International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

To Study the Impact of Cyber Threats and Cyber Protection Management to Safeguard workplaces

Shonan Kanuga [1*], Dr. Priyanka Ranawat [2]

[1] *Research Scholar, Department of Management, NIMS University, Rajasthan, India*
[2] *Assistant Professor, Department of Management, NIMS University, Rajasthan, India*

ARTICLE INFO

Article history:
Received: 03-07-2025
Received in revised form: 12-08-2025
Accepted: 05-09-2025

Keywords:
Cyber Threats, Cyber Protection Management, Workplace Security, Cybersecurity Awareness, Data Breaches, Risk Mitigation, Intrusion Detection, Information Security, Organizational Resilience, Cyber Risk Management.

ABSTRACT

The increasing digitalization of modern workplaces has heightened exposure to cyber threats, making cyber security a critical component of organizational safety and resilience. This study examines the impact of cyber threats on workplace operations and analyzes the effectiveness of cyber protection management practices in safeguarding organizational environments. It explores various forms of cyber threats including phishing, malware, ran somware, data breaches, and insider attacks and evaluates how these threats compromise confidentiality, integrity, and availability of information systems. The study further investigates protection strategies such as security policies, employee awareness programs, encryption mechanisms, intrusion detection systems, and incident response protocols. Findings emphasize that a well-structured cyber protection framework, supported by continuous monitoring and workforce training, significantly reduces vulnerabilities and enhances overall organizational security posture. The research underscores that integrating technological, human, and managerial controls is essential for creating a resilient and secure workplace capable of withstanding evolving cyber risks.

Introduction

For more than two decades, the Internet has played a significant role in global communication and has become increasingly integrated into the lives of people around the world. Innovations and low cost in this area have significantly increased the availability, use and performance of the Internet, thus that today the Internet has about 3 billion users worldwide (Tan et al., 2021). The Internet has created a vast global network that has generated billions of dollars annually for the global economy (Judge et al., 2021). At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental

organizations and government and governmental institutions, are carried out in cyberspace (Aghajani and Ghadimi, 2018).

Most media activities are transferred to this space, most financial exchanges are done through this space and a significant proportion of citizens' time and activities are spent interacting in this space (Priyadarshini et al., 2021). The share of income from cyberspace businesses in the Gross domestic product (GDP) of countries has increased significantly and among the indicators set to measure the extent of development, cyberspace indicators have a major share [1]. A significant part of the material and spiritual capital of countries is spent on this space and a significant part of the material income and spiritual achievements of citizens are obtained or have a major impact on this space (Amir and Givargis, 2020). In other words, different aspects of citizens 'lives are literally intertwined with this space, and any instability, insecurity and challenges in this space will directly affect different aspects of citizens' lives (Li et al., 2020).

Figure 1: Different types of cyber security

For more than a decade, analysts have pondered the possible consequences of cyber-attacks (Shin et al., 2021). There are various scenarios for severe and sometimes widespread physical or economic damage, including the function of a virus that attacks the financial documents of an economic system or disrupts a country's stock market, or by sending an incorrect message, it will cause the country's power plant to stop and fail, or even by disrupting the air traffic control system, it will cause air accidents (Snehi and Bhandari, 2021; Ahmed Jamal et al., 2021). Therefore, until governments come up with a clear definition of a cyber-attack that is accepted and favored by the

international community, it will certainly be very difficult for experts to address the complex and diverse dimensions and aspects of the issue and provide legal advice and analysis (Cao et al., 2021). Therefore, the question that arises is what is a cyber-attack, what are its characteristics and whether basically any attack that takes place in cyberspace can be considered a kind of attack in its traditional and classic sense or not (Gupta Bhol et al., 2021).

The phrases "cyber security" and "information security" are synonymous to some extent, although they are not the same thing [2]. Information security, as it is often known, refers to the ability of an organization to protect the flow of information across all of its departments. Cyber security, on the other hand, refers to the ability to protect a user's assets and the environment in which they operate from intrusion by an outside party. At the same time, information security is making strenuous efforts to execute the general security objectives, which include safeguarding confidentiality, integrity, and availability while also assuring accountability and carrying out audits [3]. Even though the definitions are relatively analogous to one another, the scopes of each are unique and get progressively more extensive when compared to one another. Our article will be organized as follows: in the first section, we will give an over- view of the present state of the art by focusing on the impact that cyber security has on businesses and governments. Following that, we will talk about the significant financial harm that has been inflicted by breaches in cyber security. After that, we will present a rundown of some of the countermeasures that are used in the realm of cyber security in the subsequent section of this article. In the second part of our conversation, we will examine the key differences between information security governance and cyber security. After that, we will highlight the new framework that is based on EAS-SGR [4].

The science fiction author William Gibson first used the term "cyberspace" in the title of his novel "Burning Chrome" which was published in 1982. Since the release of his novel "Neuromancer" in 1984, which first popularized the word "cyberspace" to describe the virtual world of information networks, science fiction has never been the same again. The term "cyberspace" was originally popularized by William Gibson in his novel "Neuromancer". The

word “cyberspace” refers to the common digital universe that exists across all of the computer net- works of the globe and has come to be used to characterize the total information space [5]. This shared digital universe is referred to as the Internet. The use of automated teller machines, conversing on the phone, engaging in online chat rooms, transferring information through computers, and other similar pursuits are all examples of activities that take place in cyberspace. Because “cyberspace” has more or less become a mainstream euphemism for the internet, one may use the word “exits in cyberspace” to metaphorically allude to the internet as a web- site.

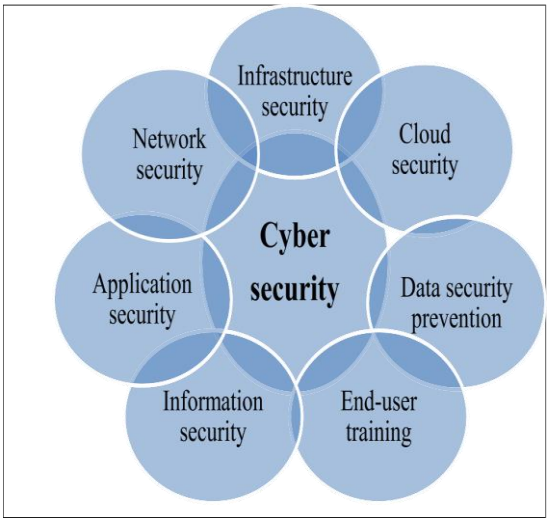

Figure 2: Security triangle (CIA)

The use of electronics and the electromagnetic spectrum to store, alter, and otherwise convey information (or data that has been processed) via networked systems and the physical infrastructures that are linked with them is what defines the region known as cyberspace. It is a method of characterizing the virtual three-dimensional environment that is formed by computer networks and through which electrical signals can travel in text, audio, and video format [6]. This environment can be thought of as being similar to the world of a video game. Cyberspace is the name given to the geographical region of the world in which the use of computers and other forms of electronic processing is most common.

This is true regardless of the type of endeavor: private or commercial. Simple desktop publishing tasks (such as Word, Excel, PowerPoint, and Outlook) are examples of such disciplines. Other examples include scanning and accessing the web online [7]. The fields of data mining, data networks, artificial intelligence, robotics, cyber forensics, biometrics, and computer imaging are among the most complex subfields in computer science. Additionally, the word “cyberspace” is used to refer to all operational regions that are dominated by human-computer interactions and are

driven by a range of high-tech computer systems.

Literature review

Ahmed Jamal A., et al. (2021) [1] presented a comprehensive review of the security challenges in cyber-physical systems (CPS) and discussed the increasing role of machine learning in mitigating these threats. Published in *Materials Today: Proceedings*, their study highlighted the complex interaction between cyber and physical components, which creates vulnerabilities exploitable by advanced attackers. They examined various machine learning techniques such as anomaly detection, supervised learning, and deep learning and evaluated their effectiveness in identifying intrusion patterns and enhancing system resilience. The review emphasized that although machine learning improves threat detection accuracy, challenges such as data imbalance, model explainability, and computational overhead still limit its full-scale implementation. This work contributes valuable insights into the integration of intelligent algorithms for strengthening CPS security architectures.

Al-Ghamdi, M. I. (2021) [2] explored the relationship between cybersecurity knowledge and the ability of individuals to prevent cyberattacks, focusing on how awareness and training influence security outcomes. Published in *Materials Today: Proceedings*, the study argued that adequate knowledge of cybersecurity practices such as safe browsing, recognizing malicious activity, and handling sensitive data significantly reduces vulnerability to attacks. The research underscored that human error remains a major entry point for cyber threats, making user education essential for organizational security. The findings demonstrate that continuous training programs and awareness campaigns can effectively minimize risks, reaffirming the critical role of human factors in cybersecurity defense mechanisms.

Alghamdi, M. I. (2021) [3] In another 2021 study, Alghamdi examined the impact of cybersecurity awareness on employee behavior within organizational settings, particularly focusing on the Saudi Arabian context. Published in *Materials Today: Proceedings*, the study revealed that employees with higher cybersecurity awareness exhibit more responsible digital practices, stronger adherence to IT policies, and reduced susceptibility to social engineering attacks. The research highlighted behavioral components such as cautious email handling, secure password

practices, and compliance with corporate security protocols. Alghamdi emphasized that organizational culture, leadership support, and structured training programs play key roles in shaping secure employee behavior. The study offers practical implications for improving organizational cybersecurity maturity through behavior-focused strategies.

Alghamdie, M. I. (2021) [4] presented a novel study on strategies for preventing cybersecurity threats, emphasizing proactive and defense-in-depth approaches. The work, published in *Materials Today: Proceedings*, discussed multiple prevention mechanisms such as intrusion detection systems, encryption techniques, multi-factor authentication, and secure network architectures. The study also highlighted emerging technologies, including artificial intelligence and blockchain, which enhance security by providing predictive analysis and tamper-resistant data structures. Alghamdie argued that effective prevention requires a combination of technological tools, policy enforcement, and continuous monitoring. The study provides a holistic understanding of how layered defense mechanisms can significantly reduce the likelihood and impact of cyberattacks.

Alhayani, B., et al. (2021) [5] focused on intelligent computational methods for defending against cyberattacks, outlining some of the most effective AI-driven techniques used to detect and mitigate threats. Published in *Materials Today: Proceedings*, their research evaluated machine learning, deep learning, and pattern recognition algorithms that help organizations analyze large datasets, identify abnormal behavior, and respond rapidly to cyber intrusions. The study emphasized that smart computational tools significantly improve detection accuracy and reduce false positives compared to traditional security systems. However, the authors noted that the success of these methods depends on data quality, algorithmic robustness, and continuous system updates. The study underscores the growing importance of computational intelligence in modern cybersecurity defense frameworks.

Alkatheiri, M. S., Chauhdary, S. H., & Alqarni, M. A. (2021) [6] introduced a seamless security apprise method aimed at enhancing the reliability and sustainability of energy-based smart home applications. Published in *Sustainable Energy Technologies and Assessments*, their study emphasized the growing need for secure smart home ecosystems as IoT devices

increasingly integrate with renewable energy systems. The authors proposed a security-aware architecture that supports continuous monitoring, real-time updates, and adaptive threat detection, ensuring uninterrupted operation of smart home applications. Their approach improves both system reliability and user trust by minimizing vulnerabilities in interconnected home energy systems. This study contributes significantly to the ongoing development of secure and sustainable smart home technologies.

Alzubaidi, A. (2021) [7] focused on measuring cybercrime awareness among Saudi nationals by presenting a dataset published in *Data in Brief*. The dataset captured citizens' knowledge levels, attitudes, and behavioral tendencies toward cyber threats, providing a valuable resource for researchers analyzing regional cybersecurity preparedness. The study highlighted variations in awareness across demographics, emphasizing that higher levels of cybercrime literacy correlate with safer online behaviors. Alzubaidi underscored the importance of public education, national cybersecurity policies, and culturally tailored awareness programs to strengthen defense against cyberattacks. This dataset serves as a foundational tool for future empirical research and policymaking in cybersecurity within Saudi Arabia.

Amir, M., & Givargis, T. (2020) [8] explored the Pareto-optimal design space for cyber–physical systems (CPS), offering a methodological framework for balancing performance, energy consumption, latency, and reliability. Published in *Internet of Things*, their study utilized multi-objective optimization to identify trade-offs involved in designing efficient CPS architectures. By applying algorithmic exploration techniques, the authors demonstrated how engineers can systematically evaluate design alternatives that align with system constraints and operational requirements. Their findings highlight the need for optimizing CPS configurations in mission-critical environments where real-time processing and energy efficiency are paramount. This research provides a structured approach for achieving optimal system designs in increasingly complex CPS environments.

Arend, I., et al. (2020) [9] investigated how individual tendencies toward passive versus active risk behaviors predict cybersecurity practices. Published in *Computers & Security*, their work revealed that individuals with passive-risk tendencies—who avoid uncertain or risky situations—are more

likely to engage in secure cybersecurity behaviors such as cautious online activity and adherence to security protocols. Conversely, active-risk individuals tend to underestimate threats and take fewer precautions, increasing system vulnerabilities. The study underscores the psychological dimension of cybersecurity, demonstrating that personality traits significantly influence user behavior. These insights offer valuable implications for designing targeted cybersecurity training that accounts for diverse risk profiles within organizations.

Ashraf, J., et al. (2021) [10] proposed IoTBoT-IDS, an innovative intrusion detection framework for identifying botnet attacks in smart city networks. Published in *Sustainable Cities and Society*, their approach leveraged statistical learning techniques to analyze IoT traffic patterns and detect anomalies associated with botnet activities. The authors highlighted the growing susceptibility of smart city infrastructures to cyber threats due to the rapid expansion of IoT devices and interconnected services. IoTBoT-IDS demonstrated high detection accuracy, low false-positive rates, and scalability across diverse smart city applications. This study contributes a robust security solution that enhances urban digital resilience and supports the development of safer, smarter city systems.

Beechey, M., Kyriakopoulos, K. G., & Lambotharan, S. (2021) [11] investigated evidential classification and feature selection techniques to enhance cyber-threat hunting, as published in *Knowledge-Based Systems*. Their study focused on applying Dempster–Shafer theory and machine-learning-driven feature selection to improve the detection and classification of cyber threats in uncertain environments. The authors demonstrated that evidential reasoning can effectively manage incomplete or ambiguous security data while maintaining high detection accuracy. By integrating reliable feature selection methods, the proposed model reduced computational complexity and enhanced system interpretability. This work contributes significantly to advanced threat intelligence by offering a robust decision-making framework for real-time cyber-threat hunting in complex networks.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2021) [12] discussed the critical role of cybersecurity in protecting national infrastructure within the broader context of homeland security. Featured as a

chapter in *Introduction to Homeland Security* (sixth edition), their work examined the vulnerabilities of essential services such as energy, transportation, and communication systems to cyberattacks. They emphasized how increasing digitalization has expanded the threat landscape and underscored the need for integrated risk-management strategies, public-private collaboration, and strong policy frameworks. The authors highlighted various national and international initiatives aimed at strengthening cyber resilience. This chapter provides a comprehensive understanding of cybersecurity as a core component of modern infrastructure protection.

Cao, J., et al. (2021) [13] proposed a hybrid-triggered security controller to safeguard networked control systems (NCS) facing multiple types of cyberattacks. Published in *Information Sciences*, their study focused on designing a controller capable of maintaining system stability and performance even when subjected to denial-of-service attacks, deception attacks, and data-injection threats. By incorporating hybrid triggering mechanisms, the model reduced communication overhead and improved robustness against attack-induced disturbances. The research demonstrated how advanced control theory can be effectively applied to enhance the resilience of critical cyber-physical infrastructures. The findings offer valuable design insights for securing industrial automation systems and smart manufacturing environments.

Chen, J.-K., et al. (2021) [14] examined the prevalence and correlates of cyber deviance among adolescents in Taiwan, published in *Children and Youth Services Review*. Their study explored online behaviors such as hacking attempts, cyberbullying, unauthorized access, and digital piracy, identifying key demographic, psychological, and social factors associated with deviant activities. The research highlighted how peer influence, impulsivity, and exposure to digital risks significantly contribute to adolescents' engagement in cyber deviance. The authors stressed the importance of parental monitoring, school-based digital literacy programs, and targeted interventions to reduce harmful online behaviors. This work contributes critical insights toward understanding youth cyber-risk behaviors in the digital era.

Dash, N., Chakravarty, S., & Satpathy, S. (2021) [15] proposed an improved Harmony Search-based Extreme Learning Machine (ELM) to enhance intrusion detection

performance, as published in *Materials Today: Proceedings*. Their hybrid approach combined the fast learning ability of ELM with the optimization capability of the Harmony Search algorithm to improve accuracy, reduce false positives, and enhance generalization in intrusion detection systems. By optimizing model parameters and feature selection, the proposed system demonstrated superior performance compared to traditional machine-learning methods. The study highlighted the increasing importance of evolutionary algorithms and intelligent computing methods in strengthening cybersecurity defenses against evolving network threats.

Methodology

Cyber security is an important issue in the infrastructure of every company and organization. In short, a company or organization based on cyber security can achieve high status and countless successes, because this success is the result of the company's capability to protect private and customer data against a competitor. Organizations and competitors of customers and individuals are abusive [8]. A company or organization must first and foremost provide this security in the best way to establish and develop itself (Rodríguez-deArriba et al., 2021). Cyber-security includes practical measures to protect information, networks and data against internal or external threats. Cyber-security professionals protect networks, servers, intranets, and computer systems. Cyber-security ensures that only authorized individuals have access to that information (Ahmed Jamal et al., 2021). For better protection, it is necessary to know the types of cyber security.

Cybercrime is any unauthorized activity involving a system, equipment or network. Two different types of cybercrime are: Crimes that use a system as a target, and the crimes that a system unknowingly plays a role in creating. The security of any organization begins with three principles: confidentiality, integrity, and availability [9]. These three principles are referred to as the security triangle, or CIA, which has served as the standard for systems security since the first computer systems (Palmieri et al., 2021). The principle of confidentiality states that only authorized sources can access sensitive information and functions. Example: Military secrets

(Confidentiality). The principles of integrity claim that only authorized individuals and resources can modify, add or remove sensitive information and functions. Example: A user enters incorrect data into a database (Integrity). Availability Principles claim that systems, functions, and data must be avail- able on demand upon agreed parameters based on SLA service level (Availability) (Nguyen and Golman, 2021).

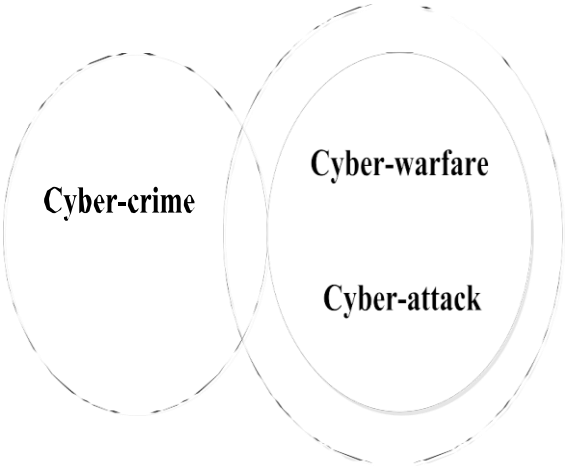

Figure 3: Distinction between cyber-crime, cyber-warfare, and cyber-attack.

The best cyber- security methods go outside the principles outlined mentioned. Any advanced hacker can bypass this easy defense. As a company grows, cyber-security becomes more difficult. Another limitation of cyber-security is treatment with the growing participates with the virtual and actual worlds of data exchange. An important challenge in cyber-security is the absence of eligible occupational to do the work [10]. Many people are at the lower extremity of the vision of cyber-security with general skills. Cyberspace coverage is a broad topic. In the following article, we will review the main types of cyber security.

The country's cyber policy is now a part of the policy of national security. Even if we consider a country's cyber-security policy in line with the State Department policy or the economic policy, these types of laws and policies are not as sovereign as the constitution. In fact, policy is created and published in reports and lectures through discussion of various points and discussions. Policies are created to guide and decide on laws and regulations. The policy itself is not related to rules and regulations. At best, laws, agreements, and rules represent a meaningful and wise policy. In the corporate environment, different departments are expected to follow the rules for fear of sanctions, as the sanctions will continue until the

delinquent sector closes [11]. For instance, human resource, civil, or costing policies are coded to the extent that any non-compliance with the notification rules closes the relevant section. Middle managers support processes such as hiring staff or filing expenses, and are expected to incorporate communicative policies into departmental activities and to create indicators at the departmental level to assess policy compliance.

This is still often considered to be the most critical obstacle that businesses must overcome. At the same time, the volume and scope of attacks continue to increase, and hackers are concurrently accessing information systems increasingly deeper to obtain extremely sensitive data [12]. Based on this analysis, we need to take a more cautious approach to IT risk management and cyber security threats, and we also need to develop a new framework that will assist IT managers in protecting their systems, and more importantly, preventing their systems from being used for cybercriminal activity, which has recently taken center stage in the security arena. Both of these steps are necessary for us to meet our responsibilities.

Figure 4: Concept of information security.

The Risks and Consequences of Cyber Threats

Cyber threats are any hostile acts that are carried out by individuals or groups making use of technology to inflict harm to individuals, businesses, or even nations. These activities can be carried out by anyone, anywhere, at any time. These dangers can manifest themselves in a wide variety of ways, including cyberattacks, data breaches, hacking, identity theft, ransomware, phishing, and many more.

Financial Loss: Individuals and businesses are both susceptible to suffering big monetary losses as a result of cyberattacks. Cybercriminals may steal critical financial information, carry out fraudulent transactions, or demand ransom payments to decrypt material that has been encrypted.

The financial expenditures that can be incurred in detecting and managing cyber assaults, in addition to the possible legal obligations and fines, can be significant.

Reputational Damage: Individuals, corporations, and even national governments all run the risk of having their reputations damaged by cyberattacks. A loss of confidence on the part of customers, partners, and the general public can be the result of data breaches and the leaking of sensitive information [13]. The damaging effects of unfavorable publicity and reputational harm to the brand can have lasting repercussions, including the loss of consumers, partners, and commercial possibilities.

Loss of Intellectual Property: Theft of intellectual property (IP) can be the consequence of cyber threats, and examples of IP include trade secrets, private information, and data relating to research and development. This can have a substantial influence on the competitive edge and market position of a firm, which can ultimately result in financial losses and a loss of market share.

Malware

An attacker using malware will inject malicious software into a target system or network that is unaware of the attack to cause damage, disrupt operations, or obtain unauthorized access to steal sensitive information, banking data, and passwords. Email attachments and websites that have been compromised can be vectors for the distribution of malware such as viruses, worms, and Trojan horses [14]. Malware, after it has been installed on a computer, sets itself up to steal personal data, such as passwords and financial data, and in the most extreme circumstances, it may even take control of your entire system.

Phishing

This danger takes the form of a social engineering assault, in which the perpetrator poses as a member of the target organization to deceive its employees and customers into divulging confidential information. What's worse is that research indicated that a resounding 54% of global MSPs feel that phishing attacks are the biggest cyber security concern for enterprises and the major delivery mechanism for ransomware attacks. This information comes from a poll that was conducted worldwide. These assaults can be difficult to notice, and they involve

urgent re- quests for personal information such as usernames and passwords. These re- quests might come in the form of emails, texts, or other kinds of contact, and they are sent by impersonators of respected businesses.

Result

The country's cyber policy is now a part of the policy of national security. Even if we consider a country's cyber-security policy in line with the State Department policy or the economic policy, these types of laws and policies are not as sovereign as the constitution. In fact, policy is created and published in reports and lectures through discussion of various points and discussions. Policies are created to guide and decide on laws and regulations. The policy itself is not related to rules and regulations. At best, laws, agreements, and rules represent a meaningful and wise policy. However, cyber-security enforcement orders, rules and regulations can be provided without creating a cyber-security policy (Sakhnini et al., 2021).

In the corporate environment, different departments are expected to follow the rules for fear of sanctions, as the sanctions will continue until the delinquent sector closes. For instance, human resource, civil, or costing policies are coded to the extent that any non-compliance with the notification rules closes the relevant section [15]. Middle managers support processes such as hiring staff or filing expenses, and are expected to incorporate communicative policies into departmental activities and to create indicators at the departmental level to assess policy compliance. In the public sector, any type of organizational subdivision faces governance constraints (Baig et al., 2017). There are exceptions, in which different sections of the information classification are taken very seriously, but the company security policy provided by the CEO applies to the whole company, but the security policy issued by the CEO is limited to the domain. Technology staff is applicable.

In addition, one of the undesirable differences between corporate cyber-security policy and human resource or legal policy is that it is left to middle managers. Cyber-security policy may require that ''when the risk of disclosure of confidential information is

high, information should not be provided without carefully examining the recipient's ability to maintain information security (Arend et al., 2020). This policy leaves the assessment of data risk to a manager who may want to reduce costs using outsourcing the flow of information to the office and using people outside the office to do information analysis. Maybe the same manager wants to ignore scrutiny to reduce costs. Such a situation is the result of miscalculations of information responsibilities toward a person who is not a security expert, or perhaps the culture of the organization in question bears the risk. In any case, the division of tasks is essential. These situations become more complex and difficult due to the fact that cyber-security measures have not matured as much as accounting or human resource indicators.

These similarities come from the fact that cyber risk is a relatively new type of risk. On the one hand, first parties, also known as the target, as well as third parties, also known as a counterpart to the target, may be affected by cyber risk. Losses that are sustained as a result of cyber risk, on the other hand, are often modest and unconnected; nonetheless, they may also occur seldom yet have a large impact ("blackout scenario"). According to the explanation provided in the definition of cyber events, the term "cyber risk" does not necessarily have to be synonymous with "cyber attacks." For in- stance, software updates or natural disasters may contribute to the crystallisation of cyber risk through the disruption of corporate operations without any nefarious intent on the part of the actor. Businesses run the risk of having their availability, integrity, and confidentiality of their information compromised as a result of cyber attacks since these are the three aspects of information security that are considered to be of the utmost importance. It is possible for there to be a breach of confidentiality if sensitive information about an organization is divulged to third parties in any way, including through a data breach. When the systems are utilized dishonestly, as is the case with fraud, this can lead to problems with the integrity of the organization. In conclusion, but certainly not least, issues with availability might result in disruptions to corporate operations. The following are some of the ways in which various types of cyber attacks have unique ramifications for the targets of such attacks: However, the

ramifications of data breaches take longer to manifest, and they materialize in the form of reputational damages in addition to legal expenditures. Fraud results in direct monetary losses, whereas data breaches take longer. Interruptions to business operations make it difficult for companies to function, which results in revenue being lost. When it comes to the financial system, business interruptions are more likely to have direct short-term contagion effects than fraud or data breach, both of which tend to have an effect in the short-term on only the firm that is being targeted.

Compromised Intellectual Property

Attacks conducted over the internet can potentially result in the theft of intellectual property from a corporation. It may contain important trade secrets, data on customers, and unique technology, all of which are difficult to recover or re- place and may incur a high cost. The information technology staff has a responsibility to raise awareness of cybercrime and assist all E-Business stakeholders in comprehending the nature of cybercrime. It is the responsibility of all parties involved in e-business to raise awareness about what truly constitutes an e-business from a safety standpoint. The government's information technology sector ought to raise knowledge about the many resources that are available to e-businesses to strengthen security.

The thought process of e-business should be more heavily centered on proactive rather than reactive actions. Many e-businesses do not believe that they are at any significant risk, and as a result, they do not take the matter as seriously as they should. Their way of thinking is predicated on responding to situations as they arise rather than anticipating and preventing them.

Conclusion

The study on the impact of cyber threats and cyber protection management to safeguard workplaces highlights the growing importance of cyber security as an essential component of organizational resilience and operational continuity. As digital systems, cloud platforms, and interconnected devices become integral to day-to-day business operations, workplaces face an expanded threat landscape marked by sophisticated attacks such as phishing, ran somware, data breaches, and insider threats. Findings from the study demonstrate that cyber threats not only jeopardize sensitive information but can also disrupt critical operations, damage organizational reputation, and result in

significant financial losses. At the same time, the research establishes that effective cyber protection management comprising robust security policies, employee awareness training, advanced detection technologies, and continuous monitoring plays a pivotal role in mitigating these risks. Organizations that invest in proactive security measures, such as intrusion detection systems, strong authentication mechanisms, encryption, and incident response planning, are better equipped to prevent, detect, and respond to cyber incidents. Moreover, human behavior emerges as a crucial factor, with cyber security awareness and responsible digital practices significantly reducing vulnerabilities. Overall, the study concludes that safeguarding workplaces from cyber threats requires a comprehensive and adaptive security framework that integrates technology, governance, and workforce readiness. As cyber threats continue to evolve, organizations must adopt a culture of continuous improvement and cyber vigilance. Strengthening cyber protection management not only ensures the safety of digital assets but also enhances organizational trust, efficiency, and long-term sustainability in an increasingly digitalized work environment.

Reference

1. Ahmed Jamal A., *et al.* A review on security analysis of cyber physical systems using machine learning Mater. Today: Proc. (2021)
2. Al-Ghamdi M.I. Effects of knowledge of cyber security on prevention of attacks Mater. Today: Proc. (2021)
3. Alghamdi M.I. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia Mater. Today: Proc. (2021)
4. Alghamdie M.I. A novel study of preventing the cyber security threats Mater. Today: Proc. (2021)
5. Alhayani B., *et al.* Best ways computation intelligent of face cyber attacks Mater. Today: Proc. (2021)
6. Alkatheiri M.S., Chauhdary S.H., Al qarni M.A. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications Sustain. Energy Technol. Assess., 45 (2021), Article 101219
7. Alzubaidi A. Cybercrime awareness among Saudi nationals: Dataset Data Brief, 36 (2021), Article 106965

8. Amir M., Givargis T. Pareto optimal design space exploration of cyber–physical systems Internet Things, 12 (2020), Article 100308

9. Arend I., *et al.* Passive- and not active-risk tendencies predict cyber security behavior Comput. Secur., 97 (2020), Article 101964

10. Ashraf J., *et al.* IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities Sustainable Cities Soc., 72 (2021), Article 103041

11. Beechey M., Kyriakopoulos K.G., L ambotharan S. Evidential classification and feature selection for cyber-threat hunting Knowl.-Based Syst., 226 (2021), Article 107120

12. Bullock J.A., Haddow G.D., Coppola D.P. Cybersecurity and critical infrastructure protection Bullock J.A., Haddow G.D., Coppola D.P. (Eds.), Introduction to Homeland Security (sixth ed.), Butterworth-Heinemann (2021), pp. 425-497

13. Cao J., *et al.* Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks Inform. Sci., 548 (2021), pp. 69-84

14. Chen J.-K., *et al.* Cyber deviance among adolescents in Taiwan: Prevalence and correlates Child. Youth Serv. Rev., 126 (2021), Article 106042

15. Dash N., Chakravarty S., Satpathy S. An improved harmony search based extreme learning machine for intrusion detection system Mater. Today: Proc. (2021)