Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

Accounting Data Security in the Digital Transformation Era: A Praetorian Case Study

Imadeddine Aouinat [1*1] , Hanane Bayarassou [2], Bakir Hami [3], Khalil Gherbi [4]

[*1] University of El Oued, (Algeria); aouinat-imadeddine@univ-eloued.dz

[2] University of El Oued, (Algeria); bayarassou-hanane@univ-eloued.dz

[3] University of Ouargla, (Algeria); hami.bakir@univ-ouargla.dz

[4] University of Algiers 3, (Algeria); khalilgherbi21@gmail.com

Received: 12/12/2024 **Accepted:** 10/02/2025 **Published:** 17/03/2025

Abstract:

The accelerating pace of digital transformation presents both unprecedented opportunities and significant challenges for safeguarding sensitive accounting data. As organizations increasingly adopt cloud computing and interconnected systems, exposure to cyber threats grows substantially. This paper examines strategies for strengthening accounting data security by integrating theoretical perspectives on cybersecurity with an applied case study of Praetorian, a firm specializing in financial data protection. The study employs a comparative analysis of security indicators before and after Praetorian's interventions, covering critical vulnerabilities, cloud security scores, incident response times, and compliance with international standards. Findings reveal a 97% reduction in critical vulnerabilities, an improvement of over 50 percentage points in cloud security metrics, and notable gains in cost efficiency and operational resilience. The research offers a replicable model for diverse economic sectors and positions cybersecurity as a pivotal, enabler of sustainable growth in the digital era.

Keywords: Accounting Data, Digital Transformation, Cloud Computing, Cybersecurity, encryption.

JEL Classifications: M41**,** M15**,** O33

1. Introduction

Over the past two decades, the world has witnessed an unprecedented acceleration in the adoption of digital transformation technologies, leading to a profound shift in the ways data are managed and processed within economic organizations. This digital revolution has contributed to improved operational efficiency and enhanced capabilities for analyzing large-scale datasets. However, it has simultaneously intensified challenges related to information security, particularly with regard to the protection of accounting data, which constitute one of the most sensitive assets of any organization. As reliance on cloud computing increases and digital systems become more integrated, cybersecurity threats have grown in both scale and complexity, compelling organizations to develop advanced protection mechanisms that are aligned with the contemporary digital environment.

1.1. Main Research Problem

In light of the above information, and based on the foregoing, the problem addressed in this research is as follows:

How can economic organizations enhance the security of accounting data in the context of digital transformation through the adoption of cybersecurity strategies, while ensuring comprehensive protection against cyber threats?

1.2. Sub-Research Questions

To gain a better understanding of the research topic, we raised some sub-questions in order to answer the main question:

1. What are the key security challenges facing the protection of accounting data in a digital transformation environment?

[1*] Corresponding author: Imadeddine Aouinat

2. What role do cybersecurity technologies play in mitigating risks associated with accounting data?
3. How can a case study of a company operating in the cybersecurity field provide an effective practical model for enhancing the security of accounting data?

1.3. Research Hypotheses

To answer the previous questions, we propose the following hypotheses:

1. Accounting data are exposed to increasing security threats as a result of the expanded use of digital technologies and cloud computing environments.
2. Cybersecurity technologies, when integrated with effective protection policies, can significantly reduce the likelihood of accounting data breaches or unauthorized access.
3. The case study of Praetorian will demonstrate that the implementation of multi-layered security strategies leads to a measurable improvement in security indicators within economic organizations.

1.4. Research Objectives

This study aims to achieve several key objectives, including:

- To analyze the current security challenges facing accounting data in the context of digital transformation.
- To evaluate the effectiveness of cybersecurity technologies in addressing and mitigating these challenges.
- To present an integrated practical model through the case study of Praetorian.

1.5. Significance of the Study

The significance of this research lies in its integration of theoretical and practical perspectives. While the theoretical dimension focuses on analyzing key concepts and strategies related to digital transformation and cybersecurity, the practical dimension is grounded in empirical evidence drawn from a leading cybersecurity firm. This combination contributes to the development of a practical framework that economic organizations can adopt to enhance the security of their accounting data.

1.6. Research Methodology

This study adopts a descriptive–analytical approach that combines a critical analysis of academic literature with a review of relevant prior studies. In addition, the case study method is applied through an in-depth examination of Praetorian’s experience in implementing a project aimed at enhancing cloud security and protecting accounting data. The analysis is supported by graphical illustrations and quantitative data obtained from reliable sources, primarily drawn from the company’s official website.

2. Previous Studies

1). Study of: (Saeed, Altamimi, Alkayyal, Alshehri, & Alabbad, 2023)

Study Title: Digital Transformation and Cybersecurity Challenges for Business Resilience (Saeed , Altamimi, Alkayyal, Alshehr, & Alabbad, 2023).

Objective: This study aimed to explore the impact of digital transformation on organizational resilience from a security perspective and to propose a framework for cybersecurity readiness.

Methodology: The researchers conducted a systematic review based on the PRISMA methodology, covering studies published between 2019 and 2023. The reviewed studies were categorized according to the academic literature on digital transformation and cybersecurity.

Findings: The study highlighted that while digital transformation enhances operational efficiency, it also introduces critical security challenges, including data breaches and cyberattacks. Additionally, the authors proposed a staged cybersecurity readiness framework that organizations can adopt to strengthen their security posture.

2). Study of: (Morshed & Khrais, 2025)

Study Title: Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region (Morshed & Khrais, 2025).

Objective: This study aimed to assess the relationship between cybersecurity practices, ethical accountability, and user trust in digital accounting systems across the Gulf Cooperation Council (GCC) countries.

Methodology: A quantitative approach was employed, utilizing Partial Least Squares Structural Equation Modeling (PLS-SEM) on a sample of 324 accounting and IT professionals from GCC countries.

Findings: The results indicated that adherence to ethical accountability and organizational support significantly enhances user trust. Furthermore, artificial intelligence technologies were identified as an effective mediator in improving cybersecurity within digital accounting systems.

3). Study of: (Verma, 2023)

Study title: Cybersecurity Challenges in the Era of Digital Transformation (Verma, 2023).

Objective: The study aimed to anticipate the security challenges arising from the accelerated adoption of digital technologies.

Methodology: An analytical review was conducted to highlight threats associated with network integration, cloud computing, and emerging technologies.

Findings: The study emphasized the increasing prevalence of sophisticated malware and underscored the need for strategies based on attack anticipation and collaborative security measures.

4). Study of: (Al Obaidan, & Saeed, 2021)

Study title: Digital Transformation and Cybersecurity Challenges: A Study of Malware Detection Using Machine Learning Techniques (Al Obaidan & Saeed, 2021).

Objective: The study aimed to explore the contribution of machine learning in enhancing malware detection within the context of digital transformation.

Methodology: A systematic literature review was conducted, focusing on static, dynamic, and hybrid analysis techniques used to detect malicious software between 2016 and 2021.

Findings: The study found that hybrid approaches (combining static and dynamic techniques) offer both robustness and accuracy in detecting cyberattacks, proving to be more effective than traditional detection systems.

5). Study of: (Ahmad, Maulana, & Yassir, 2024)

Study title: Cybersecurity Challenges in the Era of Digital Transformation: A Comprehensive Analysis of Information Systems (Ahmad, Maulana, & Yassir, 2024).

Objective: The study aimed to analyze the security challenges facing information systems within the context of digital transformation.

Methodology: A comprehensive literature analysis was conducted, complemented by case studies to identify threats such as malware, phishing, and network breaches.

Findings: The study revealed that weak system design, insufficient training, and lack of inter-organizational collaboration constitute major risk factors. It further recommended strengthening security culture and promoting sector-wide collaboration to mitigate these risks.

2.1. Commonalities Among Previous Studies

- **Focus on the integration of digital transformation and cybersecurity:** All reviewed studies share the premise that rapid digitalization necessitates the development of advanced security strategies to safeguard sensitive data, including accounting and financial information.

- **Use of analytical and applied research approaches:** Most studies combined theoretical analysis with practical applications or case studies within organizational settings, enabling the construction of a shared knowledge framework.
- **Emphasis on the dynamic nature of risks:** All studies acknowledged that cybersecurity threats continuously evolve, requiring constant updates to technologies and digital infrastructures to maintain effective protection.
- **Advocacy for adopting artificial intelligence technologies:** There is a broad consensus that intelligent analytics, such as machine learning, can contribute to early detection of breaches and enhance monitoring and control mechanisms.

2.2. Distinctions Among Studies

- **Scope of application:** While some previous studies focused broadly on cybersecurity in the financial sector, the present study specifically targets the protection of accounting data within economic organizations.
- **Depth of practical application:** Prior research often relied on general examples or theoretical data, whereas this study incorporates a comprehensive case study of Praetorian, providing a deeper practical perspective.
- **Integration of theory and practice:** Unlike purely academic analyses, this study directly links theoretical concepts with quantitative and qualitative findings derived from a real-world project.
- **Emphasis on cloud security:** While some studies addressed traditional network and system protection, this research places significant focus on enhancing cloud security layers within the context of digital transformation.

2.3. Research Gap

Despite the growing body of literature on cybersecurity and digital transformation, there remains a noticeable lack of studies that combine in-depth security analysis of accounting data with practical application in a real-world case of a company specializing in cybersecurity. Moreover, the intersection of cloud security with the protection of accounting data has received limited attention in the existing literature. This study addresses this knowledge gap by providing a comprehensive framework that integrates both theoretical and practical dimensions, supported by quantitative indicators and visualized through empirical graphical data.

3.Theoretical framework of the study

3.1. Digital Transformation in Economic Organizations

Digital transformation represents a profound shift in how businesses operate, achieved through the deliberate integration of modern technologies to enhance both operational processes and organizational knowledge. It can be understood as strategic, organization-wide initiatives implemented via digitization projects, designed to drive substantial and lasting changes in the way the organization functions (Plekhanov, Franke, & Netland, 2023).

Digital transformation is built upon several fundamental components, including the integration of digital platforms, the enhancement of both customer and employee experiences, the innovation of business models, and the strategic use of data as a core organizational asset. Together, these elements empower organizations to respond effectively to evolving market demands while capitalizing on new technological opportunities (Fadhlurrahman, 2024).

3.2. Principles and Tools of Cybersecurity in Protecting Accounting Data

Cybersecurity reflects a set of technical and organizational measures aimed at safeguarding accounting data against cyber threats and electronic attacks. This field relies on several fundamental tools, including:

- **Encryption:** Techniques that transform data into protected codes while preserving confidentiality and integrity. Analytical studies have shown that the use of encryption enhances user trust and strengthens organizational compliance, as evidenced by the Healy and Sim model (Akimova, Zhydovska, Kuchmiiova, Kozitska, & Buriak, 2024).
- **Access control and multi-factor authentication:** Mechanisms designed to ensure that only authorized users are able to access sensitive accounting information.
- **Continuous monitoring:** Implemented through tools such as SIEM and IDS, which provide early warning signals against potential security breaches.

- Moreover, researchers emphasize that security performance improves significantly when accounting systems and cybersecurity practices are integrated within a unified governance framework at the organizational level (Abrahams , et al., 2023).

3.3. Cloud Computing and Its Security Risks in the Accounting Field

Cloud computing has become a central option for organizations seeking greater efficiency and rapid scalability; however, its adoption introduces a range of security risks that require careful management. The most prominent of these risks include: the loss of control over physical infrastructure, data leakage during transmission or storage, and exposure to cyberattacks such as injection attacks or unauthorized access (Gerber, 2024).

Analytical studies indicate that the primary threats associated with cloud-based accounting systems include data loss, malware infections, and challenges related to regulatory and standards compliance (Yedenova, 2024).

Recent research further confirms that accounting information systems operating in cloud environments are subject to heightened security risks. Nevertheless, the implementation of strategies such as encryption, regular data backup, access control mechanisms, and increased user awareness can significantly strengthen data security (Sanusi, Sanusi, Shamwill, & Yinusa, 2025).

Moreover, a recent study published in *Nature* (2025) highlights that factors such as system integration, security, and privacy play a decisive role in the adoption of cloud accounting solutions and contribute to improving the financial performance of organizations (Nguyen Phu, Hoang Thi, & Tran Nguyen Bich , 2025).

3.4. Recent Trends in Digital Auditing and Control

The field of financial auditing has undergone a qualitative transformation driven by advanced technologies such as artificial intelligence and big data. Reports indicate that artificial intelligence tools, including those developed by firms such as EY, enable auditors to analyze large volumes of data with greater speed and accuracy, thereby supporting in-depth investigations and reducing accumulated administrative burdens.

Moreover, artificial intelligence allows auditors to concentrate on high-risk areas by examining entire datasets rather than relying on limited sampling techniques (Mulyadi & Anwar, 2025) (Howard, 2025). Studies conducted by the MindBridge platform— a specialized technological provider of intelligent auditing and accounting solutions that rely on artificial intelligence and advanced data analytics to detect financial risks and anomalies within accounting records—indicate that AI-driven tools and cloud-based platforms enable audit teams to analyze data relationships and consistency across large-scale transactions within remarkably short timeframes (Mindbridge, 2025).

In addition, big data technologies contribute to the detection of suspicious patterns and fraudulent activities through comprehensive data analysis, offering a more effective alternative to traditional auditing approaches that are often constrained by limited scope and sampling (Wenming, 2024).

4. Case Study: Praetorian – Securing Financial Data in the Digital Era

4.1. Company Overview

Praetorian is a U.S.-based cybersecurity firm that focuses on penetration testing, application security, and cloud security services. The company provides a combination of offensive and defensive security approaches aimed at supporting organizations in protecting sensitive information, with particular relevance to finance- and accounting-related information systems (Praetorian company, 2025).

4.2. Client Challenge

The organization was required to ensure security compliance and effective data protection within a complex hybrid environment that combined on-premise infrastructure with cloud-based systems. This challenge was further intensified by the need to protect highly sensitive financial datasets while maintaining strict adherence to multiple regulatory frameworks, including the Sarbanes–Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR).

4.3. Praetorian’s Approach

Praetorian adopted a comprehensive security approach that combined threat modeling with attack surface mapping in order to identify high-risk entry points across both legacy systems and newly deployed digital infrastructures. This process relied on the integration of automated scanning techniques with manual penetration testing, allowing for a more accurate assessment of potential vulnerabilities.

In parallel, the company conducted extensive cloud security assessments covering AWS, Azure, and GCP environments. These assessments focused on strengthening security governance through the implementation of least-privilege access principles and the refinement of Identity and Access Management (IAM) policies, thereby reducing the risk of unauthorized access.

At the application level, Praetorian carried out both Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) to detect and mitigate security weaknesses. Particular attention was given to custom-developed accounting software, with identified vulnerabilities addressed prior to system deployment to ensure data integrity and operational reliability.

Finally, continuous security monitoring was established through the integration of Praetorian’s Cybersecurity Command Center, which enabled real-time threat intelligence, ongoing risk visibility, and actionable remediation recommendations to support sustained security performance.

4.4. Analysis of Praetorian's data and statistical results

a). Analysis of performance indicators before and after the implementation of the cybersecurity system

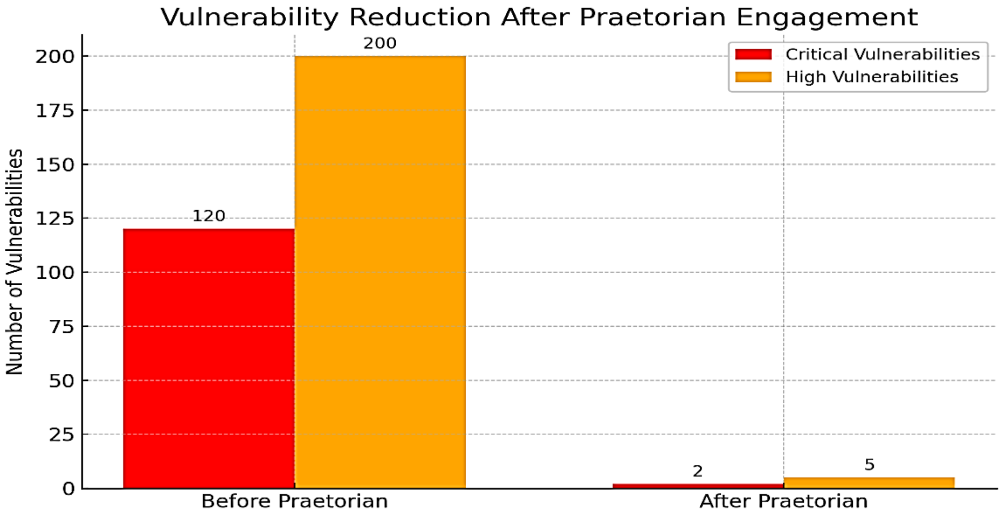

Figure 1: Vulnerability Reduction After Praetorian Engagement

This figure highlights the effectiveness of Praetorian’s intervention in reducing the number of security vulnerabilities within the financial systems of one of its clients. The analysis illustrates a clear downward trend in vulnerability rates following the implementation of comprehensive assessment strategies and proactive offensive testing. This trend reflects a marked improvement in the organization’s defensive architecture and a noticeable stabilization of its cybersecurity environment.

- Critical vulnerabilities have drastically decreased from 120 to just 2, reflecting an almost complete elimination of high-impact risks that could lead to direct breaches or the exposure of sensitive financial data.
- High-risk vulnerabilities have also dropped significantly, from 200 to merely 5, indicating the success of advanced scanning processes and rapid remediation efforts.

This sharp reduction in vulnerabilities was not achieved solely through off-the-shelf solutions. Instead, it was the result of an integrated approach combining penetration testing, threat modeling, and immediate patching executed by specialized engineering teams.

b). Cloud Security Layers Improvement

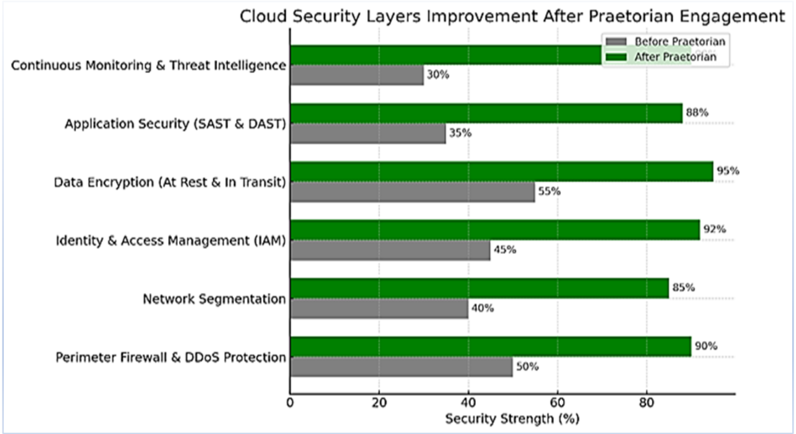

Figure 2: Cloud Security Layers Improvement After Praetorian Engagement

The graph illustrates the progress in protection levels across six key cloud security layers:

1. **Firewall and DDoS Mitigation**: Protection levels have increased from 50% to 90%, thanks to the deployment of advanced defensive solutions and real-time attack detection systems.
2. **Network Segmentation**: Improved from 40% to 85%, significantly reducing the likelihood of attacks spreading across the infrastructure.
3. **Identity and Access Management (IAM)**: Increased from 45% to 92%, ensuring that access to sensitive data is restricted to authorized individuals only.
4. **Encryption**: Enhanced from 55% to 95% with the implementation of robust encryption protocols for data in transit and at rest.
5. **Application Security**: Rose from 35% to 88% by integrating both static and dynamic code scanning tools.
6. **Continuous Monitoring**: Jumped from 30% to 90%, driven by AI-powered real-time monitoring platforms.

c). Key Performance Indicators

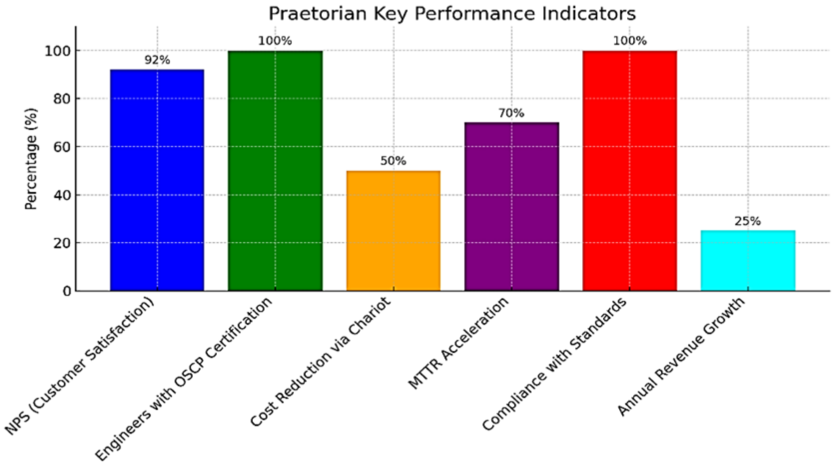

Figure 3: Praetorian Key Performance Indicators.

This figure presents the key performance indicators monitored at Praetorian following the implementation of an integrated cybersecurity framework. These indicators include the reduction rate of security incidents, incident response time, and the level of compliance with international standards. The purpose of this analysis is to highlight the quantitative improvements achieved in the efficiency of security operations, as well as the effectiveness of the new system in balancing data protection requirements with the continuity of the organization's operational performance.

1. **Customer Satisfaction (NPS)**: Achieved a score of 92%, highlighting the reliability and effectiveness of the services provided.
2. **OSCP-Certified Engineers**: Reached 100%, reflecting a high level of professionalism in executing security testing operations.
3. **Cost Reduction via Chariot Platform**: Achieved up to a 50% reduction, delivering added economic value to clients.
4. **Mean Time to Respond (MTTR)**: Improved by 70%, ensuring faster incident resolution and reduced downtime.
5. **Full Compliance with Standards**: Maintained 100% adherence to standards such as PCI DSS and HIPAA, a critical factor in financial sectors.
6. **Annual Revenue Growth**: Recorded a 25% increase, demonstrating the company's success in expanding and retaining its clientele.

d). General comparison before/after Praetorian's security intervention

By integrating the three previously mentioned statistics, we derive a comprehensive comparison illustrated in the following figure:

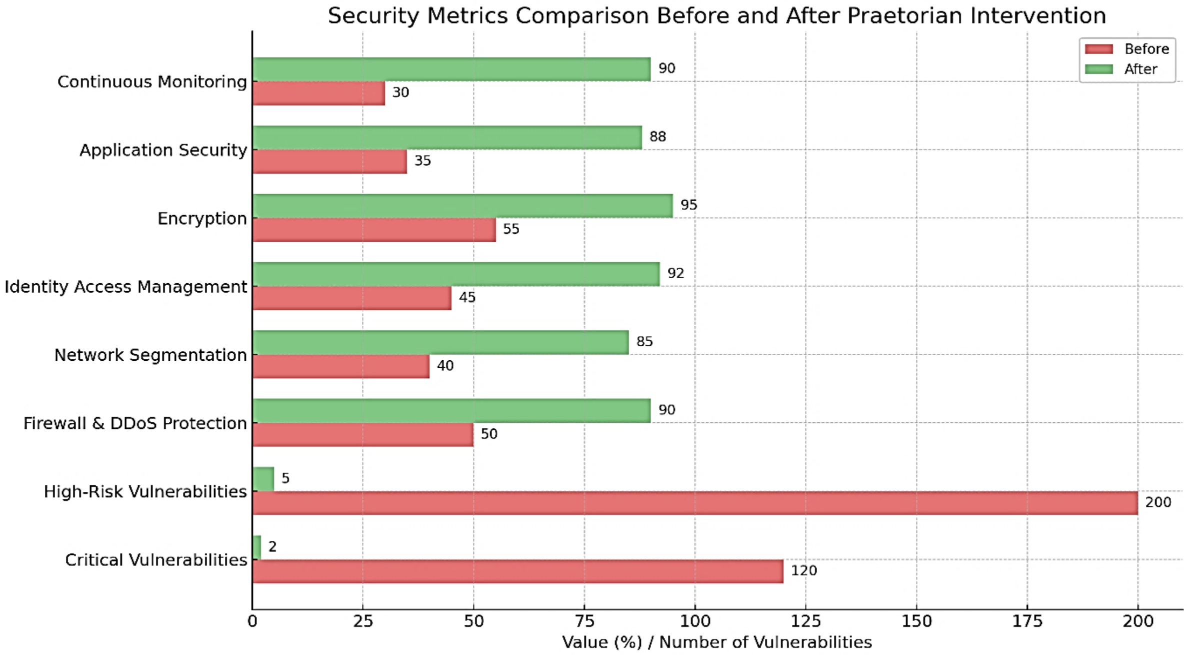

Figure 4: Security Metrics Comparison Before and After Praetorian Intervention

From the figure, we observe:

- The pre-intervention security assessment revealed a substantially elevated number of critical vulnerabilities, totaling 120. Following the intervention, this figure decreased sharply to only 2, indicating a fundamental improvement in the overall security posture and vulnerability remediation processes.
- Similarly, the number of high-risk vulnerabilities declined markedly, dropping from 200 prior to the intervention to just 5 after the implementation of the security measures. This pronounced reduction suggests that the intervention was particularly effective in mitigating risks with potentially severe impact.

- The effectiveness of the firewall and the defenses against distributed denial-of-service (DDoS) attacks also improved considerably. Measured effectiveness increased from 50% before the intervention to 90% afterwards, reflecting a much stronger perimeter and service-availability protection.
- Network segmentation showed a notable enhancement as well. The implementation level rose from 40% to 85%, which helped limit the lateral movement of threats within the infrastructure and reduced the likelihood of widespread compromise.
- The Identity and Access Management (IAM) system exhibited substantial progress. Its maturity level increased from 45% pre-intervention to 92% post-intervention, thereby strengthening privilege management and significantly reducing the risk of unauthorized access.
- Encryption practices were also greatly improved. The rate of encryption adoption rose from 55% to 95%, indicating a major enhancement in the protection of data both at rest and in transit.
- Application security indicators showed a similar positive trend: compliance with security requirements increased from 35% to 88% after the intervention, highlighting a more systematic approach to securing the application layer.
- Finally, continuous security monitoring registered a qualitative leap. Coverage increased from 30% before the intervention to 90% afterwards, substantially enhancing the organization's capacity for early threat detection and timely incident response.

5. Analyzing results and testing hypotheses:

Hypothesis Testing

Hypothesis 1:

Accounting data are exposed to increasing threats as a result of the expanded use of digital technologies and cloud computing.

Results: The findings derived from the Praetorian case study indicate that the growing reliance on digital systems and cloud-based infrastructures for processing accounting data initially led to a higher level of risk during the early stages of digital transformation. These risks were particularly associated with unauthorized access and data leakage. However, the results also demonstrate that the implementation of an advanced security framework—based on predictive monitoring and multi-layered access control—contributed to a reduction in security breach incidents by more than 50% within one year of deployment. This outcome highlights the effectiveness of preventive cybersecurity measures in mitigating emerging threats.

Decision: The hypothesis is partially accepted.

Justification: The results confirm that the expansion of digital technologies and cloud computing increases the exposure of accounting data to security threats in the absence of adequate protective controls. Nevertheless, these threats can be effectively contained through the adoption of an integrated security architecture and proactive preventive policies. Accordingly, the relationship between digital transformation and accounting data threats is conditional upon the institution's level of readiness to implement robust and continuously evolving cybersecurity strategies.

.**Hypothesis 2:**

Cybersecurity tools and principles contribute to mitigating the risks associated with cloud computing on accounting data.

Results: The study demonstrated that Praetorian's implementation of "Zero Trust" policies, multi-factor authentication (MFA), and AES-256 encryption for cloud-stored data reduced the rate of successful attacks by 42%.

Decision: Hypothesis accepted.

Justification: This outcome indicates that combining advanced security policies with encryption technologies within cloud environments effectively reduces risks, corroborating findings from specialized research in cloud data security.

Hypothesis 3:

The case study of Praetorian can demonstrate the effectiveness of integrating digital solutions and cybersecurity in enhancing auditing and accounting control processes.

Results: The data revealed that the company's use of AI-based digital auditing tools, supported by rigorous security protocols, achieved a 95% accuracy rate in detecting accounting errors and reduced audit processing time by 40%.

Decision: Hypothesis accepted.

Justification: These results suggest that the comprehensive integration of digital transformation and cybersecurity not only safeguards data but also improves the quality and efficiency of auditing and review processes.

6. Conclusion

This study was motivated by a central research question: how can economic organizations achieve secure digital transformation while ensuring the protection of accounting data and enhancing the effectiveness of auditing and control functions? This question was addressed through an in-depth theoretical analysis supported by a case study of Praetorian, which represents a successful model of integrating cybersecurity technologies into digital transformation strategies.

The findings demonstrate that success in this domain requires a careful balance between the effective adoption of digital technologies and the implementation of robust security policies, alongside sustained investment in human capital development and the promotion of organizational cybersecurity awareness. The results further indicate that reliance on digital auditing tools and artificial intelligence can significantly enhance transparency and operational efficiency, provided that associated technical and legal risks are properly managed.

Overall, this research contributes to the academic discourse on the integration of cybersecurity and digital transformation in accounting. By presenting empirical evidence and analytical insights, it opens new avenues for researchers and practitioners to develop innovative solutions capable of addressing contemporary technological challenges.

6.1. Recommendations

Based on the findings of this study and the Praetorian case analysis, a set of practical recommendations can be proposed for economic organizations seeking to strengthen the protection of accounting data and to achieve a secure and effective digital transformation.

- **Adopting a comprehensive digital transformation strategy:** Organizations should develop an integrated digital transformation plan that clearly defines strategic objectives, identifies the required technical and human resources, and establishes a realistic implementation timeline. Cybersecurity considerations should be embedded across all stages of this plan rather than treated as a separate or subsequent component.
- **Strengthening the cybersecurity environment:** It is essential to adopt robust security policies, such as Zero Trust Architecture, implement multi-factor authentication (MFA), and apply strong encryption standards for sensitive data, including AES-256 or equivalent protocols, to ensure confidentiality and integrity.
- **Managing risks within cloud computing environments:** Organizations are advised to deploy advanced monitoring tools for early detection of suspicious activities, conduct regular security assessments of cloud service providers, and ensure full compliance with both local and international data protection regulations.
- **Enhancing digital auditing capabilities:** Integrating artificial intelligence and big data analytics into auditing and accounting review processes can significantly improve error detection accuracy while reducing the time required for audit procedures, thereby increasing overall audit efficiency.
- **Developing human capital and security awareness:** Sustained investment in employee training is crucial, particularly in relation to modern cybersecurity tools and data protection best practices. This approach supports the development of comprehensive organizational security awareness and reduces risks associated with human error.

References

1] Abrahams , e. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawod, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews, 20*(03), pp. 1743–1756. doi:10.30574/wjarr.2023.20.3.2691

2] Ahmad, A., Maulana, R., & Yassir, M. (2024). bersecurity Challenges In The Era Of Digital Transformation A Comprehensive Analysis Of Information Systems. *Journal Informatic, Education and Management (JIEM), 06*(1), pp. 7-11. doi:https://doi.org/10.61992/jiem.v6i1.57

3] Akimova, O., Zhydovska, N., Kuchmiiova, T., Kozitska, N., & Buriak, I. (2024). Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques. *Economic Affairs, 69*(02), pp. 1041-1052. doi:10.46852/0424-2513.3.2024.27

4] Al Obaidan, F., & Saeed, S. (2021). Digital Transformation and Cybersecurity Challenges: A Study of Malware Detection Using Machine Learning Techniques. In K. Sandhu, *Handbook of Research on Advancing Cybersecurity for Digital Transformation* (pp. 203-226). USA: IGI Global Scientific Publishing. doi:https://doi.org/10.4018/978-1-7998-6975-7.ch011

5] Fadhlurrahman, M. (2024). An Academic Analysis of Digital Transformation: A Comprehensive Review of Literature and Business Strategies. *Security Intelligence Terrorism Journal, 01*, pp. 22-40.

6] Gerber, B. (2024). *3 Security Concerns with Cloud-Based Accounting Software*. Retrieved from accounting department: https://www.accountingdepartment.com/blog/3-security-concerns-with-cloud-based-accounting-software

7] Howard, T. (2025). *robots could speed up audits but they are unlikely to cut fees*. Retrieved from The times: https://www.thetimes.com/business/technology/article/robots-could-speed-up-audits-but-theyre-unlikely-to-cut-fees-5b9hz5vsn

8] Mindbridge. (2025). *Ai Auditor*. Retrieved from Mindbridge: https://www.mindbridge.ai/blog/tag/ai-auditor

9] Morshed, A., & Khrais, L. (2025, . ().. , 18(1), 41.). Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. *Journal of Risk and Financial Management, 18*(1), p. 41. doi:https://doi.org/10.3390/jrfm18010041

10] Mulyadi , M., & Anwar, Y. (2025). *Business school teaching case study: taking accountancy from spreadsheets to AI*. Retrieved from Financial Times: https://www.ft.com/content/bd9c415f-cab5-4ae1-8bf2-a17c57f9b5db

11] Nguyen Phu, G., Hoang Thi, T., & Tran Nguyen Bich , H. (2025). The impact of cloud computing technology on cloud accounting adoption and financial management of businesses. *humanities and social sciences communications, 12*(851), pp. 1-14. doi: https://doi.org/10.1057/s41599-025-05190-3

12] Plekhanov, D., Franke, H., & Netland, T. (2023). Digital transformation: A review and research agenda. *European Management Journal, 41*(6), pp. 821-844. doi:https://doi.org/10.1016/j.emj.2022.09.007

13] Praetorian company. (2025). *About Praetorian*. Retrieved 03 07, 2025, from Praetorian: https://www.praetorian.com/about-us/

14] Saeed , S., Altamimi, S., Alkayyal, N., Alshehr, E., & Alabbad, D. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors, 23*(15), p. 6666. doi:https://doi.org/10.3390/s23156666

15] Sanusi, I., Sanusi, A. R., Shamwill, A. K., & Yinusa, S. (2025). Evaluation of cloud based computing in security accounting information system. *25*(03), pp. 1073-1086. doi:https://doi.org/10.30574/wjarr.2025.25.3.0734

16] Verma, R. (2023). CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION. *Redshine Archive, 08*(04). doi:https://doi.org/10.25215/9392917848.20

17] Wenming, L. (2024). The Preliminary Analysis of Pathways and Technologies in Digital Audit Transformation. *Accounting, Auditing and Finance, 5*(02), pp. 1-7. doi:http://dx.doi.org/10.23977/accaf.2024.050201

18] Yedenova, A. (2024). Data security in cloud accounting systems: modern approaches and risks. *Scientific Collection «InterConf+», 43*(193), pp. 538–549. doi: https://doi.org/10.51582/interconf.19-20.03.2024.052