Global Scientific and Academic Research Journal of Economics, Business and Management
ISSN: 2583-5645 (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/journals-gsarjebm-home/

Cyberattacks: A Huge Concern for Small Business Sustainability

BY

[1*]Prof. Dr. Joel Chagadama, DBA, [2]Prof. Dr. Desire S. Luamba, DBA, [3]Prof. Dr. Ir. Edouard M. Mutamba, PHD.

[1]President, Start Light Consulting LLC, Manassas, VA-USA https://orcid.org/0000-0002-7253-6977
[2]Vice President and CEO, Star Light Consulting LLC, Manassas, VA-USA https://orcid.org/0000-0001-5138-1550
[3]Professor Faculty of Polytechnic, University of Lubumbashi, D.R. of Congo
https://www.researchgate.net/profile/Mutamba-Mwema

Article History

Received: 21/12/2022
Accepted: 26/12/2022
Published: 28/12/2022

Vol – 1 Issue – 2

PP: -60-75

Abstract

Cyber-attacks have caused considerable damage to small businesses' profitability, sustainability, and longevity. Based on the cybersecurity enhancement framework, this qualitative multiple case study aimed to explore practical strategies small businesses use to minimize cyberattacks and risks. The sample size of this study was five successful small business owners in Washington, D.C., who successfully implemented strategies that reduced the risk of cyberattacks in their organizations over 5 years. Data were collected using company documents, public sources, and semi-structured interviews. The three vital themes that emerged from the research analysis were: security policy and procedures, employee training, and risk management. A strategic recommendation for small business effectiveness was investing in antivirus software, hiring I.T. experts, and learning from other companies' cyberattacks experience. In addition, small business leaders or managers may use the results of this study to protect customers, employees, and confidential company data, thereby improving their business effectiveness and ultimately increasing employment opportunities for the local community members.

Keywords: *Cyberattack risks, Business effectiveness, Antivirus software*

1. INTRODUCTION

Cyberattacks have disrupted the operating models of several small businesses across the globe [1, 2]. Unfortunately, many small businesses lack the cybersecurity strategies to protect their digital systems paramount for storing, accessing and disseminating data and information, thereby becoming an easy target for cybercriminals. Several surveys have shown that small business owners feel vulnerable to cyberattacks as cyber incidents continue to rise worldwide. In the United States, Cyber-attacks cost small businesses $86 billion in losses annually, an average of $188,000 per incident [3, 4]. Despite being widespread, cybersecurity is one of the least understood phenomena and the most pressing challenge threatening many small businesses in this modern era [5, 6, 7]. Having sound, effective strategies to mitigate the effect of cyber-attacks is critical to ensuring a business's reputation and productivity. Small business leaders must understand how to safeguard their organizations' reputations, anticipate cyberattacks, and improve business operations. Unfortunately, the lack of strategies to mitigate cyberattack risks associated with technology has left many small businesses in difficult situations, such as reduced productivity or closure.

This qualitative multiple case study aimed to explore practical strategies small businesses use to protect their businesses from cyberattacks. The targeted population consisted of five small business managers located in Washington, D.C., who have implemented effective strategies to reduce cyberattacks in their companies over the past five years. The implications for positive social change comprise the likelihood of helping small business leaders to create effective strategies to mitigate cyberattacks that will contribute to sustaining business effectiveness. Furthermore, these strategies may help safeguard small businesses from data breaches, thereby increasing businesses' economic growth, stimulating the socioeconomic lifecycle, and increasing customers' confidence, which leads to potential employment gains for community residents.

Following Janglou and Sohrabi [8], we used Cybersecurity Enhancement Framework (CEF) as the conceptual framework of this study. CEF was prepared and published by the

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

National Institute of Standards and Technology (NIST) in February 2014 in collaboration with the private sector [9]. According to NIST, the CEF emanated from the 2013 Presidential Executive Order (E.O.) 13636, which directed NIST to partner with industry leaders in developing the cybersecurity enhancement Framework. NIST developed the cybersecurity enhancement act through year-long workshops, extensive outreach and consultation with industry experts and companies, and public commentary. As a result, the CEF offers a process businesses use to understand and develop comprehensive approaches to enhance the mitigation of cyberattack risks. In addition, the CEF provides risk management guidelines that enable organizations to prioritize informed decisions on effectively illuminating loopholes cybercriminals may manipulate. Furthermore, the CEF allows business leaders to dynamically select and direct improvements in cyberattacks and risk management for businesses. Nevertheless, many small business owners lack strategies to reduce cybersecurity threats and vulnerabilities.

2. LITERATURE REVIEW

An appraisal of the professional and academic literature reflects and amalgamates information collected from several pieces of literature or scholarly sources related to cyberattacks. This section critically evaluates the research problem, assesses sources, and identifies the gaps. As technology advances, old techniques become outdated and old-fashioned, providing a staggering incentive for technological innovation and reshaping processes and systems. This qualitative analysis advocated for innovative ways small companies can keep up with the emerging trends and seek alternative solutions to hedge cyberspace when addressing imperviousness in their business environment.

2.1 Analysis and Synthesis of Cybersecurity Framework

The conceptual framework of this study was a Cybersecurity Enhancement Framework (CEF) developed in response to an unparalleled rise in cyberattacks over the past few years. According to Wang et al. [10] and Ghiasi et al. [11], the CEF provides businesses with a blueprint for preventing, detecting, and responding to cyberattacks. Additionally, the framework allows companies to encourage, share and communicate any emerging trends and impending risks and threats in the market amongst internal and external organizational stakeholders [12]. Furthermore, I.T. security professionals use the CEF to maintain compliance with regulatory standards [13]. In addition, the CEF provides a standard classification or vocabulary for describing cyberattacks. Finally, it is a reference resource that small businesses may use to structure their personnel, including staff training, and crafting a job description, as part of cyberattack preparedness.

Furthermore, the CEF provides a preemptive risk-based, easy-to-understand roadmap using technology-neutral language for cyberattack management. According to Pranggono and Arabo [14], organizations with no existing cyberattack policies can quickly adapt and apply cyberattack enhancement frameworks to mitigate cyber threats in their organizations. The National Institute of Standards and Technology (NIST) designed CEF to protect critical national infrastructures such as power generation stations, water/wastewater management, and transportation systems. Small businesses can also adapt and utilize CEF to manage and improve cybersecurity risks in their organizations [9, 15,10]. The CEF is voluntary, not prescriptive, and small business leaders can use this framework to manage and analyze different risk management tools, techniques, and practices. Gordon et al. [16] pointed out that several companies and government agencies globally have embraced the NIST CEF to protect their cyberinfrastructure.

The CEF consists of security actions, outcomes, and valuable references standardized across critical infrastructure sectors [9]. Creating such a framework was to achieve reliably functioning essential infrastructure in the United States. Additionally, the framework offers standardized guidelines and practices that promote communication and outcomes across different organizations and industries about cyberattacks activities, from the executive to the operations level employees [13, 16, 15]. According to Congress [9], the framework consists of five simultaneous and continuous core functions, (a) Identify, (b) Protect, (c) Detect, (d) Respond, and (e) Recover. These core functions provide business leaders with a comprehensive overview of business management practices related to cyberattack risks. With technological advancement, artificial intelligence, and advanced dark web tools, cyber thieves are becoming more complex and dangerous, requiring a coordinated effort from all parties to advance the economy's well-being [13, 17, 18].

According to Corn [17], the increased complexity and connectivity pose more significant security challenges to crucial business infrastructures and the national economy, public safety, and health. In addition, any organization that effectively manages its vital infrastructure reaps greater financial, reputational, and growth rewards. Gordon et al. [16] opined that the CEF assists business owners with a ground plan to starve cyberattack risks per the executive order. NIST created implementation tiers that allow businesses to determine their cybersecurity risks and identify processes if they align with their business approaches to manage risks. According to NIST, the four tiers are building upon the previous tier, namely: Tier 1 (Partial), Tier 2 (Risk-Informed), Tier 3 (Repeatable), and Tier 4 Adaptive [12]. According to the framework, these four tiers describe cybersecurity risk in an organization and how their practices can measure against the framework guidelines [12].

The CEF guides businesses in improving their cyberattack postures [16, 15]. The implementation tier approach allows organizations to determine critical service delivery activities and concentrate on outlays to capitalize on the impact of their cybersecurity investment [19]. Finally, the framework profile assists in identifying the areas of improvement by comparing the current profile (i.e., existing or as-is) with the target (i.e., to-be or goal) profile. Therefore, NIST [19] suggests that systematic implementation of the framework cores will enable organizations to explain the current and target security state,

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

pinpoint areas of improvement, gauge progress towards the target state, and seamlessly communicate among different stakeholders.

2.2 Early days of computer networking and cybersecurity

The Internet was founded in 1969 by the U.S. department of defense and had four connected nodes in the network [20, 21]. The internet's founders predominantly used the internet on government and university computers to communicate and collaborate through emails with minimum regard to security [22]. According to Orman, the early users were only a small group of people who trusted each other and hence put minimal emphasis on safety. Furthermore, as a pastime activity, non-malicious collegial pranks would often be played among friends giving birth to viruses. For example, Bob Thomas created the first known virus, "The Creeper," in 1970, which had no adverse effect [23]. Nevertheless, fast forward to today, the collegial and non-malicious viruses and pranks evolved into more serious threats with the potential to inflict unrepairable pain on organizations and upstage economies, disrupting and throwing nations into turmoil.

As technological advancement and innovation continue to evolve and become more accessible, computers and the internet have become integrated and ingrained into all aspects of our lives and ways of doing business. Increasingly affordable portable computers and other high-tech devices can now connect wirelessly to the internet, resulting in unprecedented cyber threats for small businesses. Orman [23] asserted that the exponential evolution of the Internet of Things (IoT) devices and connectivity has resulted in increased network traffic, posing significant cybersecurity challenges to many organizations. Similarly, Waheed et al. [24] opined that cyberattacks, hacks, and information security breaches are increasingly becoming more frequent, threatening our way of life. Eggers further underscored the need for more robust cyber policies as he believed that future cyberattacks would be more catastrophic and impactful than observed. Cyberattacks have progressively become more frequent, impactful, and sophisticated [25, 26]. In addition, computer systems have become more complex, interconnected, and reliably accessible [27, 14, 4]. Sharif and Mohammed [4] posited that technological advances such as cloud computing, mobility, and remote working paradigms create substantial security challenges for small businesses.

Similarly, a study conducted by Kaushik and Guleria [28] highlighted a set of challenges remote work arrangements and technological evolution present to small businesses. These threats relate to security and trust assumptions in online systems regarding hardware, operating system, and applications. Similarly, Serror et al. [29] added that IoT devices are attractive targets for botnets because security is not a priority for many small businesses. As a result, small business leaders must continuously safeguard their enterprises on a massive scale to ensure that their digital platforms are resilient against cyberattacks. In addition, Gordon et al. [16] opined that small businesses take regular scans of their perimeter and have real-time risk analysis and surveillance for breaches at physical and digital entry points. These vulnerability assessment processes enable small business leaders to identify and assess vulnerabilities within their systems, allowing for faster application of authoritarian measures to minimize the damage.

In their study, Hossain et al. [30] found that 70% of devices connected to the internet are easily accessible and vulnerable to cyberattacks. Similarly, Loishyn et al. [31] agreed that the number of cyberattacks is rapidly growing due to the scientific and technological progress of digital technologies. Deo et al. [32] added that companies and their employees opened their doors to cyber criminals who now use the increased digital footprint and traffic to find vulnerabilities to siphon off money. In 2020 alone, there were over 700 thousand attacks against small businesses, with damages totaling 2.8 billion dollars, and every year the numbers continue to rise [33]. In addition, with technological development and new trending remote work arrangements, more company systems are targeted by scrupulous individuals. Cybercriminals use covert and side channels in cryptographic cores, system bus, high-performance elements such as caches and branch predictors, and hardware Trojans [30]. Similarly, critical business, employees, and customers' personal information can easily be exposed online, and adversaries have a greater incentive to exploit these systems.

According to Firch and PurpleSec [34] and Romanosky et al. [35], in light of the COVID-19 pandemic, cybercrimes have been rising, with small businesses continuously being the most exposed and targeted. In 2017, as Ventures [36] experienced, some of the major hacks, namely WannaCry and NotPetya cyber attacks, highlighted the scale, complexity, and sophistication of these attacks. Furthermore, Deo et al [32] added that cybercriminals are launching Covid-19-themed attacks that drop malware capable of disrupting systems, stealing data and employee credentials using phishing emails with malicious attachments. Therefore, small businesses must continue to enhance their cyber presence and adapt to emerging business trends to stay relevant and fend off these increasingly innovative ways of attracting unsuspecting targets [37].

Attackers take over vulnerable company websites or create temporary ones to host malicious code, lure unsuspecting employees to these sites, and then drop malicious code on their digital devices [32]. Therefore, small business leaders must understand their challenges and make the coveted effort to find solutions to mitigate the risk for their business survival. In addition, they need to quickly make their company's employees aware of scams and then train them how not to fall victim to them. Unfortunately, a lack of robust cybersecurity policies and a wealth trove of confidential data makes small businesses a tempting target for cyberattacks. The confidential data include personally identifiable information from credit card and social security numbers, date of birth, addresses, and personal health data [38, 35, 30]. On the other hand, businesses' confidential data include intellectual property, trade secrets, proprietary source codes,

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

or information these small businesses use, giving them a competitive advantage [39].

Contrarily, Crosignani et al [40] argued that business escapes the full impact of cyberattacks as the effects proliferate downstream to the customers of directly hit firms. According to the authors, businesses directly hit by cyberattacks halt their production, limiting the impact severity while the downstream disruptions to customers are severe. Furthermore, [40]. opined that customers worldwide had lost $7.3 billion, four times larger than the losses the firms directly hit by the cyberattack. Although this might be true for larger companies, small businesses lack adequate resources and financial reserves to cushion their operations, putting them at a high risk of going out of business. Kayumbe and Michael [41] found that the impact of cyberattacks is more severe on smaller companies than on larger firms due lack of financial reserves to withstand an attack. Becket al. [42] opined that small businesses that fail to access customers' information are punished two-fold, first by the punitive monetary toll of the breach and second by the loss of customers due to a lack of trust and fear of patronaging the organization.

According to a Small Business Administration (SBA) survey conducted in 2021, data breach costs upwards of $200,000 per incident, and surveys show that 20 percent of customers immediately terminated their relationship with a compromised business. Similarly, a study conducted by Bartik et al. [43] found that 60 percent of small businesses close permanently six months after a cyberattack. Hence, small business leaders must develop effective security strategies to protect their interests. Lee [44] agreed and opined that small businesses struggle to implement complex cybersecurity systems due to financial restraints making them more vulnerable to cyberattacks. With small businesses' financial security and future on the line, they must have measures to screen questionable network activity. The best practices inside an organization are vital and represent the front line of information security. Well-tabulated cybersecurity policies in easy-to-understand language should be the first weapon in combating and protecting organizational data. The aim is to determine a level of protection to ensure that corporate data and networks are safe and secure.

2.3 Cost of Cyberattacks

Cyberattack is one of our time's most pressing but least understood challenges [39]. These attacks come from foreign nations, criminal syndicates, and activists after intellectual property, bank accounts, social security numbers, and anything valuable that can be used for financial gain or to gain a competitive edge. Technological advancement and easy access to more portable and affordable gadgets easily connectable to the internet have revolutionized how we consume the internet [42]. We are now using the Internet in increasingly innovative and practical ways. This technology is now ingrained into our DNA, underpinning the modern economy and the bedrock of our future. That is why small businesses need cost-effective ways to address cybersecurity challenges to participate in the global marketplace without fear. Likewise, small business leaders need practical strategies that they might use to fend off directed cyber-attacks.

A cyber-attack threatens the existence and longevity of any thriving small business. Cyber-attacks are more prevalent in small businesses due to limited resources and a lack of security expertise, making them more vulnerable to spear-phishing attacks. According to SBA [33], 71 percent of companies with less than 100 employees are attractive targets for cybercriminals looking for a quick cash-out. As a result, small businesses endure substantial financial losses making it challenging to stay in business, ultimately causing many Americans to lose their jobs [42]. Several scholars have posited that small businesses cannot afford to ignore the risks of cyberattacks, so it is vital to take adequate measures. Users can do simple steps to get safe by installing software protection firewalls, antiviruses, anti-malware, etc.

Cyber-attacks are malicious attempts by criminals to infiltrate, illegally gather, and possibly damage a computer or network system [45]. Sharif and Mohammed [4] opined that cybercrimes are profit-driven criminal activities orchestrated through identity fraud, ransomware attacks, email and internet fraud, and attempts to steal financial records, credit cards, or other payment card information. Cyberattacks can lead theft of personal, financial, and confidential information. The actual cost of data breaches is challenging to determine as some of the costs are immediate and others delayed [40]. Certain expenses are almost unavoidable, direct, and relatively easy to quantify. At the same time, others remain intangible, largely dependent on the operating sector and region and the attack's nature, and can spread over many years following the data breach [14]. Additionally, these attacks can damage the organizational reputation and its continued existence. Financial losses due to an organization's cyberattacks and other information system failures are preventable with investment in different security measures and the purchase of data protection systems [4].

Furthermore, as pointed out in a study conducted by Kamiya et al. [45], cyberattacks are costly, especially for small firms. After an attack, smaller companies will likely face expensive remediation and mitigation costs, litigation costs, fines, and possibly a reputation loss. However, it is incumbent on small business owners to inform themselves about the circumstances that influence the cost of data breaches and how these numbers affect their operations. In addition, the growing sophistication of cybercriminal threats calls for a multifaceted and agile approach beyond detection and disruption, incorporating deterrence and prevention [46]. In response to the prospect of infiltration by malicious actors, small business owners need to implement proactive methods for loss prevention, including a formal incident response plan; a compliance plan comprised of policies, audits, training, and education; detection systems; and procedures for maintaining evidence of an incident.

2.4 Cyberattack and Risk Identification

Cyberattacks exploit vulnerabilities in company systems by attacking servers, firewalls, computers, printers, routers,

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

switches, and more to steal, modify or remove access to valuable data. As stated by Hajal [47], hackers usually target small businesses because their systems are more accessible to compromise due to inadequate financial resources. Cyberattacks also use malicious software such as spyware, virus, ransomware, and worms known as malware to send dangerous links or email attachments. Opening or clicking on the links will corrupt the computer hard drive or organizational network system to make the system inoperable. In addition, these criminals utilize emails through reputable sources with the intent to install harmful software or steal sensitive data such as login credentials, credit card numbers, or any other company secrets.

Identifying cyberattack risks requires understanding the preferred approaches intruders and hackers take. Categorizations of cyber risk represent the prior knowledge that the organization has regarding the types of assets to be protected and the type of vulnerabilities and threats [48]. The organization must establish and update the taxonomies corresponding to assets, cybersecurity vulnerabilities, and cybersecurity threats over time to facilitate risk identification [48, 11]. The organization must know the importance of establishing and maintaining updated taxonomies to address the ever-changing cybersecurity environment and ongoing or periodic cyber risk identification.

Esteves et al. [49] suggested two stages typical hackers take: exploration and exploitation. During the initial stage of an attack, hackers typically take on a quest that combines deliberate and intuitive thinking and relies on intensive experimentation. When hackers gain access to the system, exploitation to achieve their goals begins. On the other hand, the Cyber Kill Chain framework classified cyberattacks into seven stages [44]. Every seven steps, from 'reconnaissance' to 'act on objective, ' present unique threats and vulnerabilities. Every intruder and hacker exploits vulnerabilities of an appropriate asset type and launches attacks. For the cyber risk assessment, risk identification requires two major activities: (1) identify the types of assets to be protected and the type of vulnerabilities and threats from external actors, and (2) identify the types of assets to be protected and the type of vulnerabilities and threats from internal actors. To facilitate the reader's understanding, imagine that an organization identified significant cyber vulnerabilities and threats regarding network servers and email systems arising from external hackers and cyber vulnerabilities and threats related to laptop/desktop mishandling from internal users.

2.5 Virtual Private Network

One of the tools remote workers and telecommuters use to connect to their organization's computing systems is the Virtual Private Network (VPN) [47]. A VPN is an ideal way to protect the organization's strategy, especially when accessing a public Wi-Fi network. A VPN encrypts all information transmitted through the computer or any device and helps prevent many cyberattacks. Many workers opt to work from home, so employees can easily access and upload files to their company's servers. Abukari and Bankas [50] argued that VPNs are designed for remote workers to have online privacy and anonymity by changing their public internet into a private network using a specific communication channel. The security of VPNs lies in creating a communication tunnel and protecting the connection by encrypting data. However, remote workers use unsecured Wi-Fi networks to access work files through the VPN can be the back door that lets hackers. The VPN can be exposed to hackers snooping on that unsecured network, compromising the teleworker's security. Their organization has informed our research in this paper. Even though VPNs have their security challenges regarding data breaches [50].

The business environment has dramatically transformed over the past year and a half. Innovation is no longer a competitive differentiator; small businesses now rely on the flexibility and capacity to incorporate technology to continue providing services [39]. Unfortunately, this digital transformation has ignited an influx of new, more formidable cybersecurity threats. Ransomware attacks are rampant, and hackers use business vulnerabilities to infill cyber-attacks are complex and difficult to fathom as they come in various shapes and sizes, from a targeted attack against a database server to numerous phishing emails with mischievous attachments or URLs [50]. These attacks can significantly damage small businesses if a security breach compromises confidential personal and business data. While knowing the purpose of a cyber-attack can be helpful but should not be the main priority. Instead, per Mittal et al. [15], business leaders should prioritize knowing and understanding how the attack occurred and how to prevent them from succeeding.

Small business leaders need effective strategies that save time and resources without forgoing quality or security [50, 44, 15]. In addition, the pandemic has propelled a new era of work arrangements, and more companies now have most of their workforce working remotely [14]. Mittal et al. [15] added that these changes in the employer-employee relationship brought challenges to the mix. Unfortunately, the arduous and time-consuming process is counterproductive, muddles communication, and creates unnecessary hurdles virtual working environment. In addition, cyber-attacks can radically impede business operations, primarily if the company relies heavily on technological gadgets. Regardless of the industry's size, companies are susceptible to sophisticated cyber-attack. Thus, businesses must take preemptive actions and implement a severe approach to cyber security to help minimize risk. In addition, efficient cyber resilience can enhance the business's reputation and brand image, protect it from losses, and much more.

Additionally, regulatory agencies are compounding additional challenges to business leaders by enforcing more stringent data privacy regulations [44, 14]. As a result, negligence has become nearly as great a risk as the I.T. threats themselves [15]. While a ransomware attack is not always preventable, failure is 100% preventable through sound risk management practices [14]. Small business leaders can rest easy knowing that their company's most protected data is secure, and employees can access and execute their duties in privacy and security. A safe way of accessing information needed to

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

perform work assignments effectively frees time, enhances productivity, and protects employees' daily work integrity. Preventing a breach of the organizational network and its systems requires protection against various cyber-attacks. In addition, the appropriate countermeasure needs to be deployed for each attack to deter it from exploiting a vulnerability or weakness. Therefore, any organization's first line of defense is to assess and implement security controls.

3. METHODOLOGY AND DESIGN

3.1 Methodology

Researchers use qualitative, quantitative, and mixed methods to analyze a phenomenon [51]. A qualitative methodology helps explore the phenomenon analyzed from participants who have experienced the phenomenon [52]. For this study, we used the qualitative method because it was crucial to identify and explore practical business strategies from participants who lived or experienced cyberattacks. On the other hand, the quantitative method that characterizes and analyzes relationships among variables was not helpful for this study because we did not test or explore the relationship between variables [53]. Finally, the mixed method, which combines qualitative and quantitative methods [54], was also inappropriate because we did not test hypotheses to analyze variables' relationships to cyberattacks.

3.2 Design

Yin [51] stated that the principal qualitative designs for qualitative research include (a) case study, (b) phenomenology, (c) ethnography, and (d) narrative. As a research design, we used a multiple case study design. The case study design is helpful for researchers to explore a single phenomenon bound in time [53, 51]. A multiple case study design helped us explore in-depth and compare small business leaders' strategies to mitigate cyberattacks and improve their security systems. Some researchers use phenomenology design to explore participants' personal lived experiences [55] or ethnographic designs to explore participants' cultures, behavior, or beliefs [56]. However, both phenomenological and ethnographic designs were not appropriate because we did not examine the meanings of participants' personal lived experiences or participants' cultures. The narrative design, which focuses on exploring individuals' personal life experiences [57], was also inappropriate because this study's purpose was not to focus on narrating participants' life stories.

4. RESEARCH AND INTERVIEW QUESTIONS

The research question of this study was: What strategies do small business managers or leaders use to mitigate cyberattacks in their businesses? The six interview questions we used for this study were: (a) What are your views concerning the importance of reducing cyberattack systems from data breaches at your small business? (b) What strategies did the company implement to protect the data breaches in your organization? (c) How did you disseminate your cyberattack strategies to preserve the organization's systems from data breaches circulated to employees? (d) What are your views on how employees recognize the importance of cyberattack strategies for your business? (e) What will be the best way to increase strategies to mitigate cyberattacks in your organization? (f) How does the company respond to cyberattack threats made against the company? (g) Does your business experienced cyberattack threats? If yes, can you describe the company's risks and actions to mitigate them?

5. DATA COLLECTION AND ANALYSIS

5.1 Data Collection

The data collection for this study was made through face-to-face semi-structured interview questions with five participants who voluntarily agreed to participate. Participants were top managers or leaders who have experienced cyberattacks and used effective strategies to protect data breaches from cyberattacks. Participants were selected using sampling methodology, and interviews took place at participants' offices. Participants were informed about the primary goal of this study and received all information needed to be participants before the interview, which lasted 30 to 45 minutes. Per Kallio et al. [58], using semi-structured interviews enables the researcher to obtain reliable information and better understand participants' perspectives of the research topic. After the interviews, we used member-checking for interview response validation and research credibility. share regarding your strategies to reduce voluntary employee turnover?

5.2 Data Analysis

As highlighted by Yin [51], data analysis consists of five distinct processes, which are as follows: (a) data compiling, (b) disassembling of data into subsets, (c) reassembling data into patterns/themes, (d) interpreting of the data, and (e) developing of conclusions. To Analyze data, we used NVivo 12. NVivo 12 is a software used in qualitative research to code and categorize data according to emerging themes and data similarities. We also used data triangulation for research consistency, collecting data from different sources. For our data triangulation, we explored companies' internal documentation and technical reports to examine the research question, including tax issues, bank payment through the website, and time of the website inactivity. Vindrola-Padros and Johnson [59] added that analyzing in-depth technical, financial, or managerial reports may help explore other hidden causes of firms' sustainability or productivity. For example, a critical review of an organization's payment through the website record may provide reliable information regarding the impacts of cyberattacks on short or long-term planning [60]. After collecting data from field notes, semi-structured interviews, and company sources, we confirmed that data saturation had occurred after interviewing the fifth participant.

6. FINDINGS AND CONCLUSION

6.1. Presentation of Findings

The primary study question for this qualitative multiple case study was: What strategies do small business owners use to protect their business from cyber-attacks? First, Morse [61] and Yin [51] noted that data saturation provides enough information to ensure the study's validity. Then, with the aid of the NVivo 12 software, we identified emerging themes,

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

such as security policy and procedures, employee training, and risk management. The sub-themes that emerged were (a) security controls, (b) resiliency plan, (c) internal controls, (d) employee training, (e) employee awareness, (f) people management, (g) outsourcing I.T., and (h) cybersecurity insurance.

Theme 1: Security Policy and Procedures

Table 1

Frequency of Codes Directly Related to Theme 1: Security Policy and Procedures

Code	*N*	% of the frequency of codes
Security Controls	46	48.42%
Resilient Plan	28	29.47%
Internal Cyber-controls	21	22.11%

Note. N= frequency and total ∑Ni=100

The security policy and procedures concept was the first central theme in this study resulting from data analysis. The cybersecurity policy and procedure's theme emerged from interview questions 2, 4, and 5, in which participants presented their cybersecurity strategies to protect their companies from costly cyberattacks. Cyberattacks security policy is a formal statement established to influence behaviors and actions, setting confines in which employees operate. On the other hand, procedures define how employees apply the policy to achieve a favorable result. Together, cyber policies and procedures will help ensure that cyberattacks are minimum. Data were collected from all five participants' responses and reviewed I.T. procedure documents from participant companies. The cybersecurity policy and procedures dictate employee behaviors and provide guidelines on steps to take when the system gets compromised [62, 63, 3]. Therefore, employees must be aware, educated, and trained to behave accordingly and follow prescribed procedures. All five participants agreed that cyberattacks policies and procedures should be part of any small business operational manual. Therefore, it is imperative that small businesses cautiously craft guiding principles in the form of policies and procedures that employees can use to address issues related to cyberattacks.

Moreover, a well-crafted document facilitates the attainment of a safe cyber operating space where employees can freely express their talents with minimal fear of cyberattacks. In addition, the policy and procedure would, at minimum, provide the organization the ability to prevent future attacks and swiftly address them as they occur. Cybersecurity means fortifying business and consumer data from cyber-attacks [64]. Company cybersecurity policy and procedure documents give employees a roadmap and information on how to behave in any situation. For example, P1 explained, "Employees cannot plug in any phone charging devices to their computer or transfer data to non-company sanctioned devices." P2 added, "We have a written cybersecurity policy and procedures to follow when employees log into the company cyberspace." The company's cybersecurity policy and procedures are critical to protecting customer and employee confidential data.

Similarly, P5 added, "we have a set of well-defined security standards and information security policy that every staff member must read and sign. These signed documents become part of the employee file and are periodically revised." Similarly, P4 and P5 agreed by providing policy documents that all new hires sign as they receive company laptops. Finally, Senarak [65] opined that a lack of adequate plans is catastrophic and negatively affects small businesses' ability to stay in activity. P1, P2, P3, and P4 agreed that the company had written security policies necessary to bring awareness to potential cyber security threats, especially those induced by the various virus, malware, and ransomware programs. In addition, implementing multiple methods, such as computer virus scans and operating system patch updates, can help prevent data breaches. P1 and P2 security documents presented one of the most effective methods for preventing cyber threats, "implementing a layered security approach."

Lateral compartmentalization safeguards the company's cyberspace from unintended interference by unqualified or unauthorized persons, a process used to reduce potential threats and vulnerabilities. P1 said, "We must ensure the expansion and application of the company security policies, standards, and procedures to ensure our staff is following best practices. We focus on developing standards and policies based on the company's needs and requirements." P4 agreed and added, My company has clear security policies and procedures that guide how every department follows when working." P4 and P5 agreed and added that an effective security policy needs to support the company-wide business strategy creating a program that meets the organization's needs and advances security controls. For example, owners of small businesses could enforce access control policies based on classifying how confidential and sensitive the data is and employee seniority [66]. The data classification process alleviates insider and external risks from accessing the company network, reducing the impact of data compromise.

Security controls. The subtheme of security control emerged from the review of the organizational documents provided and participants' responses. Security controls are acutely vital for a company's defenses as all security actions result at some point from administrative decisions [67]. Moreover, as technology transformational trends continue, the business landscape impacts our lives significantly. They are protecting company data, the systems that house the data, and the employees that work with that data are increasingly becoming relevant. P3, P4, and P5 acknowledged having established security controls within their organizations. Furthermore, administrative, physical, and technical rules must be congruent with the organization's focus to achieve a secure cyber environment. Any area left uncontrolled leaves a gap for cyber attackers to find success.

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

Small businesses need to continue conducting risk assessment processes to balance implementation controls and minimize the risk of breaches that will demand time, effort, and money to remedy. All participants highlighted the need for the leadership to be proactive in controlling their business environment and have a properly planned contingency plan. A cyberattack is not just an I.T. problem but also a business productivity problem, a public relations problem, and a legal problem [68]. Therefore, security controls could be valuable for managing risk and cyber threats [69]. Therefore, small business owners need to devise security policies to include security controls to protect business data.

Resiliency plan: small businesses should have a properly chalked-out cyber resiliency plan that helps provide a fast response and manages a data breach. As the sophistication of cyber threats, such as ransomware, continues to evolve, small businesses need to shift their focus from threat prevention to a cyber resilience model for holistic cyber security that includes recovery plans [69]. Cyber resilience requires organizations to also focus on the ability to respond to an attack, mitigating damage while protecting critical data and enabling recovery to restore business continuity [70, 68]. A successful business should be able to withstand and recover from attacks or compromises enabled by cyber resources [68]. Cyber resiliency refers to the organization's ability to withstand a data breach or a cyber-attack. Fisher et al. [70] argued that a resilient cybersecurity plan has five parts Identify, Protect, Detect, Respond, and Recover. For example, P4 said, "we have a strategy that allows us to swiftly restore data, bringing uncompromised applications back online and minimizing the downtime. We back up all data daily and store different servers that are easily accessible to enable quickly restore data restoration from the last date before data was compromised." Additionally, P2 and P5 added that resilient plans should have elaborate protocols that employees can follow to handle a situation when a breach occurs. Thus, cyber resilience plans can aid small business leaders in instituting robust remedies against the changing cyber threat scenario, with more powerful and adaptable ways to face cyber threats if properly administered.

Internal cyber controls. From participant responses and company documents, prior research is compatible regarding internal cyber controls. Small business leaders that have developed a set of internal cyber-control are in a position to prevent and protect company assets and data from potential threats [70, 65]. In addition, employees that follow established internal controls can carry out their duties in a way that protects clients, the organization, and the bottom line. Responses from participants revealed that internal cyber control was necessary for helping employees perform their jobs and protect company assets, consumer data, and confidential employee files. P1 said, "My employees are aware of the importance of internal cyber controls. These controls directly impact employees' ability to perform their job duties." P3 added, "Our employees all recognize and appreciate the importance of protecting our data." P4 and P5 elaborated on employees' consequences and penalties that can be as stiff as up to termination.

As the use of computers and advancement in technological gadgets than allows employees to conduct business increases, the risk of cybersecurity and data incidents continues to rise. Small business employees must understand the importance of observing internal controls to minimize the possibility of exposure [68]. Many companies are adopting a hybrid work model considering the pandemic and changing working trends. Efficient internal control is the first line of defense for mitigating cyber threats. All participants alluded to the need for their security teams to make a concerted effort to enforce adherence to the protocol on all the devices users connect to company networks.

Furthermore, participants raised concerns about the challenges they face in securing devices. According to P3 and P4, employees increasingly connect to company cyberspace with unmanaged devices generating blind spots for security teams. Therefore, small businesses must implement user access restrictions critical to maintaining internal cyber security. For example, business owners must always know and limit access to sensitive information and always put safeguards to minimize unauthorized access. Internal cyber controls include password requirements, multi-factor user authentication at login and logical access controls, proper turnoff of computers when they are not in use, antivirus software and firewalls installed, and access controls to confidential information [65]. Internal controls mitigate risk and reduce the chance of an unwanted risk outcome. Having internal cyber-controls as a built-in part of the company security programs is the key to ensuring that the business operates effectively. The small business leaders and their management team must communicate the importance of internal controls downward, and every process must occur within the control environment's parameters.

Theme 2: Employee training.

The second theme that emerged from data analysis was employee training. The concept of training was the second central theme of the study, with the following subthemes (a) security-focused culture, (b) awareness, and (c) people management. Table 2 is an illustration of the frequency of codes from NVivo 12 directly related to the theme of the training.

Table 2

Frequency of Codes Directly Related to Theme 2: Training

Codes	*N*	% of the frequency of codes
Security-focused culture	32	50.79%
Employees awareness	17	26.98%
People's management	14	22.22%

Note. N= frequency and total ∑Ni=100

Training is an essential tool small business leaders could use to empower their employees and prepare them to become the first line of defense. Regular training seminars and inviting

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

cybersecurity experts to speak will reinforce awareness and enable employees to make better judgments and decisive decisions in protecting the organization's system and confidential information. The responses from all five participants stressed the importance of training in combating data breaches and hedging against organizational system breaches. Additionally, the archival documents from the participant companies corroborated the participants' reactions quite spectacularly. Regular training of employees on cybersecurity improves the organization's overall security by eliminating needless miscalculations that may lead to data losses and breaches, enhancing the company's reputation, and bolstering employee confidence [71].

Furthermore, when employees receive adequate cybersecurity and safety training, the organization increases productivity and minimizes operation costs [72]. P1 said, "It is our company policy to periodically conduct training sessions where we invite I.T. experts to speak and educate employees on cyber security issues, threats, and how to recognize fishing emails." P2, P3, and P5 agreed and added that all their employees with access to the Information Resources undergo security awareness training regularly. Based on the response provided by P3 and the policy documents from all five small businesses, it is evident that cybersecurity training is part of effective strategies to protect the company from possible cyberattacks.

P4 responded, "We normally invite cybersecurity experts to come and speak at our company training sessions allowing employees to hear fresh voices and ask questions." P3 added, "We train our employees. Training does not have to be formal. For example, a simple 5 to 10 minutes conversation with employees on how to deal with ethical emails with attachments or the importance of regularly changing passwords helps instill a cybersecurity mentality. The policy document from organization 4 stated, "The organization shall continuously evaluate the cyberattacks prevention skills held by all the employees and promote regular training to address any potential skill gaps." Analyzing the response by P3 and the details in the organization's archival document from Organization 4 reveals how organizations invest more time and resources in training programs to address cybersecurity threats effectively. P4 explained that their organization uses two strategies: sending the employees to train and conducting in-house training for people in the I.T. security department. In addition, according to P4, external training happens at least once every month, where an individual in the team receives the necessary skills. Based on the response by P4, organizations also adopt a mix of training methodologies to ensure that their cybersecurity strategies are convincing enough.

Security-focused culture. Small business owners also continuously educate their employees on proper internet usage [69]. In addition, small business leaders must continue reinforcing adherence to company rules and guidelines to curtail cyberattack exposure. User training education brings about awareness, allowing employees to understand their role in keeping the organization secure and report any unusual activity. According to P1 and P3, creating a standard training schedule is complementary to creating a work culture centered on security. P5 added that building a vibrant security-centered workforce exudes confidence and efficiency. Therefore, small business owners must promote a workforce that adheres to acceptable security practices and various tips to ensure continued prosperity. In addition, security practices need to be continuously reinforced through training to remind employees not to drop guard.

Therefore, everyone in the organization – from the new hire to the top management – must understand the need to take security seriously and feel responsible and accountable for maintaining security. P2 stated, "as part of our business policies, we continuously reinforce a security culture by educating and training every employee on security measures. In addition, at every meeting, we emphasize the departmental manager's need to talk vigorously about cybersecurity. Security of our organization system is our number one goal, and our treasured assets would only help keep our system safe." As per all participants, data security is vital to organizational success, and creating security-focused culture addresses how confidential company data can be safe and protected. In addition, delving deeper into the experience other organizations and industries are experiencing, good or bad, can help plan and prevent similar pitfalls and help guide the company through these challenging times. Developing security-focused culture encourages employees to act responsibly and prioritize company-wide security-focused behavior. According to P5, "We always encourage our employees to report security incidents to immediate supervisor and appropriate correction measures could be instituted." Small business leaders could also encourage employees to view their work and company equipment as valuable assets. Finally, instilling a security-focused culture instills confidence. Cyber security becomes an acceptable way of doing business, aiding in solving the threat of internal security breaches and preventing external security breaches.

Employee Awareness. Employee awareness signifies a general understanding of the organization's risks and threats from employees' online activities [73]. As stated by Brady et al., Employees make up the band of I.T. users in an organization, meaning that their understanding of cybersecurity, in general, would help quite significantly in guaranteeing data safety and protection. Based on the participants' responses, cybersecurity awareness positively affects an organization's cybersecurity status. All five participants collaborated on communicating their online presence's dangers and financial implications. As pointed out by P2, P4, and P5, if employees are well-informed and aware of the risks involved, they tend to refrain from accessing or opening suspicious emails.

All participants echoed the importance of cybersecurity training awareness as a ubiquitous initiative for small companies. Cybersecurity awareness entails understanding and defending a company's digital assets [73]. Employees should understand cyberattacks, the potential impact of a cyber-attack on their organization, and steps they should take

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

to minimize risk and defend their organization against cyber crimes. P2 and P4 added that awareness in small businesses was the cornerstone for strategic cyber defense. P5 said that the effectiveness of security controls is contingent on the people executing them. According to Alahmari and Duncan [71], awareness is paramount in empowering employees to be decisive when faced with challenging cybersecurity threats. Therefore, there is a need for a security-focused culture critically enable employees to make an informed judgment when faced with a threat to the security of information assets in the organization.

The responses revealed that these leaders recognize the importance of employee awareness and its role in protecting their businesses [74]. For example, P1 asserted, "My employees are aware of the importance as it directly impacts their ability to perform their job duties. I always try to keep employees informed through emails, company bulletins, and memos on new information I might have come across." All five participants agreed that communicating and spreading information among employees helps employees stay alert and cannot become cyber victims. The findings were clear; each participant believed employee awareness is a fundamental component in the war against cybercrime and armed their employee accordingly.

The research participants' responses and reviewed documents espoused He et al. [74] conclusion that cybersecurity awareness among employees is paramount to building a cyber-security-conscious culture. In reality, most small business leaders allocate minimal time to establishing effective cybersecurity strategies due to fear of cost and operating on lean budgets. Brady et al. [74] and Fisher et al. [69] exposed this reality by noting that financial constraints in small businesses discourage the business owner from making adequate investments in I.T. infrastructure. As pointed out by all participants, maintaining an informed workforce is cost-effective, and companies can maintain a dedicated security focus staff.

People's management. After reviewing the participants' responses and I.T. security procedure documents, the people's management subtheme emerged. All five participants strongly believed that managing employees' behavior, especially when using company equipment with access to a company-wide system, is vital to protecting information security. It is crucial that small business owners assign greater weight to cybersecurity and not overlook employees' cybersecurity behavior. Employees act in a particular way, guided by the strategy and philosophy they follow to safeguard informational assets. Luamba et al. [75] argued that employees are the leading cause of data breaches for small businesses because of their direct pathways into company systems.

Similarly, Firsch and PurpleSec [34] claimed that most successful hack attacks result from avoidable human errors. Alahmari and Duncan [71] added that users' behaviors are the biggest threat to information security in any given organization. P1, P2, P4, and P5 stressed the need to manage and restrict who has access to what information. The rigorous authentication mechanism is pertinent to achieving a much more secure cybersecurity system [75, 33]. Technology is a vital ingredient in any business's continued prosperity plan, and it is, therefore, critical that small business leaders make a concerted effort to monitor how employees conduct company business [76].

According to Luamba [77], employee actions such as inappropriate use of company resources to surf the web to watch pornography, gamble, conduct personal business, and recreational internet browsing are security policy violations. Furthermore, Blye and Luamba [78] warned that a lack of proper oversight of employee actions poses a grievous risk to an organization's intellectual property, including criminal activity such as theft and corporate espionage. He and Zhang [73] opined that people are the primary source of information security incidents. Chagadama [79] and Unsonst and Sandberg [80] noted that steadfastly dedicated employees ensure that business systems and gadgets are safe and always mindful of the cyber surroundings.

Owners of small businesses could develop strategies to manage employees' evaluations and behaviors when using and logging into company-managed cyberinfrastructure and determine ways to enforce positive employee behavior [78]. All participants agreed that oversight is critical to curbing some unruly employee behaviors. Small business owners should focus on improving cybersecurity strategies and find ways to motivate employees to prioritize the protection of organizational networks, company gadgets, and confidential data. Small business owners should not diminish the impact of human factors in cybersecurity because employees' actions, intentionally or otherwise, can negatively impact organizational cyberspace. Instead, small business owners should make employee training their top priority as their first defense against cyberattacks. Blye and Luamba [78] and El-Bably [76] recommended recruiting and training staff as security policy guidelines and encouraged them to be vigilant in protecting the organization's information security.

Theme 3: Risk Management

The third theme that emerged from data analysis was risk management and had two subthemes (a) outsourcing I.T. services and (b) cyber insurance. Table 3 is an illustration of the frequency of codes from NVivo 12 directly related to the theme of the training.

Table 3

Frequency of Codes Directly Related to Theme 3: Risk Management

Code	*N*	% of the frequency of codes
Outsourcing I.T. Services	48	60%
Cyber Insurance	32	40%

Note. N= frequency and total ∑Ni=100

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

Cybersecurity risk management was the third central theme in this research, and the theme had two subthemes (a) outsourcing I.T. services and (b) cyber insurance. The themes came from the five participants' responses and the company I.T. security and procedural documents I reviewed. The findings correlate with Eling et al. [20], analysis that explained cybersecurity risk management as an essential and vital process for controlling risks related to data breaches. Risk management necessitates identifying, assessing, and managing cyber threats [73]. Additionally, several scholars attribute cyber threats or risks to various sources, including cyberattacks, financial uncertainty, strategic management errors, accidents, and natural disasters [73,80]. A deficiency in understanding cyber risks leads to unfortunate consequences that will affect both the tangible and intangible assets of the organization, even worse, may lead to bankruptcy [71]. As a result, small business leaders need strategies to manage the risk posed by cyber thieves and quickly identify, evaluate, and mitigate the risk related to their business's availability, confidentiality, integrity, and customers' data.

All participants echoed the need for implementing a systematic, structural approach to risk management that emphasizes the implications of cybersecurity. P1, P3, and P4 underlined the importance of implementing risk management strategies emphasizing conformance with an organizational goal, standards, and regulations. All the participations used the NIST blueprint as the guiding framework for crafting the risk management strategy. P2 and P5 echoed the same sentiment advocating for governance structure as a successful cyber risk management tool. P2, P3, and P5 focused on systematically evaluating and responding to cyber risk to safeguard data processes through organizational information systems effectively. P3 elaborated further on systematic cybersecurity and risk management processes, stating that "systematic risk management is the cornerstone of securing the information technology environment and is critical to delivering actionable cybersecurity strategy. For example, the security of systems in a government health organization may depend on a thorough risk assessment, the analysis of the associated outcomes, and the risk relevance to the organization and its stakeholders [76, 81, 82].

Effective management of cybersecurity requires the highest level of security measures. Therefore, leaders of small businesses must find ways to emphasize the importance of minimizing risks for continued success [78]. In addition, a step-by-step, easy-to-understand blueprint guides employees on what to do when they feel they have been compromising. P1 and P4 added that communication is vital to successfully implementing cybersecurity policy and ensuring that employees follow procedures. P3 said, "we all make mistakes, some that are very costly, but what is important is how we communicate and warn one another. The key is not to victimize employees but incentivize them to come forward early to allow for the urgent application of prescriptive remedies and quickly thwart and stop the infection." As a result, early detection of risks can save the organization money and minimize operational disruptions [77]. However, the risk will always be ubiquitous, even with quality I.T. infrastructure and practices and strict security measures.

Consequently, the framework for managing cybersecurity recommended by NIST [83] is rooted in a risk-based approach. Protecting confidential organizational data calls for robust and comprehensive investment in security technology, cybersecurity risk management strategies, and constant consultation with I.T. experts. In addition, owners of small businesses can also reduce the financial burden but proactively applying preventive measures [78]. Outsourcing I.T. and cyber insurance are the two emerging themes described below.

Outsourcing I.T. The concept of outsourcing I.T. services emerged from four participants' responses and their company security and procedure documents reviewed. According to Dana et al. [84], most small businesses are still in their expansion stage. They do not have enough financial resources to support having an in-house I.T. department or hiring a full-time I.T. employee. Therefore, outsourcing the services becomes a viable option, as pointed out by all the participants who confirmed to have contracted the I.T. services to a third party. P1, P2, and P4 further explained that they decided to outsource the I.T. services as they could not afford a high-quality I.T. expert.

Similarly, P5 said, "technology is continuously changing, and as small businesses, we lack the financial resources to keep up with all the emerging technologies and trends. Therefore, we can't afford to keep it and do not have the resources. Therefore, it is better to contact the I.T. professional and focus on what we do better: serve our customers and make them happy." In addition, outsourcing can help small business owners with the expertise required to decompress complex I.T. challenges, thereby saving them money and time that they could invest in solving other hot issues [84]. For example, owners of small businesses can consult and contract I.T. experts to periodically monitor and identify areas where their business systems are vulnerable to cyber-attacks and obtain recommendations that can be useful to protect business data against cyber-attacks. Pankowska [85] posited that small companies could benefit from outsourcing their I.T., as they can focus their energy, time, and money on growing the business.

The forward-thinking I.T. business leader recognizes the need to incorporate outside resources, seeking to leverage sophisticated tools and subject matter the I.T. experts possess by contracting their services [86]. P5 discussed the need for small business owners to be vigilant and avoid emphasizing the need to save a buck over the company's cyber security. As he pointed out, cost should not only be the determining factor for outsourcing I.T. services. When contracting I.T. services, the provider must have the necessary skill set to perform the services expertly. P3 also agreed with third-party vendors, stating that they often use vendors to perform certain types of specialized security services. DeFord [87] recommended having a retainer with a reputable cybersecurity company that guarantees quick response time in the event of a cyber-attack.

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

An effective cybercrime prevention strategy includes having immediate access to resources as soon as an incident occurs. Per Deford [87], speed is the most critical factor in the new era of cybersecurity. PA1 shared that part of his strategy was to put a company on a retainer, specifically to handle the analysis after a cyber-attack or data breach has occurred. PA1 explained that obtaining a retainer is hiring a company whose job is to be on call to analyze the data files and better understand the nature of the breach.

Consulting I.T. experts' services include thoroughly assessing, implementing, and maintaining security systems. For example, P1 stated, "we outsourced and consulted I.T. experts and incorporated their input when we drafted our thorough incident response plan." In addition, outsourcing experts specializing in I.T. services have privileged access to knowledge gained through their broad clientele, which they can use effectively in anticipating and mitigating threats. Furthermore, this will provide an extra layer of protection to prevent and minimize risks and quickly resolve any security issue. For example, P2 stated, "we have outsourced I.T. services to cybersecurity experts trying to capitalize on their cybersecurity expertise to manage network equipment, including the installation of patches and updates. By outsourcing the I.T., we feel that the company network and equipment have some level of protection from attacks." P3 said, "we bring in I.T. experts to conduct comprehensive system audits periodically, flashing out any deficiencies within the company computer system." Having an outside expert provides a new set of eyes and a unique perspective that enables us to address the identified new vulnerabilities [88]. After reviewing P1's I.T. service award, they received honors for relying on I.T. experts to provide secure services. Most cybersecurity I.T. experts have tremendous experience, know how to deal with cyberattack issues, and are likely to find solutions quicker before any damage occurs.

Cybersecurity insurance. Cyber insurance emerged in the early 1990s as an indispensable tool for mitigating financial liabilities that arise from breaches [89, 90, 79]. A cyber insurance policy will be a buffer that protects the small business by assuming all that may arise from cyber-attacks for a monthly fee or premium. Cyber Insurance is, therefore, one of the ways small business leaders can protect their company assets and liabilities stemming from cyber-attacks. All five participants quickly pointed out that they have purchased cyber insurance gives them a sense of security, knowing that in case of a cyber-attack, the insurance will cover the cost of recovery and any losses. For example, P4 said, "small businesses should first take out insurance that covers the cost of recovery or replacement of equipment that may be written off or inoperable after a cyber-attack." P3 agreed and said, "insurance alleviates some of the fears and gives you some comfort from the unknowns." Purchasing cyber insurance transfers risks of various cyber incidents, including data breaches, business interruptions, and network damage, from the small business to the insurance company [91]. P2 added that no systems or software could give 100% protection; therefore, it is equally important to have proper insurance coverage to include any damages in case of a breach. Purchasing a cyber insurance policy will help transfer risk, covering the recovery cost, any potential loss incurred during the downtime, and any litigation or compensatory cost emanating from the data breach [90].

Furthermore, when protected by cyber insurance, the risk is transferred to the insurance company that assumes ownership and will meet the costs resulting from the data breach [92]. In addition, clients will hold the company responsible for compromising their information and expect compensation for the losses they may suffer from such a breach. Participants P1, P2, P3, P4, and P5 indicated that they employed cyber insurance as part of their strategy to protect their businesses against financial losses. Cyber risk insurance adds a valuable layer of protection for residual risks and offers incentives to improve risk management, but it is no substitute for effective cyber risk mitigation. Cyber risk is difficult to insure due to the nature of the risk, and as technology evolves, attackers continue to grow exponentially. The role of insurance is to transfer risks from the insured and pool those risks within the insurer [92, 90, 79].

6.2. Conclusion

Our findings strengthened this approach by including (a) a security policy and management, (b) employee training, and (c) a risk management policy to protect confidential company data from cyber-attacks. In addition, owners of small businesses could utilize this study's findings to improve strategies to mitigate cyberattacks and prevent future cyberattack threats. The Internet has opened many opportunities for small, middle, and large businesses to increase their visibility, leveling the playing field and enabling innovation in organizations to promote and offer goods and services to clients. Despite the beautiful opportunity the internet brings, there is a growing need for improving I.T. security and mitigating cyberattacks to sustain business longevity and productivity. Cyberattacks are scouring for opportunities and vulnerabilities that they can capitalize on and enrich themselves. Small businesses must fight back and protect their organizations, as most cyber-attacks can be prevented or detected using basic security practices. Prevention is crucial to lessening the risk of data breaches. Investing in cybersecurity software, soliciting help from I.T. experts, and being aware of the standard attack methods used by hackers can enable small business leaders to implement strategies that may help protect and reduce unwarranted access to organizational-sensitive data. Conscientious about workplace cyber security can make an enormous difference in efficient cyber resilience.

REFERENCES

1. Laitinen, M., & Armstrong-Smith, S. (2022). Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organizations. *Cyber Security: A Peer-Reviewed Journal*, *5*(3), 190-205.
2. Raineri, E. M., & Fudge, T. (2019). Exploring the sufficiency of undergraduate students' cybersecurity knowledge within top universities' entrepreneurship

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

programs. *Journal of Higher Education Theory & Practice*, *19*(4).
3. Slusky, L. (2020). Cybersecurity of online proctoring systems. *Journal of International Technology and Information Management*, *29*(1), 56-83.
4. Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138-156.
5. Xiao, J., & Feroskhan, M. (2022). Cyber attack detection and isolation for a Quadrotor UAV with modified sliding innovation sequences. *IEEE Transactions on Vehicular Technology*.
6. Buzdugan, A., & Capatana, G. (2022). *Cyber security maturity model for critical infrastructures in education, research, and business technologies*. Springer, Singapore.
7. Gleirscher, M., Johnson, N., Karachristou, P., Calinescu, R., Law, J., & Clark, J. (2022). *Challenges in the safety-security co-assurance of collaborative industrial robots. In The 21st Century Industrial Robot: When Tools Become Collaborators*. Springer, Cham.
8. Jangjou, M., & Sohrabi, M. K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. *Archives of Computational Methods in Engineering*, 1-22.
9. Congress, U. S. (2014). Cybersecurity Enhancement Act of 2014. *Public Law*, 113-274.
10. Wang, B., Dabbaghjamanesh, M., Kavousi-Fard, A., & Mehraeen, S. (2019). Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach. IEEE Transactions on Industry Applications, 55(6), 7300-7309.
11. Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., & Alhelou, H. H. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9, 29429-29440. https:/doi.org/10.1109/ACCESS.2021.3059042.
12. National Institute for Standards and Technology (NIST), (2020). International Resources. Retrieved from Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework/international-resources
13. Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. Government Information Quarterly, 36(2), 346-357.
14. Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), e247.
15. Mittal, A., Gupta, M. P., Chaturvedi, M., Chansarkar, S. R., & Gupta, S. (2021). Cybersecurity enhancement through blockchain training (CEBT)–A serious game approach. International Journal of Information Management Data Insights, 1(1), 100001.
16. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST cybersecurity framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1), tyaa005.
17. Corn, G. P. (2021). National security decision-making in the age of technology: Delivering outcomes on time and on target. Journal of National Security Law & Policy, 12(1), 61-70
18. Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry, 13(4), 597.
19. National Institute for Standards and Technology (NIST), (2022). Cybersecurity Framework: Helping Organizations to Better Understand and Improve Their Management of Cybersecurity Risk. https://www.nist.gov/cyberframework.
20. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125.
21. Roberts, L. (1988). The Arpanet and computer networks. In A history of personal workstations, 141-172.
22. Orman, H. (2003). The Morris worm: A fifteen-year perspective. IEEE Security & Privacy, 1(5), 35-43. DOI: 10.1109/MSECP.2003.1236233
23. Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S. S., & Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Computing Surveys (CSUR), 53(6), 1-37.
24. Eggers, S. (2021). A novel approach for analyzing the nuclear supply chain cyber-attack surface. Nuclear Engineering and Technology, 53(3), 879-887
25. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). An innovative approach in combating economic crime using forensic accounting techniques. Journal of Financial Crime. 27(4), 1253-1271.
26. Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.
27. Bedford, J., Farrar, J., Ihekweazu, C., Kang, G., Koopmans, M., & Nkengasong, J. (2019). A new twenty-first-century science for effective epidemic response. Nature, 575(7781), 130-136. https://doi.org/10.1038/s41586-019-1717-y
28. Kaushik, M., & Guleria, N. (2020). The impact of pandemic COVID-19 in workplace. European Journal of Business and Management, 12(15), 1-10.

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

29. Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2020). Challenges and opportunities in securing the industrial internet of things. IEEE Transactions on Industrial Informatics, 17(5), 2985-2996.
30. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In 2015 IEEE World Congress on Services, 21-28.
31. Loishyn, A., Hohoniants, S., Tkach, M., Tyshchenko, M., Tarasenko, N., & Kyvliuk, V. (2021). Development of the concept of cybersecurity of the organization. TEM Journal, 10(3),1447-1453.
32. Deo, G. P., Raj, G., & Perumal, R. (2020). How Covid-19 is dramatically changing cybersecurity.
33. Small Business Administration (SBA). (2021). Stay safe from cybersecurity threats. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats.
34. Firch, J., & PurpleSec, L. L. C. (2021). Cyber security trends you can't ignore in 2021. Available online: https://purplesec. us/cyber-security-trends-2021/
35. Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity, 5(1), tyz002.
36. Ventures, C. (2019). 2019 official annual cybercrime report. In Recuperado el.
37. Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management, 23(1), 1-11. http://dx.doi.org/10.4102/sajim.v23i1.1277
38. Aswathy, S. U., & Tyagi, A. K. (2022). 10 Privacy breaches. Security and Privacy-Preserving Techniques in Wireless Robotics, 163
39. Bamberger, K. A., Canetti, R., Goldwasser, S., Wexler, R., & Zimmerman, E. J. (2022). Verification dilemmas in law and the promise of zero-knowledge proofs. Berkeley Technology Law Journal, 37(1).
40. Crosignani, M., Macchiavelli, M., & Silva, A. F. (2021). Pirates without borders: The propagation of cyberattacks through firms' supply chains. FRB of New York Staff Report, (937).
41. Kayumbe, A., & Michael, L. (2021). Cyber threats: Can small businesses in tanzania outsmart cybercriminals. International Research Journal of Advanced Engineering and Science, 6(1), 141-144.
42. Beck, E., Goin, M. E., Ho, A., Parks, A., & Rowe, S. (2021). Critical digital literacy as method for teaching tactics of response to online surveillance and privacy erosion. Computers and Composition, 61, 102654.
43. Bartik, A. W., Bertrand, M., Cullen, Z., Glaeser, E. L., Luca, M., & Stanton, C. (2020). The impact of COVID-19 on small business outcomes and expectations. Proceedings of the national academy of sciences, 117(30), 17656-17666. https:/doi.org/10.3386/w27613/
44. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.
45. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749.
46. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. Journal of Communication Engineering & Systems, 11(1), 1-6.
47. Hajal, G. E. (2022). Teleworking and the jobs of tomorrow. Research in Hospitality Management, 12(1), 21-27.
48. Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cybersecurity risks. Cluster Computing, 23(3), 1827-1843.
49. Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. MIT Sloan Management Review, 58(3), 71.
50. Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11(4), 1401-1407.
51. Yin, R. K. (2019). Case study research and applications: Design and methods (6th ed.). SAGE. Publications.
52. Ghauri, P., Gronhaug, K., & Strange, R. (2020). Research methods in business studies. Cambridge University Press.
53. Annansingh, F., & Howell, K. (2016). Using phenomenological constructivism (P.C.) to discuss a mixed approach in information system research. Electronic Journal of Business Methods, 14(1), 39-49.
54. Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? Journal of Marketing Thought, 3(1), 1-7.
55. Moustakas, C. E. (1994). Phenomenological research methods. SAGE Publications.
56. Templeton, R. (2016). Doctorate motivation: An (auto)ethnography. Australian Universities' Review, 58(1), 38-44. https://eric.ed.gov/?id=EJ1091203
57. Saunders, M. N. K., Lewis, P., & Thornill, A. (2019). Research methods for business students (8th ed.). Pearson Education Limited.
58. Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide.

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

Journal of Advanced Nursing, 72(12), 2954-2965. https://doi.org/10.1111/jan.13031
59. Vindrola-Padros, C., & Johnson, G. A. (2020). Rapid techniques in qualitative research: A critical review of the literature. Qualitative Health Research, 30(10), 1596-1604. https://doi.org/10.1177/1049732320921835
60. Yu, H., Abdullah, A., & Saat, R. M. (2014). Overcoming time and ethical constraints in the qualitative data collection process: A case of information literacy research. *Journal of Librarianship and Information Science, 46*(3), 243-257.
61. Morse, J. M. (2015). Data were saturated. *Qualitative Health Research, 25*(5), 587-588 https://doi.org/10.1177/1049732315576699
62. Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employee's compliance with cybersecurity control procedures. ACM Transactions on Management Information Systems (TMIS), 12(2), 1-29.
63. Sabillon, R. (2022). Audits in cybersecurity. Research Anthology on Business Aspects of Cybersecurity, 1-18.
64. Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), e23692. https: doi.org/10.2196/23692.
65. Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. The Asian Journal of Shipping and Logistics, 37(1), 20-36.
66. Sabitha, S., & Rajasree, M. S. (2017). Access control-based privacy-preserving secure data sharing with hidden access policies in cloud. Journal of Systems Architecture, 75, 50-58.
67. Tyagi, N., Fatima, H., & Rakesh, N. (2021). Emerging technologies and cyber security: New horizons of cyber security solutions. Emerging Technologies in Computing, 153-170.
68. Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: The growing need for a cyber-resiliency workforce. I.T. Professional, 20(3), 23-30.
69. Fisher, R., Porod, C., & Peterson, S. (2021). Motivating employees and organizations to adopt a cybersecurity-focused culture. Journal of Organizational Psychology, 21(1), 114-131.
70. Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity, 5(1), tyz013.
71. Alahmari, F., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 1-5
72. Zhuang, P., Zamir, T., & Liang, H. (2020). Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Transactions on Industrial Informatics,17(1), 3–19.
73. He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249-257.
74. Brady, G. M., Truxillo, D. M., Bauer, T. N., & Jones, M. P. (2021). The development and validation of the privacy and data security concerns scale (PDSCS). International Journal of Selection and Assessment, 29(1), 100-113.
75. Luamba, S. D., Blye, L. J. M., Williams, A. I., & Chagadama, J. (2021). Innovative strategies for small retail companies' sustainability. Forex Publication 9(3), 330-338
76. El-Bably, A. Y. (2021). Overview of the impact of human error on cybersecurity based on ISO/IEC 27001 information security management. Journal of Information Security and Cybercrimes Research, 4(1), 95-102.
77. Luamba, D. (2019). Strategies small business owners use to remain sustainable (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses database. (UMI No. 13806347)
78. Blye, M. L., & Luamba, D. (2021). Fraud in nonprofit organizations: How to mitigate it? *International Journal of Business and Management*, (4), 385-392.
79. Chagadama, J. (2022). Small construction business owners' strategies to reduce voluntary employee turnover (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses databases. (UMI No. 29215802)
80. Umsonst, D., & Sandberg, H. (2022). Experimental evaluation of sensor attacks and defense mechanisms in feedback systems. Control Engineering Practice, 124, 105178.
81. Trappe, W., & Straub, J. (2021). Journal of cybersecurity and privacy: A new open access journal. Journal of Cybersecurity and Privacy, 1(1), 1.
82. Hu, W., Chang, C. H., Sengupta, A., Bhunia, S., Kastner, R., & Li, H. (2020). An overview of hardware security and trust: Threats, countermeasures, and design tools. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 40(6), 1010-1038.
83. National Institute for Standards and Technology (NIST). (2018). Framework for Improving the Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
84. Dana, L. P., Nguyen, H. T., & RafalKuc, B. (2021). Strategic outsourcing risk management of Van Hien University in Vietnam. International Journal of

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**

Advanced Multidisciplinary Research and Studies, 1(2), 1-6.

85. Pankowska, M. (2019). Information technology outsourcing chain: Literature review and implications for development of distributed coordination. Sustainability, 11(5), 1460.
86. Banerjee, S., Swearingen, T., Shillair, R., Bauer, J. M., Holt, T., & Ross, A. (2022). Using machine learning to examine cyberattack motivations on web defacement data. Social Science Computer Review, 40(4), 914-932
87. DeFord, D. F. (2022). Sustainable digital health demand cybersecurity transformation. Frontiers of Health Services Management, 38(3), 31-38.
88. Heller, R., Toregas, C., & Hoffman, L. (2019). Reach to teach: Preparing cybersecurity experts as adjunct community college faculty. Proceedings of the 11th International Conference on Computer Supported Education, 338–343.
89. Erickson, A., & Neilson, T. (2018). Cybersecurity – the No. 1 threat facing manufacturers. Journal of Industrial Management 60(4), 24 -27
90. Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., & Dobalian, A. (2020). Trends and best practices in health care cybersecurity insurance policy. Journal of Healthcare Risk Management, 40(2), 10-14.
91. Department of Homeland Security (2020). ICS-CERT: Industrial Control Systems - Computer Emergency Response Team. https://us-cert.cisa.gov/ics.
92. Corradini, I. (2020). Building a cybersecurity culture in organizations (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing.

*Corresponding Author: **Prof. Dr. Joel Chagadama, DBA.**