Journal of
Information System and Technology Auditing

Research Paper

Investigating the Impact of Cyberattacks on Digital Auditing based on Becker's Criminal [1,2]

Avan Jamshidi*[3] and Javad Jamshidi[4]

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 1, No. 1, Spring & Summer 2025
pp. 34-39

Received: 2025.02.09
Revised: 2025.07.02
Accepted: 2025.09.02

1. Introduction

Digital transformation and the adoption of modern technologies such as artificial intelligence, blockchain, and big data analytics have revolutionized auditing processes. These technologies enhance accuracy, transparency, and speed, significantly improving audit efficiency (Sirios et al., 2020). However, the increasing reliance on digital infrastructures has made auditing environments an attractive target for cyberattacks. These attacks, including financial data theft, data manipulation, ransomware, and disruptions to technological infrastructure, can severely threaten the security and credibility of digital auditing. According to Becker's criminal theory, criminals, including hackers, make decisions based on a rational analysis of costs and benefits. Suppose the costs of committing a crime (such as the likelihood of detection and punishment) are low and the benefits (such as access to valuable data) are high. In that case, the likelihood of criminal activity increases. In this framework, weak cybersecurity

---

[1] https://doi.org/10.22034/JISTA. 2025. 540907.1058
[2] Selected Paper of 22nd National Accounting Conference of Iran
[3] Ph.D., Department of Accounting, Faculty of Social and Economic Sciences, Alzahra University, Tehran, Iran/ Lecturer at National Skill University. (Corresponding Author) Email: t.jamshidi@alzahra.ac.ir
[4] Master's degree, Department of Law, Criminal Law and Criminology,Payame Noor University, Tehran, Iran. Email: javadjamshidi@yahoo.com

measures and the attractiveness of digital audit data make cyberattacks one of the most significant challenges in digital auditing. Cyberattacks not only threaten data security but also have broad economic and organizational consequences. These attacks impose direct and indirect costs on organizations, including expenses for data recovery, security infrastructure enhancement, and compensating affected stakeholders. These costs have significantly increased in recent years. Furthermore, disruptions in digital audit processes can undermine stakeholder trust in financial reports and damage organizational credibility (Ghosh & Sherman, 2021). On the other hand, analyzing cyberattacks within Becker's theoretical framework suggests that enhancing cybersecurity and reducing vulnerabilities can deter criminals. This requires identifying the behavioral patterns of cybercriminals and designing strategies to reduce the attractiveness of digital targets (Anderson & Moore, 2020). Additionally, legal reforms and stricter regulations play a crucial role in improving digital audit security (Boehm & Schwartz, 2021). In this Research the Question is How does Becker's criminal theory influence cyberattacks in digital auditing?

2. MATERIALS AND METHODS

This research is a qualitative method with a thematic analysis approach. Data were collected from two main sources: a study of documents and reports related to cyber-attacks and semi-structured interviews with experts in the field of auditing and cybersecurity. The interviews were conducted based on a predetermined framework, but participants were allowed to freely express their opinions and experiences. For data analysis, MaxQuda software was used, which allowed for initial coding, grouping of codes into main themes, and extracting relationships between them. In this research, a purposive sampling method was used and cybersecurity experts, auditors, and managers of organizations were selected. These individuals must have sufficient experience in the field of digital auditing and cybersecurity. Criteria such as at least 5 years of relevant work experience, knowledge of cyber threats and digital auditing, and experience in cyber risk management were considered

for their selection. Sampling was conducted by identifying qualified individuals in professional networks and using a snowball method in 1403, with some of the initial interviewees introducing other professionals. Interviews continued until theoretical saturation was reached, and after interviewing 15 people, the data became so repetitive that no new information was obtained.

3. RESULTS AND DISCUSSION

The study's data analysis categorized the effects of cyberattacks on digital auditing into five main areas:

1) Direct Impacts of Cyberattacks Cyberattacks directly impact the accuracy, reliability, and efficiency of digital auditing systems. These attacks can lead to financial data alterations, deletion of sensitive information, and disruptions in auditing processes. Some direct consequences include reduced accuracy of financial reports, system malfunctions, and diminished client trust in auditing procedures. When financial data is unintentionally altered, the credibility of audit reports is questioned, exposing organizations to legal challenges.
2) Risks and Costs Another major consequence of cyberattacks is the increase in security costs and legal risks. Organizations that experience cyberattacks must allocate significant resources for data recovery, security system enhancements, and compensating affected parties
3) Cybercriminals' Motivations Cyber attackers are primarily motivated by financial and informational gains. They exploit security weaknesses in auditing systems to steal sensitive data, manipulate records, and sell information on black markets. Some attackers also engage in economic espionage or sabotage against competitors. Given the low cost of executing cyberattacks and the readily available tools, attackers are increasingly targeting digital auditing systems.
4) Preventive Measures To counter cyberattacks, organizations must implement preventive measures. These include employee training on cybersecurity threats, adopting advanced security technologies such as blockchain and data encryption, and enforcing strict security policies.

Social and Ethical Consequences Cyberattacks have social and ethical ramifications beyond technical and financial damages. These include reduced public trust in digital auditing systems, concerns about data confidentiality, and legal challenges for auditors. In many cases, companies that fall victim to cyberattacks suffer significant declines in reputation and customer trust. Analysis Based on Becker's Theory Becker's criminal theory posits that increasing the costs of committing crimes can reduce criminal activity. In the context of cyberattacks, these costs include stricter legal penalties, improved security systems, and reduced access to hacking tools. The present study indicates that companies that invest more in cybersecurity and enforce stricter regulations are less likely to be targeted by cyberattacks.

4. CONCLUSION

This research demonstrates that cyberattacks pose a significant threat to digital auditing and can have substantial financial and reputational consequences. Key findings emphasize the following: Strengthening cybersecurity and training employees should be a top priority for organizations. Increasing the cost of committing cybercrimes can reduce attackers' motivations. Policymakers and managers must adopt a comprehensive and proactive approach to combating cyberattacks. Given the growing importance of digital auditing in the modern world, addressing cyberattacks is not just a technical necessity but also a strategic imperative. Previous studies highlight that cyberattacks have become one of the main challenges in digital auditing processes. Recommendations also includes:

1) Strengthen security infrastructure: The findings show that weaknesses in security infrastructure are the main factor facilitating attacks.
2) Train employees: Human error is one of the main factors for attackers to infiltrate.
3) Strengthen legal deterrence:To reduce the motivation of attackers, it is necessary to implement stricter legal penalties and deterrent policies.

Keywords: Cyber Attacks, Digital Auditing, Becker Criminal Theory, Information Security

JEL classification: *M4*

References

Anderson, R., & Moore, T. (2020). The economics of information security. Science.

Ageeva, O., Karp, M., & Sidorov, A. (2020, March). The application of digital technologies in financial reporting and auditing. In *Institute of Scientific Communications Conference* (pp. 1526-1534). Cham: Springer International Publishing.

Becker, G. S. (1968). Crime and Punishment: An Economic *Approach. Journal of Political Economy*, 76(2), 169-217.

Böhme, R., & Schwartz, G. (2021). Cybercrime and its economic impact. *Journal of Cyber Policy.*

Bonabi Ghadim, Rahim, (2024). Cybersecurity based on audit evidence, *Fourth National Conference on Cyber Defense, Maragha,* http://civilica.com/doc/1917436.(in persian)

Ghosh, S., & Sharman, R. (2021). Trust and security in digital auditing systems. *Computers & Security.*

Nakhaei, Habibullah; Barzegrawal, Mohammad. (۲۰۲۴), Studying the impact of digital technologies on the quality of financial reporting and auditing, *Quarterly Journal of New Approaches in Management Sciences*, Volume 4, Number 2.(in persian)

National Institute of Standards and Technology (NIST). "Cybersecurity Framework for Critical Infrastructure." Available at: https://www.nist.gov/cyberframework.

PwC Global (2023). "Digital Auditing and Cybersecurity: A Practical Guide for Organizations*." PricewaterhouseCoopers Publications.*

PwC. (2022). Cyber threats in the age of digital transformation. PwC Insights.

Sirois, L. P., Bédard, J., & Bera, P. (2020). The role of technology in modern auditing. *Accounting Horizons*.

Zare Bahnamiri, M. J. , Maleki, M. H. , Hasankhani, F. and Ramsheh, M. (2023). A Framework for Identifying and Analyzing Key Drivers Affecting Future of Auditing in Iran with a Focus on Blockchain Technology. *Empirical Research in Accounting*, *13*(3), 27-56. doi: 10.22051/jera.2023.41640.3047.(in persian)

Zheng Guohong , Xia Zhongwei , He Feng, Xiao Zhongyi.(2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk, *Research in International Business and Finance* 73 (2025).

Wang. L. (2025), Digital transformation, audit risk, and the low-carbon transition of China's energy enterprises, *Finance Research Letters*, 106445