaction
Microsoft Excel	68% of spreadsheet breaches caused by human error breach	Only <20% of organizations actively mitigate spreadsheet risk	90-95%
TallyPrime	~43% of SMB attacks target small businesses like Tally users	Likely <50%—SMB staff often lack adequate training	80-88%
SAP S/4HANA	~80-90% of ERP deployments are vulnerable to misconfigurations & access control issues	Likely <50%—ERP security awareness remains low	87-90%
Zoho Books	84% of accounting firms saw phishing; 61% saw ransomware	Only 36% of employees can reliably spot phishing	88-89%

Table 2: Era features tools impact examples

Era	Key Features	Tools/Techniques Used	Impact on Accounting	Examples
Ancient Accounting	Manual record-keeping, clay tablets, papyrus	Stone tablets, tally sticks, handwritten ledgers	Basic recording of transactions	Clay tablets in Mesopotamia, Egyptian papyrus scrolls
Medieval Period	Double-entry bookkeeping introduced	Pen and paper, ledgers, journals	Improved accuracy and error detection	handwritten ledger books
Industrial Revolution	Standardized accounting practices, increased complexity	Typewriters, mechanical calculators	Supported growth of businesses and industries	Use of mechanical calculators, ledger books in factories
Early 20th Century	Introduction of accounting standards and audits	Manual accounting with calculators	Greater consistency, transparency, and trust	Introduction of GAAP (Generally Accepted Accounting Principles), manual book keeping techniques.
Late 20th Century	Computerized accounting systems, spreadsheets	Desktop computers, software like Excel	Automation of calculations, faster data processing	Microsoft Excel, early accounting packages like Peachtree
Early 21st Century	Enterprise Resource Planning (ERP) integration, cloud adoption	ERP software (SAP, Oracle), cloud platforms	Real-time data access, integrated business processes	SAP ERP systems, QuickBooks Online, Xero cloud software
Current Era	AI, automation, block chain, data analytics	AI-powered tools, block chain, Big Data analytics	Predictive insights, enhanced security, strategic decision-making	AI tools like Black Line, block chain for audit trails

4.1 Significance

Digital transformation has changed the accounting profession by automating tasks such as data entry and reconciliations, lowering human error and improving accuracy. Cloud-based tools offer real-time access to financial data whenever it is needed, therefore accelerating both decision-making and regulatory compliance through an automated audit trail, and frequent standards updates. Interfaces with ERP systems support more enriched financial reporting and allows accounting practitioners to shift from manual processing to advisory services, bolstering their place as financial stewards. Scalable platforms that leverage AI, block chain and ML capabilities provide predictive capabilities, aid in fraud detection and immutability of records that are increasingly important in a technology savvy world. There are also increased risks associated with cyber security created by these digital transformations. As per industry data, 70% of organizations reported cyber incidents while transforming their digital capabilities. 82% of the incidents are related to mismanaged digital transformation projects and in accounting firms, data security was viewed as a significant risk by 45% of accounting firms, with 82% reporting experiencing a cyber-security breach, and 72% of firms are increasing investment in their project for cyber security. While the benefits of digital transformation are clear, most SMEs and accounting firms remain ill-prepared with limited resources, training, and cyber security awareness; with less than one-third of organizations including cyber security training in their project. The professional accounting environment demonstrates a gap between the digital transformation of accounting processes and an organization's cyber security preparedness. The gap can be bridged by increased utilization of robust security practices, policymaker support, ongoing training and a secure implementation framework. For practitioners, educators, managers, and policymakers, presenting the need for increased cyber security measures will ultimately guide the profession towards building a future of secure technology-driven financial stewards of data in our increasingly digitized world.

4.2 Challenges

- **Growing Cyber Risk Landscape:** Firms' transition to cloud-enabled, connected accounting systems increases exposure to the risks of data breaches, ransomware and phishing, thus increasing the chances of unauthorized data access and theft of sensitive financial information.
- **Gaps in Cyber Awareness for Employees:** While accountants are trained to prepare financial reports, they have little cyber security knowledge which includes how to detect, respond, or prevent breaches of accounting software and applications.
- **Regulatory & Compliance Pressures:** As businesses face a myriad data-protection legislation and industry regulations, it takes considerable time and effort to continuously update their security policies as digital tools quickly evolve. Budget and Resources Limits In particular, small and mid-sized firms with limited budgets and time constraints may find it difficult to invest in preventive technologies and provide ongoing training and education to their staff regarding the organization's policy, procedures and technologies.
- **Integration & Adaptation Challenges:** In an era of accelerating digital transformation, organizations may

find the integration of traditional practices with the realities of new technologies brings an element of confusion and vulnerability. This requires organizations to be extremely wide-ranging and scope for progress. Organizations can develop an array of solutions to be modular in nature; implement, require ongoing training, and take reasonable actions to periodically update policies.

5. Findings

1. **Reduce Chances of Fraud:** AI, Block chain and Automation reduce fraud but only with mature cyber security agility frameworks - showcasing the difference in utilizing the tools.
2. **AI Increases Audit Depth & Productivity:** An EY pilot identified genuine fraud which required full scrutiny, while a Deloitte project estimated a ~25% decrease in AUDIT time and AUDIT costs. EY Boston's internal tests for fraud risk indicated 88% faster to detect fraud risk, and 94% accuracy when conducting complex evidence assessments.
3. **Block chain Increases Transparency with Trade-Offs:** Block chain provides a verifiable and transparent ledger to increase accuracy of transactions and reduce fraud opportunities. However, there are issues with the integration, regulatory approvals, scalability, privacy rights and energy use.
4. **Emerging Fragilities & Governance:** Digital platforms are introducing new vulnerabilities: AI "black box" complications and algorithmic biases Blockchain's treatment of uncertain and inconsistent situations in protecting privacy data. Mitigation of these challenges must be accompanied by strong governance, encryption, ethical action standards, and ongoing scrutiny-thinking
5. **Request for Structured Governance & Ethics Frameworks:** To meaningfully adopt these technologies, there will need a significant governance regimes; encryption protocols for sensitive data protection, continuous, ongoing training/learning; and development of rules of ethics which is point of orientation. In the absence of established governance, current artefacts/systems will risk perform poorly or even increase risk.

6. Recommendations

Inclusion of strong processes to establish a secure cyber environment employed will protect the processes around accounting's digital transformation. Consider, for example, employing Zero Trust Architecture to continuously validate access, multi-factor authentication, and encrypt data when stored and transmitted in an authenticated manner using TLS 1.3 and AES-256 (the strongest encryption protocols). Security audits and penetration tests should be conducted regularly (at least once per year) to uncover potential vulnerabilities, alongside continual / real-time security monitoring employing AI systems to notify practitioners of anomalies. The ability to respond quickly reduces exposure and ensures confidence in the firm's technology framework. Creating a written information security policy (WISP) for all employees to follow promotes consistent security measures, while security awareness training should address human errors. The firm should safeguard third-party integrations, secure communications, and the incident response plan, and maintain an organized process for quickly stopping a cyber-breach attempt. If possible, the employer should also be adopting an incident response plan to gather as much information as it can the event of a recognized breach or potential security incident. In conclusion, accounting firms have a defensible position in the management of secure financial data through accounting's digital transformation; protecting the position is critical as we move more into a - BECOME - through our transformations process.

7. Conclusion

AI, block chain, and cloud computing are transforming accounting with a greater efficiency, higher accuracy, and improved strategic insight but these technologies also require solid cyber security to stem against risk. AI-enabled tools, like EY’s fraud detection engine, reduce human time spent on audits by ~25% and also outperform traditional sampling in detecting anomalies. Accounting firms frequently lack a formal process to assess these tools and face challenges in mitigating risks like algorithmic bias and impaired “black box” decision-making processes. Block chain can provide an unalterable, cryptographically secure ledger that potentially reduces reconciliation and audit time by 60% and improves fraud detection by 30%, but adoption remains hampered by the complexity and environmental impact of the technology, regulatory uncertainty, issues with standardization, interoperability challenges, and the inherent vulnerabilities within smart contracts. And without robust cyber security, accounting firms leave themselves open to risk especially small and mid-size businesses (SME) that operate with little to no budget for elevated security, are less inclined to train employees, or are facing regulatory changes day-to-day. To protect against these risks, organizations using new or evolving technology should adopt comprehensive cyber security frameworks that include zero-trust architecture, multi-factor authentication, TLS 1.3/AES-256 encryption, penetration (Pen)-testing, AI-driven threat detection, incident response plans, policy governance, training for employees, and vetting of third-party suppliers. Digital tools offer life-changing advantages for accounting but without integrated cyber security and human capital investment, firms will never be able to feel confident about data integrity, trust and compliance in an entirely digital financial world.

References

1. Hasan L, *et al*. Cyber security in accounting: protecting financial data in the digital age. Deleted Journal. 2024 Nov 1;2(6):64–80. https://ejaset.com/index.php/journal/article/view/132 https://doi.org/10.59324/ejaset.2024.2(6).06
2. Sudhamathi RK. Artificial intelligence in accounting profession: a way forward. Asian J Res Banking Finance. 2022;12(3):7–9. https://doi.org/10.5958/2249-7323.2022.00012.8
3. Sairam S. Innovative accounting practices: bridging traditional methods with modern financial reporting. J Inf Syst Eng Manag. 2025 Mar 12;10(20s):186–192. https://doi.org/10.52783/jisem.v10i20s.3030
4. Nayyef YH. Transformations in the field of accounting and their impact on accounting practices: an analytical study to understand insights and challenges. J Humanit Soc Sci Res. 2024 Jul 17;3(3).

https://doi.org/10.33687/jhssr.003.03.0348

5. Rajagopal D. The transformation of accounting system into digital accounting in India. Int J Sci Res. 2022 Dec 5;11(12):1045–1048. https://doi.org/10.21275/sr221219212259
6. Why SMEs need to adopt business automation tools. Newman Web Solutions Agency. 2024 Aug 29. www.newmanwebsolutions.com/blog/business-automation-tools
7. Surya D, *et al*. Cyberattacks on the accounting profession: a literature review. Media Riset Akuntansi Auditing Informasi. 2024 Aug 30;24(2):255–272. https://doi.org/10.25105/v24i2.19953
8. Cybersecurity and the accounting sector. ACCA Global. https://www.accaglobal.com/uk/en/technical-activities/uk-tech/in-practice/2021/August/cybersecurity-and-the-accounting-sector.html
9. Cybersecurity in accounting: protecting financial data in the digital age. ResearchGate. https://www.researchgate.net/publication/385866387_Cybersecurity_in_Accounting_Protecting_Financial_Data_in_the_Digital_Age
10. A brief history of accounting: where did it start. Babington. https://babington.co.uk/insights/helpguidance/brief-history-of-accounting/
11. Cybersecurity an AI accelerator across the business. EY. https://www.ey.com/en_gl/insights/consulting/transform-cybersecurity-to-accelerate-value-from-ai
12. Abu Dabaseh *et al*. Exploring the role of digital transformation in mitigating accounting fraud: a cybersecurity perspective. Int Rev Manag Mark. 2025. https://econjournals.com/index.php/irmm/article/view/18490?utm_source=chatgpt.com