REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 22/04/2024 Revised: 03/05/2024 Accepted: 17/05/2024 Published: 12/06/2024

Impact Of Cyber Attacks on Accounting and Business

Dr. Devajit Mahanta[1*] and Dr. Nupur Kalita[2]

[1*]He receive his Ph.D degree from the Kalinga University in year 2020. He has been worked as a Assistant professor and HOD, Department of B.Voc. (Information Technology), Nalbari Commerce College (under Gauhati University), Nalbari, Assam (India).

[2]He receive his Ph.D degree from the B.R Ambedkar Bihar University in year 2012. He has been worked as a Assistant professor and HOD, Department of Accountancy, Nalbari Commerce College (under Gauhati University), Nalbari, Assam (India).

Abstract:
Today internet have crosses every barrier and have changed the way we use to talk, play games, work, accenting ,finance ,shop, make friends, listen music, see movies, order food, pay bill, medicine making etc. The criminal activities in internet that either targets or uses a computer, a computer network or a networked device are daily increases in the world which is known as internet crime or cyber crime. Now days various form of malicious activity targeting IT systems and/or the attackers or threat actors using them to gain unauthorized access to systems and data they contain which is called Cyber attack or cyber security attack increases rapidly. This paper focusing cyber attacks causes and impacts on accounting and Business based on the various previous research paper of cyber attacks and accounting. The results of the study show that cyber attacks are caused by various agents.

Keywords: Cyber attack, Cyber Crime, accounting and Business

I. INTRODUCTION

Since the last few years, India has been the target of increasing cyber crime and attacks from both within and outside the country. As a developing country with rapid internet penetration, cybersecurity is becoming an increasingly urgent concern. A significant case of cyberattack occurred in August 2018, Pune witnessed a devastating cyber attack on Cosmos Cooperative Bank. The attackers employed sophisticated techniques, including malware injection and unauthorized transactions, leading to a massive financial breach. The aftermath was severe, with unauthorized withdrawals from numerous accounts, causing significant financial distress.This incident underscored the importance of real-time monitoring, robust authentication processes, and regular security audits in financial institutions. In year between 2017 and 2018, India faced a series of concerning data breaches related to Aadhaar, the nation's biometric identification system. The breaches ranged from unauthorized access to Aadhaar databases to instances of personal information being made available on public platforms. The impact of these breaches was significant, as they potentially exposed over 1.1 billion of individuals to identity theft and fraud. The compromised data included names, addresses, biometric details, and in some cases, even bank account information linked to Aadhaar.These breaches served as a stark reminder of the critical importance of safeguarding sensitive personal information in an increasingly digital world. STL Digital advocates for robust data protection measures and offers cutting-edge solutions to fortify digital identity systems. In May 2017, the world witnessed one of the most widespread and devastating cyberattacks in history, known as the WannaCry ransomware attack. India was the third worst-hit nation by Wanna Cry ransomware, affecting more than 2 lakh computer systems. This ransomware attack hit banks in India and a few enterprises in Tamil Nadu and Gujarat. Several major organizations, including banks, government agencies, and healthcare facilities, fell victim to this global cyber assault.

The attack exploited a vulnerability in outdated versions of the Microsoft Windows operating system, encrypting files and demanding a ransom in Bitcoin for their release. The ransomware quickly spread through unpatched systems, leading to widespread disruptions. This attack underscored the necessity of regular software updates, robust firewalls, and comprehensive backup systems to protect against such threats.The accounting profession is increasingly being targeted by cyberattacks, emphasizing the importance of increased cybersecurity measures within organizations (Zadorozhnyi et al., 2020). The impact of cyberattacks on the accounting profession is not only financial, but also includes broader organizational resilience and trust in financial reporting. Cybersecurity incidents can disrupt business operations, compromise sensitive financial information and erode stakeholder trust (Daoud & Serag, 2021). Therefore, there is an urgent need for accounting professionals to increase their cybersecurity awareness and adopt proactive measures to protect accounting data. As organizations navigate the complex cybersecurity landscape, the role of governance in ensuring sustainable cybersecurity practices is increasingly important. Boards of directors are increasingly taking on an oversight role to oversee cybersecurity risk management and ensure effective implementation of cybersecurity measures (Alashi & Badi, 2020). This shift reflects a broader recognition of the important relationship between governance, cybersecurity and accounting or business continuity. However, there is a research gap in the existing literature related to the specific approach required by the accounting profession in the face of evolving cyber

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 22/04/2024 Revised: 03/05/2024 Accepted: 17/05/2024 Published: 12/06/2024

threats. This focusing on the integration between cybersecurity governance and the specific needs of the accounting and business profession, which has not been discussed much in depth in previous research.

II. LITERATURE REVIEW

a. Cyber Threats to Accounting and Business System

It's an unfortunate reality that small and medium-sized accounting firms and Business System are some of the most popular targets of cybercriminals. With reams of sensitive client financial data sitting on their servers, they represent potential goldmines for hackers and other bad actors. However, in many cases, they have less IT security protection and don't have the staffing resources to protect against threats. It is therefore crucial that they focus on accounting and Business System cybersecurity.Gaining an awareness of cybersecurity threats is the first step in protecting your firm. Let's look at five of the most common types of cyberattacks affecting businesses today, including accounting firms and Business System.There are five of the most common types of cyberattacks affecting businesses today, including accounting firms and Business System.

i) Ransomware

Ransomware is a cyberattack that acts by encrypting all the files on a device or software. This makes it impossible for you to use any of your systems. The attackers typically demand money in exchange for removing the encryption and re-opening access to our files. A recent evolution of ransomware is "triple extortion." Hackers copy the data and threaten to leak it if the ransom is not paid. The demand has three components that aim to:

a. Get the encryption key to regain use of your systems
b. Destroy the copy; and
c. Prevent the data leak

The frequency of ransomware attacks is astounding.

ii. Phishing

Phishing affects businesses and individuals. Often, phishing scams come with the threat of installing ransomware or other dangerous programs onto our systems. It can also trick people into divulging personal or sensitive information about their business or personal financial accounts.A common phishing method involves sending out a fraudulent email that looks like it's coming from a legitimate source. An example would be a note from what appears to be a trusted vendor asking the business to update its account information. The email likely includes a link to click. If we do click it, you might unintentionally download threatening software.The software from phishing scams might lock us out of our systems, or could give the hackers access to our passwords and login info to our business accounts.

iii. DDoS

DDoS stands for distributed denial of service. It is a different kind of cyberattack that might be hard to detect at first. A simple denial of service (DoS) attack is a bit different from DDoS activity. DoS happens when a server is flooded with what looks like legitimate website traffic. The server is overwhelmed and crashes. During the attack, the organization is unable to use its systems. All facets of operations might be affected. In a DDoS attack, the hacker uses several devices at once to execute the activity. They take control of those devices with vulnerable security systems. They take them over so you can no longer control them internally. Instead, the hacker operates them remotely as part of a "botnet," or group of internet-connected tools.

Iv. Malware

Malware is a category of computer software that scammers trick users into downloading onto their devices. Sometimes, it can happen to a business without anyone knowing. Clicking a random link can be all it takes for malware to enter our systems.

v. Insider threats

Insider threats are a catch-all category for threats that result from the unintentional or intentional actions of someone an organization trusts. This includes employees and contractors with access to sensitive information. Unintentional insider cyberthreats include opening the door to things like ransomware and malware. Someone with computer access at work might accidentally click, download or access a file that causes a security violation.
Intentional insider cyberthreats occur when someone with access deliberately tries to disrupt a company's systems or make them vulnerable to infiltration. They might change company data on purpose or install malware to meet these nefarious end goals. here are many ways to safeguard against insider threats. In the U.S., the federal government has training and other resources to help protect businesses. Exploring other IT security options for your practice, such as moving your digital assets to the cloud, are other options.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Received: 22/04/2024 Revised: 03/05/2024 Accepted: 17/05/2024 Published: 12/06/2024

III. RESEARCH METHODOLOGY

Data Collection

I have collected article from various accredited journals has the highest quality of published articles. The accredited journals article are-

1. The Role of Governance In Achieving Sustainable Cybersecurity For Business Corporations. Journal of Information Security and Cybercrimes Research, 3(1), 97-112.
2. Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals At Public Health Care Facilities.
Applied Clinical Informatics, 12(04), 924-932.
3. Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity Awareness and Market Valuations. Journal of Accounting and Public Policy, 37(6), 508-526.
4. Cha, J., Singh, S., Pan, Y., & Park, J. (2020). Blockchain-Based Cyber Threat Intelligence System Architecture For Sustainable Computing. Sustainability, 12(16), 6401.
5. Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber Security Assurance Process from The Internal Audit Perspective. Managerial auditing journal, 33(4), 360-376.
6. Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity Insurance and Risk- Sharing. Journal of Accounting and Public Policy, 37(6), 527-544.
7. Curtis, M., Torriti, J., & Smith, S. T. (2018). Demand Side Flexibility and Responsiveness: Moving Demand in Time Through Technology. Demanding energy: Space, time and change, 283- 312.
8. Dornheim, P. (2023). Determining Cybersecurity Culture Maturity and Deriving Verifiable Improvement Measures. Information and Computer Security.
9. Ettredge, M., Guo, F., & Li, Y. (2018). Trade Secrets and Cyber Security Breaches. Journal of Accounting and Public Policy, 37(6), 564-585.
10. Ettredge, M., & Richardson, V. J. (2002,). Assessing the Risk in E-commerce. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 11-pp). IEEE.
11. Gao, Y., Li, X., Peng, H., Fang, B., & Philip, S. Y. (2020). Hincti: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE Transactions on Knowledge and Data Engineering, 34(2), 708-722.
12. Gong, S. and Lee, C. (2021). Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform. Electronics, 10(3), 239.
13. Gordon, M. (2015). Lessons from the Front: A Case Study of Russian Cyber Warfare.
14. Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2002). An Economic Perspective on The Sharing of Information Related To Security Breaches: Concepts and Empirical Evidence.
15. Guerrero, J., Zúñiga, K., Certuche, C., & Pardo, C. (2020). A Systematic Mapping Study About Devops. Journal De Ciencia E Ingeniería, 12(1), 48-62.
16. Gunawan, B. (2023). Cybersecurity and Strategic Management. Foresight and Sti Governance, 17(3), 88-97.
17. Haapamäki, E. and Sihvonen, J. (2019). Cybersecurity in Accounting Research. Managerial Auditing Journal, 34(7), 808-834.
18. Herdiana, Y., Munawar, Z., & Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal Ict Information Communication & Technology, 20(1), 42-52.
19. Hesford, J. W, Lee, S.S., Van Der Stede, W. A., & Young, S.M. (2007). Management Accounting: A Bibliographic Study. Management Accounting Research, 5(1), 3- 26.
20. Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The Relationship Between Board- Level Technology Committees and Reported Security Breaches. Journal of Information Systems, 30(3), 79-98.
21. Islam, Md. S., Farah, N., and Staffor, T. F. (2018). Factors Associated with Security/Cybersecurity Audit by Internal Audit Function. Managerial Auditing Journal, 33, 4, 377- 409.
22. Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the Front Line of Prevention and Education. Journal of Nursing Regulation, 10(4), 48-53.
23. Leenaars, C., Freymann, J., Jakobs, K., Menon, J., Ee, T., Elzinga, J., & Drinkenburg, P. (2018). A Systematic Search and Mapping Review of Studies on Intracerebral Microdialysis of Amino Acids, and Systematized Review of Studies on Circadian Rhythms. Journal of Circadian Rhythms, 16(1).
24. Muravskyi, V., Farion, V., & Hrytsyshyn, A. (2021). Quality of Accounting Information And Principles of Its Cyber Protection. Scientific Notes of Ostroh Academy National University Series Economics, 1(23(51)), 103-109.
25. Muravskyi, V., Pochynok, N., & Farion, V. (2021). Classification of Cyber Risks in Accounting. Herald of Economics, (2), 129.
26. Nadeem, M. (2023). Exploring the Interplay of Cybersecurity and Cybercrime In Pakistan's Digital Landscape., 4(4), 207-222.
27. Preuveneers, D. and Joosen, W. (2021). Sharing Machine Learning Models as Indicators of Compromise For Cyber Threat Intelligence. Journal of Cybersecurity and Privacy, 1(1), 140-163.

28. Rahman, A., Mahdavi-Hezaveh, R., & Williams, L. (2019). A Systematic Mapping Study of Infrastructure as Code Research. Information and Software Technology, 108, 65-77.
29. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An Instrument For Evaluating The Effectiveness of Enterprise Information Security Programs. Journal of Information Systems, 30(1), 71-92
30. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The Influence of A Good Relationship Between The Internal Audit and Information Security Functions on Information Security Outcomes. Accounting, Organizations and Society, 71, 15-29.

For the search, keywords such as 'cyber attacks,' 'accounting ',' Cyber Crime', 'Business System' 'security,' and 'cyber security governance' were used to ensure relevant coverage. The period of journals looked at was from 2005 tom2021, to cover recent developments in the field. The criteria for the selected journals included a focus on accounting, information technology, and cybersecurity . Each journal selected has a specific scope, so it is important to establish a clear sample frame in determining the object and subject of the study. This ensures that the selected articles are not only of high quality, but also relevant to the research topics covered. The selection of appropriate keywords plays a key role in the search for similar articles, ensuring that the literature obtained supports the objectives of this study.

IV. DISCUSSION

a. Classification by Article

The frequency distribution of appearances in different journals is significantly different. Out of a total of 30 occurrences, two journals, the International Journal of Accounting Information Systems and the Journal of Accounting and Public Policy each contributed the highest percentage of 16% of the total. This suggests that there is more research focus or publications in the area represented by these journals compared to other journals on the list. In addition, the Journal of Information Security and Journal of Information Systems also stood out with each contributing 8% of the total appearances, indicating two journals of excellence in more relevant topics related to information security and information systems. Thirteen other journals have only one appearance 3% of the total, meaning there is no single dominant journal in this area of accounting, Business System and information systems. Journals with less publication volume, such as Automation in Construction and Technological Forecasting and Social Change, have stated that research in these areas of management is less occurring or perhaps of less academic interest. Managerial Auditing Journal, with a contribution of 11% of the total, reflects another key area in accounting and Business System, that of managerial auditing.

b. Classification of Articles Based on Research

The study categorized five research methods used in the observed studies. The most commonly used method was analytics, which was used in 23 cases or about 61% of the total studies. This analysis shows a strong preference for the analytical approach in the observed studies. Furthermore, literature review was used in 5 cases or about 13% of the total research, indicating that researchers also relied on previous research in developing their understanding. Survey methods were also quite commonly used, appearing in 8 cases or about 21% of the total research. This suggests that collecting data directly from respondents is still a popular approach in research today. In addition, there was one case where Mixed Methods, a combination of survey and analytics, was used, accounting and Business System for about 3% of the total research. Finally, qualitative research methods were used in one case, also about 3% of the total. From this analysis, it can be concluded that analytic approaches dominate in the observed studies, followed by literature reviews and surveys, while qualitative approaches are less commonly used.

V. RESULT

a. Causes of Cyber Attacks accounting and Business

In an analysis of the literature related to the causes of cyberattacks, various factors have been identified as key contributors to the increasing frequency and complexity of cyberattacks on accounting information systems. Research drawn from Scopus-accredited journals shows that weaknesses in network security, non-compliance with security protocols, and lack of cybersecurity awareness and training among employees are common causes of these attacks. In addition, the use of outdated and unprotected software, as well as the increasing amount of sensitive data stored digitally, are also triggers for cyberattacks. Taking these factors into account, the following figure maps the various causes of cyberattacks that have been identified in previous research, providing a comprehensive and in-depth view of the key issues faced by organizations in protecting their accounting and Business and information systems from cyber threats. Cyberattacks are complex threats that can be triggered by a number of internal and external factors. Internally, organizations face vulnerabilities due to simple infrastructure setups that may not be sufficient to withstand cyber threats; this aspect is explored in depth by Gordon et al. (2015, 2016), and Steinbart et al. (2016). A large part of this table is dedicated to flaws in technological control systems, as Li & Efrim Boritz (nd), Curtis et al. (2018), Islam et al. (2018), and Gordon et al. (2016) argue, this can lead to exploitable loopholes. These vulnerabilities are compounded by human error, a factor examined by Haapamäki & Sihvonen (2019) and Kamerer & McDermott (2020), noting how unintentional errors by personnel can trigger significant security incidents. Collectively, these studies encapsulate the spectrum of challenges organizations face in securing their digital frontiers. This flowchart effectively brings these

perspectives together, presenting a holistic picture of cybersecurity risks grounded in empirical research. Each connecting point and path represents not only a potential weakness but also a focal point for defensive strategies, as outlined in the collective academic inquiry into cybersecurity management.

b. Impact of Cyber Attacks on accounting and Business

An analysis of the literature regarding the impact of cyberattacks shows that such incidents can have far-reaching and serious consequences on organizations, particularly in the context of accounting information systems. Studies published in accredited journals reveal that the impact of cyberattacks is not only limited to direct financial losses, but also includes operational disruption, reputational damage, and loss of stakeholder trust. In addition, the theft of sensitive data can lead to legal and regulatory violations leading to significant fines and litigation. The long-term impacts of a cyberattack include reduced business performance and increased costs for recovery and security system upgrades. As such, the following figure will map out the various impacts of cyberattacks that have been identified in the research, providing a comprehensive overview of the consequences that organizations must anticipate and manage to protect their operational integrity and sustainability. Although accounting information systems may be built by external vendors, the ultimate responsibility for protecting client data rests with the accounting firm and Business System itself. Therefore, a cyberattack incident not only hurts the company providing the information system but also hits the reputation of the accounting firms and Business System and auditors using the system, as clients expect that all parties involved in the management of financial information will maintain the confidentiality and integrity of that data. It is also important to integrate cybersecurity awareness in an organization's culture. Effective training and awareness programs can improve staff's ability to recognize and respond effectively to cyber threats. Adopting a human-focused approach in cybersecurity will enhance the overall defense layer and reduce the likelihood of breaches due to human error (Kahyaoglu & Caliyurt, 2021).

Thus, addressing cybersecurity challenges in accounting requires more than just technical solutions; it requires a holistic approach that combines technology, procedures, and human education to form an effective defense against cyber threats.

VI. CONCLUSIONS

The impact of cyberattacks on the accounting and Business profession requires a proactive approach to cybersecurity. Organizations need to prioritize cybersecurity awareness, training and integration of advanced technologies to effectively mitigate cyber risks. By fostering a strong cybersecurity culture, implementing best practices, and utilizing predictive analytics, the accounting and Business profession can improve its cybersecurity posture and protect critical financial information from cyber threats. Cybersecurity is a significant concern for businesses worldwide, because cyber attackers constantly target corporate data and information technology (IT) resources to make money or gain a geopolitical advantage .Cybersecurity can be defined as securing individual or organizational electronic data from unauthorized access. An attempt to gain unauthorized access is termed a cyber-attack, and these attacks may entail the theft of private data, intellectual property, confidential business strategy plans, and/or the disruption of mission critical IT systems. Organized crime syndicates and nation-state paramilitary cyber organizations have also started using cyber-attacks as an operational strategy that has led to the development of advanced persistent threats (APTs), which are becoming increasingly difficult for organizations to defend against despite having formalized cybersecurity systems .Cyber threat intelligence (CTI) has emerged as a potential solution for businesses to address security events' increasing quantity and complexity. Cyberattacks are not only a threat to finances, but also to overall organizational resilience and trust in financial reporting. They can disrupt business operations, threaten sensitive financial information and erode stakeholder trust. Therefore, cybersecurity awareness and the implementation of proactive measures to protect accounting data are critical. Strong cybersecurity measures, including a solid security culture, continuous monitoring and training, and integration of advanced technologies, are necessary to effectively mitigate cyber risks. Training and experience also play an important role in encouraging good cybersecurity behavior among accounting and Business professionals. As cyberattacks continue to evolve, it is important for organizations to adopt a comprehensive security strategy, taking into account both internal and external factors that affect cyberattack risk. This involves a deep understanding of a company's external context, recognizing and addressing internal vulnerabilities, and using advanced technology and predictive analytics. This shift reflects the importance of effective governance in ensuring effective implementation of cybersecurity measures. The board of directors plays a critical role in overseeing cybersecurity risk management and ensuring sustainable cybersecurity within the organization. As such, protection against cyberattacks and preparedness for their consequences requires a proactive and sustainable approach to cybersecurity. The accounting and Business profession should continue to raise awareness of cyber threats and adopt appropriate measures to protect financial data and ensure continued business continuity.

VII. REFERENCES

1. The Role of Governance In Achieving Sustainable Cybersecurity For Business Corporations. Journal of Information Security and Cybercrimes Research, 3(1), 97-112.
2. Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals At Public Health Care Facilities. Applied Clinical Informatics, 12(04), 924-932.
3. Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity Awareness and Market Valuations. Journal of Accounting and Public Policy, 37(6), 508-526.
4. Cha, J., Singh, S., Pan, Y., & Park, J. (2020). Blockchain-Based Cyber Threat Intelligence System Architecture For Sustainable Computing. Sustainability, 12(16), 6401.
5. Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber Security Assurance Process from The Internal Audit Perspective. Managerial auditing journal, 33(4), 360-376.
6. Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity Insurance and Risk- Sharing. Journal of Accounting and Public Policy, 37(6), 527-544.
7. Curtis, M., Torriti, J., & Smith, S. T. (2018). Demand Side Flexibility and Responsiveness: Moving Demand in Time Through Technology. Demanding energy: Space, time and change, 283- 312.
8. Dornheim, P. (2023). Determining Cybersecurity Culture Maturity and Deriving Verifiable Improvement Measures. Information and Computer Security.
9. Ettredge, M., Guo, F., & Li, Y. (2018). Trade Secrets and Cyber Security Breaches. Journal of Accounting and Public Policy, 37(6), 564-585.
10. Ettredge, M., & Richardson, V. J. (2002,). Assessing the Risk in E-commerce. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 11-pp). IEEE.
11. Gao, Y., Li, X., Peng, H., Fang, B., & Philip, S. Y. (2020). Hincti: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE Transactions on Knowledge and Data Engineering, 34(2), 708-722.
12. Gong, S. and Lee, C. (2021). Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform. Electronics, 10(3), 239.
13. Gordon, M. (2015). Lessons from the Front: A Case Study of Russian Cyber Warfare.
14. Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2002). An Economic Perspective on The Sharing of Information Related To Security Breaches: Concepts and Empirical Evidence.
15. Guerrero, J., Zúñiga, K., Certuche, C., & Pardo, C. (2020). A Systematic Mapping Study About Devops. Journal De Ciencia E Ingeniería, 12(1), 48-62.
16. Gunawan, B. (2023). Cybersecurity and Strategic Management. Foresight and Sti Governance, 17(3), 88-97.
17. Haapamäki, E. and Sihvonen, J. (2019). Cybersecurity in Accounting Research. Managerial Auditing Journal, 34(7), 808-834.
18. Herdiana, Y., Munawar, Z., & Putri, N. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. Jurnal Ict Information Communication & Technology, 20(1), 42-52.
19. Hesford, J. W, Lee, S.S., Van Der Stede, W. A., & Young, S.M. (2007). Management Accounting: A Bibliographic Study. Management Accounting Research, 5(1), 3- 26.
20. Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The Relationship Between Board- Level Technology Committees and Reported Security Breaches. Journal of Information Systems, 30(3), 79-98.
21. Islam, Md. S., Farah, N., and Staffor, T. F. (2018). Factors Associated with Security/Cybersecurity Audit by Internal Audit Function. Managerial Auditing Journal, 33, 4, 377- 409.
22. Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the Front Line of Prevention and Education. Journal of Nursing Regulation, 10(4), 48-53.
23. Leenaars, C., Freymann, J., Jakobs, K., Menon, J., Ee, T., Elzinga, J., & Drinkenburg, P. (2018). A Systematic Search and Mapping Review of Studies on Intracerebral Microdialysis of Amino Acids, and Systematized Review of Studies on Circadian Rhythms. Journal of Circadian Rhythms, 16(1).
24. Muravskyi, V., Farion, V., & Hrytsyshyn, A. (2021). Quality of Accounting Information And Principles of Its Cyber Protection. Scientific Notes of Ostroh Academy National University Series Economics, 1(23(51)), 103-109.
25. Muravskyi, V., Pochynok, N., & Farion, V. (2021). Classification of Cyber Risks in Accounting. Herald of Economics, (2), 129.
26. Nadeem, M. (2023). Exploring the Interplay of Cybersecurity and Cybercrime In Pakistan's Digital Landscape., 4(4), 207-222.
27. Preuveneers, D. and Joosen, W. (2021). Sharing Machine Learning Models as Indicators of Compromise For Cyber Threat Intelligence. Journal of Cybersecurity and Privacy, 1(1), 140-163.
28. Rahman, A., Mahdavi-Hezaveh, R., & Williams, L. (2019). A Systematic Mapping Study of Infrastructure as Code Research. Information and Software Technology, 108, 65-77.
29. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An Instrument For Evaluating The Effectiveness of Enterprise Information Security Programs. Journal of Information Systems, 30(1), 71-92
30. Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The Influence of A Good Relationship Between The

Internal Audit and Information Security Functions on Information Security Outcomes. Accounting, Organizations and Society, 71, 15-29.
31. Lenka, A.; Goswami, M.; Singh, H.; Baskaran, H. Cybersecurity Disclosure and Corporate Reputation
32. Abu, M.S.; Selamat, S.R.; Ariffin, A.; Yusof, R. CTI–issue and challenges. Indones. J. Electr. Eng. Comput. Sci. 2018, 10, 371–379.
33. www.stldigital.tech/blog/10-biggest-cybersecurity-attacks-in-indian-history/
34. www.caseware.com/resources/blog/5-key-cybersecurity-threats-accounting-firms/