Scientific Research Publishing

Journal of Information Security, 2024, 15, 24-39
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework

Binita Saha, Zahid Anwar

Computer Science, North Dakota State University, Fargo, USA
Email: binita.saha@ndsu.edu, zahid.anwar@ndsu.edu

How to cite this paper: Saha, B. and Anwar, Z. (2024) A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. *Journal of Information Security*, **15**, 24-39.
https://doi.org/10.4236/jis.2024.151003

Received: November 14, 2023
Accepted: January 12, 2024
Published: January 15, 2024

Abstract

Technological shifts—coupled with infrastructure, techniques, and applications for big data—have created many new opportunities, business models, and industry expansion that benefit entrepreneurs. At the same time, however, entrepreneurs are often unprepared for cybersecurity needs—and the policymakers, industry, and nonprofit groups that support them also face technological and knowledge constraints in keeping up with their needs. To improve the ability of entrepreneurship research to understand, identify, and ultimately help address cybersecurity challenges, we conduct a literature review on the state of cybersecurity. The research highlights the necessity for additional investigation to aid small businesses in securing their confidential data and client information from cyber threats, thereby preventing the potential shutdown of the business.

Keywords

Entrepreneurship, Cybersecurity, Small and Medium Businesses, Data Breach, Hacking, Security

1. Introduction

Entrepreneurship is the process of establishing and managing a new business that generates jobs, spurs research and development, and takes on any associated risks with the aim of generating profit. Entrepreneurs, also known as small business owners, are known for their innovative ideas and their contribution to the economy. Their innovative mindset has often been found to be more pronounced compared to larger companies. Almost all net new job creation has come from new businesses [1], in addition to product innovation and social

welfare gains. A company is referred to be a small business if it employs at most 1500 people and generates less than 38.5 million dollars in annual revenue [2]. Small businesses play a crucial role in fostering community development, providing local employment, and serving local markets. The U.S. Small Business Administration reported in 2021 [3] that there are 32.5 million small firms operating in the United States, with a workforce of 61.2 million employees which is 99.9% of all companies in the country.

Startups are essential to the economy and contribute significantly to job creation. Additionally, they provide innovation to established industries by taking risks that established organizations may avoid. Despite the numerous benefits of small businesses, the reality is that not all startups succeed. According to U.S. Bureau of Labor Statistics data [4], approximately 20% of small firms in the United States fail in the first year of their business, and around half of all small firms cease to exist by the end of their fifth year. Surprisingly, the failure rate remains constant during the economic downturn from 2008 [5]. However, The COVID-19 pandemic has significantly impacted small businesses, with 41% of company closures documented on Yelp's business listing and review site [6] since March 2019.

Some common reasons for unsuccessful startups include lack of proper planning and management, corruption, insufficient funding, insufficient market research, and cyber-attacks. Cyber-attacks, in particular, pose a significant threat to businesses, as they can cause major harm and, in some cases, lead to the closure of the business. As attackers become more technologically advanced and discover new vulnerabilities, cyber-attacks are becoming more frequent, causing even greater harm to businesses [7] [8] [9]. Attackers often target smaller firms under the assumption that these businesses may not be adequately prepared to handle a network security breach [10].

Businesses that are attacked by cybercriminals can face operational disruption and altered business practices. The cost to the majority of these smaller businesses can quickly mount up. The United States has held the record for the greatest cost of a data breach for the past 12 years with a total cost of 9.44 million dollars [11], which is more than double the worldwide average. This is especially true if a threat successfully infiltrates a system and stays undetected; which is entirely achievable in the absence of network monitoring and automated threat detection tools. In addition to the monetary damages incurred by small businesses due to cyber-attacks, these enterprises may also have to bear legal expenditures, compliance penalties, reputation damage, and customer loss. These effects might quickly bring a business to its knees. According to National Cyber Security Alliance, Out of every five small businesses that fall victim to an attack, three of them end up shutting down their activities. When a small or medium-sized company is breached, more than half of them shut down within six months [12], and more than 60% of CEOs of small and midsize businesses report not having an active, up-to-date, or any, cybersecurity strategy [13].

Many people believe that large organizations are more vulnerable to cyber-attacks than small businesses due to the size of their operations, but this is not necessarily true. Based on the Verizon DBIR report [14], there was a relatively small gap between the number of data breaches experienced by large and small organizations in 2021. Specifically, there were 307 breaches reported by large companies and 263 by small companies, showing a roughly equal incidence of breaches between the two kinds of organizations. Additionally, large firms discover breaches faster than small organizations in more than half of the cases because they have strong and established security.

Entrepreneurs are often afraid of setting up businesses because of cybersecurity concerns and the cost associated with that. While larger businesses often have the resources necessary to handle cyber security, small businesses frequently do not. According to Paulsen [15], small firms are the most vulnerable when it comes to cyber security, and they frequently do not know what to protect.

In this paper, we have followed a systematic review process of existing work related to entrepreneurs' perceptions and decision-making about different types of cyber-attacks, management capability to recover from attacks, security measures to protect their assets from business, and management-related journals with high-impact factors. From the existing research, some key themes have been found:

- One of the main reasons businesses has data breaches is due to employees who are careless and engage in irresponsible activity within the firm.
- E-commerce is not preferred by small businesses because of their complex policy recommendations and security issues.
- Boundary control is important for managing workplace cyber safety.
- Small businesses are wary of using digital money to combat electronic crime and cyber security risks.

A critical area of concern for these businesses is cybersecurity. While foundational studies like those of Luo *et al.* [16], Kshetri [17], and Hudakova *et al.* [18] have provided a comprehensive understanding of cybersecurity risks and their management in larger enterprises, there remains a distinct gap in research specifically addressing the cybersecurity needs of SMBs. This gap is particularly concerning given the differing operational scales, resource availability, and risk profiles of SMBs compared to larger corporations.

From the above discussion, we can see that little research has been conducted on focusing small businesses' cybersecurity but clearly not enough. Alahmaei *et al.* [19] found that the majority of research on this area has been conducted on Uk and Australia. According to a report by the Small Business Administration [20]. It is estimated that small companies contribute 44% of the U.S. economy. Our research aims to fill this critical gap by conducting a systematic review of the existing literature, focusing on the perceptions and decision-making processes of entrepreneurs regarding cybersecurity, and the specific challenges and strategies relevant to SMBs. This approach is driven by the need to under-

stand why SMBs are targeted by cybercriminals and how they can effectively protect their data and assets. The review covers a range journals and conferences, shedding light on underexplored areas such as the economic impact of cyber-attacks on SMBs, the role of employee behavior in data breaches, and the adoption of digital technologies in the face of security challenges.

2. Types of Cyber-Attack a Small Business May Experience

Cyberattacks pose a major threat to businesses, particularly small firms are frequently targeted by hackers because they are hacking "sweet spot" [21]: they are big enough to contain important information, but they take less cyber-precautions than bigger companies, making them more susceptible. There are several types of cyberattacks that businesses may face, including technical, phycological and physical attacks; a taxonomy is shown in Figure 1.

2.1. SQL Injection Attacks

A SQL attack [22] injects malicious SQL codes into a database query, exploiting vulnerabilities in data-driven applications. This unauthorized database manipulation can result in significant data breaches, undermining both the confidentiality and integrity of sensitive business data. Such attacks pose a severe risk to small businesses, as they can lead to substantial information losses and compromise data security.

2.2. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

DoS and DDoS attacks are designed to overwhelm a network with excessive traffic, thereby disrupting normal business operations. Typically, these attacks utilize botnets, which are networks of compromised computers, to flood the target network with an overwhelming number of requests [23]. The impact on small businesses can be devastating, leading to significant operational downtime and a loss of customer trust due to disrupted services.

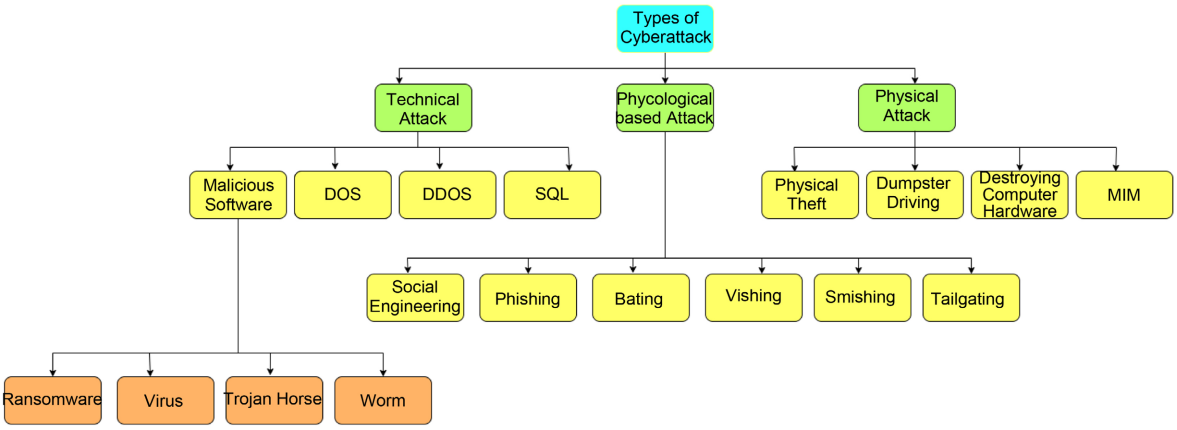

Figure 1. Different types of cyber-attack.

2.3. Malicious Software (Malware)

Malicious software like ransomware, Viruses, Worms, and Trojan horses, refers to various forms of malicious software aimed at damaging or exploiting computer systems [24]. In Ransomware, hackers lock a computer and ask for money in return for access. A survey by cybersecurity venture predicts that by 2021, a business would anticipate a ransom attack every 11 seconds [25]. Viruses and worms can steal, delete, or corrupt files and personal data, while Trojan horses, disguised as legitimate software, perform harmful activities upon installation. The presence of malware can lead to severe data and financial losses for small businesses, alongside reputational damage. Moreover, it can reduce the CPU processing speed of the infected computers and destroy hard drive space [26] [27].

2.4. Physiological Based Attack

Social engineering is psychological manipulation of users which can occur through tactics such as phishing, bating, vishing, smashing, and tailgating [28]. Phishing [29] is a type of attack that occurs through an email that appears to be from a trusted source, but it has the bad motive of stealing sensitive data like personal information, credit card information, etc. Baiting is a highly manipulative social engineering technique with a false promise of tempting offers. Victims fall into a trap by clicking on some phishing link or downloading some malicious software, which ends up compromising valuable data [30]. Another name for vishing is a voice phishing attack. It is a phone-based attack where a scammer request for personal and confidential information over the phone and pretends as a representative of the police, government, tax department, bank, or the victim's employer. Smishing or SMS phishing is similar to vishing but occurs through text messages that contain malicious links or request private information from the victim.

2.5. Physical and Other Security Attacks

Besides technical and psychological attacks, some other security attacks can happen. For example, someone can physically enter to the office or personal workspace to steal valuable information. Altering or destroying computer hardware is another type of cyber-attack that can lead companies to lose valuable data. For new companies/small companies, it is tough to start over from scratch again. Another unique way of attacking someone is dumpster driving while attackers look for confidential information in trash cans of offices or outside/external dumpsters.

Overall, small businesses are susceptible to a range of cyber-attacks, each characterized by distinct mechanisms and resulting impacts. SQL Injection attacks exploit database vulnerabilities, leading to significant data breaches that compromise sensitive information. DoS and DDoS attacks disrupt operations by overwhelming network resources, significantly hindering business functionality

and eroding customer trust. Malware, encompassing ransomware, viruses, worms, and Trojan horses, poses threats through data encryption, information theft, and system damage. Social engineering attacks exploit human vulnerabilities, manipulating individuals to divulge confidential information through deceptive tactics like phishing, baiting, vishing, and smishing. Physical and other security attacks, including unauthorized access and hardware tampering, represent direct threats to physical assets and critical data. Collectively, these attacks underline the need for robust cybersecurity measures in small businesses to safeguard against diverse and evolving digital threats.

3. Methodology

This study employs a systematic literature review, a methodological approach grounded in the theory of comprehensive and structured knowledge synthesis. According to Tranfield *et al.* [31], systematic reviews provide an exhaustive summary of literature relevant to a specific research question. This method is particularly apt for our study, which aims to analyze the breadth of research on cybersecurity in small and medium-sized businesses (SMBs) from 2010 to 2023.

Our focus on peer-reviewed journals, conference papers, doctoral dissertations, and Master's theses is based on the theoretical perspective that such sources represent the most rigorous and reliable forms of academic output, as suggested by Terjesen *et al.* [32]. The systematic review process, as outlined by [31], involves a comprehensive search across multiple databases, including Scopus, ProQuest, Science Direct, SpringerLink, and IEEE Xplore, using a predetermined set of keywords.These keywords, encompassing various aspects of entrepreneurship and cybersecurity, were chosen following the broad definition of entrepreneurship by Ireland *et al.* [33] and align with Keupp *et al.*'s [34] emphasis on the importance of SMB data in entrepreneurship research. The inclusion of keywords like "entrepreneurial," "cybersecurity," "hack," and "breach" reflects the theoretical understanding that entrepreneurship in the context of cybersecurity spans a wide range of subtopics and issues, particularly for SMBs.

The decision to employ a systematic literature review is further substantiated by the need for an exhaustive and unbiased assessment of the current state of cybersecurity in SMBs. This approach aligns with the theoretical frameworks of knowledge gaps and research synthesis, aiming not only to summarize existing knowledge but also to identify under-researched areas, as per [34]. Through this comprehensive review, we provide valuable insights into the field, highlighting areas that require further investigation and contributing to a more complete understanding of the challenges facing SMEs in cybersecurity.

4. Cybersecurity Challenges and Impacts in Small to Medium-Sized Businesses

This section explores the multifaceted cybersecurity challenges facing small and medium-sized businesses (SMBs) and the significant impacts of cyber attacks on

these entities, drawing insights from existing research and recent data.

4.1. Current State of Cybersecurity in SMBs

In the evolving landscape of cybersecurity, several key studies have highlighted the varied challenges and risks that businesses face. Luo *et al.* [16] propose a risk assessment framework focusing on digital interdependence and regulatory complexities. Complementing this, Kshetri [17] analyzes global cybercrime patterns, while Hudakova *et al.* [18] identify cyber incidents as a primary business risk. August *et al.* [35], Say *et al.* [36], along with D'Arcy *et al.* [37], investigate the economic impacts and organizational factors influencing the occurrence of data breaches. These studies collectively underscore the critical need for robust cybersecurity strategies across all business scales, especially in SMBs. Cyber-criminals are aware that few small organizations prioritize cybersecurity or have complete strategies to stop or respond to any attack. The statistics [38] below explains how vulnerable and easy targets small businesses are to attack in today's world.

1) In 2021, 61% of small and medium-sized businesses (SMBs) fell victim to a cyber-attack.

2) The Verizon 2021 Data Breach Investigations Report [39] states that over the past few years, the number of small businesses affected by cyber-attacks has been rising rapidly over the past few years.

3) In 2021, 82% of ransomware attacks targeted businesses were SMBs with 1000 or fewer employees.

4) The majority of malicious emails, including spam, phishing, and email malware, are targeted at companies with fewer than 250 employees.

5) Small businesses with fewer than 100 employees are at an increased risk of cyber-attacks, receiving 350% more threats than larger companies.

6) Shockingly, 27% of small firms with no cybersecurity measures in place have reported the collection of their customers' credit card information by cyber-criminals [40].

These statistics paint a concerning picture for small businesses, highlighting the critical need for these organizations to prioritize cybersecurity and implement effective measures to protect themselves and their customers from cyber-attacks. The alarming trend of small businesses being targeted by cyber-criminals underscores the importance of developing and implementing a comprehensive cybersecurity strategy that protects the assets, reputation, and success of these organizations.

4.2. Financial Impact of Cyber-Attacks

A successful cyber attack can have a significant financial impact on small to mid-sized businesses (SMBs). SMBs are the principal target of cybercrimes [41]. They are particularly vulnerable to the financial impact of cyber incidents, as they may lack the resources to recover from an attack fully. The financial costs of

these attacks associated with a data breach are more than $2.2 million per year and it will grow 15% over the next five years [42]. According to a survey [43], 60% of small businesses that experience a cyber attack shut down their business within six months. In 2020, over 700,000 attacks against small businesses resulted in damages totaling $2.8 billion [38]. Furthermore, the 2021 IBM report found that the average total cost of data breaches rose to $4.24 million [44], marking the highest average total cost in 17 years. According to Cybersecurity Ventures, economic wealth has never been transferred more quickly than it has through cybercrime: It is projected to grow from $3 trillion in 2015 to $10.5 trillion globally by 2025 which is shown in **Figure 2** [45]. In addition to these direct costs, small businesses may also suffer lost revenue and reputational damage as a result of a cyber attack, which can be difficult to recover from. These data points highlight the critical importance of investing in cybersecurity measures and developing a comprehensive response plan to help mitigate the risk of financial loss from cyber incidents.

4.3. Industry-Specific Implications of Cyber-Attacks

According to the Statista 2022 report [46], the business and healthcare sectors are the most vulnerable to cyberattacks, with a notable shift from medical to business record breaches between 2013 and 2022 in the USA, as shown in **Figure 3**. In 2016 alone, the business sector saw around 500 breaches, nearly doubling the following year, and by 2022, it became 1500 only in business sector. Additionally, over 700,000 small businesses were victims of cyberattacks in 2020, with losses reaching 2.8 billion dollar. The surge in cybercrime, against SMBs, calls for urgent adoption of advanced cybersecurity measures [38]. Over 700,000 SMBs were victims of cyberattacks in 2020, with substantial financial losses [46]. The prevalent types of attacks include malware, phishing, and data breaches [38], further emphasizing the need for proactive cybersecurity strategies.

Figure 2. Growth of cybercrime cost by year of 2025.

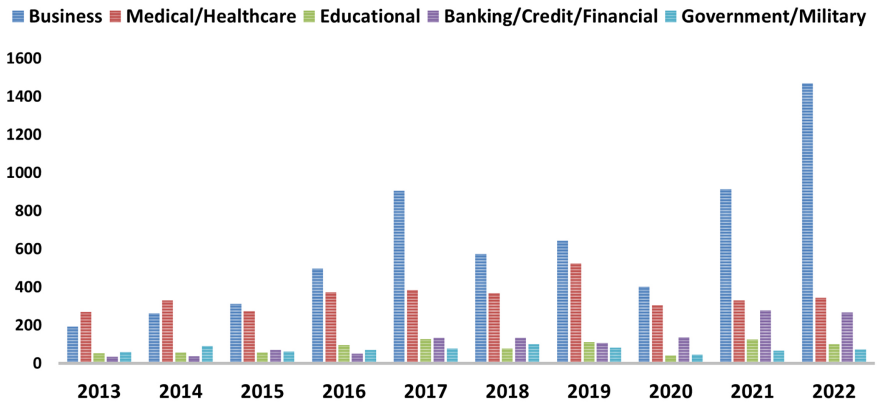

Figure 3. Data breaches in USA from 2013-2022 by industry.

4.4. Cyber Attacks Impacts on SMBs

A 2022 survey [38] **Figure 4** indicates that malware (18%), phishing (17%), and data breaches (16%) are the most common attacks on small enterprises. This uptick in cybercrime highlights the urgent need for these organizations, particularly small businesses, to adopt advanced cybersecurity measures and best practices to safeguard against these increasing threats. The financial and reputational damages from cyber incidents can be severe, sometimes leading to business closure [47]. IBM and the Ponemon Institute [44] report that data breaches in small companies incur substantial costs, exacerbating the vulnerability of these businesses to cyber threats [48].

4.5. Breach Discovery and Management Strategy

Cyber attacks have become a major threat to organizations, with certain sectors being more vulnerable than others shown in **Figure 5** [49]. A report by Check Point Software [49] found that schools and universities, were the most vulnerable targets, with over 1600 attacks per week, resulting in personal information theft and class suspensions. The second most vulnerable target was government and military organizations, suffering 1136 attacks per week. Communications companies and ISPs were the third and fourth most impacted with over 1000 attacks per week each. In terms of weekly cyberattacks, healthcare is ranked fifth but this is number one when it comes to ransomware [50] as they generate very sensitive information. The lack of security infrastructure in these sectors might be the reason for such a high frequency of attacks. Other sectors, on the other hand, suffered fewer than 1000 attacks per week. Cybersecurity measures are essential to ensure the protection of these industries and the sensitive information they handle. Breach discovery is very crucial for businesses. The moment a company or business becomes conscious of a breach is referred to as breach discovery. IBM [11] states that it typically takes companies 197 days to detect the breach, and up to 69 days to bring it under control. The more day it takes to detect a breach, the more expensive it becomes. For entrepreneurs, this expense becomes a burden and they feel no other option but closure of the business. If a

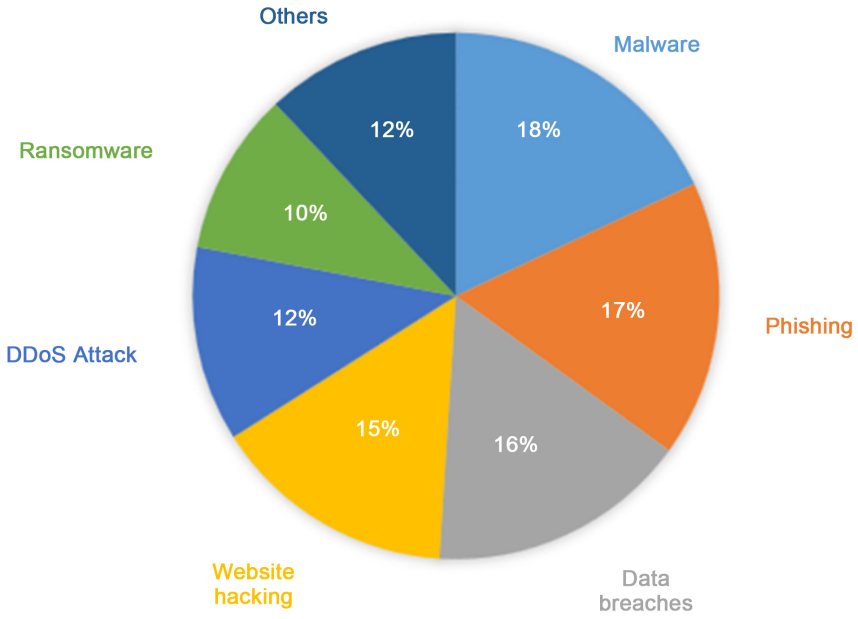

Figure 4. Different types of cyberattacks small businesses have experienced in 2022.

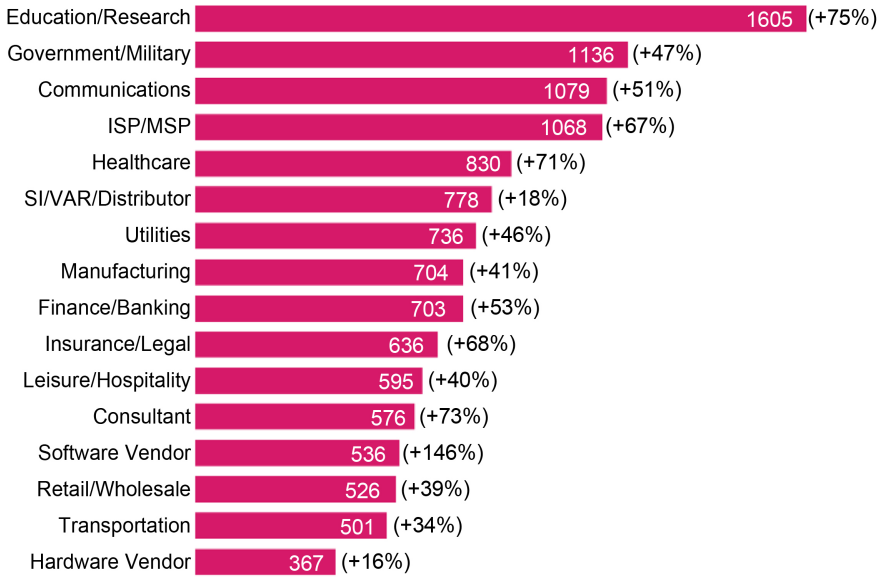

Figure 5. Industry-specific average weekly cyber attack in 2021, compared to 2020.

company manages to resolve a breach within thirty days, it can save more than $1 million compared to companies that take longer to handle the situation. Delayed responses to a data breach can lead to significant consequences, such as loss of customer confidence, decreased productivity, or hefty fines [45].

To avoid such problems, establishing a data breach response strategy is a proactive approach to preparing for such incidents. By implementing a risk management strategy to address potential breaches, owners can minimize the impact on the company and financial performance. For instance, an incident response plan can guide the team through the various stages of detection, con-

tainment, investigation, remediation, and recovery.

5. Discussion

Small business ventures, entrepreneurship, digital firms, and self-employment are vital for community building, innovation of new products, job creation, and ultimately the economy. Furthermore, research shows [51] that self-employment can have a positive impact on one's overall well-being. More than half of all firms [52] throughout the world is unprepared to deal with cyber-attacks. Cyber-attacks can harm a business venture's reputation and diminish customers trust, resulting in loss of sale and customers and it can have a negative impact on the economy as a whole.

Our literature review and subsequent analysis indicate that the high-impact journals in the areas of business, management, entrepreneurship, and organization science study a multitude of factors behind the poor organizational performance, growth, reputation amongst customers, and trustworthiness of small businesses.

Research works have considered digital interdependence, regulatory complexity, corruption, C-level turnover rate, corporate social performance, market assessment, day-to-day operations, leadership, climate change, office environment, and security readiness. These works assert that proper strategic planning and risk analysis is important for organizational performance and has a role in giving a positive and trustworthy image to customers.

Though the literature addresses security, privacy trust factors there is limited research on cybersecurity, which is rapidly becoming a critical factor for the survival of small businesses now and in the future. Some computer science and engineering domains are studying this area but cyber attacks are a result of both technical and human error. Experts in social and human behavior, psychological sciences, humanities will be needed side-by-side with Computer Scientists in understanding how organizations may better protect themselves.

Cybersecurity poses many questions that have been unaddressed so far in the literature. This includes but is not limited to understanding the following factors regarding SMBs: cybersecurity readiness, the role of cyber-insurance, the influence of in-person vs. virtual offices, and understanding of how click paralysis is a barrier to an employee's optimum work capacity. Business perceptions need to be determined namely where cyber-security ranks as a hindrance as compared to other obstacles such as corruption, regulatory complexity, etc. Another important aspect for investigation is how SMBs measure up with regard to their use of security policies and safeguards as compared to bigger incumbent enterprises because of radically different financial, labor, and survival contexts.

Click paralysis refers to the phenomenon where a person is unable to make a decision due to an overwhelming amount of choices or information which can lead to decreased productivity, increased stress levels, missed deadlines, and decreased job satisfaction. This can have a significant impact on small businesses in

the digital age, where a multitude of websites, products, and services to choose from. Additionally, small business owners may experience click paralysis when it comes to implementing cybersecurity best practices, such as regularly backing up data, keeping software up-to-date, and creating strong passwords. The many options and technical details involved can make it difficult to know where to start and what steps to take, causing the business owner to become paralyzed and take no action. Given the increasing reliance on technology and the growing threat of cyberattacks, it is imperative that small businesses take proactive steps to address click paralysis and ensure the protection of their networks and data.

In the computer science domain, there has been a number of research works advancing the technical aspects of cyber security defense using state-of-the-art tools such as machine learning, artificial intelligence, etc but clearly it is not adequate when considering the volume of successful cyber attacks that occur every day. A number of different aspects of security have been explored in business management and organizational publications, but the emphasis on cybersecurity, cyberattacks, and data breaches in particular has been low. It is important to bring the expertise of both computer scientists as well as social scientists to dig further into cyber-security to understand why it has become such a critical component in business failures, to define the nature of cyber-security risks, and to answer fundamental questions concerning SMB management competencies in connection to these dangers.

6. Conclusion and Future Work

Small and mid-sized businesses are especially vulnerable to cyber-attacks as they are often perceived by attackers as easy targets. These businesses may lack the resources, knowledge, and preparedness to defend themselves against cyber threats, making them an attractive target for attackers. The aftermath of a successful cyber-attack can be devastating for entrepreneurs, leading to significant financial losses and damage to reputation, both of which are critical resources for businesses. To address these challenges and support the success of entrepreneurs, it is essential to understand the nature of the threats they face and their level of preparedness and management capabilities. It is therefore imperative to increase awareness of the importance of cybersecurity for small businesses and equip them with the necessary resources and assistance.

To this end, we are planning to conduct a comprehensive survey targeting small to mid-sized businesses. Our aim is to evaluate the current state of cybersecurity for these businesses, identify the threats they face, and assess their preparedness and ability to recover from an attack. The results of this survey will provide valuable insights into the needs of entrepreneurs with regard to cybersecurity and will be used to inform policy guidance on cybersecurity that will benefit entrepreneurs in the long run.

By understanding the challenges faced by entrepreneurs and addressing them through a comprehensive policy framework, we hope to empower entrepreneurs

to build more secure and successful businesses. Through this survey, we aim to support the development of a cybersecurity landscape that benefits businesses and promotes entrepreneurship in the digital age. By better understanding the impact of cybersecurity on small businesses and how they can protect themselves, we can foster a more secure and prosperous future for our communities and the economy as a whole.

Data Availability

No Data were used or analyzed in this study. Therefore, Data sharing is not applicable for this study. However, other materials can be obtained from authors by request.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Conflicts of Interest

The authors of this paper declare that they have no conflict of interest.

References

[1] Haltiwanger, J., Jarmin, R.S., Miranda, J. (2013) Who Creates Jobs? Small versus Large versus Young. *Review of Economics and Statistics*, **95**, 347-361. https://doi.org/10.1162/REST_a_00288

[2] Cameron, A. (2021) Think Small—Small Business, That Is. What Is Considered a Small Business? https://smallbusiness.patriotsoftware.com/what-is-considered-small-business-classification-size/

[3] U.S. Small Business Administration (2021) 2021 Small Business Profile. https://advocacy.sba.gov/wp-content/uploads/2021/08/2021-Small-Business-Profiles-For-The-States.pdf

[4] U.S. Bureau of Labor Statistics (2022). https://www.bls.gov/

[5] KATHERINE GUSTAFSON (2020) What Percentage of Businesses Fail and How to Improve Your Chances of Success. https://www.lendingtree.com/business/small/failure-rate/#:%E2%88%BC:text=According%20to%20data%20from%20the,%2C%20roughly%2050%25%20have%20faltered

[6] (2020) Yelp, Business Listing Review. https://business.yelp.com/

[7] Tariq, N. (2018) Impact of Cyberattacks on Financial Institutions. *Journal of Internet Banking and Commerce*, **23**, 1-11.

[8] McShane, M. and Nguyen, T. (2020) Time-Varying Effects of Cyberattacks on Firm Value. *The Geneva Papers on Risk and Insurance-Issues and Practice*, **45**, 580-615. https://doi.org/10.1057/s41288-020-00170-x

[9] Green, J. (2015) Staying Ahead of Cyber-Attacks. *Network Security*, **2015**, 13-16. https://doi.org/10.1016/S1353-4858(15)30007-6

[10] Wolf, F., Aviv, A.J. and Kuber, R. (2021) Security Obstacles and Motivations for

Small Businesses from a CISO's Perspective. 30*th USENIX Security Symposium* (*USENIX Security* 21), 11-13 August 2021, 1199-1216.

[11] (2022) Cost of a Data Breach 2022. https://www.ibm.com/reports/data-breach?utmcontent=SRCWW&p1=Search&p4=43700072379268628&p5=p&gclid=CjwKCAiAh9qdBhAOEiwAvxIokwvOeUHHL6ooYQv8MPXRv8Z0x3sJEy4gc7lXmJmknB8itcQ2NX1bhoCuqoQAvDBwE&gclsrc=aw.ds

[12] National Cyber Security Alliance (2021). https://staysafeonline.org/

[13] CISCO, National Center for the Middle Market (2018) Cyberthreats and Solutions for Small and Midsize Businesses. https://www.vistage.com/wp-content/uploads/2018/04/Cybersecurity-Research-Note.pdf

[14] (2021) 2021 Verizon Data Breach Investigations Report. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

[15] Paulsen, C. (2016) Cybersecuring Small Businesses. *Computer*, **49**, 92-97. https://doi.org/10.1109/MC.2016.223

[16] Luo, Y. (2022) A General Framework of Digitization Risks in International Business. *Journal of International Business Studies*, **53**, 344-361. https://doi.org/10.1057/s41267-021-00448-9

[17] Kshetri, N. (2005) Pattern of Global Cyber War and Crime: A Conceptual Framework. *Journal of International Management*, **11**, 541-562. https://doi.org/10.1016/j.intman.2005.09.009

[18] Hudakova, M., Gabrysova, M., Petrakova, Z., Buganova, K. and Krajcik, V. (2021) The Perception of Market and Economic Risks by Owners and Managers of Enterprises in the V4 Countries. *Journal of Competitiveness*, **13**, 60-77. https://doi.org/10.7441/joc.2021.04.04

[19] Alahmari, A. and Duncan, B. (2020) Cybersecurity Risk Management in Small and Mediumsized Enterprises: A Systematic Review of Recent Evidence. 2020 *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (*CyberSA*), Dublin, 15-19 June 2020, 1-5. https://doi.org/10.1109/CyberSA49311.2020.9139638

[20] The Small Business Administration (2021). https://www.cnbc.com/2017/01/17/small-business-owners-pay-over-83000-dollars-in-regulatory-costs-in-first-year.html

[21] (2022) Types of Cyberattacks That Threaten Businesses, Part I: Malware and Ransomware. https://online.eou.edu/resources/article/types-of-cyberattacks-that-threaten-businesses-part-i/

[22] Lawal, M., Sultan, A.B.M. and Shakiru, A.O. (2016) Systematic Literature Review on SQL Injection Attack. *International Journal of Soft Computing*, **11**, 26-35.

[23] Prasad, K.M., Reddy, A.R.M. and Rao, K.V. (2014) DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms—A Survey. *Global Journal of Computer Science and Technology,* **14**, 15-32.

[24] Yuryna Connolly, L., Wall, D.S., Lang, M. and Oddson, B. (2020) An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability. *Journal of Cybersecurity*, **6**, tyaa023. https://doi.org/10.1093/cybsec/tyaa023

[25] Morgan, S. (2020) Global Ransomware Damage Costs Predicted To Exceed $5 Billion in 2017. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

[26] Hughes, L.A. and DeLone, G.J. (2007) Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both? *Social Science Computer Review*, **25**, 78-98. https://doi.org/10.1177/0894439306292346

[27] Kaur, J. (2019) Taxonomy of Malware: Virus, Worms and Trojan. *International Journal of Research and Analytical Reviews*, **6**, 192-196.

[28] Raineri, E.M. and Resig, J. (2020) Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. *Journal of Applied Business & Economics*, **22**, 13-23. https://doi.org/10.33423/jabe.v22i12.3876

[29] Khonji, M., Iraqi, Y. and Jones, A. (2013) Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, **15**, 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

[30] Iuga, C., Nurse, J.R. and Erola, A. (2016) Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks. *Human-Centric Computing and Information Sciences*, **6**, Article No. 8. https://doi.org/10.1186/s13673-016-0065-2

[31] Tranfield, D., Denyer, D. and Smart, P. (2003) Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, **14**, 207-222. https://doi.org/10.1111/1467-8551.00375

[32] Terjesen, S., Hessels, J. and Li, D. (2016) Comparative International Entrepreneurship: A Review and Research Agenda. *Journal of management*, **42**, 299-344. https://doi.org/10.1177/0149206313486259

[33] Ireland, R.D., Reutzel, C.R. and Webb, J.W. (2005) Entrepreneurship Research in AMJ: What Has Been Published, and What Might the Future Hold? Academy of Management Briarcliff Manor, NY. https://doi.org/10.5465/amj.2005.17843937

[34] Keupp, M.M. and Gassmann, O. (2009) The Past and the Future of International Entrepreneurship: A Review and Suggestions for Developing the Field. *Journal of Management*, **35**, 600-633. https://doi.org/10.1177/0149206308330558

[35] August, T., Dao, D. and Niculescu, M.F. (2022) Economics of Ransomware: Risk Interdependence and Large-Scale Attacks. *Management Science*, **68**, 8979-9002. https://doi.org/10.1287/mnsc.2022.4300

[36] Say, G. and Vasudeva, G. (2020) Learning from Digital Failures? The Effectiveness of Firms' Divestiture and Management Turnover Responses to Data Breaches. *Strategy Science*, **5**, 117-142. https://doi.org/10.1287/stsc.2020.0106

[37] D'Arcy, J., Adjerid, I., Angst, C.M. and Glavas, A. (2020) Too Good to Be True: Firm Social Performance and the Risk of Data Breach. *Information Systems Research*, **31**, 1200-1223. https://doi.org/10.1287/isre.2020.0939

[38] (2022) 35 Alarming Small Business Cybersecurity Statistics for 2023. https://www.strongdm.com/blog/small-business-cyber-security-statistics#small-business-cybersecurity-overview

[39] (2021) Diving Back into SMB Breaches. https://www.verizon.com/business/resources/reports/dbir/2021/smb-data-breaches-deep-dive/

[40] (2021) 51% of Small Business Admit to Leaving Customer Data Unsecure. https://digital.com/51-of-small-business-admit-to-leaving-customer-data-unsecure/

[41] Aguilar, L. (2015) The Need for Greater Focus on the Cybersecurity Challenges

Facing Small and Midsize Businesses.
https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses

[42] Morgan, S. (2020) Cybercrime to Cost the World $10.5 Trillion Annually by 2025. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[43] Shepherd, M. (2023) 30 Surprising Small Business Cyber Security Statistics. https://www.fundera.com/resources/small-business-cyber-security-statistics

[44] (2021) Cost of a Data Breach Report 2021. https://www.dataendure.com/wp-content/uploads/2021_Cost_of_a_Data_Breach_-2.pdf

[45] Mclean, M. (2023) 2023 Must-Know Cyber Attack Statistics and Trends. https://www.embroker.com/blog/cyber-attack-statistics/

[46] (2022) Number of Data Breaches in the United States from 2013 to 2019, by Industry. https://www.statista.com/statistics/273572/number-of-data-breaches-in-the-united-states-by-business/

[47] Pfleeger, S.L. (2009) Useful Cybersecurity Metrics. *IT Professional Magazine*, **11**, 38-45. https://doi.org/10.1109/MITP.2009.63

[48] Osborn, E. (2015) Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMES. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e/download_file?file_format=application%2Fpdf&safe_filename=01-15.pdf&type_of_work=Working+paper

[49] (2023) Check Point Press Releases. https://tinyurl.com/ye8d95ee https://www.checkpoint.com/press-releases/check-point-software-releases-its-2023-security-report-highlighting-rise-in-cyberattacks-and-disruptive-malware/

[50] James, N. (2023) 160 Cybersecurity Statistics 2023—The Ultimate List of Stats and Trends. https://www.getastra.com/blog/security-audit/cyber-security-statistics/

[51] McAdam, M., Crowley, C. and Harrison, R.T (2022). Digital Girl: Cyberfeminism and the Emancipatory Potential of Digital Entrepreneurship in Emerging Economies. *Small Business Economics*, **55**, 349-362. https://doi.org/10.1007/s11187-019-00301-2

[52] Goud, N. (2022) More than Half of Businesses Are Not Prepared for Cyber Attacks. https://www.cybersecurity-insiders.com/more-than-half-of-businesses-are-not-prepared-for-cyber-attacks/