Journal of Information Technology Management and Business Horizons
"Volume 1, Issue 1, Year 2024"
website: https://www.c5k.com

Research Article

Involving Cybersecurity to Protect Small to Medium-Sized Businesses

Shuchona Malek Orthi[1,*], Mohammad Abu Saleh[2], Md. Mehedi Hasan[3]
[1]*College of Business, Westcliff University, Irvine, CA 92614, USA*
[1]*Department of Business Administration, International American University, Los Angeles, CA 90010, USA*
[3]*Department of Electronics and Communications Engineering, East West University, Jahurul Islam Avenue Jahurul Islam City, Aftabnagar, Dhaka-1212, Bangladesh*
**Corresponding Author: s.orthi.339@westcliff.edu*

ARTICLE INFO

Article history:
5 Jul 2024 (Received)
13 Aug 2024 (Accepted)
21 Aug 2024 (Published Online)

Keywords:
Cybersecurity, Cyber threads, Cyber Bully in SME, Cyberattack, IT Protection.

ABSTRACT

Risk management is a fundamental element for organizations, particularly small and medium-sized enterprises (SMEs), to protect their systems and data from cyberattacks. Information technology (IT) is a fundamental requirement for SMEs, providing access to essential services and data sharing. Cybersecurity is crucial for organizations to prevent unauthorized access to data centers and other computerized systems, ensuring a strong security posture against malicious attacks. SMEs should have multiple layers of protection across potential access points, including data, software, hardware, and connected networks. Employees should be trained on compliance and security processes, and tools like unified threat management systems can detect, isolate, and remediate potential threats. Data protection approaches, including data privacy, integrity, and availability, are essential for protecting critical data. Cybersecurity plays a significant role in IT technology issues, involving tools, policies, security concepts, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies. SMEs face various forms of cyberattacks, such as malware, denial of service (DoS) assaults, and phishing, which can cause significant financial losses and damage to their reputation. The purpose of the study is to shed light on the cyberthreats that small and medium-sized enterprises face as well as some preventative measures.

DOI: https://doi.org/10.63471/jitmbh24001 @ 2024 Journal of Information Technology Management and Business Horizons (JITMBH), C5K Research Publication

1. Introduction

Small and medium-sized enterprises (SMEs) are a fundamental element in the growth and stability of economies worldwide. In the UK, over 99% of all private sector businesses are SMEs, with over 5.6 million SMEs and approximately 16,284,000 employees (Alahmari & Duncan, 2020). Information technology (IT) has become a fundamental requirement for SMEs due to its benefits such as accessibility to essential services like online networks and data sharing among employees. Cloud computing is an example of useful IT technology that helps organizations reduce costs and adapt to difficult economic conditions. Electronic commerce has also become a necessary form of technology for SMEs to prosper in the competitive economic environment. The use of reliable IT technology in SMEs supports their growth and boosts their competitive advantage (Antunes et al., 2021).

Cybersecurity is crucial for organizations to protect their systems, including data, from cyber threats. It involves implementing a robust security strategy to prevent unauthorized access to data centers and other computerized systems. An effective cybersecurity strategy ensures a strong security posture against malicious attacks that can access, alter, delete, destroy, or extort sensitive data (Adewusi et al., 2024; Tarter, 2017). Organizations should have multiple layers of protection across potential access points, including data, software, hardware, and connected networks. Employees should be trained on compliance and security processes. Tools like unified threat management systems can detect, isolate, and remediate potential threats, alerting users if additional action is needed. A strong cybersecurity strategy is essential for organizations to prevent cyberattacks and ensure a quick recovery plan in case of a successful cyberattack (Jahankhani et al., 2022).

*Corresponding author: s.orthi.339@westcliff.edu (Shuchona Malek Orthi)

Cite: Shuchona Malek Orthi, Mohammad Abu Saleh, Md. Mehedi Hasan (2024). Involving Cybersecurity to Protect Small to Medium-Sized Businesses. *Journal of Information Technology Management and Business Horizons*, 1(1), pp. 29-36.

Cybersecurity is also crucial for SMEs, as it enforces the security of all data within a network to protect it from criminal or unauthorized access. Cybercrime is one of the fastest-growing crimes affecting businesses of all levels, especially in relatively smaller and medium-sized enterprises, making it essential to protect sensitive client data, protect companies from breaches, and create a legal buffer (Bada & Nurse, 2019; Jahankhani et al., 2022).

Data protection approaches include data privacy, data integrity, and data availability. Protecting critical data has formed the backbone for many businesses. Many companies worldwide are currently facing different types of cyberattacks, including phishing, denial of service (DoS) attacks, and malware. Poor cybersecurity can lead to near-ruin, as seen in the case of Florida-based IT company Kaseya's ransomware attack in 2021 that spread through its cooperate networks to affect 200 other companies (Adewusi et al., 2024; Bada & Nurse, 2019).

Cybersecurity has a crucial role in IT technology issues that plays a significant role and involves the use of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies to protect the cyber environment and user assets (Bagwell, 2016; Berry & Berry, 2018). The importance of cybersecurity cannot be overstated, as successful cyberattacks can significantly impact the UK's national security and economic stability. Small business managers often lack knowledge and awareness of the importance of security tools, affecting the adoption rate of cybersecurity (Ncubukezi et al., 2020). Risk management is a serious concern for SMEs, as they face different risks due to their small financial and non-financial resources. Traditionally, business strategies show less attention to risk management implications, leading to underestimating risks and causing unfortunate consequences, such as affecting tangible and intangible assets and even leading to bankruptcy (Berry & Berry, 2018).

Numerous businesses throughout the globe are presently experiencing various forms of cyberattacks. Cyberattacks have the power to destroy a business, causing major financial losses and harm to its reputation. The three most prevalent forms of cyberattacks are malware, denial of service (DoS) assaults, and phishing. The study aims to give an overview of cybersecurity risk management in SMEs, the perspectives of recent studies, and crucially, potential directions for future study.

2. Literature review

Cybersecurity is a multi-faceted phenomenon that encompasses protection against malware and hacker attacks, affecting individuals, corporations, and government-run infrastructure. It is often used situationally, but its broadness may make it difficult to understand the theoretical aspects of cybersecurity. This paper explores cybersecurity from critical security studies and critical theory angles, distinguishing it from related concepts like information security and computer security (Walters & Novak, 2021). A taxonomy of cybersecurity is suggested, and it is concluded that cybersecurity must be analyzed critically to fully understand its impacts and implications. Cybersecurity is a shared responsibility, with the Federal government taking a whole-of-government approach to countering cyber threats. This involves leveraging homeland security, intelligence, law enforcement, and military authorities to provide domestic preparedness, criminal deterrence, and national defense. However, much of the nation's critical infrastructure and other potential targets are not owned by the Federal government, and the Federal government cannot provide cybersecurity for every private network. Therefore, cybersecurity must be analyzed critically to fully understand its impacts and implications (Bay, 2016).

One of the most serious crimes committed by computer specialists is cybercrime. This essay discusses the necessity of cyber security as well as some of the effects of cybercrime. Cybersecurity serves as a safeguard against cybercrime, which is a collection of actions taken by individuals to disrupt networks, steal confidential and sensitive information from others, hijack bank accounts and details, and move funds to their own. This essay provides thorough information about cybercrime and cybersecurity. The text covers several aspects of cyber security, such as its kinds, necessity, challenges, benefits, and drawbacks, as well as the background and nature of cybercrime (Buch et al., 2017).

Artificial Intelligence (AI) and machine learning are intertwined in the field of cyber security. Machine learning, a subset of AI, enables systems to learn from historical data, identify patterns, and make logical decisions with minimal human intervention. This integration of cyber security and ML can enhance security, improve the performance of cyber security methods, and support effective detection of zero-day attacks. This paper discusses the advantages, issues, and challenges of uniting cyber security and ML, as well as the various attacks, and provides a comparative study of techniques in both categories. Future research directions are also provided to further explore the potential of these technologies in enhancing cyber security (Wazid et al., 2022). Cyber security is crucial for businesses to prevent data breaches, regulatory fines, and business disruption. Effective cyber security not only drives innovation and revenue but also provides genuine benefits for small and medium-sized enterprises (SMEs). Defending against cybercrime can lead to more valuable organizations and increased efficiency. As organizations move towards digitizing processes, business leaders need to redefine their thinking about security to ensure the protection of sensitive information and prevent cybercrime. By focusing on cyber security, businesses can drive growth and success (Lloyd, 2020).

However, security guidance is a crucial aspect of maintaining information security, with research primarily focusing on preventing security threats using technological countermeasures. A qualitative study conducted in Korea revealed a deep-rooted preventative mindset among businesses, driven by a desire to ensure technology availability and a lack of awareness of enterprise security concerns. The study identified nine security strategies, which were analyzed through a qualitative focus group approach. Security managers from eight organizations were asked to discuss their security strategies, and the findings revealed that many organizations use a preventive approach to maintain technology availability. Some other methods were also used to support the prevention strategy on an operational level. This research highlights the importance of deploying multiple strategies across an enterprise to combine, balance, and optimize systems (Ghelani, 2022).

Medium-sized enterprises (SMEs) are often overlooked in information security and cybersecurity management due to their size, scope, and financial resources. However, a project based on ISO-27001:2013 was conducted in Portugal, involving fifty SMEs. The project was conducted by a business association, the Polytechnic of Leiria, and an IT auditing/consulting team. The methodology was designed and implemented in SMEs, and the results showed a clear benefit to the audited and intervened SMEs. The results showed an increase in the robustness of information security management and increased cyber awareness among collaborators. This project highlights the importance of cybersecurity management in enterprise management, particularly for SMEs (Antunes et al., 2021).

The literature provides what cyber security and cybercrime are. It also enlightens the need for cyber security in businesses. Now, the current research aims to clarify the cyber threats in small and medium-sized businesses and some of the ways to avoid the threats.

3. Methodology

This paper adopts the systematic review procedures for business and management studies, which are divided into three stages: planning, conducting, and reporting. The first stage, "planning the review," is inspired by previous studies and involves identifying the need for a review. The second stage, "conducting the review," involves identifying the main research area, selecting the right studies, assessing these studies, extracting data, and analyzing the extracted data.

The keywords used in the review were searched in six major academic databases presented in Table 1.

Table 1. Database collection table.

Source	No of papers	Percentage (%)
IEEE	16	23.18%
Elsevier	14	20.28%
ProQuest	14	20.28%
Scopus	12	17.39%
SpringerLink	8	11.59%
Science Direct	5	7.24%

For preparatory inclusion, the title, keywords, or abstract of the articles had to contain a combination of two groups of keywords:

i. Cybersecurity risk
ii. E-business and information risk.

This research focuses on recently published studies published between 2015 and 2023, including some previous studies. All articles were selected based on two factors:

i. Each article must address a different area of cybersecurity in SMEs only.

ii. They must contain an empirical study.

Around 69 articles out of 75 were chosen for this paper, but more were excluded due to a lack of empirical methods or unclear methodology.

The remaining selected articles were used to proceed to the second and third stages of the study that is the thread analysis, Strong Authentication Mechanism, and related issues. The data analysis methods and main findings of this study are presented, followed by the conclusion and limitations of this research.

4. Results and discussions

The articles on cybersecurity risk management, analyzed using NVivo analysis software tools, provide insights into five major perspectives on SMEs' cybersecurity risk management: threats, behaviors, practices, awareness, and decision-making. These perspectives are categorized into different types of cybersecurity risk management, starting with the most frequently mentioned type in the literature. The analysis of these articles highlights the importance of effective cybersecurity management strategies.

A. Risk Analysis and Threat Modeling

Risk assessment is an effective method for ensuring cybersecurity inside an organization. To ensure cybersecurity, decisions must be made in a manner that is acceptable and unique to each firm. This enables the business to adjust and personalize its cybersecurity protocols to suit its requirements. Risk assessment plays a crucial role in helping organizations identify ways to mitigate possible risks and hazards and help to isolate them.

Furthermore, risk assessment plays a vital role in assisting organizations in preserving their physical and human resources, which in turn protects their assets. Risk assessment plays a crucial role in preventing the firm from incurring legal and operational costs in the case of a loss. Techniques for threat modeling describe the steps required to guarantee cybersecurity.

→ To start, asset identification is a fantastic strategy that involves creating an inventory of all assets, both physical and digital, including staff, software, hardware, and other resources to define the desired scope.

→ The next step is threat identification, which describes every possible method by which the assets that have been identified may be accessed or compromised. Phishing, malware, and insider assaults are common dangers.

→ The third step is vulnerability assessment, which highlights the system's vulnerabilities and gives high-risk locations priority.

→ Lastly, the distribution of resources to effectively handle and reduce the risks mentioned.

B. Strong Authentication Mechanisms

Strong authentication is essential to cybersecurity. To protect data privacy, this involves limiting data access to just those who are authorized. This is especially important for businesses whose workers or clients often use a networked system remotely.

For example, a strong authentication system like CAPTCHA shields the company from highly automated hacks. Additionally, authentication ensures data integrity by guarding against data modification and change. Regular records that detail user access foster employee accountability for staff members.

- Multifactor authentication: A powerful authentication technique known as multifactor authentication (MFA) requires a user to complete two or more independent authentication procedures to obtain access or complete a transaction. For primary verification, a username and password are required. To get secondary authentication, the user must employ techniques like fingerprint scanning or a one-time password (OTP) that is emailed to them. Because multifactorial authentication strengthens data security, it's crucial on several levels.

- Other authentication factors: Single-factor authentication techniques including passwords, pins, biometrics, face recognition, text/email codes, and voice recognition are examples of additional authentication methods. Multifactorial authentication is generally more secure than single-factor authentication. Fig. 1 shows several authentication methods to prevent cyber threads.

Fig. 1. Five authentication methods.

C. Secure Network Infrastructure

The fundamentals of network security are the safeguards that keep a network safe from illegal access and preserve its integrity. Fig. 2 shows a healthy and secure network infrastructure for business offices. Firewalls, intrusion detection/prevention systems, data encryption, and virtual private networks (VPN) are some examples of these network security methods. A firewall monitors and regulates traffic, granting access to the network to only trusted addresses, shielding a network from a wide area network such as the Internet.

- Intrusion detection systems: Intrusion detection systems keep an eye on network traffic in order to spot any unusual activity and report it. This is a little departure from intrusion prevention systems, which keep an eye out for network policy breaches and take additional action to stop any suspected threats.

- Network segmentation: Segmenting the network is another technique to secure data. This is a method for improving performance and enhancing security in networks by segmenting the network into smaller parts. It applies to networked devices. As a result, it divides the network into sections to restrict access in the case of a cyberattack. Sensitive data is shielded and isolated in this way.

Use of VLANS: Virtual private networks (VPNs) are an additional means of guaranteeing data security. These are crucial because they provide consumers with a secure connection when they utilize the Internet to access the company's network. Using VLANs is one method of doing network segmentation. Devices can connect within a network by grouping together and creating a Virtual Local Area Network (VLAN), which separates traffic for each group to achieve segmentation. Fig. 2 shows network security infrastructure inside a business.

Regular vulnerability assessments guarantee ongoing threat detection and neutralization to maintain data protection because cybersecurity is a continuously changing field. Additionally, it enables ongoing monitoring of private information to guarantee total data security. Frequent vulnerability assessments are crucial for spotting times when the system is unavailable and helping to make sure the secure network infrastructure is operating as intended.

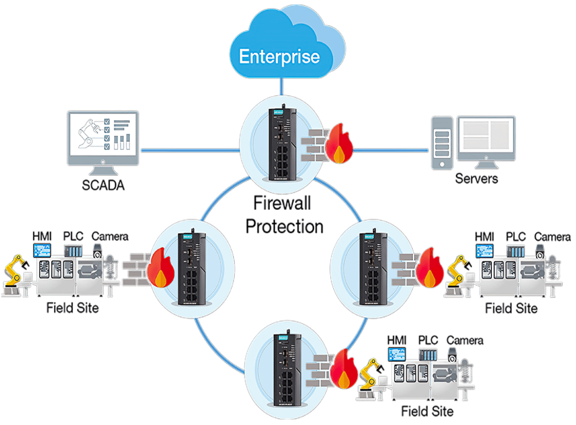

Fig. 2. Network security infrastructure inside a business.

D. Data Encryption

By using data encryption, cybersecurity may also be ensured. Information is encoded throughout this procedure, changing from plaintext to cipher text so that only those with the proper authorization may decode it. Only those who own the decryption key may access the data, even in the event of a cyberattack.

Websites frequently use TLS/SSL to protect sensitive data, including credit card numbers and pins. Using a technique known as digital certificates, the Transport Layer Security/Secure Sockets Layer (TLS/SSL) establishes an encrypted connection between a user's computer and a server or website. It guards against changes and guarantees data integrity. Furthermore, it uses digital certificates, such as those issued by reliable Certificate Authorities, to verify user identities. Thus, data security is guaranteed by this.

Data-at-rest encryption refers to data encryption on a device that is not linked to any network. It's a safety precaution meant to safeguard information on storage devices. The first is complete disc encryption, which encrypts data stored on a hard drive using hardware or software. Because of the ongoing encryption and decryption, which might cause downtime and sluggish processing, this could have an effect on performance.

File encryption is the process of encrypting a single file to improve security and restrict access.

Database encryption safeguards information at the database level, including transactions and customer records. Application encryption processes data to guarantee that it is encrypted before being stored by encrypting the programs themselves.

E. Patch Management

Updating software on time is essential to preserving data security. This is so that flaws and malfunctions that occasionally cause crashes and jeopardize data security may be fixed by software upgrades, as exemplified in Fig. 3 updates also include fixes that address software vulnerabilities that might be exploited by hackers. Additionally, software updates guarantee that gear and software continue to be current and compatible. This guarantees data integrity and the seamless operation of applications.

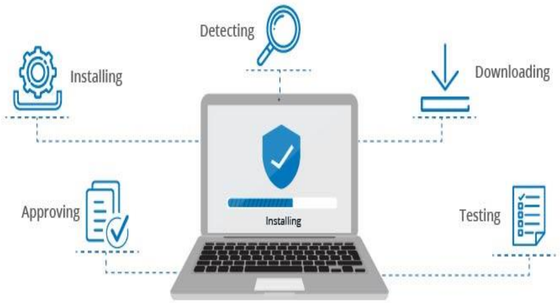

Fig. 3. Patch and vulnerability management.

Regular software upgrades also enable feature additions, which add cutting-edge capabilities to improve functionality and user pleasure. Software upgrades also enhance customer privacy by guaranteeing that data collecting conforms with privacy rules to prevent legal consequences.

Patches are essential for preserving the integrity of data. Security patches play a critical role in addressing vulnerabilities that hackers exploit to obtain unauthorized access to a network. Software compatibility with new hardware and software is maintained by compatibility patches. Hotfixes are crucial for resolving critical and urgent problems before planned releases. Bug fixes guarantee that the product runs normally and address functional concerns. To improve user experiences, feature patches add new features or update current ones.

An example of a compromise caused by an unpatched vulnerability is that the Wannacry ransomware assault in 2017 provided a crystal-clear illustration of what occurs when fixes are not applied. Even with a patch, the National Health Service organizations in the UK were vulnerable to this onslaught since they were left unpatched, which allowed the ransomware to continue exploiting the vulnerability for several months.

F. Employee Training and Awareness

The human dimension is a crucial component of cybersecurity that is often overlooked. To improve data security, employees should be urged to adopt safe browsing habits such as using strong passwords, staying away from dubious links when connected to the network, and logging out of accounts after usage. It is possible to motivate them to report any atypical or dubious actions.

When managing sensitive data, employees should be advised to stay away from public WiFi as it is not secure. As an alternative, you may urge them to utilize VPNs when using free public WiFi.

Additionally, since some potentially harmful advertisements may expose your computer to a cyberattack, they can be instructed on how to use ad blockers. Regular training programs may be implemented to promote safe surfing behaviors and maintain staff awareness of cybersecurity. These consist of training sessions and conferences that give staff members skills and scenarios for managing a cyberattack.

Supervisors can support the implementation of safe browsing behaviors among their staff members and so aid in the enforcement of data security. Interactive questionnaires may be used to identify areas that need more training and to assess employee comprehension. Newsletters are another useful tool for educating staff members about frequent cyber threats. Social engineering is a novel strategy that leverages psychological tricks to coerce individuals into revealing sensitive or private information, hence jeopardizing data security. For example, through phishing, in which emails purporting to be from reputable sources attempt to get sensitive data, including the name of your childhood pet.

Employees can receive training in a variety of social engineering awareness strategies to assist them know what to look for and avoid. One way to check for mistakes is to check for spelling and typos, which should raise red flags. Employees may also be cautioned to be on the lookout for odd sender addresses as another indicator that an email source might be harmful. Pretexting is another popular social engineering technique in which the sender fabricates emotionally charged scenarios in order to control a desired result, such as having lost a relative to cancer. The practice of "baiting," in which a sender presents gifts and requests that a recipient click on a link, has also been added to the list. Last but not least, a popular approach involves a sender making several urgent demands for your answer or asking you to do a task quickly in order to trigger a fight-or-flight response that prevents reasoning from working.

G. Incident Response Planning

An incident response plan is a planned and recorded approach that details what to do in the case of a cyberattack. It provides a straightforward explanation of how to recognize, stop, and handle data security risks. It describes potential dangers and how to mitigate them in an effort to lessen the impact of the assault on the organization. It makes evident the procedures and tools the company has in place to lessen and stop losses and harm brought on by a cyberattack.

Employee duties are explicitly defined in an incident response strategy, which guarantees that any hack is handled effectively and professionally. It is also helpful in minimizing costs brought on by an assault by hastening the organization's operational recovery. Rebuilding quickly is also essential to preserving the organization's credibility. The communication chain that guarantees an efficient exchange of information and prompt decision-making is also described in an incident response plan shown in Fig. 4.

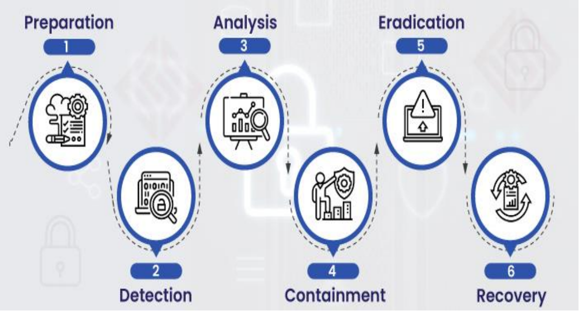

Fig. 4. Six-step incident response.

Planning for incident response starts with thorough previous planning that includes a detailed description of protocols and procedures. The formation of a reaction team, the assignment of responsibilities, and finally the training and equipping of the response team follow. After that, hardware and software are installed in order to recognize and detect security threats.

Upon identification, a threat is subjected to analysis and assessment to ascertain its potential impact. Prompt containment measures are then taken to avert further spread and harm. After that, the threat is eliminated by getting rid of all associated malware. The next step is recovery, which involves improving cybersecurity to thwart future assaults and returning the system to its previous state.

The process of developing mechanisms for a company's defense and recovery in the case of E-danger is known as a business continuity plan. Even amid a crisis, the company can keep providing its goods and services. Plans for disaster recovery, business unit recovery, operations continuity, and emergency response are among the strategies used to safeguard, maintain, and rebuild the company. These business continuity planning strategies support many business continuity planning components using a variety of instruments, such as data backups, evacuation plans, and safety regulations.

H. Cloud Security

Cloud computing, unlike personal computers, uses a network of remote servers to store, manage, and process data. This poses cybersecurity risks and threats to data security, including data breaches, data losses, decreased processing speeds, and vulnerabilities in Application Programming Interfaces (APIs). The shared responsibility model defines the security responsibilities between the provider and the user, with popular cloud computing models including IaaS, PaaS, and SaaS.

The service provider maintains the network infrastructure, provides virtual hardware like servers, and offers storage. It falls on the user to protect stored data, secure the network, and apply regular patches. PaaS (Platform as a Service) provides tools for building and managing software applications, while the user is responsible for data protection, securing the network, and managing access. In SaaS (Software as a Service), the provider delivers ready-to-use software applications over the internet, provides physical and networking infrastructure, and protects user data from unauthorized access.

Best practices for securing data in the cloud include using data encryption, multifactor authentication, regular audits, data backup, data masking techniques, and network security measures such as VPNs, firewalls, and network segmentation. Understanding the responsibilities of the cloud service provider in ensuring data security is crucial, as it involves separating and excluding sensitive information and storing as little as possible on the cloud to limit the possibility of data compromise.

I. Compliance and Legal Considerations

Data breaches can have significant legal implications, leading organizations to develop policies to prevent legal action. These include the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Gramm-Leach-Bliley Act (GLBA), and Federal Information Security Management Act (FIMSA). Legal consequences of data breaches include lawsuits and fines, which can be costly for organizations. Compliance audits and reporting are also crucial to identify vulnerabilities and prevent breaches before they occur. Regular audits ensure that company policies comply with laws and data privacy regulations, and encourage the use of the latest security technology. Departments are held responsible for data breaches, promoting vigilance in ensuring and promoting data security. Other cybersecurity practices that can eliminate vulnerabilities include backup data, use of anti-virus and anti-malware, 2-factor authentication, and HTTPS on websites. By implementing these measures, organizations can ensure the protection of their data and avoid financial losses and legal consequences.

5. Conclusion

This study highlights the importance of cybersecurity risk management in businesses due to their market shares. Despite the availability of technical solutions, there is a lack of knowledge and awareness of these solutions, particularly from the managerial perspective. Cybersecurity decision-making relies on three perspectives: threat, behavior, and awareness. The study investigates recent studies using the systematic review method to understand the management's role in combatting cybersecurity risks among SMEs. It reveals five management perspectives that play a significant role in combating and reducing cybersecurity risks. Future research should explore the relationships between these perspectives to develop more accurate solutions theoretically and practically. Studying SMEs' cybersecurity behavior could minimize potential threats, particularly for those relying on e-commerce. More empirical studies of cybersecurity risk management in SMEs are required, especially for developing countries. The study acknowledges limitations, such as using specific keywords and academic databases to select the right articles and a specific period for collecting articles. In conclusion, practices such as risk assessment, robust authentication, network security infrastructure, data encryption, patches, employee training, and incident response planning are crucial for ensuring cybersecurity. Prevention is better than cure, and proactive measures are better than reactive measures.

References

Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews*, *21*(1), 2263-2275.

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA),

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219-238.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.

Bagwell, M. A. (2016). *Organizational decisions about cyber security in small to mid-sized businesses: A qualitative study* Northcentral University].

Bay, M. (2016). What is cybersecurity. *French Journal for Media Research*, *6*, 1-28.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10.

Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of cyber security and cybercrime.

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*.

Jahankhani, H., Meda, L. N., & Samadi, M. (2022). Cybersecurity challenges in small and medium enterprise (SMEs). In *Blockchain and Other Emerging Technologies for Digital Business Strategies* (pp. 1-19). Springer.

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer fraud & security*, *2020*(2), 14-17.

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST),

Tarter, A. (2017). Importance of cyber security. *Community Policing-A European Perspective: Strategies, Best Practices and Guidelines*, 213-230.

Walters, R., & Novak, M. (2021). Cyber security. In *Cyber security, artificial intelligence, data protection & the law* (pp. 21-37). Springer.

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT express*, *8*(3), 313-321.