THREATS TO BUSINESS ACCOUNTING DATA IN THE DIGITAL AGE

NEAGU (ION) ANA-REBECA
PH.D. STUDENT, "VALAHIA" UNIVERSITY OF TÂRGOVIȘTE
E-mail: rebecaneagu@yahoo.com

GORE BEATRICE-ELENA
PH.D. STUDENT, "VALAHIA" UNIVERSITY OF TÂRGOVIȘTE
E-mail: gorebeatrice32@yahoo.com

ION LAURENȚIU-EDUARD
PH.D. STUDENT, "VALAHIA" UNIVERSITY OF TÂRGOVIȘTE
E-mail: laurentiu.ion1992@yahoo.com

RADU FLORIN
PH.D. PROFESSOR, "VALAHIA" UNIVERSITY OF TÂRGOVIȘTE
E-mail: florin.radu@valahia.ro

Abstract

This paper we have examined the vulnerability of accounting data to cyber attacks and the limits of protection afforded to it to counterbalance the benefits of the digital era (Bellanova, 2017), so that we can conclude whether digitization brings sufficient benefits to cover the inherent shortcomings. The solutions proposed to businesses by professionals in the field regarding the potetization of accounting data are vast (Gutwirth et al., 2010) and can sometimes mislead the decision maker, i.e. lead to the wrong decision on the most efficient and adapted solution to the business needs. This paper examines the risks experienced by businesses, at the economic level, as a result of increasingly prevalent fraudulent behaviours originating from both the internal and external environment of the company, fostered by the digitalization of the accounting profession and the accounting professional's reaction to these challenges. According to Weinberger (2011), Big Data is an indicator of the changes undergone by businesses in the market, changes due to the impact of information in digital format, which is too numerous to master and control (Aradau et al., 2015).

Keywords: *Big Data, security, cyber attacks,, accounting date, AI, risky behavior*

JEL classification: *D23, D73, M21, M41*

1. Introduction and context of the study

According to Cosmin Neagu, Client Director & Global Client Network Manager, Aon Romania, an average of 20,000-30,000 cyberattacks are identified and registered in our country every day. He states that the highest incidence of attacks takes place in the Romanian capital, mainly towards the pharmaceutical industry and as a typology, in proportion of 60% we encounter the ransomware attack, followed by the DDoS attack and Phishing.

According to Aon Romania, the lack of knowledge of the risks to which we expose ourselves as a result of the implementation of digital technology at the enterprise level costs us approximately 8,440 billion dollars per day, an amount that is estimated to triple in just three years.

What are the main risk factors when it comes to the cybersecurity of a company's accounting data and what do cyberattacks aim for? According to the authors, the greatest threat to the security of a company's accounting is represented by the employees themselves, through negligence and lack of specific knowledge, but also through the exploitation for personal interest of the confidential data to which they have access in terms of their job duties. To these are added third parties, who

pursue illicit purposes, such as data theft and obtaining material benefits, removal of competence, etc.

The digital age has revolutionized the way businesses manage their accounting data, integrating advanced digital technologies and accounting information systems (AIS) into their operational processes. At the same time, this digitalization has brought significant challenges, especially in the context of cybersecurity. Accounting data is the main target of cybercriminals, given its economic value and strategic importance.

Cyberattacks, including unauthorized access, data manipulation, and financial fraud, generate significant financial losses and affect trust in companies' digital infrastructures. Moreover, internal policies such as notification automation and monitoring of connected devices have proven to be effective solutions in preventing unauthorized access. At the same time, persistent attacks, such as ransomware, continue to highlight weaknesses related to employee education regarding the risks associated with digital technologies, highlighting the importance of investing in awareness and training programs.

In this article, we look at the threats to accounting data in the digital context, the use of security technologies such as behavioral biometrics, and the adoption of audit technologies for data protection. The study aims to provide an overview of the challenges and solutions available, thus contributing to improving risk management in business.

2. Methodology

This paper is based on the case study method of multiple companies, which faced cyberattacks during 2024. Through it, we analysed the frequency of the types of risks and the consequences generated in order to highlight their incidence and impact on companies. We believe that through this methodology, a favorable context is created for assessing the challenges generated by the digitization of accounting and not only, which, faced with the benefits provided by it, lead to an important decision at the level of the company.

To analyze the threats to accounting data in the digital age, this paper uses a mixed methodology, based on case studies, literature analysis and modeling techniques. By using this integrated approach, the research aims to identify cyber risks, assess their impact on accounting data and explore the use of emerging technologies to prevent and manage these risks.

The method used aims to analyze cybersecurity incidents, which affected the accounting data of renowned companies. This case study includes, among others, an internationally recognized organization, namely Starbucks, which reported a security breach in 2024, with a significant impact on financial and operational data. The main objective is to identify the typologies of cyber threats, to assess their impact and to propose practical solutions for the protection of accounting data.

The use of privacy-enhancing technologies (PETs) allows for more secure management of accounting data, as they are designed to ensure both anonymization and compliance with legal requirements. Replacement PETs, such as anonymisation tools, are used to protect users' identities and prevent unauthorised access, thus helping to reduce the risks associated with unauthorised surveillance and cyber fraud. At the same time, complementary PETs are used to demonstrate compliance with legal regulations without disrupting accounting data logistics, providing a solution tailored to operational and legal requirements. The analysis of these technologies allows the identification of advantages in reducing the exposure of sensitive data, the impact on compliance and limitations in complex accounting environments.

Privacy Impact Assessments (PIAs) are integrated into the methodological framework as a systematic process for assessing the risks associated with digital accounting projects. This approach analyses the effects on privacy by engaging stakeholders, including technology specialists and legal experts, helping to formulate solutions that meet the needs of security and transparency. PIAs are used to identify accounting data vulnerabilities and develop risk mitigation strategies, taking into account critical issues such as discrimination, information asymmetries and algorithmic logistics.

The integration of PET and PIA allows for a holistic approach to data protection, where privacy and compliance are treated as central elements of an effective digital security system. Through this methodology, the aim is to obtain a complex perspective on the challenges and opportunities of accounting data governance in the digital age.

3. Case study on risks to financial accounting data

The range of cyberattacks encountered in the daily life of companies in the economic market is increasingly diversified, including types such as: malware, DDOs, phishing, ransomware, credential stuffing, etc., but the largest share is held by ransomware attacks (Bajpai & Enbody, 2023).

The ransomware attack involves locking the victim's data and blackmailing them by paying a generous amount in exchange for ransoming the database. This type of attack is all the more dangerous as it not only targets substantial material losses, but implicitly threatens people's lives (Begovic et al, 2023).

Another type of cyberattack identified by the authors as being in vogue is credential stuffing. Its origin lies in the convenience of users (Yu et al, 2024), who, in order to facilitate access to personal accounts, registered on various websites/applications, use the same address and password. Thus, the attacker can destroy multiple accounts by using confidential credentials composed in another application/on another website.

In the following, we have presented four cases of interest for the subject of this article, which illustrate the situation of both national and international companies that have suffered significant damage as a result of unexpected cyber attacks.

Company Name	Attack date	Type of attack	In fact
Varta AG (manufacturer of batteries for the automotive, consumer and industrial sectors; country of origin: Germany)	February 2024	Ransomware	The German-born company temporarily halted production at five factories following a cyberattack, which led to a drop in VARTA's share price by 4.75 percent.
Starbucks (coffee shop chain; country of origin: USA)	November 2024	Ransomware	Following a cyber attack on a software provider of the company, it was unable to pay employees. The attack targeted employees' work schedules and their timesheets.
Altex (company that sells electronics, home appliances, IT and multimedia products; country of origin: Romania)	November 2024	Credential stuffing	Following two cyber attacks, personal data of a significant number of customers were compromised, such as: name, surname, email, account passwords, order history, financial

			data about bank cards used on the platform.
Bologna FC (football club; country of origin: Italy)	December 2024	Ransomware	This cyberattack exposed the sports club, its players, but also third parties, such as sponsors, active fans to considerable risks, such as identity theft, economic fraud and other forms of exploitation.

4. Analysis and discussion

Regarding the case of Altex in Romania, among the solutions identified and that we consider to be appropriate in order to prevent the repetition of such incidents we list: the automation of notifications for any connection from a device other than the usual one, the real-time display of the devices active on the platform and the detailed history of connections, policies to strengthen the complexity of the users' password, etc.

We believe that version 2.5 is an innovative way to protect personal, accounting, financial and other data. of the WhiteRabbitNeo tool. He presents himself as an expert in the field of vulnerability identification, demonstrating precision and speed of reaction to test possible vulnerabilities and provide remedies to alarming situations in almost real time.

In the context of the increase in the number of cyberattacks, the analysis of user behavior and the implementation of innovative technological solutions become essential for preventing risks and strengthening data security, both personal and organizational. An eloquent study was conducted on the behavior of students in Pakistan (Khan et al, 2022), a study that reveals problems similar to those observed in other international contexts, including in the case of security incidents in Romania, such as the Altex case. The study of 294 students in Pakistan showed that most of them engage in risky behavior in the digital environment, highlighting the use of weak passwords, sharing personal information, and a lack of proactive security measures. These behaviors are similar to the problems encountered in the case of Altex, where users of the platform did not have visibility on suspicious connections or their detailed history.

A lack of user awareness of cyber risks facilitates critical vulnerabilities that can be exploited by attackers, including unauthorized access to accounting and financial data. It highlights the importance of solutions such as automating login notifications, displaying active devices in real-time and strengthening the complexity of user passwords, practices that have proven effective in the case of Altex.

Comparatively, in Pakistan, the introduction of technologies similar to WhiteRabbitNeo, along with tailored educational policies, could significantly improve security awareness and reduce risky behaviors. The use of advanced technologies, such as Privacy Impact Assessments (PIAs) and privacy-enhancing technologies (PETs), could increase protection against cyber threats.

The implementation of proactive technology solutions, such as PETs and automated vulnerability identification tools (such as WhiteRabbitNeo), can significantly contribute to reducing the exposure of organizations and individual users to risks

The widespread adoption of ERP and AIS (Accounting Information Systems) systems has required audit firms to integrate advanced technologies to maintain data integrity and financial compliance, a key aspect in the context of increasing cyber risks. Studies on user behavior, as well as recent cases, such as that of Altex, emphasize the importance of implementing effective technological tools. For example, the use of advanced solutions, such as WhiteRabbitNeo v2.5, can

support auditing firms in quickly testing vulnerabilities and fixing them, providing increased protection for sensitive data.

However, research indicates that the adoption of these tools varies depending on the resources and size of the organization. Smaller firms, for example, have difficulty accessing advanced technologies due to financial constraints or a lack of technical skills. In this respect, the solutions proposed to improve security in the case of Altex, such as automatic notifications for suspicious connections or real-time display of active devices, could be applied in a similar way to strengthen control within audit processes. This integrated approach, combining audit technologies and cybersecurity measures, can significantly contribute to preventing security breaches and maintaining trust in digital accounting systems.

5. Recommendations

In Romania, a fairly well-known security company, namely Bitdefender, has made available to any user, free of charge, a description software, through which data damaged by ransomware attacks can be recovered. This approach started from the analysis of the ShrinkLocker ransomware.

Education and awareness play a fundamental role in strengthening the cybersecurity posture at the individual and organizational levels. Organizing dedicated training programs, both in academia and in public and private institutions, can significantly improve the level of preparedness in the face of cyber threats. In the university environment, the integration of cybersecurity modules into the educational curriculum contributes to the development of the skills of future professionals. At the organizational level, regular employee training sessions can prevent risky behaviors and improve the implementation of best practices.

The adoption of advanced technologies is an essential element for effective cyber risk management. Supporting audit firms and small businesses by facilitating access to high-performance technological tools and offering solutions compatible with existing infrastructures can help increase the efficiency of organizational processes.

The integration of behavioral biometrics technologies or solutions such as WhiteRabbitNeo can significantly reduce risks and improve the security of digital infrastructures. In this respect, clear and coherent regulations are a necessary basis for the responsible adoption and use of these technologies. International standardization of audit practices and digital data protection measures can provide a legislative and operational framework to guide the deployment of technologies in various sectors.

Through such regulations, organizations can benefit from greater legal certainty and strategic guidance in the use of advanced technologies. Partnerships between organisations, technology providers, professional bodies and educational institutions are essential for accelerating the implementation of technological innovations. These collaborations can facilitate the exchange of knowledge and expertise, support the adoption of advanced technologies, and contribute to the development of solutions tailored to the specific needs of organizations.

Therefore, we believe that an ecosystem of cooperation between relevant actors can support both the improvement of the cybersecurity posture and the sustainable development of the digital environment.

6. Conclusions

In the context of accelerated digitalization, we believe that cybersecurity is emerging as a fundamental priority, given the exponential increase in ransomware, phishing and DDoS attacks, which affect both large organizations and small and medium-sized enterprises equally. Deficiencies in cyber education and the lack of implementation of effective protection measures significantly

amplify vulnerabilities at the organizational and individual level, highlighting the need to develop proactive strategies for risk prevention and management.

According to the authors, a determining factor in the accentuation of cyber vulnerabilities is user behavior, characterized by poor practices, such as the use of insecure passwords, negligence in updating software and lack of awareness of cyber threats. In developing countries, such as Pakistan, these risks are amplified by the digital divide and limited access to information technology education. These findings highlight the need to implement educational programs, appropriate public policies and awareness campaigns aimed at reducing risky behaviors.

Therefore, we believe that, despite the significant benefits of adopting advanced technologies, such as behavioral biometrics or innovative solutions, such as WhiteRabbitNeo, their implementation remains limited, especially in the case of small and medium-sized enterprises. These limitations are associated with insufficient financial resources, lack of information technology skills and the complexity of integrating technological solutions into existing processes. Thus, the adoption of these technologies requires a personalized approach, adapted to the specifics and organizational needs.

In this context, we conclude by stating that education and legislative regulations play an essential role. The implementation of specialized education in cybersecurity and auditing, along with clear regulations supported by professional bodies, is imperative for improving user skills and facilitating the adoption of advanced technologies. At the same time, creating a legislative framework that supports the integration of security solutions into organizational processes contributes to strengthening cyber resilience and developing a secure and sustainable digital environment.

7. Bibliography

[1]**Aradau C., Blanke T.,** The (Big) Data-securityassemblage: Knowledgeand critique, Big Data & Society Journal, 2015, 1-12, DOI: 10.1177/2053951715609066;

[2]**Bajpai P., Enbody R**., KnowThyRansomwareResponse: A Detailed Framework for Devising Effective Ransomware Response Strategies, Digital Threats: Research and Practice, 2023, vol. 4(4), 1 – 19, https://doi.org/10.1145/3606022;

[3]**Begovic. K, Al-Ali A., Malluhi Q.,** Cryptographicransomwareencryptiondetection: Survey, ComputersandSecurity, 2023, 132, https://doi.org/10.1016/j.cose.2023.103349;

[4] **Bellanova R.,** Digital, politics and algorithms: Governing digital data through the lens of data protection, European Journal of Social Theory, 2017, vol. 20(3), 329-347, DOI: 10.1177/1368431016679167;

[5] **Gutwirth S., Poullet Y., De Hert P.,** Data protection in a profiledworld, Dordrecht: Springer, 2010;

[6] **Jackson D., Allen C.,** Enablers, barriersandstrategies for adoptingnewtechnology in accounting, International Journal of Accounting Information Systems, 2024, 52, https://doi.org/10.1016/j.accinf.2023.100666;

[7] **Jasim Y., Raewf M.,** The Impact of Information Technology on the Accounting System, Journal of Humanities and Social Sciences, 2020, 4 (1), 50-57, https://doi.org/10.24086/cuejhss.v4n1y2020.pp50-57;

[8**] Karpoff M. J.,** The Future of Financial Fraud, Journal of Corporate Fiance, 2021, 66, 101694, https://doi.org/10.1016/j.jcorpfin.2020.101694;

[9] **Khan N.F., Ikram N., Saleem S., Zafar S.,** Cyber-securityandriskybehaviors in a developing country context: a Pakistani perspective, Security Journal, 2023, 36, 373-405, https://doi.org/10.1057/s41284-022-00343-4;

[10] **Lardo A., Corsi K., Varma A., Mancini D.,** Exploringblockchain in theaccountingdomain: a bibliometricanalysis, Accounting, Auditing&; AccountabilityDiary, 2022, 35(9), 204-233, https://doi.org/10.1108/AAAJ-10-2020-4995;

[11] **Nnamoko N., Barrowclough J., Liptrott M., Korkontzelos I.,** A behaviourbiometricsdataset for user identification and authentication, Data in Brief, 2022, 45, https://doi.org/10.1016/j.dib.2022.108728;

[12**] Němec D., Machová Z., Kotlán I., Kotlánová E., Kliková C.,** Corruption in public administration as a brake on thetransitionto Industry 4.0', Sage Open Journal, 2022, 12(1), https://doi.org/10.1177/21582440221085009;

[13] **Ren Y., Ren Y., Tian H., Song W., Yang Y.,** Improvingtransactionsecuritythroughblockchain-basedfraudprotection", ConnectionScience Journal, 2023, 35 (1), 2163983, https://doi.org/10.1080/09540091.2022.2163983;

[14] **Rosli K., Yeow P., Eu-Gene S.,** Adoption of audit technology in audit firms', in Hepu Deng and Craig Standing, ACIS 2013: Information systems: TransformingtheFuture: Proceedings of the 24th AustralasianConference on Information Systems, 2013, 1-12;

[15] **Roszkowska P**., Fintech in Financial Reporting and Auditing to Prevent Fraud and Protect Capital Investments," Journal of Accounting and Organizational Change, 2021, 17 (2), 164-196, https://doi.org/10.1108/JAOC-09-2019-0098;

[16] **Sigetova K., Uzikova L., Dotsenko T., Boyko A.,** Recent Trends in World Financial Crime, Financial and Credit Activity: Problems of Theory and Practice Journal, 2022, 5 (46), 258-270, https://doi.org/10.55643/fcaptp.5.46.2022.3897;

[17] **Utama A.A.G.S., Basuki B.,** Exploring Theme-BasedTwitter Data in ForensicFraudAccounting Studies," Cogent Business &; Management Journal, 2022, 9 (1), 2135207, https://doi.org/10.1080/23311975.2022.2135207;

[18] **Weinberger D.,** Too Big toKnow: RethinkingKnowledgeNowthattheFactsAren'ttheFacts, Experts Are Everywhere, andtheSmartestPerson in the Room isthe Room, NY: Basic Books, 2011;

[19] **Yu X., Tang D., Zhao Z., Zhao W.,** Privacy-preserving compromised credential checking protocol for account protection, Computers Standards & Interfaces, 2024, 89, DOI10.1016/j.csi.2023.103823;

[20]https://www.securityweek.com/whiterabbitneo-high-powered-potential-of-uncensored-ai-pentesting-for-attackers-and-defenders/

[21] https://dnsc.ro/citeste/stirile-saptamanii-din-cybersecurity-28-11-2024

[22] https://www.reuters.com/business/retail-consumer/starbucks-faces-disruptions-following-ransomware-attack-software-supplier-2024-11-25/

[23] https://arenait.ro/altex-romania-amendata-20-000-euro-brese-securitate-datelor/