International Journal of Cybersecurity Engineering and Innovation

ARTICLE INFO

Article History: Received: 24-11-2025, Revised: 01-01-2025, Accepted: 03-01-2025, Published: 07-01-2025
Corresponding author Email: m_almaiah@ju.edu.jo
DOI:

Vol. 2026 No.1

Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights

Mariam Alrajeh[1], Mohammed Almaayah[1], Udit Mamodiya[2]

[1] *College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

[2] *Asso. Prof. & Asso. Dean (Research), Poornima University, Jaipur, India, Jaipur, Raj. India*

Abstract

Industrial organizations increasingly rely on interconnected information and operational technologies, making them more vulnerable to cyber threats. This paper presents a two part study aimed at identifying critical cybersecurity threats in industrial manufacturing environments and examining effective countermeasures to mitigate these risks. The first part of the study conducts a case study of an industrial manufacturing company with comprehensive production capabilities, including the manufacturing of corrugated boards, trays, and containers for various sectors. Through interviews and discussions with company personnel, key cyber threats affecting the company's systems were identified, along with an evaluation of the security measures previously implemented to reduce vulnerabilities. The second part of the paper provides a systematic review of existing literature focusing on security countermeasures relevant to the threats identified in the case study. By linking practical industrial challenges with theoretical and empirical research, this study highlights common cybersecurity risks in industrial environments and outlines effective strategies for enhancing security resilience. The findings offer valuable insights for industrial organizations seeking to improve their cybersecurity posture and reduce exposure to evolving cyber threats.

Keywords: Cyber Risk Analysis, Security Practices, Industrial Manufacturing, cybersecurity threats.

1. Introduction

In fact, risks can lead to failure regardless of an organization's size, whether small or large. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Organizations that proactively identify, assess, and address risks before they materialize are more likely to succeed. Effective risk management is essential to protect the organization, its people, assets, and profits from both physical and financial consequences. Moreover, proper risk management minimizes the negative impact of risks on organizational objectives while maximizing the ability to seize potential opportunities [1]. Consequently, risk management strategies have become a necessity for companies and organizations to mitigate threats and risks, particularly those related to information technology and data. A comprehensive risk management plan therefore encompasses all organizational processes aimed at identifying, analyzing, and monitoring threats to digital assets, including sensitive corporate data and personal customer information [2].

Implementing a new risk assessment plan would allow it to focus on its goals and mission to ensure research compliance, ensuring its objectives carry out operations and initiatives. Every step must be taken in the risk management process effectively. Those steps are planning, identifying, analyzing, responding, implementing, and monitoring. These are fundamental to examine the dangers that happened previously and to clarify the threats that may emerge later. Finally, we should always be thorough with our decision- making because the right decisions can eliminate many risks in our lives. The case study has become essential for understanding the impact of risk management and assessment on organizations. [3]. This paper has been divided into two sections; in the first section, I have conducted a case study on an industrial company to assign and study the critical cyber threats that the company's systems encounter. In addition, essential security measures were taken to reduce threats and vulnerability in previous years. The information was collected by having interviews and discussions with the company took some documents from them to help me in this search. The second section contains the various literature reviews on the countermeasures used to reduce the risks facing industrial companies identified through the case study.

Risk management is an essential part of properly managing and regulating organizational safety. The primary objective of risk management is to eliminate or reduce the risk to create a safer workplace. Risk management is not a short-term process but rather a continuous process of innovation that seeks a better environment. The main motives that drive companies to undertake risk management are:

• Contribute to users' protection and safety and the preservation of partner properties [1].

• It provides the company's total benefit by eliminating or reducing the real risks, whether they are recurring or have significant impacts [2].

• Contribute to understanding and enhancing employers' awareness to understand all necessary procedures related to risk management to maintain the company and its continuity [1].

• It determines the best ways to confront and deal with those risks and sets priorities, procedures, and executive programs necessary to face them [3].

Neglecting and ignoring risks and the incapability to manage them properly and fortunate manner leads to an increase in cost and time. Since the traditional methods of forecasting risks depend on sense and intuition, it was necessary to use advanced and more effective strategies to help management face potential risks in research. Industrial companies may encounter many technology risks; there are risks in this area that may cause many severe problems for a company, such as hacking, which is forced entry, breaking barriers, and protective firewalls for servers and devices that serve programs and systems. The industrial company may also infect with some viruses, which are programs that, if they penetrate the servers, may cause destruction or loss of data or other damage caused by viruses. An unauthorized person may try to access systems, programs, or databases, by illegally obtaining the username or password. Additionally, the company's main assets, such as systems or devices that serve the company's most critical operations or services, may fail and stop [1]. After many companies in the recent period encountered many different problems, risk management and assessment have become the primary function in anticipating these issues and addressing these problems to help companies avoid the risk that may occur. On the other hand, companies have become obligated to submit some reports to the competent authority, such as the National Cyber Security Authority, about the company's position in terms of cyber security. So, Security Risk and Analysis Management has contributed to this topic. The scope of the study is the most critical threats that occur in industrial companies and what are the countermeasures used to end or reduce this risk. We conducted a case study in an industrial company with overall industrialization capabilities to produce sheets, trays, and corrugated containers to meet the years of food, dairy, industrial, agricultural, soft drink, and commercial sectors. It is a work environment that may encounter many different risks and may produce several problems; the most important is the company's reputation, which it has sought to achieve for a long time.

2. Background of the research

After the interview and analysis of industrial company documents in this section, I categorized these into threats that the industrial company was exposed to, description to clarify this threat, context to find out where exactly it happened, and the countermeasures used in that case. To recognize the solutions and mitigation of industrial company risks and how organizations can protect themselves from such attacks. Subsequently, the identified threats were filtered and classified according to the IT domains illustrated in Figure 1.

Table 1. Most common threats in industrial manufacturing

Unsecured Access From company Remote Branches	• The company has systems, and these systems need modifications over time. Supplier asks the company that a port should be open in the firewall to allow remote access to their system. This way is unsafe since port forwarding is an outdated access technique, its configuration is not encrypted, and port forwarding does not ask for network authentication. • Branches need a Remote connection to the company's network.	LAN/ WAN network	• Using VPN, so the link from branches to Head office is encrypted, and there will be a login/password requirement for the remote connection. • Company has weekly monitoring of users connecting to the VPN. • company has (Remote Ethernet Devices) is a small box you deploy to your remote sites, and it establishes a VPN back to your central Sophos UTM so that anything connected to the RED is seen as part of your network. Company branches will have a more secure virtual connection to the head office with these devices.
Breaches or hacking done by Techshell-Iran.	NCA has sent an email and required companies to submit reports based on their Criteria. Because there have been breaches or hacking done by Techshell-Iran, which is affecting several KSA companies	WAN network	• Company had EDR/XDR for their Sophos antivirus. • Company is currently in a skillset upgrade program they are training our Helpdesk, Network Admin and Cyber Officer as this is important to combat Cyber Threats
Industrial company eCommerce	Need to fully secure from threats and hackers	Web Application	• Collaborate with the supply chain to perform penetration testing to secure and protect the website by checking for exploitable vulnerabilities. • The supply chain submitted the VAPT report to the IT team, then IT worked on adjusting vulnerabilities.

After identifying the potential cyber threats affecting the industrial company, a systematic filtering process was applied to remove redundancies and focus on the most critical risks. The remaining threats were then analyzed and classified according to their relevance to specific IT domains, as illustrated in Figure 1. This classification enabled a clearer understanding of how different threats impact various components of the organization's information technology infrastructure, including networks, systems, applications, and data. By organizing the threats in this manner, it became possible to prioritize security concerns and align appropriate countermeasures with each domain, thereby supporting a more structured and effective cybersecurity risk management approach.

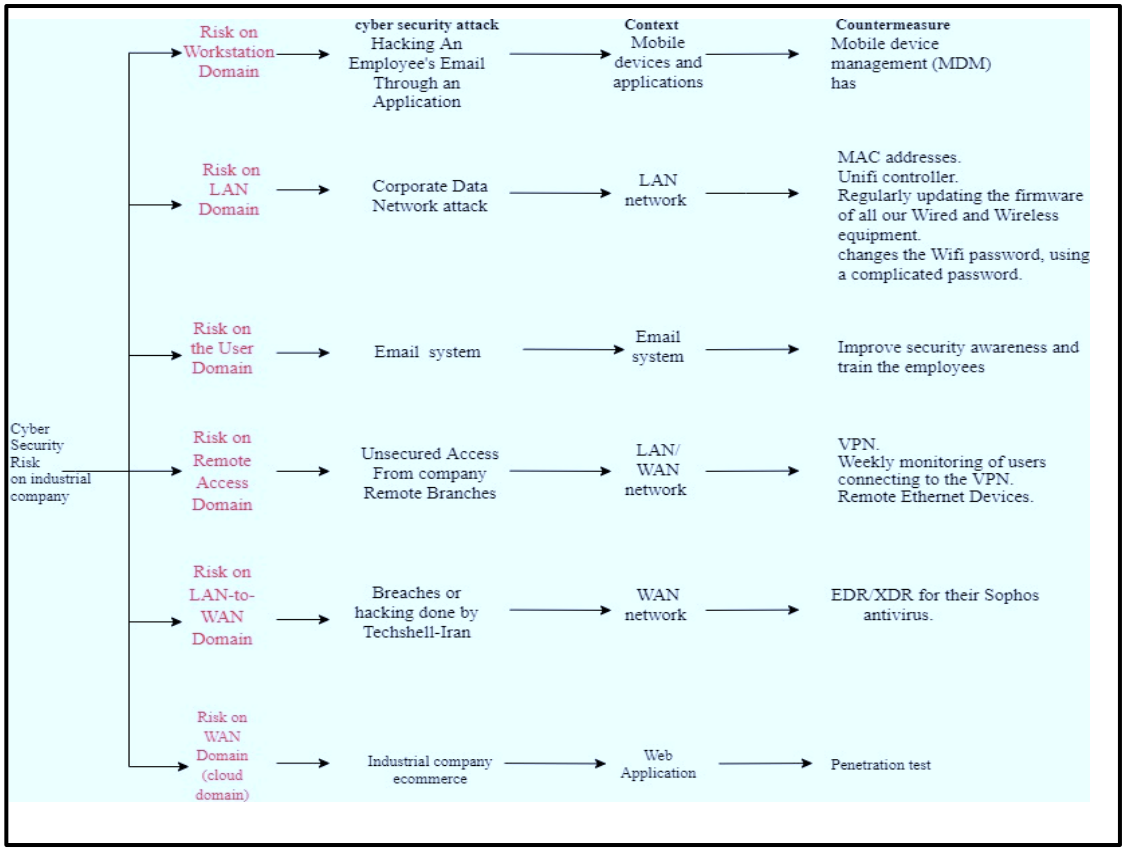

Figure 1. The identified threats were filtered and classified according to the IT domains illustrated in.

3. Literature Review

The second section contains the various literature reviews on the countermeasures used to reduce the risks facing industrial companies identified through the case study. This review aims to answer three questions:
What vulnerabilities in industrial companies make them vulnerable?
What is the highest threat that may affect industrial companies?
What mitigation techniques should be used to reduce this threat?

3.1 Related works

In this section, the paper will provide various literature reviews that investigate the same topic regarding industrial company threats, risk analysis, and industrial company risk mitigation. Hussain and Geoffrey [4] conducted a literature review on the most critical problems and issues facing organizations in developing human knowledge to protect against social engineering attacks. It is necessary to identify the challenges that organizations may face in implementing training and awareness programs to increase the level of awareness of computer users. If information security awareness about the latest technologies used by social engineers is not well maintained, organizations increase the risk of being attacked. The primary objective of information security training and awareness programs is to encourage employees to develop skills in identifying, disrupting, and reporting any attempts dangerous to social engineering. Strengthening information security training and awareness programs can help organizations achieve better results versus social engineering techniques.

Wosah and Win [5] analyzed the literature for various existing phishing mitigations. Users often fall into this type of attack because users are not familiar with how to initiate phishing attacks or how to visually identify legitimate websites to distinguish them from legitimate ones. Existing solutions are either residing in the servers or installed in the users' system and what systems are unknown to the user. Only the system reading determines whether the user will continue or not. This

research paper exposed email and website phishing solutions in phishing attack detection. It is a user education approach that has been introduced to help novice users become aware of the conditions of phishing attacks and may be able to reduce or avoid this risk and possibly stop it as soon as possible. Phishing detection research should be geared towards user-friendliness and identification of a phishing attack by developing a system that can display both email and website's authenticity and malicious nature.

Aakanksha et al. [6] conducted a literature review to classify phishing attacks and possible defense schemes. They classified Phishing attacks into two categories: Social engineering and malware attacks. The most critical defensive techniques used in phasing are user education and software-based defense application, which are divided into (network-level protection, authentication mechanisms, backup, client-side tools, and server-side tools). They explained that a lack of awareness among users is a factor associated with the success of phishing attacks. Educating the user is a requirement to reduce phishing attacks. Nabie et al. [7] conducted a literature review. They found that the human factor will always be a security vulnerability regardless of how secure the network is from a technological point of view. They introduced advanced layered defense in which companies add multiple layers to their security schemes. If a mechanism fails in the outer layer, a tool in at least one inner layer can help mitigate the risks. And there are precautionary measures that must be followed, which are (Security Policy, Technical Procedures, Network Guidance, Audits and Compliance, Education, and Training). Ndichu et al. [8] reported methods and techniques for remote access and recorded vulnerabilities using CVSS to show the importance of security for each area. They found that the VPN is the most widely implemented means of remote access. It has many advantages, but in return, it has risks. It cannot enforce security policies because it does not analyze data packets and cannot regulate access because it does not perform authentication. It cannot detect errors or abuse. Because it does not check the contents of data packets, it can allow high-risk devices to enter the network.

Iqbal and Riadi [9] followed two types of methods, the Literature and Observation Method, and they analyzed a VPN using OpenVPN and applied it to an unsecured public network. They found that using VPN using OpenVPN is very effective and provides good protection. The results showed that it is safe from inhalation. Pandikumar and Tseday [10] conducted a static or dynamic analysis. With the increasing use of web applications, web application security has become vital for confidential user data. They find that most of the vulnerabilities are caused by incorrect verification of inputs. A solution to these problems is penetration testing, which evaluates the security of a computer system or network by simulating an attack from malicious third parties. Vulnerability assessment identifies and reports perceived vulnerabilities. They prioritized managing web application vulnerabilities, given the complex malware targeting client computers within the enterprise. Setiawan and Setiyadi [11] conducted literature studies and analysis of frequent attacks to analyze the various techniques and attacks usually performed on the website. They found that the Vulnerabilities are SQL Injection, Port Status, XSS / Script / HTML Injection, and Directory List. This research used access technology and website script to eliminate this risk and improve security. Radziszewska [12] analyzed the literature and found a correlation between user quality and user experience. Site quality can be a risk of losing users. This paper presents the most well-known evaluation criteria used in various e-commerce sites. It proposes an overall comprehensive framework for evaluating the quality of any e-commerce service concerning two main areas: website features (functionality, easy navigation, information accessibility, reliability, etc.) and e-commerce customer service (product accessibility, personalization possibilities, transaction security, and privacy). Tzavlopoulos et al. [13] Evaluating the quality of e-commerce services is of research interest. Ioannis et al. found that quality has a positive and statistically significant relationship with perceived value, satisfaction, and loyalty, and negative with perceived risk. They found that higher levels of quality lead to increased pleasure and perceived value and mitigation of perceived risk. Positively influencing the adoption of desired consumer behaviors as reflected in customer loyalty. This is brought about by the ease of use of the websites, design, responsiveness, and security.

Ressy et al. [14] researched data theft using a wireless network; the wireless system does not have any restrictions on the signal that can be intercepted. Several security threats can occur data theft by sniffing, malware, and malicious code such as (viruses, worms, trojans, or logic bombs), Theft, and industrial and foreign espionage. IP and MAC filtering is a way to protect wireless networks from use and abuse by anyone. Okemir [15] search on a wireless local area network is wireless access. The most critical risks are Unauthorized Clients, Renegade Access Points, Interception and monitoring of wireless Traffic, Access Point Clone, Traffic Interception, etc. The countermeasure used in this type is MAC Address Filters, Wired Equivalent Privacy, and Service Set Identifier SSID. Lin et al. [16]. Researched the most critical risks in mobile devices and cloud computing technologies. These services face various security and access control challenges due to the lack of security solutions to provide secure access to these services. An effective security solution for heterogeneous Mobile Cloud Computing (MCC) services can ensure confidentiality and integrity.

Ping and Zheng [17] gave a thorough review of dynamic mobile malware and how it should include detected. The type of malware is Creating a backdoor, intercepting data, Manipulating hardware and inserting firmware, and creating a botnet. It is seen by Privacy preservation, the ability to identify unknown apps, Detection accuracy, and Real-time detection support. Murat and Yildiray [18] analyzed the most critical threats faced by the mobile operating systems Malware, Vulnerabilities, Attacks, and the risks posed by these threats. The result is that the Android operating system is the most OS sending malware through. Also, they show that Apple IOS is the most secure operating system because of its closed code. Ahmad Karim and Syed Adeel Ali Shah [19] conducted a comprehensive survey of current botnet attacks on mobile devices. It turns out that Android devices are less resistant to mobile robot networks. This is because it is open source, and it is a suitable environment for the spread of bot networks because users use it more. Amita G Chin and Philip Little [20] surveyed Undergraduate business students at a Regional Public University. Results display that security precautions are not adopted comprehensively. This partial adoption leads to a false feeling of confidence that does not yield efficacy, which puts users at risk. Gupta et al. [21] discussed the types of social engineering that hackers use to penetrate the minds and obtain enough information to catch the victim, steal his data, and clarify the most famous types of social engineering and ways to defend them. Drajad Wiryawan, Joni Suhartono, and Surjandy's [22] objective in this study were to concentrate on identifying basic user behavior on mobile malware for user profile analysis, as they studied the malware package detected on mobile apps in the period between 2019 and 2018 and found that it mostly came in the form of Trojans and risk tools. Then they analyzed user behavior in three categories: maintenance, operation, and modification, and found that 60 % of users do not perform maintenance, and it is the first thing they must do to protect against most threats. In this Ioan Adasc ˘ alit ˘, ei in 2019 [23] showed that the use of Mobile had increased significantly in recent years. Threats, weaknesses, and the most critical security problems for Mobile were identified in this paper. They compared iOS and Android and then found that Android is more vulnerable to threats and found that downloading applications exposes Mobile to more dangers than the device and the network by 75 %. In the study of Pawel Weichbroth and Lukasz Lysik [24], the authors have illustrated the importance of applications in smartphones where applications facilities the user's life, also applications have a large amount of personal data users. On the other hand, many threats stand in front of these applications. The study illustrated several of the best security practices on mobile phones, such as being aware of social engineering.

Table 2. Summarizing the previous literature review

Literature	Addressed Threats	Methodology	Findings and Contributions
Hussain and Geoffrey [4]	Social Engineering Attacks	Literature Review	It was found that the main goal to reduce the risk to the organization is for the organizations to carry out training and awareness programs to increase the level of awareness among employees. Hence, the employee can identify, disrupt, and report any hacking attempts.
Wosah and Win [5]	Phishing	Literature Review And Synthesis	This research paper exposed email and website phishing solutions in phishing attack detection. It is a user education approach that has been introduced to help novice users become aware of the conditions of phishing attacks and may be able to reduce or avoid this risk and possibly stop it as soon as possible.
Aakanksha et al. [6]	Classify Phishing Attacks and Possible Defense Schemes	Literature Review	They classified Phishing attacks into two categories: Social engineering and malware attacks. Defensive techniques used in phasing are user education and software-based defense application, which are divided into (network-level protection, authentication mechanisms, client-side tools, and server-side tools). User awareness is an essential factor in protecting against phishing attacks.

Nabie et al. [7]	Social Engineering Attacks	Literature Review	Precautionary measures must be followed (Security Policy, Technical Procedures, Network Guidance, Audits and Compliance, Education, and Training).
Ndichu et al. [8]	Remote Access and Vulnerabilities	Literature Review	The VPN is the most widely implemented means of remote access.it has many advantages, but in return, it has risks: • Cannot enforce security policies. • Cannot regulate access. • It cannot detect errors or abuse. • It can allow high-risk devices to enter the network.
Iqbal and Riadi. [9]	Analyzed A VPN Using OpenVPN	Literature And Observation Method	Using VPN using OpenVPN is very effective and provides good protection, and it is safe from inhalation.
Pandikumar and Tseday .[10]	Web Applications	Static Or Dynamic Analysis.	They found that most of the vulnerabilities in the web applications are caused by incorrect verification of inputs, and they found that the solution to these problems is penetration testing.
Setiawan and Setiyadi. [11]	Website Techniques and Methods of Attack	Literature Studies and Analysis	The website vulnerabilities are SQL Injection, Port Status, XSS / Script / HTML Injection, and Directory List. To eliminate this risk and improve security, use access technology and website script.
Radziszewska. [12]	E-Commerce Sites	Literature Review	The site quality can be a risk of losing users. It proposes an overall comprehensive framework for evaluating the quality of any e-commerce service concerning two main areas: website features (functionality, easy navigation, information accessibility, reliability) and e-commerce customer service (product accessibility, personalization possibilities, transaction security, and privacy).
Tzavlopoulos et al. [13]	E-Commerce Services	Literature Review	They found that higher levels of quality lead to increased pleasure and perceived value and mitigation of perceived risk. Positively influencing the adoption of desired consumer behaviors as reflected in customer loyalty. This is brought about by the ease of use of the websites, design, responsiveness, and security.
Ressy et al. [14]	Data Theft Using a Wireless Network	Literature Review	• Several security threats can occur data theft by sniffing, malware, malicious code, theft, and industrial and foreign espionage. • IP and MAC filtering is a way to protect wireless networks

Okemir [15]	Wireless Local Area Network Is Wireless Access	Literature Review	The most critical risks in wireless access: • Unauthorized Clients. • Renegade Access Points. • Interception and monitoring of wireless traffic. • Access Point Clone. • Traffic Interception. Countermeasure used in this type: • MAC Address Filters. • Wired Equivalent Privacy • Service Set Identifier SSID.
Lin et al. [16]	Mobile Devices and Cloud Computing Technologies	Survey	Risk is providing secure access to these services. An effective security solution for heterogeneous Mobile Cloud Computing (MCC) services can ensure confidentiality and integrity.
Ping and Zheng. [17]	Mobile Malware and How It Should Include Detected.	Literature Review	Devices are exposed to many malware such as creating backdoors or botnets. It can be solved by the ability to identify unknown apps, Detection accuracy, and Real-time detection support.
Murat and Yildiray. [18]	Mobile Operating Systems Malware, Vulnerabilities, Attacks, and the Risk	Literature Review	The result is that the Android operating system is the most OS sending malware through, and Apple IOS is the most secure operating system because of its closed code.
Ahmad and Syed. [19]	Current Botnet Attacks on Mobile Devices	Survey	It turns out that Android devices are less resistant to mobile robot networks. This is because it is open source, and it is a suitable environment for the spread of bot networks because users use it more.
Amita and Philip. [20]	Phishing	Survey	Results display that security precautions are not adopted comprehensively. This partial adoption leads to a false feeling of confidence that does not yield efficacy, which puts users at risk. Therefore, they must raise awareness through training and education.
Gupta et al. [21]	Social Engineering	Literature Review	Discussed the types of social engineering that hackers use to penetrate the minds and obtain enough information to catch the victim and steal his data. And the person should increase his awareness through training and use the backup.
Drajad et al. [22]	User-Behavior on Mobile Malware	Literature Studies and Analysis	They analyzed user behavior in three categories: maintenance, operation, and modification, and found that 60 % of users do not perform maintenance, and it is the first thing they must do to protect against most threats.
Ioan Adasc et al. [23]	Critical Security Problems for Mobile	Literature Review	They compared iOS and Android and then found that Android is more vulnerable to threats and found that downloading applications exposes Mobile to more dangers than the device and the network by 75 %

Pawel and Lukasz. [24]	Applications In Mobile	Literature Review	The study illustrated several of the best security practices on mobile phones, such as being aware of social engineering.

4. Analysis and Findings

Despite the importance of companies protecting their data and controlling it, it was found from the literature review that security holes are an important stage for a risk to occur [7]. The results are shown in Figure 2 indicate that the security vulnerabilities that occur in companies may be concentrated in three forms, namely: 30.6 % of businesses have sensitive data in the cloud [16], 34.3 % Of IT professionals report challenges in ensuring data privacy [15][14], and the highest ratio of security vulnerability that occurs in small and medium companies is that, have employees who do not follow data privacy at the rate of 35.1 % [6] [20].

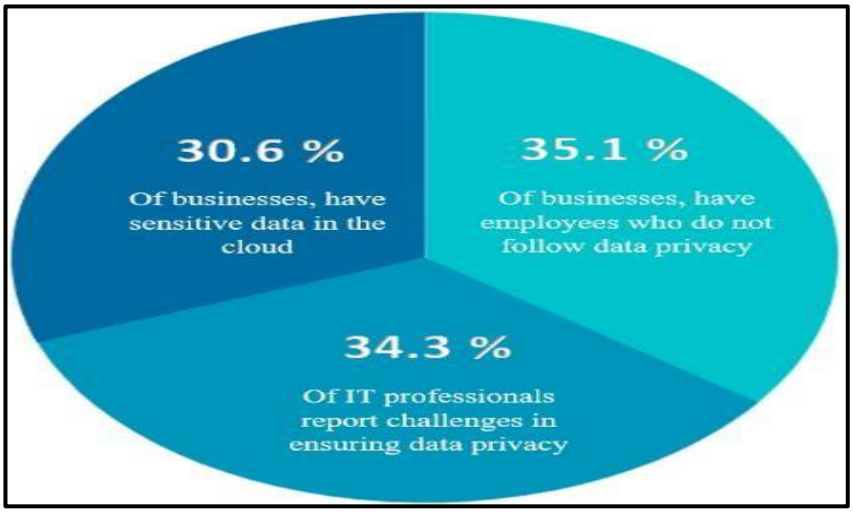

Figure 2. Data vulnerabilities in industrial companies.

58% of IT decision-makers say targeted phishing attacks are the biggest security threat to industrial companies [5]. It attempts to lure the victim into revealing sensitive information to a company. Phishing is a constant threat to companies and a significant concern of the IT department. Unfortunately for all businesses, there will always be someone in the company who falls within the scope of a phishing attack. Figure 3 shows the percentage of phishing attacks across industries.

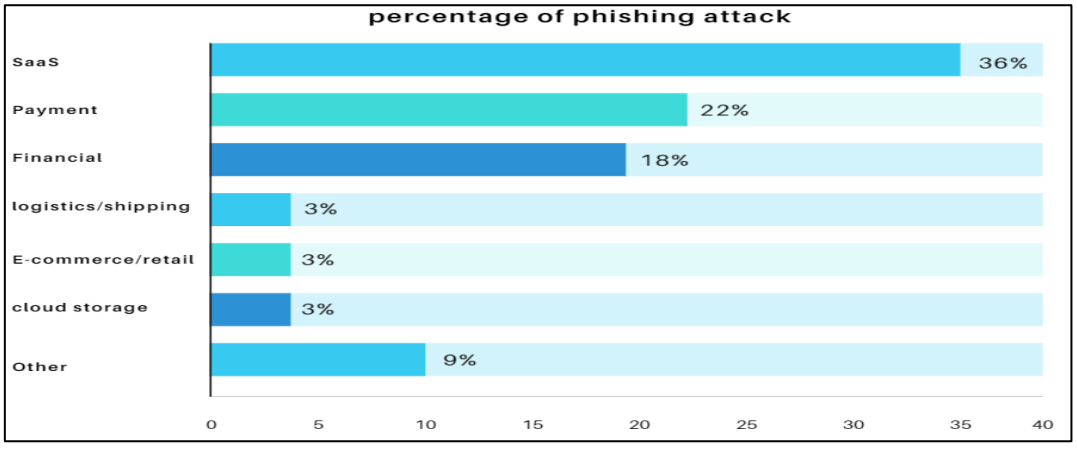

Figure 3. Percentage of a phishing attack.

This section presents the study results related to the most common mitigation methods used in previous studies that industrial companies should follow to address employees' phishing attacks [4-7]. Figure 4 shows the most effective mitigation techniques that an industry company should use to protect against phishing attacks. The most effective is a backup and disaster recovery (BDR) solution, and the second is cyber security training for all employees is most important to prevent these attacks.

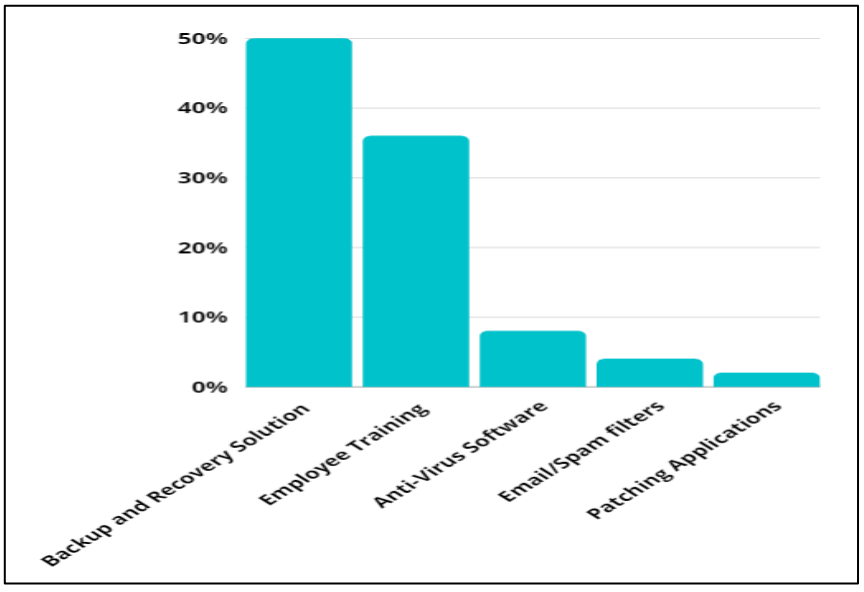

Figure 4. Findings of the most common Mitigation techniques for phishing attacks.

5. Conclusions

This study has demonstrated that the increasing integration of information technology and operational technology in industrial manufacturing environments significantly expands the attack surface and exposes organizations to a wide range of cyber threats. Through a two-part approach combining a real-world industrial case study with a systematic review of the relevant literature, the research identified critical cybersecurity threats affecting industrial systems and examined the effectiveness of existing security measures. The case study provided practical insights into the types of threats encountered in an industrial setting and highlighted the importance of previously implemented security controls in reducing vulnerabilities. The literature review complemented these findings by identifying proven countermeasures and best practices that address similar risks across industrial environments. By bridging practical observations with academic research, this paper emphasizes the need for a comprehensive and proactive cybersecurity strategy that includes technical controls, organizational policies, and continuous risk assessment. Ultimately, the findings can support industrial organizations in strengthening their cybersecurity resilience and better preparing for the evolving landscape of cyber threats.

References

[1] Silva, M. (2018, March 7). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research. Retrieved March 4, 2022, from https://www.academia.edu/36104661/Risk_assessment_and_risk_management_Review_of_recent_advances_on_their_foundation

[2] Abd El-Karim, M. S. B. A., Mosa El Nawawy, O. A., & Abdel-Alim, A. M. (2017). Identification and assessment of risk factors affecting construction researchs. HBRC journal, 13(2), 202-216.

[3] Altoryman, A. (2014). Identification and assessment of risk factors affecting construction researchs in the Gulf region: Kuwait and Bahrain. The University of Manchester (United Kingdom).

[4] Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73.
[5] Wosah, N. P., & Win, T. (2021). Phishing mitigation techniques: A literature survey. arXiv preprint arXiv:2104.06989.
[6] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629-3654.
[7] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.
[8] Ndichu, S., McOyowo, S., Okoyo, H., & Wekesa, C. (2019). A domains approach to remote access logical vulnerabilities classification.
[9] Iqbal, M., & Riadi, I. (2019). Analysis of security virtual private network (VPN) using openVPN. International Journal of Cyber-Security and Digital Forensics, 8(1), 58-65.
[10] Pandikumar, T., & Eshetu, T. (2016). Detecting web application vulnerability using dynamic analysis with penetration testing. International Research Journal of Engineering and Technology, 3(10), 430-433.
[11] Setiawan, E. B., & Setiyadi, A. (2018, August). Web vulnerability analysis and implementation. In IOP conference series: materials science and engineering (Vol. 407, No. 1, p. 012081). IOP Publishing.
[12] Radziszewska, A. (2018). Quality Assessment of E-Commerce Service in the Context of Customer Expiriences. Multidisciplinary Aspects of Production Engineering, 1.
[13] Tzavlopoulos, I., Gotzamani, K., Andronikidis, A., & Vassiliadis, C. (2019). Determining the impact of e-commerce quality on customers' perceived risk, satisfaction, value and loyalty. International Journal of Quality and Service Sciences.
[14] Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A review of ip and mac address filtering in wireless network security. Int. J. Sci. Res. Sci. Technol, 3(6), 470-473.
[15] Park, S. H., Ganz, A., & Ganz, Z. (1998). Security protocol for IEEE 802.11 wireless local area network. Mobile Networks and Applications, 3(3), 237-246.
[16] Olufemi Olakanmi, O., & Oke, S. O. (2018). MASHED: Security and privacy-aware mutual authentication scheme for heterogeneous and distributed mobile cloud computing services. Information Security Journal: A Global Perspective, 27(5-6), 276-291.
[17] Yan, P., & Yan, Z. (2018). A survey on dynamic mobile malware detection. Software Quality Journal, 26(3), 891-919.
[18] Yesilyurt, M., & Yalman, Y. (2016). Security threats on mobile devices and their effects: estimations for the future. International Journal of Security and Its Applications, 10(2), 13-26.
[19] Karim, A., Ali Shah, S. A., Salleh, R. B., Arif, M., Noor, R. M., Shamshirband, S. (2015). Mobile botnet attacks-an emerging threat: Classification, review and open issues. KSII Transactions on Internet and Information Systems (TIIS), 9(4), 1471-1492.
[20] Chin, A. G., Little, P., Jones, B. H. (2020). An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University. International Journal of Education and Development Using Information and Communication Technology, 16(1), 44-61.
[21] Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247-267.
[22] So, I. G., Gui, A. (2019). Malware Mobile Devices in Indonesia. KnE Social Sciences, 259-
267. 3.Markelj, B., Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. journal of information security and applications, 20, 84-89.
[23] Adasc ˇ alit¸ei, I. (2019). Smartphones and IoT Security. Infor- ˇ matica Economica, 23(2).
[24] Felt, A. P., Finifter, M., Chin, E., Hanna, S., Wagner, D. (2011, October). A survey of mobile malware in the wild. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 3-14).