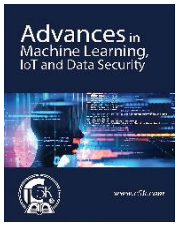
Advances in Machine Learning, IoT and Data Security

"Volume 1, Issue 1, Year 2024"

website: https://www.c5k.com



Research Article

Cybersecurity Strategies for Businesses: Protecting Data in a Digital World

Md. Mehedi Hasan[1,*], Abu Hanif[2]

[1]*Department of Electronics and Communications Engineering, East West University, Jahurul Islam Avenue Jahurul Islam City, Aftabnagar, Dhaka-1212, Bangladesh*

[2]*Department of Business Administration, International American University, 10th Floor, #1000 Los Angeles, CA 90010, USA*

**Corresponding Author: mehedihasan281295@gmail.com*

ARTICLE INFO

Article history:
05 Jul 2024 (Received)
17 Aug 2024 (Accepted)
25 Aug 2024 (Published Online)

Keywords:
***Keywords** - SIEM framework, cyber-attacks, ICT, cybersecurity, business organizations, cybersecurity threats*

ABSTRACT

As more companies and organizations continue to shift their operations online and store crucial data electronically, the exposure of their information to cyber threats becomes even higher. The upward trend in the use of Information, Communication, and Technology (ICT) has led to the creation of major cybersecurity risks and openings. Unfortunate incidences such as hacking the information, communication, and infrastructure networks of several organizations have continued to pose serious risks to organizations. Hackers and intruders nowadays have the equipment and means with which they can penetrate an organization's information systems using the easiest methods. This work brings out various internet security threats: in fact, it casts light on the numerous internet security threats as viewed by business enterprises. It also examines the preventive approaches and methods for improving security to counter these risks. In this particular study, the researchers conducted a systematic review of secondary sources, to establish how organizations should acquire and implement IT security management tools that are consistent with best practice. They pointed out that this has been made possible through the use of a particular framework called the Security Incident Event Management (SIEM) framework. SIEM tools have significant benefits as a source of data for security analysts, who can hence effectively respond to the threats more efficiently.

DOI: https://doi.org/10.103/xxx @ 2024 Advances in Machine Learning, IoT and Data (AMLID), C5K Research Publication

1. Introduction

The flexibility and reliability of service provision has from enhanced greatly because of the advancement in information technology (IT). The trend of dependency on IT can be clearly seen in many organizations where IT is necessary for thousands of operations (Borrett et al., 2013). Both for profit and not for profit organization have realized the importance of IT as most organizational activities are tech inclined. The current computerization process is becoming faster, thereby defining the need for the protection of essential IT assets (Fischer, 2014). Data and devices are often attacked by cybercriminals through hacking and other intrusions, which creates many concerns for business. It can lead to loss of funds or leakage of sensitive information which is becoming more and more prevalent due to migration to cloud environment among different business entities. Jing et al. (2014) on their part have argued that with cloud computing, the occurrence of data breaches and vulnerabilities is set to rise.

In any case, as the risks increase nowadays, many organizations globally still do not have effective strategies for addressing IT security threats, including cybersecurity threats. The following research report aims to elaborate on the main issues concerning internet security; the types of threats that overshadow business entities, ways to reduce them and the enhancement of security barriers. It seeks to emphasize the significance of implementing effective cybersecurity measures and the need for organizations to prevent new risks. By appreciating these issues organizations are in a better position to safeguard its IT asset and be assured of the

*Corresponding author: mehedihasan281295@gmail.com (Md. Mehedi Hasan)

Cite: Md. Mehedi Hasan and Abu Hanif (2024). Cybersecurity Strategies for Businesses: Protecting Data in a Digital World. *Advances in Machine Learning, IoT and Data Security,* 1(1), pp. 24-29.

safety of its information and operations as the world shifts towards digital business.

2. Literature Reviews

This paper aims at analyzing the security issues that have emerged as a result of the adoption of new technologies in the business environment. As businesses increasingly rely on advanced technologies to streamline operations and enhance productivity, they also become more vulnerable to cyber threats. This research delves into the various security challenges that accompany technological advancements, offering a comprehensive examination of the potential risks and the necessary measures to mitigate them.

This study also explores the SIEM framework to a large extent, which plays an important role in protecting computer systems and networks from cybercriminals. Thus, the scalability and flexibility of the SIEM framework, which helps to detect, analyze, and prevent threats in real-time, make it an essential element in addressing modern threats. With regards to SIEM systems, the primary benefit that is presented to organizations is the ability of making it easier to monitor and detect security breaches that could potentially lead to data loss or other cyber related harm.

The arrangement of the bulk of the research is logical and methodical, to ensure a coherent presentation of information. It opens with information on the materials and methods applied in the study, a section that gives details on the research process, data collection, and analysis tools applied. This section provides a basis for explaining why and how this research was done and why certain methodologies were employed.

The paper ends by showing the results that were obtained from the study based on the stipulated methodology. The analysis of the data section of the dissertation will cover this part focuses on presenting the study findings and their implications. The implications of the results are further explained with reference to previous research and analysis to establish relations as well as patterns that help understand the security challenges in focus.

The last section of the work explains how these findings are significant and useful. It discusses implications of the research findings and presents recommendations that organizations that want to improve their security status can implement. The paper also provides the implications of the study with suggestions on areas to consider in the future research or the advancements that can be made towards addressing the issue of cybersecurity.

In conclusion, the purpose of this research is to present readers with a broad understanding of the various security threats that are associated with emerging technologies in the business world and to establish the importance of the concept of SIEM in safeguarding organizations against such threats. Through highlighting the methods, results and implication of the study, the paper aims at presenting relevant knowledge to the field of cybersecurity and guide businesses to create effective security programs.

3. Research Methodology

This paper focused on a literature study with the aim of assessing cybersecurity threats and the possible ways of avoiding such threats. Research papers, books, and journals in the field of cybersecurity offered rich information for study (Onimisi & Nonyelum, 2018). For the purpose of identifying books or

articles with appropriate information, the university library database was searched. As illustrated in Fig. 1, each article was sourced by using key words and searching in the database that are accessible in the university.

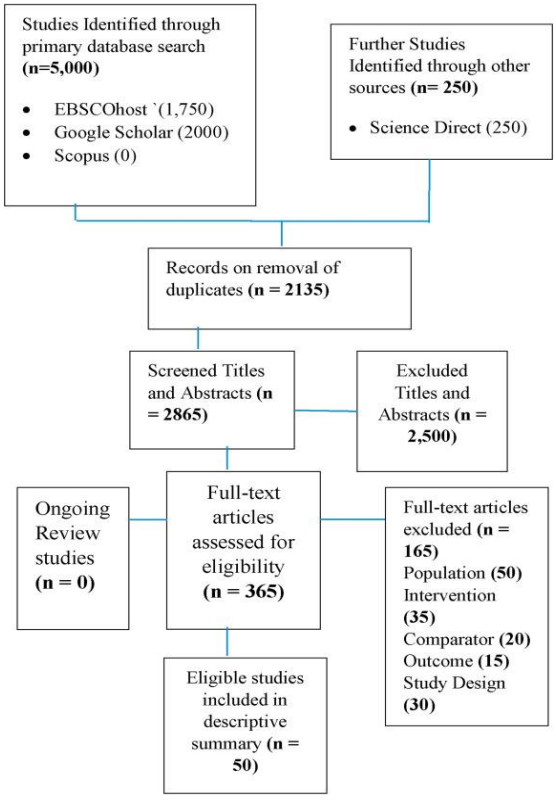


Fig. 1. PRISMA study flowchart of search

The researcher made searches in Google Scholar and other peer-reviewed articles databases and sources such as EBSCOhost, ERIC, and Academic OneFile. Search strings employed included: Information Security Culture, Cyber Security Culture, Security Culture, Organization Culture, and Organizational Culture among others. Using this extensive search strategy, the author was able to retrieve about 5000 documents – formal teaching studies alongside other papers from organizations.

However, a rigorous process of data cleaning was also required to remove duplicate entries that are often found in 'big data' sets. From this process, 2865 journals that had not appeared in the previous list were obtained, and only the titles and abstracts of these journals were reviewed. Of these, 2500 could not be included as they did not meet the specified criteria for inclusion. In addition, research studies defined as "ongoing analysis" and papers with inadequate architectural and research design approaches were also disregarded.

When discussing the significance of cyber-attacks, Flores et al. underlined the unprecedented losses in large and small business organizations, emphasizing that these dangers can be associated with data theft, manipulation, and corruption. It is important to note that such risks can significantly harm an organization's brand and decrease its competitiveness on financial markets. Cyber-attacks commonly occur to the ICT systems of different organizations through hackers and intruders using advanced technologies to penetrate information systems and cause significant damage (Weru et al., 2017). Therefore, to protect existing computer networks, organizations have to establish sophisticated security systems against these threats (Sim et al., 2018). Proactive security measures could include firewalls, intrusion detection and prevention measures, patch management and control measures, and advanced antivirus programs.

In addition, there is no denying the fact that the review recommended an integrated solution to the problem of cybersecurity. This includes technological and policy initiatives coupled with concerns of personnel, incidence management, and forms. The various IT security concerns imply a comfort zone regarding the recognition, avoidance, and management of cyber risks for security-conscious entities. These literature findings give a provisional insight of the present and future threats inherent in cybersecurity and how these risks can be prevented. In conclusion, the study contains recommendations for researchers, practitioners, and policymakers to enhance cybersecurity ademptions and approaches following the data accrued from the information integrated in the study. There is also one more issue that can be considered regular, that is the importance placed at the concepts of continued education and training which, as it has been stated, is crucial in the light of the constantly evolving threat environment.

4. Findings

4.1. Cybersecurity Threats

According to the literature, cybersecurity threats have not only persisted but also assumed different forms and become more sophisticated. Wanyoike et al. (Wanyoike, 2016), observed that 430 million new malware instances were detected in 2015 which is 36% higher to that detected in 2014. As more and more small businesses incorporate technology into their operations, these numbers illustrate the increased risk.

According to Flores et al., cyber threats are bound to affect business organizations, whether small or big ones, and bring about financial repercussions such as theft, manipulation, and data corruption. These risks are detrimental to an organization's brand and lowers the competitiveness of an organization in financial markets. Hackers and intruders often launch cyber attacks against several organizations' ICT systems with advanced technologies to compromise information systems and inflict significant losses (Weru et al., 2017). This poses a major problem to business organizations

As a result, organizations need complex security systems to prevent these dangerous threats attacking computer networks (Sim et al., 2018). Measures of protection may consist of firewalls, intrusion detection and prevention systems, patch management programs, and quality virus protection.

More threats are being expected in the cybersecurity environment because the attackers are being wise in their approach of exploiting systems. These threats include conventional malware such as viruses, worms, Trojans, and spywares, phishing, ransomware, zero-day malware, and the last but not least is advanced persistent threats (APTs). The increase in connectivity of the devices also and the expansion of The Internet of Things (IoT) have also opened new paths for threats through vectors.

SMEs remain more vulnerable to cyber threats due to limited financial resources and inadequate understanding of strategies that can be used to counter advanced IT security measures. Impact observed is cost, disruption of operations and damage to reputation within SMEs due to cyber-attacks. However, the exposures realized in these practices would still remain too high especially for most of the SMEs to provide the ultimate protection systems against such threats thus making them victims of the cyber criminals.

In this case, the primary aspect that should be addressed is the awareness and training of the employees as one of the key elements in protection against cyber threats. That is why someday, human mistakes are still the largest danger, which is being referred to as a Phishing scams action, the widespread use of weak passwords, and the overall ignorance of the population regarding online security. Other advantages include improving the sensitivity of the employees to the threats through regular trainings and educations which in turn enhances the security of the enterprise.

In a way though it can be said that a trend that will continue to rise in the future of the field of cybersecurity, therefore, will be the incorporation of yet more advanced technologies and the implementation of even more anticipatory measures. Currently, security technology is undergoing the integration of artificial

intelligence (AI) and machine learning to monitor and deal with risks in real-time. Also, it is security interesting to note that shift to zero-trust model, where even internal environment is considered to be hostile from the security perspective is the new change that is expected to enhance the security. It thus implies that in order to detect new threats, there will be a constant surveillance, security checks, the organizations and the cyber security professionals will have to work together in handling new threats.

4.2. Cybersecurity Strategies

However, cyber threats are confronting nonprofit organizations that now experience substantial evolution to incorporate contemporary information technologies. Cybersecurity has become a crucial issue that business needs to protect themselves against today in this digital age. With the growing use of e-services within organizations and people going digital making their information more accessible, Singh et al. (Singh et al., 2016) mentioned the risks of mammoth cyber threats. As seen today's users and organizations require reliable systems that will effectively store and secure their data (report, 2016).

In the modern world, computer hackers have developed more complex tactics, which therefore require elaborate equipment to enhance the protection of computer networks. Thus, having a broad security perspective is critical to current IT surroundings for guarding existing networks against inside and outside dangers (Tounsi & Rais, 2018). An exemplar of this framework could incorporate the use of firewalls, IDS/IPS systems, PM solutions, and quality AV packages (Patel & Patel, 2019). All of them serve a function of providing continuous logging and analysis of continuously generated log data within a system to identify suspicious activity as soon as possible.

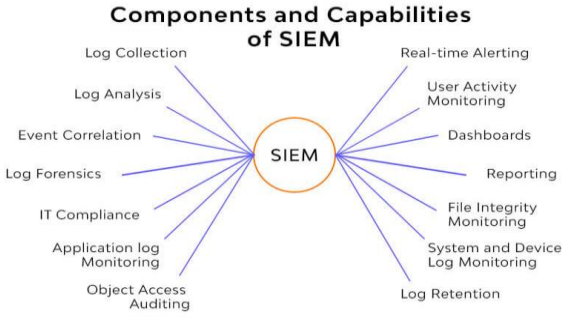


Fig. 2. The components of SIEM system

Adopting such elaborate security policies can be quite taxing for such businesses given that they lack both the funds and, in some cases, the knowledge of how to undertake such measures. Hence, it is essential to find an effective IT security management software that will help manage information technology security in an enterprise. In this context, the framework identified as Security Incident Event Management (SIEM) stands out as a potent weapon, in the words of Pham (Pham, 2018). That is why SIEM software provides security analysts with a wealth of information on security threats against the IT infrastructure of an organization (Rahman, 2016). Through the logs produced by network devices, SIEM systems are able to identify and alert to a possible attack. Fig. 2 highlights some of the key components of a standard SIEM system; correlation of numerous and varied log types from a multitude of disparate sources is required in order to maximize detection ability while minimizing false positives (Regnault et al., 2018).

Finally, Pham (De Vaus & de Vaus, 2013) also point to the need to prioritize threats by pointing out the vital assets in several departments and handling them as soon as possible. After examining the current state of global cybercrime and its growth, the need for a united legal approach is seen as even more significant. The SIEM approach helps with amplification, analysis, and correlation of events from different sources (De Vaus & de Vaus, 2013). SIEM platforms today serve key tasks of threat

identification, incident handling, and centralized log analysis.

In addition, through their work, Singh et al. (Singh et al., 2016) have advocated for IDS as another critical security instrument that complements firewalls, antivirus, and access control to improve the security of communication and information systems. IDS assumes the constant supervision of system and network activities for policy compliance and malware infiltration, then alerts the management stations (Yin, 2006). Of course, IDS is still a rather young technology, but that is all the more reason why it should be considered a truly reliable defense tool in the field of cyber protection. In their view, IDS is a critical element within the context of information security architecture which is described by Azodolmolky et al. (Azodolmolky et al., 2013).

Thus, in today's context where IT environments are not limited to simple local networks any longer, it is crucial for organizations to provide proper cybersecurity and implement such tools as SIEM frameworks to minimize cyber threats and protect confidential data adequately.

This comprehensive approach to cybersecurity involves several key components:

1. **Firewalls:** Firewalls compare the traffic patterns of the network; they act as watchdogs to the network denying any unauthorized access to the network and regulating the traffic within the network.

2. **Intrusion Detection and Prevention Systems (IDS/IPS):** These systems continually and proactively watch all activity within the network for any acts of malware and sound an alert or take an action to prevent a breach.

3. **Patch Management Programs (PM):** Here, it is required to update the software frequently and keep on providing the patch for the vulnerability that is exploited by the attackers.
4. **Quality Antivirus (AV) Packages:** Providing robust protection against malware and other malicious software.
5. **Security Incident Event Management (SIEM):** The capability of collecting and dissecting log data that is derived from various sources to address security threats and risks that are imminent in dynamic environment.

In many nonprofit organizations and small businesses, IT directors rely on limited resources to ensure that their companies do not fall victim to hackers, employing such a broad range of cybersecurity measures. Thus, it is critical to concentrate on those tools and training that provide the most significant improvements to security controls. Furthermore, it is also possible to make use of affordable security tools and technologies like the use of cloud-based security services to give adequate security cover while using less amounts of on-site equipment and facilities.

4.3. Cybersecurity Landscape and Management Strategies

The increasing improvement in information, communication, and technology has made the threat to cybersecurity even more extensive always. This means that to safeguard data, a conscious effort has to be made to address the three data (or Information System) attributes. One of them is confidentiality which is aimed to make sure that certain information is available only to specific people (Carlin, 2015). The second concept is integrity where data and programs are only acknowledged and modified based on standard of the company (Datta, 2017). The third property is reliability/availability, which is the assurance that all stakeholders within the system can gain access to the computer network and the system without much difficulty with long waiting periods.

Cybersecurity threats occur at individual and corporate levels, cutting across big and small companies, and result in variations of loss of money, valuable goods such as digital products, and/or information.

Cyber security is a complex task which is more like a hurdle for small business that need to stay abreast with technological change in the information era. IT has turned into a vital factor in handling numerous key issues concerning service provision and business processes in an organization. Thus, this paper seeks to establish the importance of ensuring that the availability and deployment of IT security management tools adhere to best practices.

One of those tools which should be implemented according to the provided guidelines is the Security Incident and Event Management (SIEM) framework. SIEM solutions enable security analysts to identify and respond to threats targeting an organization's information technology infrastructure [70:It was also more effective in lower amounts in percentage terms, relative to Phase 2 [p20]. They also gather log files from network devices all which can be used in identifying ongoing attack processes. Specific attributes that can be used to define an efficient SIEM solution include the capacity to examine log data from different sources and filter out chaff in order to help analysts review the proper number of alarms.

In addition, organizations should have governance frameworks that involve carrying out periodic risk analysis, creating awareness regarding cybersecurity risks, as well as incorporating other measures like encryption, effective authentication, and detection systems among others. Organizations must also have to be aware of the current trends and styles in the current world with regard to cybersecurity, and they are subjected to change their strategies more often to come up with the best ways of ensuring their security is well enhanced.

In conclusion, management of cybersecurity involves understanding the current and emerging forms of threats, countermeasures, and the general security environment. Using proper measures, SIEM and gaining consistent knowledge of threats cyber security can be effectively maintained to protect information systems of an organization.

5. Conclusion

Computer crime remains a topical issue affecting the information, communication, and technology networks of organizations globally. As cyber threats become more sophisticated, terrorists and criminals employ increasingly complex tools to breach the security of organizational information systems. Protection against these cyber threats requires the implementation of an effective protection system that includes antivirus programs, firewalls, and the Security Information and Event Management (SIEM) system. These tools are crucial for protecting current computer networks efficiently and preventing potential threats.

The SIEM system, in particular, is an essential component in the cybersecurity toolkit. By providing real-time monitoring and analysis of security events, SIEM systems help organizations detect and respond to incidents swiftly. They offer a comprehensive view of the security landscape, aggregating data from various sources to identify patterns and anomalies that may indicate a security breach. This proactive approach enables organizations to mitigate risks before they escalate into significant issues.

Intrusion Detection Systems (IDSs) are equally important security tools used alongside firewalls, antivirus programs, and access control means to

enhance the security of communication and Information systems. IDS works alongside systems to check for signs of policy infringements and alert of any unlawful activities. IDSs can analyze the traffic and behaviors of the systems and networks and identify different types of network intrusions, virus infections, and other malicious activities, which offers a further protection against cyber threats.

The use of antivirus programs, firewalls, SIEM systems, and IDSs all together give organizations a layered security package for defense. They all cover different facets of cybersecurity, creating a strong line of defense when the tools are used in combination. Antiviruses protect against viruses and malicious programs, firewalls regulate entry and exit in computer networks, SIEMs provide comprehensive observation and management of security events, and IDSs identify unauthorized access and policy violations.

In conclusion, there is a need to embrace the right measures of enhancing security in organizations to protect all the valuable information from such invasions and disruptions. The applied technologies and frameworks help in improving security in order to shield businesses against cyber-attacks in the coming years. This is the reason why organizations must always enhance and upgrade their cybersecurity measures to match the latest threat and protect the structural, confidential, and accessible data of their information systems. Purchasing new security systems and making people more aware of cybersecurity threats represent two important stabs in the right direction toward creating better protection against the perpetual threat of cybercrime.

References

Azodolmolky, S., Wieder, P., & Yahyapour, R. (2013). Cloud computing networking: challenges and opportunities for innovations. *IEEE Communications Magazine*, *51*(7), 54-62. https://doi.org/10.1109/MCOM.2013.6553678

Borrett, M., Carter, R., & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider? *J Bus Contin Emer Plan*, *7*(2), 163-171.

Carlin, J. P. (2015). Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. *Harv. Nat'l Sec. J.*, *7*, 391.

Datta, R. (2017). Traditional storytelling: an effective Indigenous research methodology and its implications for environmental research. *AlterNative: An International Journal of Indigenous Peoples*, *14*(1), 35-44. https://doi.org/10.1177/1177180117741351

De Vaus, D., & de Vaus, D. (2013). *Surveys in social research*. Routledge.

Fischer, E. A. (2014). Cybersecurity issues and challenges: In brief. In: Congressional Research Service.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501. https://doi.org/10.1007/s11276-014-0761-7

Onimisi, A. C., & Nonyelum, O. F. (2018). Evaluation and Analysis of Cyber Attacks in Nigeria. *IUP Journal of Information Technology*, *14*(1).

Patel, M., & Patel, N. (2019). Exploring research methodology. *International Journal of Research and Review*, *6*(3), 48-55.

Pham, L. (2018). A Review of key paradigms: positivism, interpretivism and critical inquiry. *University of Adelaide*, *58*.

Rahman, M. S. (2016). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language "testing and assessment" research: A literature review. *Journal of education and learning*, *6*(1).

Regnault, A., Willgoss, T., Barbic, S., & On behalf of the International Society for Quality of Life Research Mixed Methods Special Interest, G. (2018). Towards the use of mixed methods inquiry as best practice in health outcomes research. *Journal of Patient-Reported Outcomes*, *2*(1), 19. https://doi.org/10.1186/s41687-018-0043-8

report, I. s. t. (2016). *Symantec Product Inc*.

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, *21*(5), 619-634. https://doi.org/10.1080/13645579.2018.1454643

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal*, *3*(3), 269-284. https://doi.org/10.1109/JIOT.2015.2460333

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212-233. https://doi.org/https://doi.org/10.1016/j.cose.2017.09.001

Wanyoike, D. M. (2016). *Determinants of ICT adoption by formal small entreprises in Kenya* Entrepreneurship, COHRED, JKUAT].

Weru, T., Sevilla, J., Olukuru, J., Mutegi, L., & Mberi, T. (2017, 30 May-2 June 2017). Cyber-smart children, cyber-safe teenagers: Enhancing internet safety for children. 2017 IST-Africa Week Conference (IST-Africa),

Yin, R. K. (2006). Mixed methods research: Are the methods genuinely integrated or merely parallel. *Research in the Schools*, *13*(1), 41-47.