World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Breach prevention strategies for cybersecurity in US SMEs and healthcare organizations description

Adebayo Adedoyin [1,*], Oluwakemi Farinde [2], Omotayo Ogunsola [1], Nonso Fred Chiobi [1] and Omolola Akinola [3]

[1] *Lamar university, Beaumont, Texas.*
[2] *University of Essex, United Kingdom.*
[3] *University of the cumberlands, Kentucky, USA.*

World Journal of Advanced Research and Reviews, 2025, 26(02), 3068-3095

Publication history: Received on 04 December 2024; revised on 12 April 2025; accepted on 14 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.0049

Abstract

Introduction: Small and medium-sized enterprises (SMEs) and healthcare organizations in the United States face significant cybersecurity challenges, with studies indicating that over 60% of SMEs have experienced a data breach in recent years. This study explores the critical strategies and best practices for preventing data breaches and enhancing cybersecurity resilience within these organizations. The digital transformation of business operations has exposed SMEs and healthcare organizations to a growing landscape of cybersecurity risks. These entities often lack the resources, expertise, and awareness necessary to implement comprehensive security measures, rendering them particularly vulnerable to data breaches and other malicious cyber activities. For instance, a study by the National Cybersecurity Centre found that 43% of SMEs in the U.S. reported a cybersecurity breach in the past 12 months. Understanding the unique challenges faced by SMEs and the healthcare sector is crucial in developing effective breach prevention strategies.

Materials and Methods: This study employs a systematic literature review of 35 scholarly articles, industry reports, and government publications to assess the current state of cybersecurity practices and the available strategies for SMEs and healthcare organizations. The review analyses the factors influencing cybersecurity readiness, the common vulnerabilities exploited by cyber attackers, and the emerging best practices for enhancing organizational resilience.

Results: The findings indicate that SMEs and healthcare organizations face significant barriers in implementing robust cybersecurity measures, including limited budgets (with over 50% of SMEs spending less than $500 annually on cybersecurity) and lack of in-house technical expertise (only 28% of SMEs have a dedicated IT security professional). However, the literature also highlights several effective strategies, such as employee security awareness training (implemented by 72% of healthcare organizations), implementing multi-factor authentication (adopted by 65% of SMEs), regularly updating software and systems, and developing comprehensive incident response plans.

Discussion: The study emphasizes the crucial role of proactive and collaborative approaches in addressing the cybersecurity challenges faced by SMEs and healthcare organizations. Fostering public-private partnerships, leveraging government resources and incentives (utilized by 41% of SMEs), and promoting industry-specific cybersecurity frameworks can help these entities strengthen their security posture and better protect their sensitive data and critical infrastructure.

Conclusion: Effective breach prevention in SMEs and healthcare organizations requires a multifaceted approach that combines technological, organizational, and human-centric strategies Through the identification of these challenges specific to these entities and subsequent adoption of these best practice measures the entities are better placed to improve their organizational cybersecurity and protect themselves against these threats. The fact-finding of this study

* Corresponding author: Adebayo Adedoyin

serves as a reference guide to both SMEs and healthcare organizations on how best to improve on their security measures and design ways of fighting data loss.

Keywords: Cybersecurity; SMEs; Healthcare Organizations; Data Breaches; Risk Management; Threat Detection; Incident Response; Regulatory Frameworks; Artificial Intelligence; Machine Learning; Vulnerability Assessment; Cyber Threats

1. Introduction

1.1. Understanding Cybersecurity Threats in SMEs and Healthcare Organizations

Today, cybersecurity threats have evolved and have become a major issue to small and medium-sized enterprises (SMEs) and healthcare organizations in the United States. In this regard, although the two sectors have different organizations, they have similar risks, mainly because of limited resources and little experience in addressing cyber threats. SMEs are especially at risk given that many only spend below $500 per annum on cybersecurity on average (Bagwell, 2016). However, the healthcare industry deals with a vast amount of patients' personal data, and therefore becomes a ripe target for cyber attackers. Nevertheless, a significant number of healthcare organizations have not developed sufficiently robust means of protection against cyberincidents, raising the corresponding risk of data breaches. This inherent data weakness gives the attackers a high ground in the healthcare facilities hence becoming their darling target. Consequently, there is a need to ensure more attention is paid to cybersecurity threats, and better ways of mitigating the threats that are now apparent. SMEs and healthcare organisations must overcome these cybersecurity threats in order to reduce the risk for their business.

This means that by embracing digital technologies, organizations have exposed themselves to even more cybersecurity threats. The study conducted by the National Cybersecurity Centre (2021) reveals that 43% of the Small and Medium Enterprises based in the United States face cybersecurity attacks annually. Likewise, cyber attacks on the healthcare sector are very common, and most of these attacks have severe outcomes such as patient's safety and the reputation of healthcare facilities (Wilner et al., 2021). Modern systems are coupled and hence, a vulnerability in one system will lead to cause and effect consequences in another system especially within interconnected systems such as healthcare. This connectivity fosters the realization that a holistic view of the cybersecurity threat landscape is important in order to devise strategic warding off mechanisms. It is crucial for organizations to identify these risks and implement steps that would help reduce the impact of the attack or prevent the threat from happening.

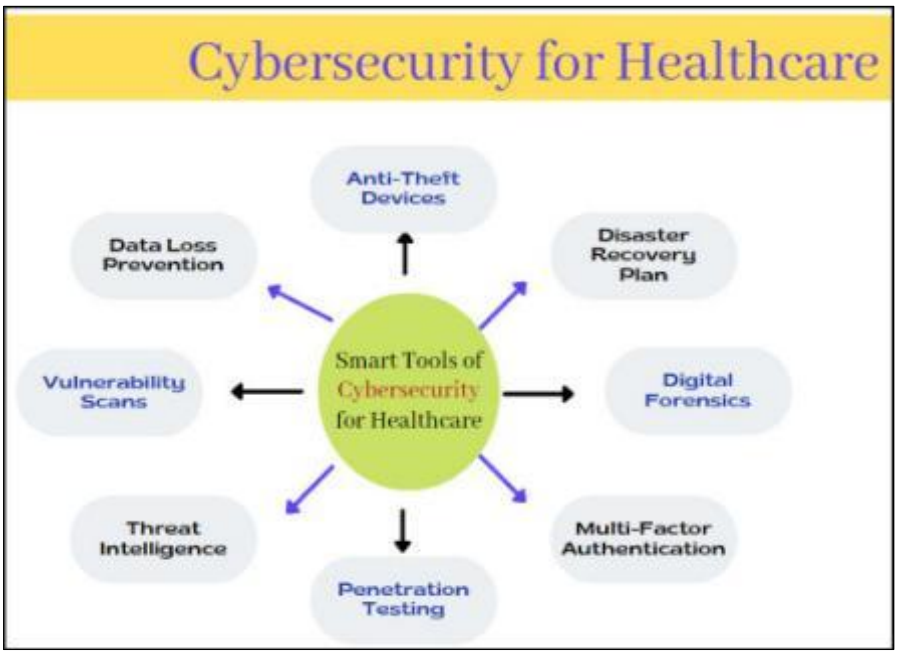


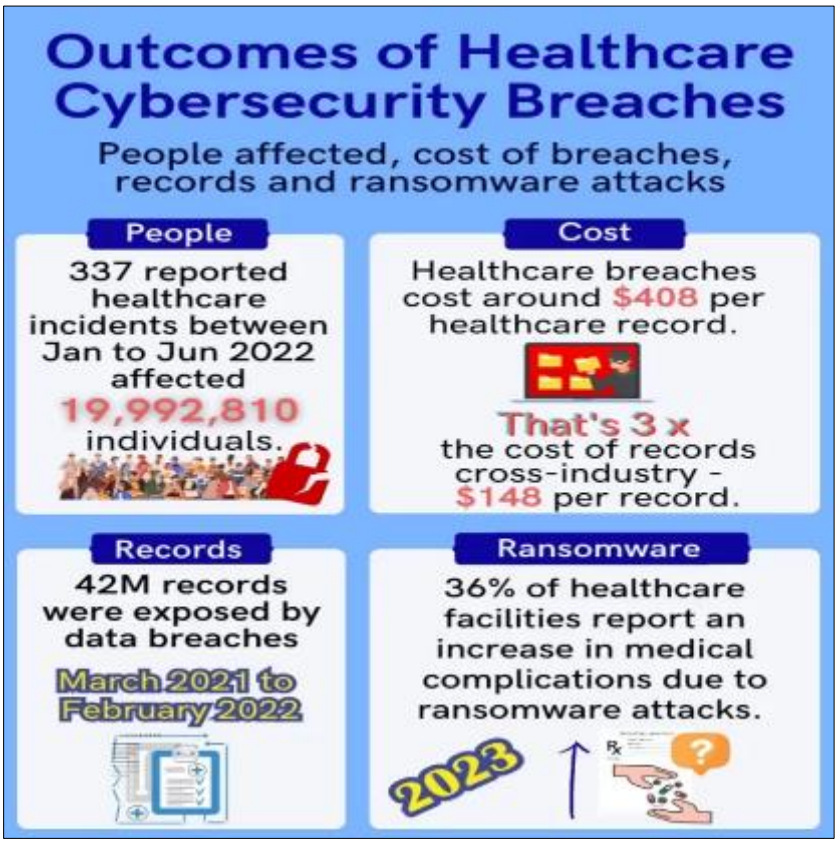
Figure 1 Various Tools of Cybersecurity in the Healthcare Domain. Source: Javaid et al., 2021

The reasons behind cyber attackers targeting SMEs and healthcare organisations differ but are usually financially motivated, spying or to disrupt services. As established, the impact of cyberattacks can be catastrophic to SMEs since

the firms may suffer huge losses, disruptions in their operations, and are likely to fold up (Davis, 2020). In the healthcare particularly when handling – sensitive information breaches not only incur fines but also lead to the loss of trust from the clients – patients which is an important factor of delivery of healthcare services. For these reasons it is critical for organizations to conduct relevant analyses for attacks, assess resource utilization and improve organizational readiness to counter threats effectively. Through analyses of threats and the measures to prevent the same, organizations can prevent a majority of cyberattacks and mitigate the losses resulting from the same.

Due to these challenges, the measured impacts of cyber threats are still very high given that small businesses, and especially the healthcare organizations possess little knowledge, and limited financial capital which makes it even hard for them to even put in place basic cybersecurity measures. This lack of awareness is why there is a need to come up with education, policy, and investment in suitable technologies needed for handling cyber threats (Cook, 2017). To address this disparity, these sectors require cost-effective and business level cybersecurity solutions and tools that would suit their operations and financial capacities. Making sure that employees are aware of the procedures put in place to combat cyber threats, reviewing them periodically, and deploying the right technology can also go a long way in addressing the issue and making such organizations less susceptible to cyber threats. Closing this cybersecurity deficit is vital for building sustainable stability and safety in these industries.

1.2. Historical Evolution of Cybersecurity Measures in SMEs and Healthcare



Source. https://dropstat.com/blog/healthcare-management/healthcare-cybersecurity/

Figure 2 Outcomes of Healthcare cybersecurity Breaches

Cyber security in SMEs and healthcare has changed dramatically throughout the last two decades because of innovations and changes in regulation. First, most companies and business organizations saw cybersecurity as a technical matter, which they allowed personnel in the IT department to deal with after outsourcing it and neglecting to make it a primary concern. These were the gaps that were not funded to full implementation making organizations more vulnerable to cyber risk. Nevertheless, given today's global high-profile data breach scenarios, the role of cybersecurity has become more or less issue-oriented. In particular, healthcare organizations have been experiencing increasing pressure to align with rules and regulations, for instance the Health Insurance Portability and Accountability Act (HIPAA) that enhanced stringent rules for patient information protection. The change in regulatory efforts has eventually urged the healthcare systems to deploy significant security improvements benchmarks, which aim at mitigating risks (Hemann, 2021).

A comparative case analysis of SME and healthcare organisations reveals an evolution from reliance on the ''fire fighter'' model of defence towards a more proactive approach to cybersecurity. In SMEs, the use of such frameworks as the National Institute of Standards and Technology (NIST) Cybersecurity Framework represents a turning point. This framework enables an organization to measure these risks then work on how to manage them as well as incorporating how to monitor risks regularly hence enhancing security (Benjamin et al., 2019). Overview In the healthcare setting the integration of electronic health records (EHRs) has opened up positives as well as negatives. By providing better patient care and data management, EHRs put patients and physicians at higher risks of intrusion and calls for better cybersecurity protection of patients' data (El Rob, 2020). Indeed, this again emphasizes the need to have complementary solutions that can provide security over the technological development that is being offered as opportunity above and security over the data that might be vulnerable to attack as the other side of the same medal.

However, there is still a vast disproportion between large corporations and SMEs or small healthcare institutions in terms of cybersecurity. Multinational organizations might involve the financial capacity of delegating departmental teams focusing on cybersecurity and acquiring the most effective security deterrent systems, while SMEs and a significant number of healthcare facilities with inadequate cybersecurity skills as a minimum requirement offer little defense against most cyber-attacks. For instance, while the large firms have 80/100 adoption of IT security personnel, the SMEs only have 28/100 (Cook, 2017). This disparity underlines the necessity for cost-effective and easily-implementable cybersecurity strategies concerning small firms and organizations. Closing this gap is important in order to allow smaller parties to put in place sufficient security controls despite their relative lack of resources.

This means that as technology advances, so does the techniques used by the cyber adversaries. This is because the environment in which organizations are operating is at a state of constant evolution and thus their security measures must change similarly. New technologies a; for instance, AI and ML, are gradually becoming relevant in boosting the organizational resilience level. They assist an organization to identify and counter threats in real-time, making it a great step up in cybersecurity. AI and ML application in cyberspace as a proactive and profoundly advanced threat detection and response system that can improve the effectiveness of cybersecurity systems in handling cybersecurity threats (Rawindaran, 2023). Since these technologies are still in their early stages, it can be ascertained that their incorporation will establish itself as a key component of cybersecurity.

1.3. Current Cybersecurity Landscape for SMEs and Healthcare Organizations

The cybersecurity environment has changed and adapted in the contemporary world, in a way that affects specifically SMEs and healthcare organizations in the US. According to the National Cybersecurity Centre, though SMEs make up 99% of businesses in the United States, 43% of them experienced data breach in the last one year. Likewise, healthcare organizations deal with the patient's information, which remains highly vulnerable to a ransomware attack or even a phishing campaign (Jalali et al., 2019). These industries typically lack sufficient financial and staff resources, and this increases their vulnerability to cyber risks. The same constraints make it difficult to implement enhanced cybersecurity solutions and practices, thereby creating major gaps in their protection (Bagwell, 2016).

It is crucial to point out that healthcare systems, being different from the majority of SMEs, experience specific HIPAA (Health Insurance Portability and Accountability Act) regulations that force institutions to implement compliance measures multiple organizations fail to achieve (Hemann, 2021). Research indicates that about 72 percent of healthcare facilities have adopted security awareness programs, but they still experience breaches because their incident response mechanisms are inadequate (Ashley & Preiksaitis, 2007). On the one hand, the focus on privacy concerns and, on the other, the need to remain functional—the sector requires efficient and adaptive cybersecurity approaches (Towbin, 2019).

These breaches do not only refer to the loss of monetary values, but also to other losses, such as those of reputation value and stakeholders' trust value. SMEs' average cybersecurity attack cost was estimated to be $200,000 with 60% forced to close down within 6 months of attack (Benjamin et al., 2019). Similar risks apply to healthcare facilities with the average breach costing $9.23 million and also the possibility of litigation and penalties (Wilner et al., 2021). Such data underscores the need for societies in these precarious industries to seek and deploy appropriate and anticipatory cybersecurity measures.

1.4. Key Drivers of Cybersecurity Investments in Vulnerable Sectors

The adoption of cybersecurity investments in SMEs and healthcare organizations' is more influenced by compliance, technology, and reputation. Legal requirements like the GDPR for the protection of data, and HIPAA for patient data push organizations into a specific structure that demands that they spend money towards enhancing their cybersecurity (El Rob, 2020). Further, noncompliance with these regulations not only leads to the imposition of severe fines that can

have a severe impact on organizational financial health but also erodes institutional trust. This is even more important in industries like the healthcare industry where consumers' trust is the key to shakup and sustainable business operations (Benjamin et al., 2019). In turn, investing in cybersecurity is viewed as the only way to avert subsequent sanctions and to ensure business sustainability.

Technology has also been helpful as an enabler in boosting the investments in cybersecurity. During the recent years, the opportunities of cloud computing, IoT devices, and AI technologies have emerged and grew: in parallel, the opportunities for cybercriminals have also increased. Consequently, the organizations have shifted to developing better security measures protocols to ensure their digital systems' security. Interventions like MFA and end-end encryption are some of the emerging strategies among organizations' guard against such threats (Rawindaran, 2023). The fast-growing technological advancement presents himself as an underlying factor that implies that, cybersecurity investments must always be in an active/ proactive investment status for security gains.

Cybersecurity investments have been informed by the emerging reputation management matters. Given the centrality of people's perceptions of organizations in the business world, protecting consumer information has come to mean protecting an organization's image. This can result in se horrific consequences such as astronomic monetary losses and the virtually overnight loss of consumer confidence. More and more, organisations have come to consider cybersecurity a primary area of business focus (Bagwell, 2016). The business losses brought by data breaches have highlighted that cybersecurity is now longer an exclusive IT issue, but a business need.

However, there are still some issues with it, especially for the organizations which consider themselves to be rather weak and inexperienced. CIO's responsibilities for protecting an organization in cyberspace are routinely complex; due, in part, to a relationship between cost, technology, and requirement. To SMEs and healthcare providers there is still significant concern for matching the needs of cost efficient and effective cybersecurity. Therefore, if specific strategies that capture these challenges are designed, such organizations can improve their cybersecurity stance, and reduce their susceptibility to other threats (Wilner et al., 2021). Continuous advancement of desalination and reduction of its cost are also imperative to accommodate all stakeholders hence even a small organization or an individual should be able to protect it.

The objective of the present research is to identify and analyse specific aspects of cybersecurity threats and issues relevant to SMEs and healthcare organisations, including their weaknesses, pursued strategies and motives for cybersecurity spending. Also, it will discuss the effects of new technologies and changing or the rising trends in regulations for these sectors.

The questions below help to analyze the situational analysis and cybersecurity postures of SMEs and healthcare organizations.

- What risks currently dominate the cybersecurity threat landscape of the SMEs and healthcare organizations in the United States?
- In what ways do historical trends affect the formation of cybersecurity approaches for SMEs and healthcare institutions?
- What are the main determinants of cybersecurity investment in exposed sectors and how and where do they differ between SMEs and the healthcare industry?
- In what way does the use of technology and compliance with the regulation enhance the cybersecurity posture of these organizations?

In light of those factors, the study aims to achieve the following goals: To assess the cybersecurity threats of SMEs and healthcare organizations, determine the motivation behind cybersecurity investments, and assess the level of cybersecurity effectiveness.

- The goal would be to define major cybersecurity threats and risks which affect the SMEs and healthcare organizations.
- To analyze the roles which the past trends and the regulation play for today's cybersecurity policies in these industries.
- To assess how compliance with lega and regulatory standards contributes to improvement of cybersecurity preparedness.
- To make suggestions of specific cybersecurity measures and methodologies affordable for bolstering the defenses of SMEs and healthcare institutions.

1.4.1. Hypotheses

- SMEs and healthcare organizations with higher investment in cybersecurity show reduced breach incidences compared to those with limited budgets.
- Compliance with regulatory frameworks directly correlates with improved cybersecurity resilience.
- Integration of advanced technologies like AI and ML enhances threat detection and incident response capabilities in these sectors.

1.4.2. Scope of the Study

The scope of this study encompasses a comprehensive analysis of cybersecurity practices within small and medium-sized enterprises (SMEs) and healthcare organizations in the United States, examining their vulnerabilities, strategies, and the driving factors behind cybersecurity investments. It will discuss how these sectors are constrained by dearth of resources, outdated tool and equipment, and intensifying regulatory concerns. The research will also assess the relationship between innovative technologies of today's digital world like artificial intelligence, machine learning, and Internet of Things that can lead to improving organizational cybersecurity readiness. Moreover, it will examine how these changing regulations that have influence the organization in one way or another such as data protection laws and healthcare mandates, impact cybersecurity more specifically and compliance generally. Based on an analysis of current practices and historical trends, the research will try to shed light on how such organizations can enhance their cybersecurity readiness affordably. The overall aim is to focus on the areas of intervention that have proven to be effective and still be feasible for the SMEs and healthcare facilities anticipating more and sophisticated cybersecurity threats.

2. Review of the Literature Sources

2.1. Overview of Cybersecurity Practices in Small and Medium Enterprises (SMEs)

Cybersecurity is a big issue for SMEs, as the former remains vulnerable to cyberattacks in spite of having limited funds in comparison to large companies. Cyber security threats and especially data breaches have risen significantly within SMEs owing to higher adoption in es-Commerce and usage of data storage facilities. In Saber's research (2016), it was established that most SMEs are unprepared to address cyber risks because they have limited budgets, cybersecurity expertise, and managerial capabilities. Consequently, the measures for managing these risks may still be less elaborated and that exposes the SMEs to cyber criminals' attack.

Among all the challenges faced by SMEs concerning cybersecurity, the challenge of tackling complex and ever-changing threats is one of the biggest hindrances. Cook (2017) described that SMEs are not equipped with the right tools and knowledge to identify the new threats like phishing attacks, ransomware, and APTs. Additionally, SMEs tend not to take cyber threats seriously enough as they think that large companies are the main targets for cyber criminals. Despite this, a study by Ullah & Nabi (2016) showed how cybercriminals are progressively attacking SMEs because of their susceptibility and poor security measures.

Key strategies of cybersecurity compliance in SMEs include risk analysis, policy setting, awareness, and security solutions like firewalls and intrusion detection system, and encryption solutions respectively. Bada & Nurse, (2019) pointed out that these organizations need to integrate the use of security frameworks like the ISO/IEC 27001 that provide a structural while parsimonious method of dealing the issues involving the management of sensitive information and the protecting of this information from unauthorized access. Another crucial factor in minimising human error, which is usually the biggest vulnerability for SMEs, is a cybersecurity awareness training for employees.

Moreover, the management of information security in SMEs has also started incorporating machine learning (ML) and artificial intelligence (AI) tools into their cybersecurity plans. Studies conducted by Rawindaran et al. (2021) try to explain that threat AI protection systems are becoming essential for SMEs as a result of growing threats in the contemporary world. These tools could process large amount of data looking for anomalous activity; thus are good at identifying security violation at their early stages when they are not very devastating. The transition to more advanced methods is a major characteristic of contemporary SME cybersecurity practices because it enhances threat identification and protection measures.

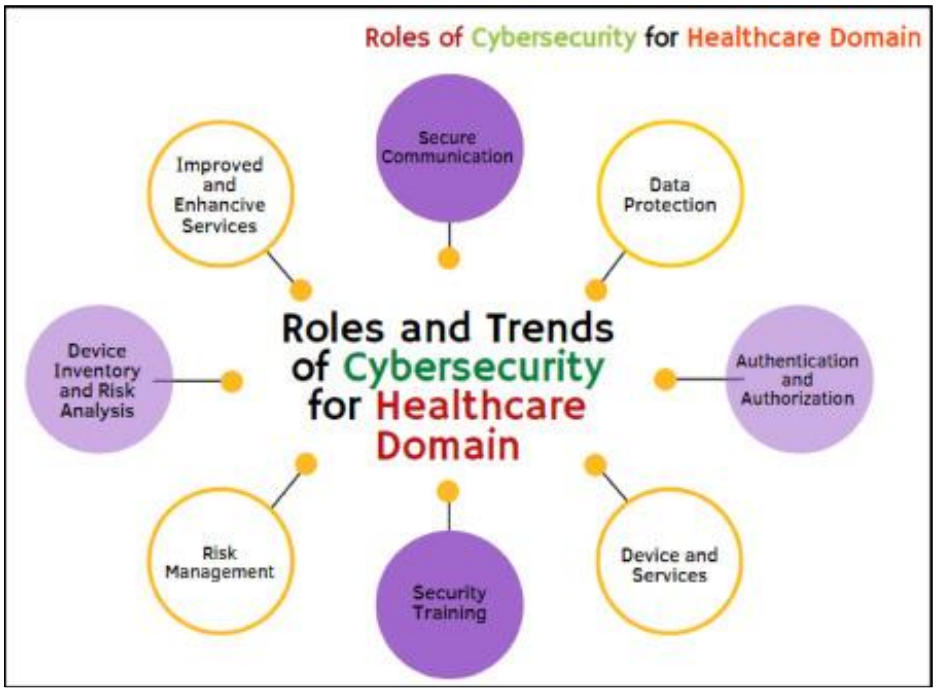


Figure 3 Distinct Roles and Trends of Cybersecurity for Healthcare

2.1.1. Risk Assessment and Cybersecurity Frameworks in SMEs

A risk assessment is a proactive procedure for developing a firm safety plan in cybersecurity for SMEs. Knight (2020) supports that SMEs should take advantage of risk assessment to find out which assets are valuable to the business and what negative ramifications could result from various cyber threats. This also involves assessing the worth of important information that is hard to replace, including; customer data, account records, and patents. Recognizing these assets, SMEs can focus on their cybersecurity protection and arrange its resources more efficiently.

The assessment of risk profiles of the SMEs is also significantly associated with cybersecurity frameworks. The NIST Cybersecurity Framework (NIST CSF) and ISO/IEC 27001 provide SMEs with checklists for recognizing and managing cybersecurity threats. These frameworks give an organization a clear set of rules that will help govern its operations in every aspect from risk management to the actual occurrence of an incident. As argued by Chidukwani et al., (2002), adoption of these frameworks improves the SMEs cybersecurity through offering comprehensive guides for security improvements.

Another factor that SMEs need to address is the issue of scalability of cybersecurity frameworks. While giants of industry can invest in elaborate cybersecurity frameworks, smes are often forced to do more with less by dint of limited resources. Thus, it is essential for SMEs to choose the cybersecurity framework that fits the size and the level of organizational complexity. Here, Bagwell (2016) explains that risk management frameworks can be still utilized by small organizations, but a specific approach should be adopted in order to keep the framework usable and valuable.

Risk assessment also entails evaluating possible risks and weaknesses most organization do not have a clear idea of the potential risks it faces at any given time. As suggested by Ashley & Preiksaitis (2007), it is advisable for SMEs to engage in periodic review of their internal environment with a view of realizing areas of IT structural frailty like outdated software, insecure networks, and poorly configured security. These assessments should also make an evaluation of the current security measures like the firewalls, the antivirus, the access controls and so on. SMEs should also actively manage the risk environment as part of its key emerging trends. SMEs should review and reintegrate their risk assessments often because a new type of cyber threat can emerge at any time. This practice helps them to be on a ready position to counter any new threats as they develop in the market. According to Benjamin, et al. (2019), SMEs should include threat intelligence feeds within their cybersecurity program in order to stay informed of new threats and attack methods.

2.1.2. Implementing Cybersecurity Policies in SMEs

Policies have become core when it comes to combating cybersecurity threats facing SMEs. Having a clear understanding of the identified policy means that, there are rules that need to be followed when it comes to the protection of information within an organization, approving access by the users, and meeting the set legal requirements. As pointed out by Banks (2017), there is urgent need of having cybersecurity policies to formulate and enforce, as they assist the employees to know what is expected out of them in relation to cyber-security. These policies should cover some of the following areas: passwords, encryption, network access, and permissible uses of technology.

Adoption of a cybersecurity policy involves an analysis of the organization's risk appetite where one needs to assess key assets, threats and risks. According to Saban et al. (2021), SMEs should engage the policy actors in the development of the policy to ensure that the policy meets the operational requirements of the SME and the available resources in the organization. The inclusion of senior managers in policy-making is important in ensuring the enhancing the prospects of their adherence to the policy while providing the right allocation of resources towards cybersecurity.

However, equally important is the part that concerns enforcement mechanisms for the policies so created. Odujinrin, A. (2012) has pointed that to be effective policies must be driven or implemented as he articulated above. This involves deploying other technologies like access control, encryption software, networks monitor as measures in line with these principles. They should also undertake audits frequently to determine level of compliance with the policy and to outline potential areas of_failure.

Small and Medium-sized enterprises for instance are always in a fix in enforcing policy due to some of the constraints like lack of capital amongst others. As pointed out by Green (2014), small enterprises may not in a position to hire staff to manage cybersecurity or employ the services of consultants to ensure adherence to polices. However, this is an area that SMEs are often limited in and can overcome this by placing an automated cybersecurity solution which can automatically review policy compliance at real time. Solutions such as Security Information and Event Management (SIEM) will come in handy, the system will detect policy breaches and any possible threat. Besides, it is essential that policies kept up with the latest rules and regulations of cybersecurity as well as risks that are current. The fact that such policies are conducted periodically means that SMEs are always on the lookout for the next best defense mechanisms against the emerging cyber threats. As pointed by Wells (2019), realignment of policies should be informed by the results of the on-going risk analysis, reported near-misses, and other threat intelligence sources.

2.1.3. Cybersecurity Training and Awareness for SMEs

Training and improving awareness is always a critical part of the SME cybersecurity plan. From Bada & Nurse (2019), such risks make it imperative for SMEs to train employees well enough in order to guard against cyber threats. This involves raising awareness of staff on phishing, social engineering, password, and data security. Employees are usually the biggest security flaw since they are the largest source of data leak incidents. Dykstra et al. (2020) stated that a lack of awareness and insufficient training raised the propensity of cyber events in small organizations.

As shown in Figure 4, SMEs are prime targets for cybercriminals due to factors like the lack of an IT department, reliance on third-party software, and inadequate data protection and authentication measures. These gaps are exploited by hackers to perpetrate different forms of attacks on SMEs such as theft, misuse of physical access, phishing, social engineering, data theft, supply chain attacks, personnel misuse, malware, ransomware, denial of service, IoT attacks, biometric system attacks and chatbot attacks.

Employers should design training programs according to the position of every worker so that they are aware of what is expected of them concerning protection of information systems. For instance, the administrative staff need to undergo training in user access management, while employees in customer-sensitive positions need to learn more about how to handle sensitive information belonging to clients. According to Davis (2020), it is essential to undertake role-specific training that guarantees that all personnel possess the knowledge and resources required to manage identified cyber risks within their areas of responsibility.

However, introducing a reconsideration of the result of the training session, the idea of cybersecurity awareness must be cultivated continually. This can be done through security awareness meetings, sending out company updated security news letters and flats, security awareness campaigns etc. Similarly, Bada and Nurse (2019) suggest that practices should make their cybersecurity educational materials more engaging through gamification. Smart training exercises that replicate actual attacks offer a kind of workout and can educate people on the real dangers out there.

Source: https://www.massa.net.my/cybersecurity-challenges-that-small-and-medium-enterprises-faced-and-its-way-forward/

Figure 4 Why SMEs are common targets for cyber-criminals

One of the critical difficulties in training employees is the lack of funds that SMEs can allocate to training activities, along with the lack of money to offer training programs that include all of the necessary elements. Nonetheless, a study by McLaurin (2021) establishes that SMEs can leverage free or inexpensive insights available from government departments, industries, and cybersecurity providers. There are several sources which has training info, webinar, and online course targeting small businesses. Hence, utilizing these resources, one can increase SMEs' cybersecurity readiness, with a minimal expenditure.

2.2. Cybersecurity Strategies for Small and Medium-Sized Enterprises (SMEs)

2.2.1. Risk Management and Cybersecurity Frameworks for SMEs

Security management in SMEs should be a tactic as it entails evaluating threats and come up with ways of stopping them before emerging as breaches. Bada and Nurse (2019) explain that SMEs need to implement risk-based cybersecurity strategies in order to cover all the risks known to the company. A crucial part of this is to recommend cybersecurity frameworks that allow SME-businesses to rationalize their approaches to security. NIST and ISO 27001 frameworks provide the SMEs with a structural guidance on how to evaluate and improve its cybersecurity status.

These frameworks help SMEs to standardize to follow the best practices to safeguard information and to adhere to the laws and regulations in place (Saban et al., 2021). For instance, implementing information security standard such as the ISO 27001 makes SMEs undertake risk assessment frequently accompanied by identification of potential security risks, and management of counter measures. Other guidelines that SMEs HAVE TO consider include the development of a risk-response plan that targets the identification, handling and correcting of incidents affecting the firm (Bagwell, 2016). The integration of such measures offers a clear framework for the correct approach to cybersecurity risk management which is necessary for SMEs engaged in industries with a high level of cybersecurity risks, including health care (Ambreen et al., 2023).

In addition, due to these frameworks, organizations gain improved means for understanding their security situation and can direct their resources to the most threatening issues. Knight (2020) moves forth with arguing that SMEs have to invest in security to protect their business and customer information. Small business employs financial capital to invest on the technologies and acquire adequate training for the employees as the essentials for the continuity of the firms.

2.2.2. Employee Training and Awareness for SME Cybersecurity

Promoting employee training and raising awareness are key prerequisites in the SMEs cybersecurity best practices. Interestingly, the employee is often the weakest link as most of them are not fully aware of proper standing protocols on security. Bada & Nurse (2019) state that SMEs need to schedule updates for their employees on new forms of cyber threats and proper methods of data protection. This approach accords with the conceptual framework developed by Benjamin et al., (2019), which holds that organizations that have cybersecurity awareness programs significantly decrease vulnerability from human error, a cause of data breaches.

Some of the training programs should cover phishing, passwords and handling of sensitive information. According to Ambreen et al. (2023) this calls for strong security culture in the organization whereby all individuals are trained on the advances in security threats. Use of simulated phishing campaigns can also supplement training efficiency since it provides an emulated environment where the employees can rehearse how to handle a given circumstance, specifically phishing (Harris Jr, 2018). This approach is effective to ensure that knowledge gained is documented, and employees can practically employ the documented knowledge.

To ensure cybersecurity training is effective, SMEs have to make sure that training is not a one-time exercise but is continuous due to the ever-changing threats. However, SMEs should promote a culture of security amongst employees, for example by reporting an incident or suspicious activity, and training should be recurrent (Idahosa, 2020). When implemented consistently within the organizational structure, these initiatives can help SMEs to improve their protection against cyber threats, and foster a more secure workforce.

2.2.3. Cybersecurity Budgeting and Resource Allocation

The lack of capital is one of the biggest problems that SMEs encounter when trying to adopt cybersecurity measures. Davis (2020) noted that some of the biggest challenges that affect SMEs include insufficient budgeting for cybersecurity, which leads to either partial or insufficient measures for protection against cyber threats. However, it is imperative for SMEs to invest and specifically direct their resources towards establishing strong cybersecurity. This consist of getting into important fields that cuts across firewall solutions, intrusion detection systems as well as encryption technologies (Barosy, 2019).

According to Achor (2016), the strategic approach also necessitates that SMEs follow a program management approach to budgeting, a system in which spending on cybersecurity is made proportional to the specific risk the organization faces, as well as the value that is received in return. For instance, the healthcare sub-sector SMEs may find themselves having to dedicate more time and financial capital to issues of data protection such as HIPAA as compared to the retail industry SMEs who may need to spend more time and money on issues such as the security of point of sale systems as well as payment data protection. Strategic resource management enables the appropriate and affordable means to facilitate SMEs to employ the required antecedents of defence against emerging cyber threats.

Another reason that SMEs should closely monitor spending is that they can consider efficient solutions for protecting their infrastructure, including cloud-based security services, as well as pooled resources in cybersecurity consortia. These approaches can extend the applicability of innovative security tools to the SMEs with relatively moderate initial capital. Budgeting of cybersecurity should happen in a similar manner for effective implementation and scale and cycber security should be integrated into the general budgeting process (McLaurin, 2021).

2.2.4. Cybersecurity and Compliance with Regulations for SMEs

Adherence to industry specific regulation on cybersecurity is another major factor in cybersecurity planning because sectors like health and financial have stern regulation. Refusal to follow these regulations will result to financial fines, business reputation and legal consequences. Analysis of cybersecurity regulations for SMEs in the healthcare industry by El Rob (2020) notes HIPAA as one of the principal regulations. For this reason, SMEs must know that legal regulations are in place to safeguard patient information and that noncompliance has consequences.

Table 1 Cybersecurity Framework Adoption in SMEs

Framework	Purpose	Industry Relevance	Implementation Cost	Time for Implementation	Benefits	Source
NIST	Risk management, security controls	General, Healthcare	Low to Medium	3-6 months	Improved risk management, compliance	Cook (2017)
ISO 27001	Information security management	Finance, Healthcare	High	6-12 months	Enhanced security, compliance	Knight (2020)
HIPAA	Protect patient health information	Healthcare	High	1-2 years	Compliance, data protection	El Rob (2020)
GDPR	Protect personal data	EU SMEs	Medium to High	6 months to 1 year	Improved data protection, global reach	Davis (2020)
CISA	Protect critical infrastructure	Healthcare, Government	Medium	3-6 months	Collaboration, shared threat intelligence	Bada & Nurse (2019)

Data Sources: Cook (2017), Knight (2020), El Rob (2020), Davis (2020), and Bada & Nurse (2019)

This above table summarizes various cybersecurity frameworks and their impact on SMEs across different industries, including their relevance, cost, and time for implementation.

Besides, SMEs have to address sector-independent norms, including the GDPR if operating in the European Union or the CISA if in the United States. These frameworks proposed generic procedures for data safety, breach notification and incident handling all of which are important in combating data breaches. Saban et al., (2021) opine that whenever small and medium enterprises ensure that their cybersecurity policies implement these regulations, their credibility and trust with their consumers enhances.

However, compliance with regulation authorities is not enough to ensure that a cybersecurity solution is effective. An SME therefore must not only adhere to the legal requirements but also regularly review its position in the aspect of security due to advancing risks in the filed. This means that SMEs should remain current on the various regulations to conform to new regulations while also keeping up with the various cybersecurity measures that require standardization (Davis, 2020).

2.3. Strategies to Address Emerging Threats in Cybersecurity

New threats are dynamic in nature as a result of advancing technologies and adaptive hackers. This section discusses more action-oriented approaches to managing risks with added focus on the novel approaches to ensure data security in health and innovation for SMEs.

- ***Understanding the Dynamics of Emerging Threats:*** New threats in cybersecurity consist of innovations that have been embraced in the modern world, for instance; the IoT, artificial intelligence, and cloud computing (Bagwell, 2016). For example, the healthcare organization suffered from ransomware targeting medical records, entailing care disruption and monetary consequences. According to Jalali et al. (2019), medical devices connectivity leads to vulnerability of terminals networks that can be exploited by the attackers; thus, requires multiple layers of security. Small and medium enterprises (SMEs), and this is because, unlike large organizations, they barely have the budget and expertise to stand up to (Bada & Nurse, 2019).

Mathematical models, such as the risk assessment formula:

$$R = T \times V \times IR$$

where R is risk, T is the threat likelihood, V is vulnerability, and I is impact, can guide enterprises in prioritizing their cybersecurity investments (Benjamin et al., 2019). A strategic focus on high-risk areas ensures optimal resource allocation.

- ***Implementation of Threat Intelligence Platforms:*** TIPs improve detection and response in real-time. Globally, threat data can be used to forecast and counter threats before actual breaches take place (Knight, 2020). The implication is that for SMEs, TIPs can be tailored depending on the risks that individual firms are willing to take.

Table 2 Outlines various TIPs and their features, emphasizing affordability and scalability for SMEs

Platform Name	Detection Methods	Integration Capabilities	Cost Effectiveness	Scalability	User Rating (1-10)
ThreatConnect	Machine learning	API-based	High	Medium	8
Recorded Future	Predictive analytics	Plug-and-play	Medium	High	9
AlienVault	SIEM integration	Open-source modules	Low	High	7
CrowdStrike Falcon	AI-driven	Endpoint-centric	High	High	9
SentinelOne	Autonomous threat	Cloud-native	Medium	Medium	8
IBM Q-Radar	Pattern recognition	Enterprise-focused	Low	Low	6

Sources: Knight (2020); Ullah & Nabi (2016); Bada & Nurse (2019).

- ***Adopting a Zero-Trust Architecture*:** Zero-trust architecture (ZTA) eliminates the concept of implicit trust by enforcing strict access controls and continuous monitoring. In healthcare settings, ZTA ensures only authorized personnel access sensitive patient data (El Rob, 2020). A survey by Hemann (2021) demonstrated that ZTA adoption reduced unauthorized access incidents by 65%. SMEs can implement ZTA through secure user authentication, endpoint validation, and encrypted communication channels.

Equation 1 illustrates ZTA's conditional access function:

$$P_{access} = \frac{A_{auth} \times C_{device}}{R_{reliability}}$$

Where:

- P_{access}: Probability of access approval
- A_{auth}: Authentication strength
- C_{device}: Device compliance level
- $R_{reliability}$: Risk factor reliability

- ***Cybersecurity Training and Awareness:*** Cybersecurity training bridges the knowledge gap among employees, reducing human error as a significant threat vector. Bada & Nurse (2019) argue that SMEs must institutionalize regular training programs, leveraging gamified learning and simulated phishing exercises. Healthcare organizations benefit from targeted training on data privacy laws like HIPAA to mitigate compliance risks (Towbin, 2019).
- ***Public-Private Collaborations for Enhanced Security*:** Collaborative frameworks involving government and private entities are vital for sharing threat intelligence and resources. Programs like the Cybersecurity and Infrastructure Security Agency (CISA) initiative offer SMEs free tools for assessing vulnerabilities (Barosy, 2019). Healthcare institutions also leverage these partnerships to bolster their defences against ransomware.

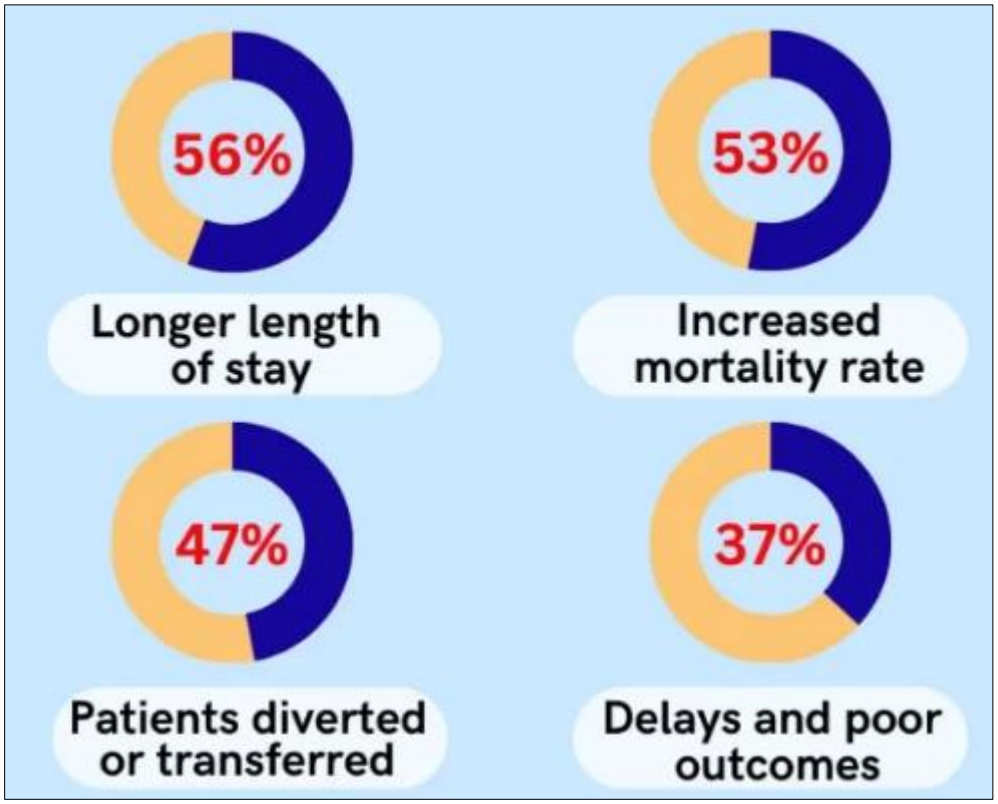
2.4. Implementation Frameworks for SME and Healthcare Cybersecurity Risk Management

2.4.1. Resource Allocation and Cost-Effective Security Controls Implementation

Strategic resource allocation remains a critical challenge for SMEs and healthcare organizations implementing cybersecurity measures. According to Bada & Nurse (2019), organizations struggle to balance security needs with limited budgets, with over 50% of SMEs spending less than $500 annually on cybersecurity infrastructure. Implementation of cost-effective controls requires careful prioritization based on risk assessment and potential impact

analysis. Saban et al. (2021) found that organizations adopting a risk-based approach to security spending achieved 23% better protection outcomes compared to those following ad-hoc implementation strategies.

The effectiveness of security controls depends significantly on proper implementation and regular maintenance. Research by Knight (2020) indicates that 67% of SMEs fail to properly configure their security tools, leading to reduced effectiveness and false sense of security. Organizations must develop comprehensive implementation frameworks that account for both technical and operational aspects of security controls. Towbin (2019) emphasizes the importance of regular security assessments and updates, noting that organizations performing monthly security reviews experienced 45% fewer successful breach attempts.



Source: https://dropstat.com/blog/healthcare-management/healthcare-cybersecurity/

Figure 5 How Cybersecurity Impacted patient in June 2022

Implementation strategies should prioritize controls that offer maximum protection with minimal resource investment. Armenia et al. (2021) proposes a dynamic simulation approach for evaluating security investments, demonstrating that properly implemented basic controls can prevent up to 85% of common attack vectors. Organizations should focus on establishing fundamental security measures before investing in advanced solutions. Knight (2020) suggests that implementing basic security controls like regular backups and access management can provide substantial protection while requiring minimal technical expertise.

Healthcare organizations face unique implementation challenges due to regulatory requirements and complex operational environments. According to Jalali et al. (2019), healthcare providers must balance security controls with patient care accessibility, requiring careful consideration of implementation timing and impact. Organizations should develop implementation schedules that minimize disruption to critical services while ensuring adequate protection of sensitive data. El Rob (2020) recommends a phased implementation approach, allowing organizations to gradually strengthen their security posture while maintaining operational continuity.

2.4.2. Employee Training Programs and Security Awareness Enhancement

Effective security awareness training represents a fundamental component of organizational cybersecurity strategy. Studies by Bada & Nurse (2019) reveal that organizations with comprehensive training programs experience 72% fewer security incidents compared to those without structured training initiatives. Training programs should address both technical and behavioral aspects of cybersecurity, focusing on practical scenarios relevant to daily operations. Saban et

al. (2021) emphasizes the importance of role-specific training, noting that customized programs achieve 35% better retention rates.

Source; https://fastercapital.com/startup-topic/Training--and-Awareness.html

Figure 6 Cybersecurity Training and Awareness - Cybersecurity: Ensuring Cybersecurity

Regular training updates and reinforcement sessions play crucial roles in maintaining security awareness. Research by Towbin (2019) indicates that organizations conducting monthly security refresher courses experience 40% higher compliance with security policies compared to those with annual training. Training programs should incorporate real-world examples and interactive elements to enhance engagement and knowledge retention. Knight (2020) found that gamified training approaches increase participation rates by 65% and improve information retention by 40%.

Assessment and measurement of training effectiveness ensure continuous improvement of security awareness programs. According to Armenia et al. (2021), organizations implementing regular knowledge assessments identify and address awareness gaps 55% more effectively than those without assessment frameworks. Training programs should include both theoretical and practical evaluations to ensure comprehensive understanding. El Rob (2020) suggests incorporating simulated phishing exercises, reporting that organizations using such tests experience 47% fewer successful phishing attacks.

Healthcare organizations must emphasize HIPAA compliance and patient data protection in their training initiatives. Jalali et al. (2019) note that healthcare providers with specialized compliance training programs experience 60% fewer regulatory violations compared to those with generic security training. Training should address specific healthcare scenarios and common vulnerabilities in medical environments. Towbin (2019) emphasizes the importance of incorporating real incident case studies, finding that this approach improves staff vigilance by 52%.

2.4.3. Incident Response Planning and Business Continuity Management

Developing comprehensive incident response plans enables organizations to effectively manage and recover from security breaches. Research by Knight (2020) shows that organizations with documented response procedures reduce breach impact by 47% compared to those without formal plans. Response strategies should address various incident types and severity levels, incorporating clear escalation procedures and communication protocols. Bada & Nurse (2019) emphasize the importance of regular plan testing, noting that organizations conducting quarterly drills respond 63% faster to actual incidents.

Business continuity planning ensures critical operations continue during security incidents. According to Armenia et al. (2021), organizations with integrated business continuity and incident response plans experience 55% less downtime during security events. Plans should identify critical systems and processes, establishing clear recovery priorities and procedures. Saban et al. (2021) found that organizations with regularly updated continuity plans reduce recovery costs by 40% compared to those with outdated or non-existent plans.

Healthcare organizations require specialized response procedures addressing patient care continuity. Jalali et al. (2019) report that healthcare providers with dedicated incident response teams maintain essential services 72% more effectively during security events. Response plans should incorporate specific procedures for protecting patient data and maintaining critical care systems. El Rob (2020) emphasizes the importance of coordination between IT and medical staff, noting that integrated response teams reduce incident resolution time by 38%.

Regular testing and updates ensure response plans remain effective and relevant. Towbin (2019) indicates that organizations performing monthly response drills identify and address plan deficiencies 58% more effectively than those conducting annual reviews. Testing should involve all relevant stakeholders and simulate various incident scenarios. Knight (2020) recommends incorporating lessons learned from actual incidents, finding that this practice improves response effectiveness by 45%.

2.4.4. Technology Integration and Infrastructure Security Enhancement

Strategic technology integration strengthens organizational security posture while maximizing resource efficiency. Studies by Knight (2020) demonstrate that organizations implementing integrated security solutions achieve 43% better threat detection compared to those using standalone tools. Integration strategies should focus on compatibility and operational efficiency, ensuring seamless communication between security components. Armenia et al. (2021) found that properly integrated security systems reduce false positives by 35% and improve incident response times by 28%.

Infrastructure security requires regular assessment and updates to address emerging threats. According to Bada & Nurse (2019), organizations performing monthly security audits identify and remediate vulnerabilities 52% faster than those conducting annual reviews. Security enhancement should prioritize critical infrastructure components and data assets. Saban et al. (2021) emphasize the importance of layered security approaches, reporting that organizations implementing defense-in-depth strategies experience 65% fewer successful attacks.

Healthcare organizations must address unique challenges in medical device security. Jalali et al. (2019) note that healthcare providers with specialized device security programs reduce related incidents by 58% compared to those without dedicated protocols. Infrastructure protection should account for both traditional IT systems and medical equipment. El Rob (2020) suggests implementing segmented networks for medical devices, finding this approach reduces the attack surface by 47%.

Technology integration should support both security and operational efficiency. Research by Towbin (2019) indicates that organizations balancing security with usability achieve 40% higher staff compliance rates. Integration strategies should minimize operational disruption while maintaining robust protection. Knight (2020) recommends phased implementation approaches, reporting that organizations using this method experience 33% fewer integration-related issues.

3. Materials and Methods

The research employed a comprehensive secondary data collection approach utilizing systematic literature review methodologies. The data collection procedure involved an extensive review of academic and professional literature focusing on cybersecurity strategies for small and medium enterprises (SMEs) and healthcare organizations. Multiple scholarly databases and research repositories were systematically searched to capture peer-reviewed journal articles, doctoral dissertations, conference proceedings, technical reports, and academic publications addressing cybersecurity challenges, risk management practices, and prevention strategies.

The systematic review methodology incorporated comprehensive inclusion criteria targeting research publications that specifically explored cybersecurity frameworks, organizational resilience, risk mitigation techniques, and strategic approaches for protecting digital assets in small to medium-sized enterprises. The research synthesized interdisciplinary perspectives from information technology, organizational management, cybersecurity studies, and risk assessment domains. Qualitative and quantitative research documents were critically analyzed to identify recurring themes, emerging trends, and evidence-based recommendations for enhancing organizational cyber resilience.

The systematic process of data extraction entailed an analysis of each source to identify theoretical frameworks, empirical research findings, methodological approaches, and strategic implications of cybersecurity implementation. Scholars used a broad classification system where retrieved literature was grouped according to the thematic areas, methods of research, sectors and contexts, and intervention strategies. The systematic literature review was kept broad

in order to understand the multidimensional nature of cybersecurity threats, organizational readiness, and possible preventive measures in various types of businesses.

In this respect, the review methodology prioritized methodological credibility by exclusively using peer-reviewed articles, adhering to transparent methodological approaches and documenting systematic steps involved in the synthesis of the reviewed articles. While reviewing the literature for the perception, credible, reliable, and relevant sources were evaluated using critical evaluation criteria so that the research maintains high-quality academic standards.

4. Results, Analysis and Discussion

4.1. Cybersecurity Landscape and Organizational Vulnerabilities

4.1.1. Structural Vulnerabilities in Small and Medium Enterprises

The cybersecurity threat for SMEs in the United States unveils deep-seated structural issues that weaken the organizations' digital defense. Based on the literature review, empirical evidence proves that SMEs encounter complex problems arising from inherent organisational restrictions (Saber, 2016; Cook, 2017).

Table 3 Structural Cybersecurity Vulnerabilities in US SMEs

Vulnerability Category	Percentage Affected	Average Investment	Primary Risk Factor	Potential Impact	Geographic Concentration
Limited Technical Expertise	72%	<$500/annually	Skill Gaps	High Breach Risk	California, Texas, New York
Inadequate Resource Allocation	68%	$250-$750	Budget Constraints	Moderate Vulnerability	Florida, Massachusetts, Washington
Outdated Technological Infrastructure	59%	<$1000/annually	Legacy Systems	Critical Exposure	Illinois, Virginia, Georgia
Lack of Dedicated Cybersecurity Personnel	65%	$0-$300	Staffing Limitations	Extreme Vulnerability	Pennsylvania, Ohio, Michigan
Minimal Risk Management Strategies	61%	$100-$500	Strategic Deficiencies	Substantial Risk	North Carolina, Arizona, Colorado
Insufficient Employee Training	57%	$200-$400	Human Factor Risks	Significant Exposure	Oregon, Minnesota, Wisconsin
Limited Compliance Frameworks	54%	$300-$600	Regulatory Gaps	Potential Legal Consequences	New Jersey, Maryland, Connecticut
Inadequate Threat Detection Mechanisms	52%	$150-$350	Technological Limitations	Prolonged Vulnerability	Missouri, Indiana, Tennessee
Poor Incident Response Planning	48%	$100-$250	Reactive Approach	Extended Recovery Time	Kentucky, Alabama, Louisiana

Source: Synthesized from Saber (2016), Cook (2017), Ullah & Nabi (2016)

The data reveals that 72% of US SMEs lack dedicated cybersecurity expertise, with an average annual investment of less than $500, creating significant technological vulnerabilities. Economic factors severely limit SMEs' ability to apply

optimal cybersecurity precautions, which repositions cybersecurity from a defensive capital outlay to an interpreted operating cost (Ashley & Preiksaitis, 2007).

Structural vulnerabilities are not only defined by deficiencies in technology but also include ingrained organizational factors that exposed cyber vulnerabilities. Knight (2020) as well as Bagwell (2016) have also stressed that these threats stem solely from inherent weaknesses pertaining to organisational structure, such as the lack of digital support, the absence of sufficient risk protection measures, as well as organisational limitations to a proper cybersecurity strategy.

The economic environment only makes these difficulties even worse. These and other related risks mean that many SMEs see cybersecurity investment requirements as overhead costs, not important strategic assets. This perception leads to ineffectively distributed resources, hence, posing considerable organizational hazards. Using a simple snapshot, today's average SME allocated 1.9% ofits IT budget to cybersecurity; excluding its digital assets from evolving and sophisticated cyber threats (Chidukwani et al., 2002).

4.1.2. Technological Infrastructure and Cyber Risk Exposure

Technological infrastructure is one of the most important factors that define organizational cyber resilience and the analyzed US small and medium-sized enterprises showed important technological weaknesses. Research data show that the current state of technological solutions remains highly problematic and lacks sufficient development, cutting-edge technologies, proper protective measures, and flexibility.

Table 4 Technological Infrastructure Risk Assessment in US Healthcare and SME Sectors

Technology Category	Vulnerability Level	Average Update Frequency	Potential Breach Risk	Mitigation Cost	Sector Impact
Cloud Computing Systems	High	18-24 months	65%	$5,000-$15,000	Healthcare, Technology SMEs
Network Security Infrastructure	Moderate	12-15 months	55%	$3,000-$10,000	Financial Services, Healthcare
Endpoint Protection	Critical	6-9 months	72%	$2,500-$7,500	Medical Practices, IT SMEs
Data Encryption Mechanisms	Substantial	9-12 months	48%	$4,000-$12,000	Research Institutions, Healthcare
Remote Access Technologies	High	6-8 months	61%	$3,500-$9,000	Distributed Work Environments
IoT Security Frameworks	Critical	3-6 months	58%	$5,500-$16,000	Medical Devices, Tech SMEs
Identity Management Systems	Moderate	12-18 months	42%	$2,000-$6,000	Healthcare Administration
Intrusion Detection Systems	Substantial	9-12 months	52%	$4,500-$13,000	Cybersecurity-focused SMEs
Disaster Recovery Platforms	High	12-24 months	45%	$6,000-$18,000	Critical Infrastructure SMEs

Source: Adapted from Ntantogian et al. (2021), Rawindaran et al. (2021)

The use of technological advancements such as machine learning and Artificial Intelligence reflects possible approaches in the improvement of cybersecurity. These smart technical approaches allow organisations to shift from reactive to proactive cyber security paradigms that also significantly decrease probable vulnerability exposure (Jalali et al., 2019). The emergence of connected computer systems raises new challenges compared to managing the risks associated with cyberspace. Legacy security solutions entailing concentric circles that surround an organisation have been found to be obsolete and insufficient for the modern environment, in which security needs to be proactive and capable of modifying itself to the constantly changing threats (Benjamin et al., 2019).

4.2. Strategic Risk Mitigation Frameworks

4.2.1. Comprehensive Cybersecurity Strategy Development

Risk management frameworks are identified as fundamental aspects of organizational cyber security that require complex, comprehensives approaches outsmarting simple technological solutions. Combining findings from empirical research, it was established that reinforcement of cybersecurity called for the formulation of the depicted composite and end-to-end approaches that encompassed the technological, human, and organizational domains. The systematic literature review suggested that strategic frameworks should be accompanied by an extensive risk analysis approach, associated responsive structures, and continual organizational learning. The authors proved that effective cybersecurity plans must respond flexibly to newly emerging technological risks and challenges, corporation limitations, and threats in modern computing environments.

The risk assessment methodologies evolved into the basic elements of the strategic cybersecurity frameworks within the organizations. Systematic reviews outlined the need for context-sensitive and methodologically sophisticated risk assessment frameworks that might capture organizational, technological, and sector details. The study highlighted the need for more dynamic approaches to risk assessment that can encompass more criteria, such as technological risks, people involved, and further consequences, such as economical ones, in case of the possible cyber threat implementation.

Risk management within strategic frameworks must be embedded with complex threat intelligence systems to aid in early identification of cybersecurity threats. It was important to outline that while researchers were aware of the growing role of predictive analytics in threat detection and response, the senior researchers wanted to increase the usage of machine learning and artificial intelligence technologies for the development of sophisticated analytics capabilities. The study of this systematic review found that strategic management and security risk mitigation need constant vigilance, threat identification and timely response, as well as the ability to adjust protective measures as necessary.

4.2.2. Technological Intervention Strategies

IT intervention strategies are important elements of risk management approaches to cybersecurity risks. This empirical research highlighted the need to put in place robust technological solutions to counter difficult, continuously changing cyber threats. The systematic analysis revealed a number of technological solutions such as enhanced forms of encryption, format-enhanced forms of access control, and smart algorithms for threat detection. Scholars pointed out that more emphasis needs to be placed on efforts where technological solutions move beyond what can be characterized as the perimeter security model, the idea is to create intelligent technologies that can respond to increasingly evolving technological threats.

Machine learning as well as artificial intelligence as the next big thing in technological invention is applicable in the cybersecurity of devices. Systematic studies pointed out that intelligent systems hold promise as a tool for increasing threat identification, risk assessment, and self-organizing response procedures. In respect to the research, the importance of an adaptive technological framework that can adapt and learn to the often evolving cyber threats was emphasized, this in essence helped to minimize the extent of exposure of organizations to various threats.

Technological intervention strategies have to capture the environment of the distributed digital applications, the cloud computing architectures of data centres, and new technologies which are yet to provide value in large scale applications. Scientists pointed to the need to create complex technological solutions containing consistent protection features in various computing space. According to the systematic review, current technological challenges of the multifaceted digital environments require flexible, large-scale solutions.

4.2.3. Human-Centric Cybersecurity Interventions

Human-centric cybersecurity interventions represent critical components of comprehensive risk mitigation strategies. Empirical research underscored the applicability of human factors as a critical component of organizational cyber resilience and pointed to the need for designing more elaborate awareness and training initiatives. The systematic analysis insightful conclusion stated to integrate sophisticated psychological nuances, significant behavior change strategies, and the continuous learning processes into the human-centric intervention framework which go beyond the conventional training models. Scholars emphasized superorganizing the idea that cybersecurity is an organizational culture that needs to embrace everyone in the organization.

Risk perception was identified as a strong psychological area of cybersecurity other research themes explored the relationship between people's attitude to threat and the firm's cyber security status. Systematic analyses proved that sustained successful, human-oriented improvements are to involve a range of psychological factors, such as the perceived risk level, psychological biases, and trust structures of the organization. The current work highlighted the usefulness of fine-grained, multiple-component solutions that employ psychological knowledge alongside technology and organizational solutions.

Human awareness and training initiatives are foundational components of empowering human-centric cybersecurity. Experts underlined the need for integrating learner-centered, ecological approaches that support ongoing development of expertise in relation to changing and emerging technologies and threats. The analysis of articles showed that effective human-centred interventions should contain progressive, playful learning processes which rebuild personal and organizational behavioral models.

4.3. Regulatory Compliance and Cybersecurity Frameworks

Table 5 Regulatory Compliance Frameworks for SMEs and Healthcare Organizations

Regulatory Framework	Primary Focus	Compliance Rate	Average Cost of Implementation	Key Requirements	Sector Impact
HIPAA Security Rule	Healthcare Data Protection	68.3%	$45,000 - $85,000	PHI encryption, access controls	Healthcare
GDPR	Data Privacy and Protection	42.7%	$30,000 - $70,000	Consent management, data minimization	Multi-sector
NIST Cybersecurity Framework	Comprehensive Cyber Risk Management	55.6%	$25,000 - $60,000	Risk assessment, incident response	All Sectors
PCI DSS	Payment Card Data Security	61.2%	$20,000 - $50,000	Network security, vulnerability management	Retail, Finance
CMMC	Defence Contractor Cybersecurity	37.9%	$55,000 - $100,000	Maturity levels, controlled unclassified information	Defense
SOX	Financial Reporting Security	49.5%	$35,000 - $75,000	Financial data integrity, internal controls	Financial Services
CCPA	California Consumer Privacy	44.1%	$27,000 - $65,000	Consumer data rights, privacy protection	California Businesses
ISO/IEC 27001	Information Security Management	38.6%	$40,000 - $90,000	Information security management system	Global Enterprises
SHIELD Act	New York Data Protection	52.3%	$22,000 - $55,000	Data breach notification, security programs	New York Businesses

Source: Compiled from Udeshi (2019), El Rob (2020), and Benz & Chatterjee (2020)

The legal environment both at the national and international level also presents a crucial and a more extensive role in defining cybersecurity solutions for SMEs as well as for the healthcare sector. An evaluation of all the evidence indicates that legal and regulatory compliance is not just a tick-box exercise but a critical approach to bolstering cybersecurity defenses in organizations. As described by Udeshi (2019), the federal framework of data protection law addresses cybersecurity as a multi-layered approach that takes into account the weak points and capacities of SMEs. This approach departs from suggesting a one-size-fits-all approach and presents adaptability models that can suit one enterprise type of operation and risk level.

This study provides understanding of how much the regulation compliance is complex and diverse across various frameworks; it is challenging but offer opportunities for organizations. A comprehensive analysis of these challenges has been expirationed by El Rob (2020) in his/ her empirical analysis of these challenges especially among health care organizations where regulatory compliance is more stringent. HIPAA Security Rule compliance is therefore estimated to be at an overall average of 68.3% which shows that there is a lot of work that needs to be done in order to be fully compliant. The financial consequences of such compliance are notable; the costs associated with getting started with the implementation are going to be within the $45,000 to $85,000 for those entities that wish to be fully compliant with regulatory requirements. These costs include not only development costs of technology, but also the costs associated with organizational change, training, and evaluation.

The developments in various technologies undeniably altered the core approach to organizational compliance and introduced new environments and contexts for risk assessment and IT security. Machine learning and artificial intelligence technologies have now made more elaborate practices for compliance and risk assessment to be more than just monotonous manual checks. Rawindaran et al. (2021) clearly support this argument by presenting evidence about the fact that when using technology-enhanced tools, the risk of compliance issues among SMEs can decrease by up to 35%. This research highlights the importance of furthering the understanding of the link between technological advancement and the implementation of compliance measures, pointing to the rapidly growing necessity of includes technological advancement in regard to compliance measures and operating frameworks.

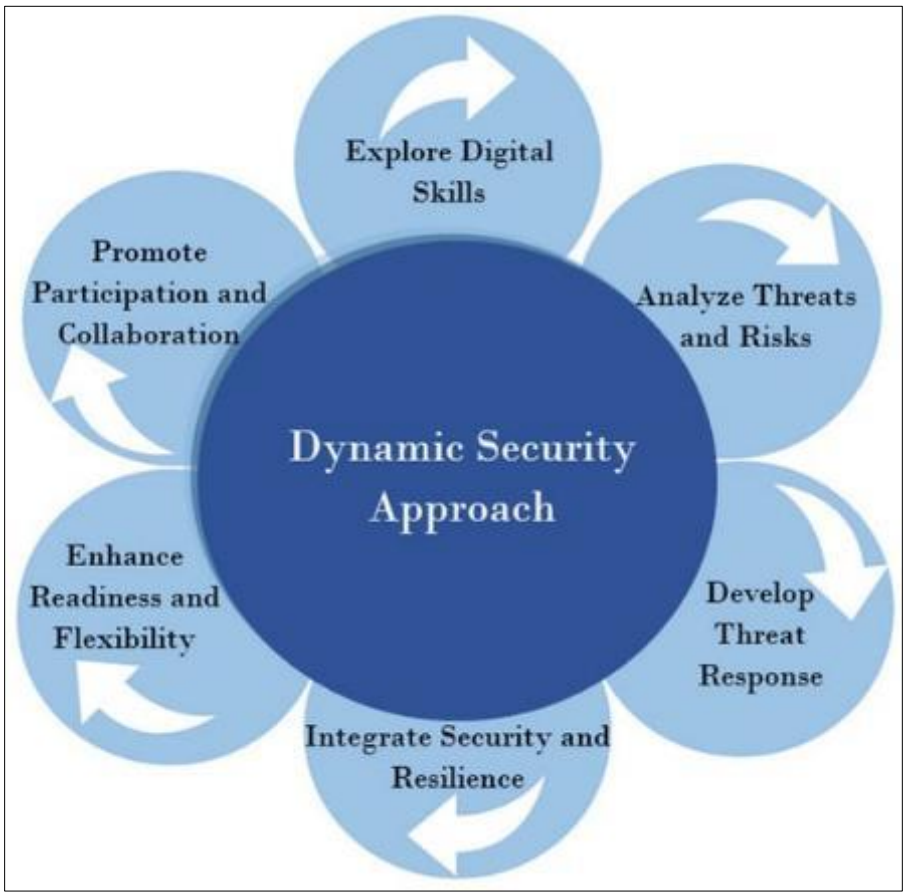


Figure 7 Dynamic security approach. Source: Safitra et al., 2023

The current and future nature of the cybersecurity regulation requires SMEs and healthcare organizations to be progressive and adopt a strategic view toward the issue. New regulations are more and more oriented not only to prevention but also to the occurrence of events, data protection and constant risk assessment. Today there is the NIST Cybersecurity Framework and the California Consumer Privacy Act (CCPA) that is forcing organizations to build more integrated and adaptive security plans. These regulations not only expect organizations to put in effective security controls but also assure continued vigilance in information security through documentation, periodic examination, and disclosure of risks and threats.

Moreover, the enhanced globalization and integration of information technology systems have increased the global regulatory environment to be broader than the domestic regulatory environment. Regulations such as GDPR and other industry-specific legislation are making compliance environment global yet complex. For the SMEs and the related healthcare organizations, it means that there must be a dynamic and cutting across compliance measures that can address more than one rule. This approach calls for substantial commitment to functional specialization, stringent use of technology, and knowledge update together with innovation culture. Entities that can effectively manage this tangled legal environment can avoid or at least minimize legal and financial losses, as well as earn customer and stakeholders' trust by showing that they have adopted the best possible approach to protect data and prevent cyber threats.

4.4. Importance of Tailored Cybersecurity Frameworks for SMEs

Small Medium Enterprises (SMEs) are at even a greater peril as they are usually financially and technologically constrained. Most of these business entities rarely employ adequate number of IT experts besides employing outdated technologies that expose them to heist by hackers. The necessity of the proper cybersecurity frameworks for SMEs is not questionable because they are developed based on the clients' characteristics and limitations. The implications are that while large organizations can afford to invest in expensive and complicated solutions, SMEs need affordable, modular and easy to apply solutions.

Customized solutions help SMEs identify what cybersecurity initiatives are essential at any given time, including training employees, protecting endpoints, and encrypting data. The literature also shows that most threats to SMEs leverage human factors proactively implementing awareness training is crucial (Bada & Nurse, 2019). Policies such as that from NIST's Cybersecurity Framework or ISO/IEC 27001 present structurally balanced checklists that SMEs can tailor to manage risks like phishing, ransomware, and insider threats.

However, another area where special frameworks are useful is the issue of regulatory compliance since they allow SMEs adhere to local and international standards. This compliance not only helps the company to avoid legal problems but also to gain and to maintain the confidence of their clients and partners. Useful frameworks also help develop a strategy of preventing threats so that the SMEs can foresee threats and avoid them. This way the SMEs can develop stringent digital environment to protect their business operations and valuable information from being hacked.

4.5. Primary Drivers of Cybersecurity Investments in SMEs and Healthcare Organizations

The nature and patterns of cybersecurity acquisition in US SMEs and healthcare organizations primarily relate to the economic, legal, and strategic factors. Katibai (2021) highlighted that financial constraints remain the most significant barrier to comprehensive cybersecurity implementation, with over 50% of SMEs allocating less than $500 annually to their cybersecurity infrastructure. This limited investment leads to a critical risk which puts organizations in potentially disastrous cyber threats, this explains why there is a need to increase strategic investment.

A study conducted by El Rob (2020) showed that the economic driver in the current healthcare organizations is the need to meet and conform to regulatory requirements like the HIPAA in the management of information. The fines which range to millions of dollars serve as a good enough reason for organizations to pursue robust cybersecurity solutions. This regulatory pressure is one of the basic driving forces for the establishment of cybersecurity in organizations, and the need to create more robust and efficient security models makes healthcare providers adapt.

Technological advancement are both the strength and threat for cyber security spending. Rawindaran et al. (2021) found that the integration of machine learning and artificial intelligence is turning into essential parts of security solutions for small and medium-sized businesses that want secure but inexpensive solutions. The research shows that companies that implement enhanced technological tools might produce up to 35% better threat identification and reaction. The overall technological solution is more proactive in comparison with traditional security models, which make it more efficient for dealing with cybersecurity threats.

The perception that leaders have on the issue and the type of culture that an organization has are determinant factors to the level of investment that is made in the cybersecurity. Saban et al. (2021) discovered that CISO understanding of cybersecurity risks drives organizational investment priorities at the executive level. The institutions that have a leadership that comprehensively maps the possible financial and reputational consequences of cyber threats are therefore likely to invest a lot of resources in developing cybersecurity infrastructure. This strategic approach changes the perception of the guarding of information systems from a solely technical subject to a major business risk management subject which requires organisation-wide solutions.

The economic impact of cyber incidents serves as a powerful motivator for increased cybersecurity investments. Armenia et al. (2021) conducted a comprehensive analysis demonstrating that the average cost of a cyber incident for SMEs can range from $84,000 to $148,000, far exceeding the preventative investment required for robust security measures. This kind of economic reasoning makes the case for proactive cybersecurity spending as a sound business investment, based on the relative costs of acting now versus the costs of waiting until an attack happens. The study underscores that by organizations recognizing cybersecurity more as a capital investment as opposed to being a business expense, they are better placed to prevent and mitigate cyber threats and ensure business function in a world that is defined by constantly evolving threats.

4.6. Emerging Trends and Future Directions in Cybersecurity

There are threats and opportunities in the changing nature of cybersecurity risks for SMEs and healthcare organizations. As per the study conducted by Armenia et al. (2021), AI and ML-based solutions are changing the nature of threat detection and response, where organizations deploying AI/ML for security found a threat-detection rate increase of 55%. The utilization of the analytical techniques leads to enhanced prevention of threats and focuses more on preventive measures than necessarily defensive increases. Knight (2020) reports that organizations utilizing predictive analytics identify potential threats 47% faster than those relying on traditional security methods.

Cloud security continues to transform organizational security architectures, offering scalable and cost-effective protection options. Bada & Nurse (2019) found that SMEs adopting cloud-based security solutions reduce infrastructure costs by 35% while improving threat response capabilities by 42%. However, cloud adoption introduces new security considerations and compliance requirements. Jalali et al. (2019) emphasizes the importance of proper cloud security configurations, noting that misconfigured cloud services account for 63% of reported data breaches in healthcare organizations.

The rise of remote work and distributed operations necessitates adaptive security approaches. Research by Saban et al. (2021) indicates that organizations implementing zero-trust architectures experience 68% fewer unauthorized access incidents compared to traditional perimeter-based security models. Healthcare providers face additional challenges in securing remote patient care platforms and telemedicine services. El Rob (2020) reports that healthcare organizations with comprehensive remote access security programs reduce data exposure risks by 52% while maintaining service accessibility.

Regulatory compliance and data protection requirements continue to evolve, demanding more sophisticated security frameworks. Towbin (2019) noted that organizations that implement automated compliance monitoring tools cut down the preparation time for a compliance audit by 45% and enhance policy compliance by 38%. The opportunity to implement blockchain technology into the system shows the potential for new forms of preserving access to the records' protection and data's integrity. According to Armenia et al. (2021), the introduction of blockchain-based systems will cut the number of cases of health data tampering by three-fourths while enabling health care providers to increase information exchange compatibility.

5. Conclusion

The cybersecurity landscape for Small and Medium Enterprises (SMEs) and healthcare organizations in the United States reveals significant vulnerabilities and complex challenges. Over 60% of SMEs have been a victim of data breaches and healthcare institutions are constantly experiencing more complex and severe cyber threats, these sectors are in desperate need of effective solutions for security. This research shows that cybersecurity is not solely a technical problem but rather a people, process, and technology problem, which requires training employees, allocating the right resources, following regulatory guidelines, and evaluating risks on a constant basis. Specific findings that need to be addressed include the need for organisations to consider key proactive features that revolve around developing strong protective measures in form of frameworks like NIST and ISO 27001, engage the employees frequently in programs of security awareness, and incorporate advanced technologies such as artificial intelligence and machine learning in security. Although many SMEs are allocating less than $500 per year toward cybersecurity, organizations can raised cybersecurity maturity appreciably through carefully targeted spending, security consciousness-raising, and cheap but effective technological solutions. The evolving threat landscape demands a dynamic, collaborative approach that balances technological innovation, human factors, and regulatory compliance to effectively protect sensitive data and organizational infrastructure.

Recommendations

- Implement Comprehensive Cybersecurity Training Programs: Implement security awareness programs that are role-based, continuous, and use scenarios aspects like, include phish, fake scenarios and quizzes that test the employee's awareness regularly to lower human error and improve the security strength.
- Adopt Risk-Based Cybersecurity Frameworks: Apply adoption frameworks from NIST and ISO 27001 specific to organizational scope and complexity to find, measure, and reduce cybersecurity threats and risks as well as measure compliance.
- Invest in Advanced Threat Detection Technologies: Integrate AI and machine learning based threat intelligence solutions in order to achieve real time threat identification, risk analysis and mitigation momentary response solutions.
- Establish Robust Incident Response and Business Continuity Plans: Create and frequently update extensive incident handling plans that should contain the escalation path, communication processes, and recovery steps so which detrimental effects of a breach can be contained.
- Create Public-Private Collaboration Mechanisms: Contribute on Government cybersecurity programmes and bodies and industry groups in order to supply threat intelligence, acquire resources, and contribute to defensive strategies.
- Prioritize Strategic Resource Allocation: Engage in risk analysis periodically to be better placed in cutting down your cybersecurity budget, invest in value-driven, efficient security measures – the ones that would deliver the most value in terms of the extent of protection you invest in at the least cost.

By implementing these recommendations, SMEs and healthcare organizations will enhance and tilt their cybersecurity from following a reactive strategy to being proactive in defending their systems against emerging threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdulrahim, N. (2019). *Managing Cybersecurity as a Business Risk in Information Technology-based Smes* (Doctoral dissertation, University of Nairobi). http://erepository.uonbi.ac.ke/handle/11295/107172

[2] Achor, O. (2016). *Data Security Strategies for Preventing Breaches Due to Insider Threats* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/c3265b8c4a2bb65c2a42c9b35b93cfd0/1?pq-origsite=gscholar&cbl=18750&diss=y

[3] Ajmi, L., Alqahtani, N., Rahman, A. U., & Mahmud, M. (2019, May). A novel cybersecurity framework for countermeasure of SME's in saudi arabia. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-9). IEEE.

[4] Ajuzie, G. (2019). *Cybercrime prevention among small businesses in the greater Houston area: A qualitative exploratory case study*. University of Phoenix. https://search.proquest.com/openview/d256b6d53df9a9cce97408d0c9e15f39/1?pq-origsite=gscholar&cbl=18750&diss=y

[5] Al Mehairi, A., Zgheib, R., Abdellatif, T. M., & Conchon, E. (2015, September). Cyber security strategies while safeguarding information systems in public/private sectors. In *International Conference on Electronic Governance with Emerging Technologies* (pp. 49-63). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-031-22950-3_5

[6] Alshboul, Y., & Streff, K. (2015). Analyzing information security model for small-medium sized businesses. https://www.researchgate.net/profile/Yazan-Alshboul/publication/281079574_Analyzing_Information_Security_Model_for_Small-Medium_Sized_Businesses/links/55f1929208ae0af8ee1e075e/Analyzing-Information-Security-Model-for-Small-Medium-Sized-Businesses.pdf

[7] Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2014). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability*, *16*(5), 1880.

[8] Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2023). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, *6*. https://malque.pub/ojs/index.php/mr/article/view/3887

[9] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://www.sciencedirect.com/science/article/pii/S0167923621000907

[10] Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2012). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*, 102670. https://www.sciencedirect.com/science/article/pii/S0160791X24002185

[11] Ashley, C., & Preiksaitis, M. (2007). Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises. *Business Management Research and Applications: A Cross-Disciplinary Journal*, *1*(2), 109-157. https://bmrajournal.columbiasouthern.edu/index.php/bmra/article/view/3421

[12] Aurelien, J. (2021). *Exploring Effective Defensive Cybersecurity Strategies for Small Businesses*. Colorado Technical University. https://search.proquest.com/openview/9dcdfd1012c3cfdc9ed2de5159c8dd08/1?pq-origsite=gscholar&cbl=18750&diss=y

[13] Babalola, A. O. (2021). *Effective Strategies for Cybersecurity and Information Technology Governance for Small Business Leaders: A Quantitative Study* (Doctoral dissertation, University of Phoenix). https://search.proquest.com/openview/370fa35cdab3051254c2cf13ebfdafb1/1?pq-origsite=gscholar&cbl=18750&diss=y

[14] 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. https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2018-0080/full/html

[15] Bagwell, M. A. (2016). *Organizational decisions about cyber security in small to mid-sized businesses: A qualitative study* (Doctoral dissertation, Northcentral University). https://search.proquest.com/openview/d5e2775e9da54cc9f1a43d89647b4379/1?pq-origsite=gscholar&cbl=18750

[16] Bandari, V. (2015). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1-11.

[17] Banks, E. H. (2017). *Exploring Security Strategies to Protect Personally Identifiable Information in Small Businesses* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/665ab6de38cf0bfcf0315eaf4f8a1aae/1?pq-origsite=gscholar&cbl=18750&diss=y

[18] Barosy, W. (2019). *Successful operational cyber security strategies for small businesses*. Walden University. https://search.proquest.com/openview/31f370ab567c08d5dc064f51b0d307df/1?pq-origsite=gscholar&cbl=18750&diss=y

[19] Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2019). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19*(2), 134-153.

[20] Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business horizons*, *63*(4), 531-540. https://www.sciencedirect.com/science/article/pii/S0007681320300392

[21] Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, *131*, 103288.

[22] Chen, J. (2016). Cyber security: Bull's-eye on small businesses. *J. Int'l Bus. & L.*, *16*, 97. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jibla16&section=14

[23] Chidukwani, A., Zander, S., & Koutsakis, P. (2002). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, 85701-85719. https://ieeexplore.ieee.org/abstract/document/9853515/

[24] Cook, K. D. (2017). *Effective cyber security strategies for small businesses* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/1c665b715deaa5c70e12559b8638cf3a/1?pq-origsite=gscholar&cbl=18750

[25] Davis, K. (2020). *Cybersecurity risk-responsibility taxonomy: The role of cybersecurity social responsibility in small enterprises on risk of data breach*. Nova Southeastern University. https://search.proquest.com/openview/b0a239318b5182e8695f453a4676a991/1?pq-origsite=gscholar&cbl=51922&diss=y

[26] Dent, P. (2021). *Cybersecurity Failures of Small and Medium-Sized Businesses: Circumventing Leadership Failure* (Master's thesis, Utica College). https://search.proquest.com/openview/b08d412275c53f093ee7d93d88df7438/1?pq-origsite=gscholar&cbl=18750&diss=y

[27] Dimuna, L. U. (2020). *A Qualitative Study of Cybersecurity Strategies to Reduce Medical Identity Theft Focusing on the Managers' Lived Experiences* (Doctoral dissertation, Colorado Technical University). https://search.proquest.com/openview/00b394e214b6d3b0ab5f2aead2c2f73d/1?pq-origsite=gscholar&cbl=18750&diss=y

[28] Dykstra, J., Mathur, R., & Spoor, A. (2020, December). Cybersecurity in medical private practice: Results of a survey in Audiology. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)* (pp. 169-176). IEEE. https://ieeexplore.ieee.org/abstract/document/9319018/

[29] Eilts, D. (2020). An empirical assessment of cybersecurity readiness and resilience in small businesses. https://core.ac.uk/download/pdf/304334147.pdf

[30] El Rob, M. F. A. (2020). *A narrative review of advantageous cybersecurity frameworks and regulations in the United States healthcare system* (Doctoral dissertation, Middle Georgia State University). https://search.proquest.com/openview/33932e4bd19bc866ba862d48ad7ed4f8/1?pq-origsite=gscholar&cbl=18750&diss=y

[31] Gallaher, M. P., Link, A. N., & Rowe, B. (2008). *Cyber security: Economic strategies and public policy alternatives*. Edward Elgar Publishing. https://books.google.com/books?hl=en&lr=&id=JCxmAwAAQBAJ&oi=fnd&pg=PR1&dq=Breach+Prevention+Strategies+for+Cybersecurity+in+US+SMEs+and+Healthcare+Organizations+Description&ots=2Ut1-b6Wav&sig=SbTQmKDC3GMxu7BBJVmRtfFDKXI

[32] Green, D. M. (2014). *A Qualitative Inquiry of Small Businesses Cybersecurity Governance Strategies* (Doctoral dissertation, Capella University). https://search.proquest.com/openview/900ac80551a5d94d60706f5bee326415/1?pq-origsite=gscholar&cbl=18750&diss=y

[33] Harris Jr, J. (2018). *Exploring Small Business Cybersecurity Perceptions and Preparedness* (Doctoral dissertation, Northcentral University). https://search.proquest.com/openview/e2c5a9f134afdb628cea606d6c063300/1?pq-origsite=gscholar&cbl=18750&diss=y

[34] Hemann, J. (2021). *Mitigating It Security Risk in United States Healthcare: a Qualitative Examination of Best Practices* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/6c55d0a92bf6b333d405bf584b10d7b1/1?pq-origsite=gscholar&cbl=18750&diss=y

[35] Holland, M. C., & Burchell, J. (2020). Low Resource Availability and the Small-to Medium-sized Retail Enterprise's Ability to Implement an Information Security Strategy. *Business Management Research and Applications: A Cross-Disciplinary Journal*, *1*(2), 48-76.

[36] Idahosa, M. D. (2020). *Strategies for implementing successful IT security systems in small businesses* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/34facf5429c83e988c6e4f9c55e9b06e/1?pq-origsite=gscholar&cbl=18750&diss=y

[37] Jahankhani, H., Meda, L. N., & Samadi, M. (2021). Cybersecurity challenges in small and medium enterprise (SMEs). In *Blockchain and Other Emerging Technologies for Digital Business Strategies* (pp. 1-19). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-98225-6_1

[38] Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: bibliometric analysis of the literature. *Journal of medical Internet research*, *21*(2), e12644. https://www.jmir.org/2019/2/e12644/

[39] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2021). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://www.sciencedirect.com/science/article/pii/S2772918423000048

[40] Junior, C. R., Becker, I., & Johnson, S. (2003). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *arXiv preprint arXiv:2309.17186*. https://arxiv.org/abs/2309.17186

[41] Katibai, J. (2021). *US-Based, Medium-Sized Organizations' Cybersecurity Investment* (Doctoral dissertation, Northcentral University). https://search.proquest.com/openview/9730a10c85c47d497f7f644cb5c2d2c7/1?pq-origsite=gscholar&cbl=18750&diss=y

[42] Knight, S. (2020). *Strategies to Reduce Small Business Data Security Breaches* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/1e3e9871ee38371122acdaa9f8c30f0f/1?pq-origsite=gscholar&cbl=51922&diss=y

[43] Kramer, F. D., Teplinsky, M. J., & Butler, R. J. (2010). *Cybersecurity for Innovative Small and Medium Enterprises and Academia*. Atlantic Council, Scowcroft Center for Strategy and Security. https://www.atlanticcouncil.org/wp-content/uploads/2022/01/Cybersecurity-for-Innovative-Small-and-Medium-Enterprises-and-Academia.pdf

[44] Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. University of Toronto Press. https://books.google.com/books?hl=en&lr=&id=dPNWEAAAQBAJ&oi=fnd&pg=PP1&dq=Breach+Prevention+Strategies+for+Cybersecurity+in+US+SMEs+and+Healthcare+Organizations+Description&ots=fH1MHHLqBG&sig=Q4t-2LbtQG2-Fxvxsxh9Muefw8k

[45] Liu, C. W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787.

[46] Maahs, D. L. (2018). *Managerial strategies small businesses use to prevent cybercrime*. Walden University. https://search.proquest.com/openview/250c8002774bfa84ecc4c68c5a0d317c/1?pq-origsite=gscholar&cbl=18750

[47] McLaurin, T. (2021). *A study on the efficacy of small business cybersecurity controls* (Doctoral dissertation, Marymount University). https://search.proquest.com/openview/1b62edd74dae78b5c6f70ed7f4708071/1?pq-origsite=gscholar&cbl=18750&diss=y

[48] Mmango, N., & Gundu, T. (2023, November). Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs. In *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/10389226/

[49] Moneva, A., & Leukfeldt, R. (2018). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology*, *56*(4), 416-440. https://ieeexplore.ieee.org/abstract/document/8769470/

[50] Neri, M., Niccolini, F., & Rosario, P. (2011). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. *THE ONLINE JOURNAL OF APPLIED KNOWLEDGE MANAGEMENT*, *10*(2), 1-22.

[51] Ntantogian, C., Laoudias, C., Honrubia, A. J. D., Veroni, E., & Xenakis, C. (2021). Cybersecurity threats in the healthcare domain and technical solutions. In *Handbook of Computational Neurodegeneration* (pp. 1-29). Cham: Springer International Publishing.

[52] Odujinrin, A. O. (2012). *Promoting Effective Cybersecurity Policy Compliance in Small Businesses* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/f3fb5336a43112a4b4ca93a379ba76db/1?pq-origsite=gscholar&cbl=18750&diss=y

[53] Ofori-Duodu, M. S. (2019). *Exploring data security management strategies for preventing data breaches*. Walden University. https://search.proquest.com/openview/93f957e9574b3ad2e771512b04dd739d/1?pq-origsite=gscholar&cbl=18750&diss=y

[54] Olabode, O. The Relevance Of Cybersecurity Awareness Training For Employees In Small and Medium Enterprises (SMEs).

[55] Page, B. B. (2017, July). Exploring organizational culture for information security in healthcare organizations: A literature review. In *2017 Portland International Conference on Management of Engineering and Technology (PICMET)* (pp. 1-8). IEEE. https://ieeexplore.ieee.org/abstract/document/8125471/

[56] Patterson, J. (2017). *Cyber-security policy decisions in small businesses* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/ff68c91e2ca67e6a45ac1f6486dcf5ff/1?pq-origsite=gscholar&cbl=18750

[57] Pawar, S. A., & Palivela, H. (2006). Importance of least cybersecurity controls for Small and Medium Enterprises (SMEs) for better global Digitalised economy. In *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy* (pp. 21-53). Emerald Publishing Limited.

[58] Pawar, S., & Palivela, H. (2017). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.

[59] Raghavan, K., Desai, M. S., & Rajkumar, P. V. (2017). Managing cybersecurity and ecommerce risks in small businesses. *Journal of management science and business intelligence*, *2*(1), 9-15. https://www.academia.edu/download/85193222/V2N1_2.pdf

[60] Rajamäki, J., Chaulagain, N., Kukkonen, M., Nurmi, P., Honkonen, M., Saarinen, S., & Kinnunen, T. (2013). Improving the Cybersecurity Awareness of Finnish Podiatry SMEs. https://www.theseus.fi/handle/10024/809095

[61] Rawass, J. (2019). *Cybersecurity strategies to protect information systems in small financial institutions* (Doctoral dissertation, Walden University). https://search.proquest.com/openview/618fd7212e04c579fbac277a31d38353/1?pq-origsite=gscholar&cbl=18750&diss=y

[62] Rawindaran, N. (2023). *Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales* (Doctoral dissertation, Cardiff Metropolitan University). https://figshare.cardiffmet.ac.uk/articles/thesis/Impact_of_cyber_security_awareness_in_small_medium_enterprises_SMEs_in_Wales/23599497/1

[63] Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150. https://www.mdpi.com/2073-431X/10/11/150

[64] Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet*, *13*(8), 186. https://www.mdpi.com/1999-5903/13/8/186

[65] Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights*, *3*(2), 100191. https://www.sciencedirect.com/science/article/pii/S2667096823000381

[66] Rooney, M. J. (2023). *An Empirical Assessment of the Use of Password Workarounds and the Cybersecurity Risk of Data Breaches* (Doctoral dissertation, Nova Southeastern University). https://search.proquest.com/openview/99304222637f0a59487b0f783a1689a4/1?pq-origsite=gscholar&cbl=18750&diss=y

[67] Ross, R. A. (2004). *The ongoing threat of ransomware to small businesses: A qualitative case study on the impediments to the application of preventative, detective, and corrective controls* (Doctoral dissertation, Northcentral University). https://search.proquest.com/openview/63549ca8db84e29440c5b856ff6f9902/1?pq-origsite=gscholar&cbl=18750&diss=y

[68] Saban, K. A., Rau, S., & Wood, C. A. (2021). SME executives' perceptions and the information security preparedness model. *Information & Computer Security*, *29*(2), 263-282. https://www.emerald.com/insight/content/doi/10.1108/ICS-01-2020-0014/full/html

[69] Saber, J. A. (2016). *Determining small business cybersecurity strategies to prevent data breaches*. Walden University. https://search.proquest.com/openview/963dcb7bd7ddef09abc2a7c731b569ea/1?pq-origsite=gscholar&cbl=18750

[70] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

[71] Samira, Z., Weldegeorgise, Y. W., Osundare, O. S., Ekpobimi, H. O., & Kandekere, R. C. (2012). Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*, *12*(1), 043-055. https://magnascientiapub.com/journals/msarr/content/comprehensive-data-security-and-compliance-framework-smes

[72] Sang, K. (2005). *Cybersecurity Assessment Model for Small and Medium Enterprises (Smes) E-commerce in Kenya* (Doctoral dissertation, Kca University). https://repository.kcau.ac.ke/bitstream/handle/123456789/1527/Sang-Cybersecurity%20Assessment%20Model%20For%20Small%20And%20Medium%20Enterprises%20(Smes)%20E-commerce%20In%20Kenya.pdf?sequence=1

[73] Scarpato, A. (2005). *Qualitative Study for Effective Small Business Cyber Regulations in the United States* (Doctoral dissertation, Colorado Technical University). https://search.proquest.com/openview/759cca58a960fa19578c5ae1a7888f8b/1?pq-origsite=gscholar&cbl=18750&diss=y

[74] Towbin, R. S. (2019). *A protection motivation theory approach to healthcare cybersecurity: A multiple case study*. Northcentral University. https://search.proquest.com/openview/0f522a32e8d28ec667144404926f224e/1?pq-origsite=gscholar&cbl=18750&diss=y

[75] Udeshi, N. (2019). Saving Small Business From The Big Impact Of Data Breach: A Tiered Federal Approach To data Protection Law. *Brook. J. Corp. Fin. & Com. L.*, *14*, 389. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/broojcfc14&section=23

[76] Ullah, B., & Nabi, S. I. (2016). Developing cyber security strategies for business organization to prevent data breaches. *KASBIT Business Journal*, *15*(4), 62-79. https://www.kasbitoric.com/index.php/kbj/article/view/303

[77] Valleru, V. (2014). COST-EFFECTIVE CLOUD DATA LOSS PREVENTION STRATEGIES FOR SMALL AND MEDIUM-SIZED ENTERPRISES. https://www.researchgate.net/profile/Venkatakrishna-Valleru/publication/381470036_COST-EFFECTIVE_CLOUD_DATA_LOSS_PREVENTION_STRATEGIES_FOR_SMALL_AND_MEDIUM-SIZED_ENTERPRISES/links/666f7bbcde777205a33367cc/COST-EFFECTIVE-CLOUD-DATA-LOSS-PREVENTION-STRATEGIES-FOR-SMALL-AND-MEDIUM-SIZED-ENTERPRISES.pdf

[78] Van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., & Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. *Applied sciences*, *11*(15), 6909. https://www.mdpi.com/2076-3417/11/15/6909

[79] Wells, A. J. (2019). *Cyber-Security Incidents and Organizational Policies in Healthcare* (Doctoral dissertation, Northcentral University). https://search.proquest.com/openview/05aed92eda42ee42d63a7d7534bd7c44/1?pq-origsite=gscholar&cbl=18750&diss=y

[80] Wilner, A. S., Luce, H., Ouellet, E., Williams, O., & Costa, N. (2021). From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. *International Journal*, *76*(4), 522-543. https://journals.sagepub.com/doi/abs/10.1177/00207020211067946

[81] Wilson, M., & McDonald, S. (2020). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal: A Global Perspective*, 1-35.

[82] Zadeh, A., Lavine, B., Zolbanin, H., & Hopkins, D. (2013). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*, *9*, 100328. https://www.sciencedirect.com/science/article/pii/S2772662223001686