E-ISSN 2986-9455
P-ISSN 2987-0925
Journal
Markcount Finance

Auditing in the Era of Cybersecurity: Challenges and Solutions

Apriyanto [1], Siti Mudawanah [2], Edi Sutanto [3], Adi Dwi Purnomo [4], Muhammad Wahid Murniawan [5]

[1] Politeknik Tunas Pemuda, Indonesia
[2] Universitas La Tansa Mashiro, Indonesia
[3] Universitas La Tansa Mashiro, Indonesia
[4] Universitas La Tansa Mashiro, Indonesia
[5] Universitas La Tansa Mashiro, Indonesia

Corresponding Author: Siti Mudawanah, E-mail; sitimudawanah8@gmail.com

Article Information:
Received August 28, 2024
Revised September 23, 2024
Accepted October 25, 2024

ABSTRACT

As threats and risks increase in the digital world, auditing in the cyber security era faces significant new challenges. Rapid digital change has increased the complexity of information systems, which makes the audit environment more complicated and requires new approaches to assessing the effectiveness of security controls. The increase in cyber threats that can threaten the integrity, confidentiality and availability of data is one of the main challenges facing auditors. Increasingly varied and sophisticated cyberattacks require proactive and adaptive audit techniques. Auditors must have the ability to evaluate cyber threats and evaluate how they impact a company's information systems and internal controls. Additionally, rapid technological advances such as cloud computing, artificial intelligence, and the Internet of Things (IoT) make auditing more difficult. To overcome this problem, risk and technology-based audits must be implemented. Lastly, training and development of auditors' skills is essential to address this issue. Auditors must keep their skills updated on cybersecurity and the latest technologies.

Keywords: *Cyber Security, Cyber Threats, Information Technology*

Journal Homepage https://journal.ypidathu.or.id/index.php/jmf

This is an open access article under the CC BY SA license
https://creativecommons.org/licenses/by-sa/4.0/

How to cite: Apriyanto, Apriyanto., Mudawanah, S., Sutanto, E., Purnomo, D, A & Murniawan, W, M. (2024). Auditing in the Era of Cybersecurity: Challenges and Solutions. *Journal Markcount Finance*, 2(2) 285-295. https://doi.org/10.70177/jmf.v2i2.1291

Published by: Yayasan Pendidikan Islam Daarut Thufulah

INTRODUCTION

In today's digital era, cyber security has become an important part of business operations due to increasing dependence on information technology(Milajerdi et al., 2019). As cyber threats evolve rapidly and information technology continues to change, auditing in the cybersecurity era is becoming increasingly difficult(Li et al., 2019).

Audits are important tasks that assess how effective internal controls and compliance are(Sultana et al., 2020). To maintain the integrity and reliability of information systems, they must adapt to these changes(Yeboah-Ofori & Islam, 2019).

With the development of technologies such as cloud computing, artificial intelligence (AI), and the Internet of Things (IoT), there are new risks and vulnerabilities that need to be considered during the audit process(Moustafa, Keshky, et al., 2020). While these technologies offer many benefits, they also open security gaps that cyber threat actors can exploit(Lois et al., 2020). Auditors must be able to identify and evaluate the risks associated with these new technologies, as well as ensure that existing controls are adequate to address cyber threats(Shah & Khan, 2020).

Additionally, the frequency and complexity of cyberattacks is increasing rapidly(Szczepaniuk et al., 2020). A more proactive and adaptive audit approach is needed due to growing cyber threats, such as ransomware, phishing, and denial-of-service (DoS) attacks.(Sibi Chakkaravarthy et al., 2020). To assess the strength of the controls and security strategies implemented by a company, auditors must understand these types of attacks and their impact on information systems(Chang et al., 2022).

Meanwhile, rules and regulations relating to cyber security are getting stricter(Moustafa, Ahmed, et al., 2020). To ensure that companies comply with legal obligations and maintain appropriate security standards, auditors must thoroughly understand applicable industry regulations, such as GDPR and HIPAA(Zengy et al., 2022).

A risk-based audit framework is critical to addressing this problem because it allows auditors to concentrate on the most vulnerable and high-risk areas of the information system(Zheng et al., 2022). A risk-based approach also allows auditors to ensure that existing security controls are functioning properly and according to the company's needs(Kechagias et al., 2022).

To detect and deal with cyber threats more effectively, it is also necessary to use advanced technology in audits(X. Zhang et al., 2019). Technology-based audit techniques and tools, such as big data analysis and real-time monitoring, can help auditors discover anomalies and potential risks more quickly and accurately(Preuveneers et al., 2020). This technology enables more thorough and in-depth audits in complex environments(Fernández-Caramés & Fraga-Lamas, 2020).

To overcome this problem, auditors must be trained and equipped with skills(Ali et al., 2023). Auditors must always update their knowledge and skills on cybersecurity and the latest technologies.(Liu et al., 2019). Getting training and certification in cybersecurity can help them better spot and assess risks(Kurniawan et al., 2022).

It is critical for management to support audits and incorporate them into company cybersecurity policies and strategies(Rosati et al., 2019). This is done to ensure that the controls and procedures implemented are in line with the company's security objectives, and close collaboration between auditors and cybersecurity teams can improve audit performance and help better deal with cyber threats(Rosati et al., 2022).

Overall, audits in the cyber security era require an integrated and adaptive approach to overcome existing problems(Hussain Seh et al., 2022). By using a risk-based framework, advanced technology, and ongoing training, auditors can add significant value in protecting companies from cyber threats and ensuring success in maintaining the integrity of information systems in an increasingly complex environment(Aslam et al., 2020).

RESEARCH METHOD

This research uses a combination of qualitative and quantitative methods to find audit problems and solutions in the cyber security era(Pozdniakov et al., 2020). The first step is to gather the latest information about the problems encountered in the cybersecurity audit and the solutions implemented(Mondal et al., 2022). This research includes a review of journals, articles, and industry reports that discuss advances in cybersecurity, audit technology, and best practices for addressing cyber threats(Ahmad et al., 2022).

Next, surveys and questionnaires were created and distributed to auditors and cybersecurity professionals at various companies(W. Zhang et al., 2022). The goal of the survey is to collect quantitative data on issues encountered in cybersecurity audits, such as the frequency of attacks, types of threats, and how effective current controls are.(Alruwaili, 2021). It also includes information about the audit methods used as well as the tools used to detect and address cyber threats(Holler et al., 2021).

To gain a better understanding of cybersecurity audit practices, in-depth interviews with auditors and cybersecurity experts were conducted(Drivas et al., 2020). These interviews provide insights from practitioners who have encountered cybersecurity audit-related issues firsthand and the approaches they use to address these issues(Jahankhani & Kendzierskyj, 2019). The results of these interviews help explain the context and provide a better understanding of cybersecurity audit practices(Panda et al., 2019).

In addition, secondary data analysis was carried out by looking at documentation, audit reports and case studies from organizations that have faced and overcome cybersecurity issues(Adeleke & Abdul, 2020). This analysis helps in discovering patterns and best practices implemented by companies that successfully manage cyber risks(Lois et al., 2021). This secondary data also complements information obtained from surveys and interviews and provides guidance for solutions that have been proven successful.

In addition, this research conducted a comparative analysis between companies that use various audit methods and cybersecurity tools(Mcak et al., 2020). The goal of this analysis is to evaluate how effective various methods are in detecting and addressing cyber threats(Al-Matari et al., 2021). By comparing audit results and the success rate of the solutions used, this research can identify the best methods and areas for improvement(Al-Karaki et al., 2022).

The results of quantitative and qualitative analysis determine the recommendations made. These recommendations aim to assist auditors and organizations in dealing with cyber threats and ensuring that the cybersecurity controls and procedures implemented are the most effective(Wallis & Johnson, 2020). They also cover ways to address identified issues and improve the effectiveness of audits in terms of cybersecurity(Marín-López et al., 2020).

Finally, the findings are validated by talking to industry experts and testing the solutions in practical situations(Hendawi et al., 2023). This ensures that suggestions and solutions are relevant and can be applied effectively in a variety of situations(Aziz et al., 2020). Discussions also help evaluate potential challenges in implementation and provide suggestions for additional adjustments(Zakaria et al., 2019).

This research aims to provide a comprehensive understanding of audit problems and solutions in the cyber security era using this mixed method(Tetaly & Kulkarni, 2022). In addition, this research provides practical guidance for increasing audit effectiveness in dealing with cyber threats(Russell, 2020).

RESULTS AND DISCUSSION

RESULTS

Research conducted on auditing in the cybersecurity era shows that auditors are addressing a number of key issues and finding ways to overcome them. First, the big problem discovered was the increasing frequency and complexity of cyberattacks. Survey results show that auditors face various types of attacks, such as phishing, ransomware, and denial-of-service (DoS) attacks, which require changes in audit techniques and risk assessments. These attacks are increasingly sophisticated and can threaten data integrity and availability, forcing auditors to continually update their methods.

Second, advances in technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT) have created new challenges for auditors to assess system controls and integrity. Data from in-depth interviews shows that the use of cloud services can blur the boundaries of a company's internal controls, while IoT and AI also bring additional risks associated with large and complex data.

Third, the readiness of the information technology infrastructure is very important for the success of the audit. The results of the analysis show that many companies, especially in the small and medium sectors, do not have sufficient hardware and software to carry out comprehensive cybersecurity audits. Companies that do not have the appropriate infrastructure often face problems implementing sufficient controls and conducting effective audits.

Fourth, compliance and regulation are significant issues. As a result of the survey, companies must comply with ever-evolving cybersecurity regulations, such as GDPR and HIPAA. Auditors often face difficulty ensuring that each element of regulations is consistently complied with, especially when regulations change or are updated regularly.

To address this issue, a fifth, risk-based framework is used. Research shows that auditors are increasingly concentrating on high-risk areas and using a risk-based approach to determine audit priorities. This framework helps auditors assess the areas most vulnerable to cyber threats and allocate audit resources more efficiently.

Sixth, it has been proven that the use of advanced technologies, such as big data analysis tools and real-time monitoring systems, is successful. Results show that this technology helps auditors find anomalies and risks more quickly and accurately. This technology enables more thorough audits and better insight into the state of an organization's cybersecurity.

Seventh, it was identified that an important solution for auditors is training and skills development. Auditors who are given specialized training in cybersecurity and the latest technologies are better able to spot and address risks. Data shows that certification and ongoing training help auditors update their skills and knowledge.

Eighth, audit integration with the company's cybersecurity strategy is the key to audit effectiveness. Research shows that audit teams and cybersecurity teams working together can improve audit results and ensure that the security controls implemented are in line with company strategy. This collaboration helps in finding and resolving security issues more quickly and efficiently.

Nine, the solutions found in this research are relevant and can be implemented effectively, as demonstrated by practical trials and discussions with industry experts. According to this discussion, risk-based strategies, advanced technology, and ongoing training are the keys to meeting the challenges of cybersecurity audits. This solution is expected to increase audit efficiency and protect companies from ever-growing cyber threats.

Overall, this research shows that auditing in the cyber security era faces major problems, but they can be overcome with the right methods, advanced technology, and sufficient training. The solutions found provide practical guidance for increasing audit effectiveness in the face of ever-evolving cyber threats.

DISCUSSION

In the era of cyber security, auditing faces complex challenges due to threats and rapid technological advances. One of the main problems is the increasing frequency and complexity of cyberattacks. Attacks such as phishing and ransomware can damage data and disrupt overall business operations. Auditors must develop a more proactive and adaptive approach in these situations. They must understand the latest attack methods and find weak points in information systems that could become targets for attacks. This means that the audit techniques and tools used must be consistently updated.

Additionally, technological advances have created new challenges in cybersecurity audits. Technologies such as cloud computing and the Internet of Things have expanded the areas that must be monitored and controlled, adding to the complexity of the audit environment. Because data and applications no longer reside in a centralized physical infrastructure, the use of cloud services often makes it difficult for auditors to establish clear control boundaries. Meanwhile, IoT devices increase the volume and variety of data that must be analyzed, which can make it difficult for auditors to spot anomalies or risks.

In addition, the capacity of a company's IT infrastructure affects audit capabilities. Many businesses, especially small and medium-sized ones, may not have sufficient resources to support the advanced technology required for a comprehensive cybersecurity audit. Weaknesses in the controls and procedures in place, as well as difficulties in implementing effective security solutions, indicate that investment is needed.

When it comes to regulations and compliance, companies must meet a variety of frequently changing regulations, such as GDPR and HIPAA. Auditors must ensure that all internal controls comply with applicable regulations and understand legal requirements and the ability to implement appropriate controls. Auditors can benefit from active involvement in training and regulatory update processes.

It is important to implement a risk-based framework to address these issues. This method allows auditors to allocate resources more efficiently by focusing their efforts on the most vulnerable and high-risk areas. A risk-based framework provides guidance on areas that need to be examined in more depth and methods that should be used to reduce risks.

Additionally, it is proven that the use of advanced technologies in audits, such as big data analysis tools and real-time monitoring systems, is successful. This technology allows auditors to detect potential threats more quickly and accurately and provides deeper insight into a company's cybersecurity posture. These tools monitor systems in real-time for early detection and help in identifying anomalies that indicate an attack or breach.

Training and development of auditors' skills is critical to meeting cybersecurity challenges. Auditors must be updated on cyber threats and new technologies through ongoing training and certification. This training also helps them apply effective audit techniques and understand the risks associated with new technologies. With continually updated skills, auditors can provide subtle and accurate assessments of new technologies.

Audits are also important to a company's cybersecurity strategy. Audit and cybersecurity teams work together to improve controls and ensure that implemented security policies align with company strategy. This synergy ensures that audits reveal the true state of existing cyber controls and protections, and help discover and address security issues more quickly.

Finally, the results have been validated through practical trials and discussions with industry experts. This shows that the solution used was successful. This process confirms that auditors can help in addressing cybersecurity issues with a risk-based approach, use of advanced technology, and ongoing training. Evaluation and adjustment of audit methods that rely on expert feedback ensures that audits remain relevant and effective in the face of evolving threats.

Overall, auditing in the cybersecurity era requires an adaptive and integrated approach to addressing issues and leveraging available solutions. By using a risk-based framework, using advanced technology, and receiving adequate training, auditors can more effectively address cybersecurity issues and maintain the integrity and security of corporate information systems.

CONCLUSION

In the era of cybersecurity, auditing faces significant challenges due to the increasing complexity of threats and rapidly evolving technology. The increasing frequency and sophistication of cyberattacks, along with technological advances such as cloud computing and the Internet of Things, are generating new vulnerabilities that require a more adaptive and integrated audit approach. Auditors must face these challenges by enhancing their skills and knowledge in cybersecurity and by applying appropriate techniques and tools.

With strict regulations and compliance, the audit process becomes more difficult. This is because auditors must stay up to date on legal changes and ensure consistent compliance. A risk-based audit framework has proven useful for addressing these issues as it allows auditors to focus on the most vulnerable areas and allocate resources more efficiently. Additional tools to more accurately detect and address threats are provided by modern technologies, such as big data analytics and real-time monitoring.

To maintain audit effectiveness and face evolving cyber threats, auditors must be trained and develop their skills. Auditors who have the latest knowledge and skills can apply audit techniques more effectively and responsively. Additionally, close coupling of audits and a company's cybersecurity strategy improves coordination and effectiveness in addressing security issues.

In the era of cybersecurity, audit success depends on risk-based strategies, advanced technology, and ongoing training. By implementing these strategies, auditors can improve their ability to deal with cyber threats and ensure that information system controls and protection remain effective.

Overall, auditing in the cyber security era requires a dynamic and holistic approach to addressing existing problems. By using the right solutions and continually updating methodologies and skills, auditors can maintain the integrity and security of information systems amidst an ever-evolving threat landscape.

REFERENCES

Adeleke, IT, & Abdul, QBS (2020). Opinions on Cyber Security, Electronic Health Records, and Medical Confidentiality: Emerging Issues on the Internet of Medical Things From Nigeria. In PB Pankajavalli & GS Karthick (Eds.), Advances in Medical Technologies and Clinical Practice (pp. 199–211). IGI Global.https://doi.org/10.4018/978-1-7998-1090-2.ch012

Ahmad, N., Laplante, P. A., DeFranco, J. F., & Kassab, M. (2022). A Cybersecurity Educated Community. IEEE Transactions on Emerging Topics in Computing, 10(3), 1456–1463.https://doi.org/10.1109/TETC.2021.3093444

Ali, A., Al-rimy, BAS, Alsubaei, FS, Almazroi, AA, & Almazroi, AA (2023). HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors, 23(15), 6762.https://doi.org/10.3390/s23156762

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2022). GoSafe: On the practical characterization of the overall security posture of an organizational information system using smart auditing and ranking. Journal of King Saud University - Computer and Information Sciences, 34(6), 3079–3095.https://doi.org/10.1016/j.jksuci.2020.09.011

Al-Matari, OMM, Helal, IMA, Mazen, SA, & Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal: A Global Perspective, 30(4), 189–204.https://doi.org/10.1080/19393555.2020.1834649

Alruwaili, F.F. (2021). Intrusion Detection and Prevention in Industrial IoT: A Technological Survey. 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), 1–5.https://doi.org/10.1109/ICECCME52200.2021.9590961

Aslam, M., Mohsin, B., Nasir, A., & Raza, S. (2020). FoNAC - An automated Fog Node Audit and Certification scheme. Computers & Security, 93, 101759.https://doi.org/10.1016/j.cose.2020.101759

Aziz, B., Suhardi, & Kurnia. (2020). A systematic literature review of cyber insurance challenges. 2020 International Conference on Information Technology Systems and Innovation (ICITSI), 357–363.https://doi.org/10.1109/ICITSI50517.2020.9264966

Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., Boddu, S., & Kobusińska, A. (2022). A Survey on Intrusion Detection Systems for Fog and Cloud Computing. Future Internet, 14(3), 89.https://doi.org/10.3390/fi14030089

Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 1641–1646.https://doi.org/10.1109/COMPSAC48688.2020.00-20

Fernández-Caramés, T.M., & Fraga-Lamas, P. (2020). Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. Sensors, 20(11), 3048.https://doi.org/10.3390/s20113048

Hendawi, S., AlZu'bi, S., Mughaid, A., & Alqahtani, N. (2023). Ensuring Cybersecurity While Leveraging Social Media as a Data Source for Internet of Things Applications. In K. Daimi & A. Al Sadoon (Eds.), Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23) (Vol. 700, pp. 587–604). Springer Nature Switzerland.https://doi.org/10.1007/978-3-031-33743-7_47

Hollerer, S., Kastner, W., & Sauter, T. (2021). Towards a Threat Modeling Approach Addressing Security and Safety in OT Environments. 2021 17th IEEE International Conference on Factory Communication Systems (WFCS) , 37–40.https://doi.org/10.1109/WFCS46889.2021.9483591

Hussain Seh, A., F. Al-Amri, J., F. Subahi, A., Tarique Jamal Ansari, M., Kumar, R., Ubaidullah Bokhari, M., & Ahmad Khan, R. (2022). Hybrid Computational Modeling for Web Application Security Assessment. Computers, Materials & Continua, 70(1), 469–489.https://doi.org/10.32604/cmc.2022.019593

Jahankhani, H., & Kendzierskyj, S. (2019). Digital Transformation of Healthcare. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds.), Blockchain and Clinical Trials (pp. 31–52). Springer International Publishing.https://doi.org/10.1007/978-3-030-11289-9_2

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.https://doi.org/10.1016/j.ijcip.2022.100526

Kurniawan, K., Ekelhart, A., Kiesling, E., Quirchmayr, G., & Tjoa, AM (2022). KRYSTAL: Knowledge graph-based framework for tactical attack discovery in audit data. Computers & Security, 121, 102828.https://doi.org/10.1016/j.cose.2022.102828

Li, F., Shi, Y., Shinde, A., Ye, J., & Song, W. (2019). Enhanced Cyber-Physical Security in the Internet of Things Through Energy Auditing. IEEE Internet of Things Journal, 6(3), 5224–5231.https://doi.org/10.1109/JIOT.2019.2899492

Liu, L., Chen, C., Zhang, J., De Vel, O., & Xiang, Y. (2019). Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs. IEEE Access, 7, 183162–183176.https://doi.org/10.1109/ACCESS.2019.2957055

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. International Journal of Managerial and Financial Accounting, 13(1), 25.https://doi.org/10.1504/IJMFA.2021.116207

Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: Opportunities risks and challenges. EuroMed Journal of Business, 15(2), 205–217.https://doi.org/10.1108/EMJB-07-2019-0097

Macak, M., Vanat, I., Merjavy, M., Jevocin, T., & Buhnova, B. (2020). Towards Process Mining Utilization in Insider Threat Detection from Audit Logs. 2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS), 1–6.https://doi.org/10.1109/SNAMS52053.2020.9336573

Marín-López, A., Chica-Manjarrez, S., Arroyo, D., Almenares-Mendoza, F., & Díaz-Sánchez, D. (2020). Security Information Sharing in Smart Grids: Persisting Security Audits to the Blockchain. Electronics, 9(11), 1865.https://doi.org/10.3390/electronics9111865

Milajerdi, S. M., Eshete, B., Gjomemo, R., & Venkatakrishnan, V. N. (2019). POIROT: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 1795–1812.https://doi.org/10.1145/3319535.3363217

Mondal, B., Chakraborty, D., Bhattacherjee, N. Kr., Mukherjee, P., Neogi, S., & Gupta, S. (2022). Review for Meta-Heuristic Optimization Propels Machine Learning Computations Execution on Spam Comment Area Under Digital Security Aegis Region. In E. H. Houssein, M. Abd Elaziz, D. Oliva, & L. Abualigah (Eds.), Integrating Meta-Heuristics and Machine Learning for Real-World Optimization Problems (Vol. 1038, pp. 343–361). Springer International Publishing.https://doi.org/10.1007/978-3-030-99079-4_13

Moustafa, N., Ahmed, M., & Ahmed, S. (2020). Data Analytics-Enabled Intrusion Detection: Evaluations of ToN_IoT Linux Datasets. 2020 IEEE 19th

International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) , 727–735.https://doi.org/10.1109/TrustCom50675.2020.00100

Moustafa, N., Keshky, M., Debiez, E., & Janicke, H. (2020). Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) , 848–855.https://doi.org/10.1109/TrustCom50675.2020.00114

Panda, S., Woods, D. W., Laszka, A., Fielder, A., & Panaousis, E. (2019). Post-incident audits on cyber insurance discounts. Computers & Security, 87, 101593.https://doi.org/10.1016/j.cose.2019.101593

Pozdniakov, K., Alonso, E., Stankovic, V., Tam, K., & Jones, K. (2020). Smart Security Audit: Reinforcement Learning with a Deep Neural Network Approximator. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1–8.https://doi.org/10.1109/CyberSA49311.2020.9139683

Preuveneers, D., Joosen, W., Bernal Bernabe, J., & Skarmeta, A. (2020). Distributed Security Framework for Reliable Threat Intelligence Sharing. Security and Communication Networks, 2020, 1–15.https://doi.org/10.1155/2020/8833765

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters. The International Journal of Accounting, 54(03), 1950013.https://doi.org/10.1142/S1094406019500136

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-Security Incidents and Audit Quality. European Accounting Review, 31(3), 701–728.https://doi.org/10.1080/09638180.2020.1856162

Russell, B. (2020). IoT Cyber Security. In F. Firouzi, K. Chakrabarty, & S. Nassif (Eds.), Intelligent Internet of Things (pp. 473–512). Springer International Publishing.https://doi.org/10.1007/978-3-030-30367-9_10

Shah, S. M., & Khan, R. A. (2020). Secondary Use of Electronic Health Records: Opportunities and Challenges. IEEE Access, 8, 136947–136965.https://doi.org/10.1109/ACCESS.2020.3011099

Sibi Chakkaravarthy, S., Sangeetha, D., Cruz, M.V., Vaidehi, V., & Raman, B. (2020). Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks. IEEE Access, 8, 169944–169956.https://doi.org/10.1109/ACCESS.2020.3023764

Sultana, M., Hossain, A., Laila, F., Taher, KA, & Islam, MN (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Medical Informatics and Decision Making, 20(1), 256.https://doi.org/10.1186/s12911-020-01275-y

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. Computers & Security, 90, 101709.https://doi.org/10.1016/j.cose.2019.101709

Tetaly, M., & Kulkarni, P. (2022). Artificial intelligence in cyber security – A threat or a solution. 030036.https://doi.org/10.1063/5.0109664

Wallis, T., & Johnson, C. (2020). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. 2020 International

Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1–10.https://doi.org/10.1109/CyberSA49311.2020.9139641

Yeboah-Ofori, A., & Islam, S. (2019). Cyber Security Threat Modeling for Supply Chain Organizational Environments. Future Internet, 11(3), 63.https://doi.org/10.3390/fi11030063

Zakaria, KN, Zainal, A., Othman, SH, & Kassim, MN (2019). Feature Extraction and Selection Method of Cyber-Attack and Threat Profiling in Cybersecurity Audit. 2019 International Conference on Cybersecurity (ICoCSec), 1–6.https://doi.org/10.1109/ICoCSec47621.2019.8970786

Zengy, J., Wang, X., Liu, J., Chen, Y., Liang, Z., Chua, T.-S., & Chua, Z. L. (2022). SHADEWATCHER: Recommendation-guided Cyber Threat Analysis using System Audit Records. 2022 IEEE Symposium on Security and Privacy (SP) , 489–506.https://doi.org/10.1109/SP46214.2022.9833669

Zhang, W., Bai, Y., & Feng, J. (2022). TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IIoT. Future Generation Computer Systems, 132, 254–265.https://doi.org/10.1016/j.future.2022.02.023

Zhang, X., Zhao, J., Mu, L., Tang, Y., & Xu, C. (2019). Identity-based proxy-oriented outsourcing with public auditing in cloud-based medical cyber–physical systems. Pervasive and Mobile Computing, 56, 18–28.https://doi.org/10.1016/j.pmcj.2019.03.004

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 8(4), 422–435.https://doi.org/10.1016/j.dcan.2021.07.006

Copyright Holder :
© Apriyanto et al. (2024)

First Publication Right :
© Journal Markcount Finance

This article is under: