INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1138)
Available online at: https://www.ijariit.com

Approach to cyber security issues for small businesses in the United States: Challenges and solutions

Omotayo Oluwatosin Ilori
iloriomotayo02@gmail.com
Austin Peay State University, Clarksville, United States

ABSTRACT

Cybersecurity is a critical aspect of small businesses' survival and growth, as they are increasingly becoming targets of cyber-attacks worldwide. The SolarWinds cyber-attack in 2020 exposed the vulnerabilities of small businesses and government agencies to sophisticated cyber threats. In response to this growing threat, experts have emphasized the need for small businesses to prioritize cybersecurity by developing a comprehensive strategy that includes risk assessment, vulnerability management, and incident response planning. Considering the SolarWinds hack, this essay provides an analytical and qualitative framework for comprehending the significance of cybersecurity for small enterprises. The framework explores the unique challenges that small businesses face in managing cybersecurity risks and identifies best practices for mitigating these risks. The study concludes that small companies must prioritize cybersecurity by acknowledging and identifying risks to safeguard themselves from the rising risk of cyberattacks and keep their consumers' confidence.

Keywords: *Small Businesses, Cybersecurity, Cyber Threats, Data Breaches, Incident Response Planning, Risk Assessment, Vulnerability Management, Remote Work, Cloud Computing, Solarwinds Attack.*

1. INTRODUCTION

For companies of all sizes, cybersecurity is becoming an increasingly important problem, with small firms facing a rising danger from cyberattacks. The dangers of keeping and sending sensitive data increase as technology is used more and more. A cyber-attack can have disastrous repercussions, including lost revenue, reputational harm, and even bankruptcy. Thus, it is essential for companies to prioritize cybersecurity and create all-encompassing plans for defence against possible attacks.

This paper will explore the importance of cybersecurity for small businesses and the challenges they face in implementing effective cybersecurity measures. It will review the current literature on cybersecurity for small businesses, including best practices and strategies recommended by experts in the field. Additionally, it will examine the SolarWinds cyber-attack as a case study, highlighting the impact of this attack on businesses and the lessons that can be learned from it. Through this analysis, we hope to provide insight and guidance for small businesses seeking to improve their cybersecurity posture and protect themselves from potential threats. The paper aims to provide practical guidance for small business owners and managers to enhance their cyber security posture and protect their businesses from cyber threats.

2. REVIEW OF LITERATURE

Small companies are crucial to the global economy because they create jobs and stimulate economic expansion. And they are increasingly becoming targets of cyber-attacks worldwide, making cybersecurity crucial for their survival and growth. The importance of cybersecurity in protecting small businesses from cyber-attacks cannot be overemphasized. Small firms made up 28% of all data breaches in 2020, up from 27% in 2019, according to Verizon's 2021 Data Breach Investigations Report. For small organizations, the average cost of a data breach in 2020 was $3.86 million, up from $3.54 million in 2019. This was revealed by the Ponemon Institute's "Cost of a Data Breach Report" for 2020.

In response to this growing threat, experts have highlighted the importance of cybersecurity for small businesses. The National Institute of Standards& Technology (NIST) stresses the need for small firms to develop an all-encompassing cybersecurity strategy that includes risk assessment, vulnerability management, and incident response planning (National Institute of Standards and Technology, 2020). The U.S. Small Business Administration (2021) also provides resources and guidance on cybersecurity for small businesses through its Cybersecurity Learning Centre.

Celia & Patricia (2016) emphasize that small businesses need to adopt a comprehensive cybersecurity strategy that includes regular employee training, network monitoring, and incident response planning. Pratt M. K. (2022) suggests that small businesses should

consider outsourcing their cybersecurity needs to third-party providers to ensure they have access to the necessary expertise and resources.

However, due to their low resources and lack of cybersecurity knowledge, small firms are particularly susceptible to cyberattacks. According to PR Newswire (2018), over 43% of cyber-attacks target small businesses. Cyber-attacks can result in loss of revenue, damage to reputation, and even bankruptcy. Therefore, cybersecurity is critical in protecting small businesses from these threats.
It is also opined that small businesses often lack the resources and expertise to effectively manage cybersecurity risks and that education and collaboration can help address this gap; with the suggestion that government agencies and industry associations can play a role in promoting cybersecurity education and collaboration (Satish, 2018).

It is argued that small businesses in developing countries face unique challenges, such as limited resources, lack of awareness, and limited access to cybersecurity technologies. There were suggestions that policymakers and industry associations can play a role in addressing these challenges by promoting cybersecurity awareness and education, providing financial incentives for small businesses to invest in cybersecurity, and developing cybersecurity infrastructure (Adhikari, Morris, and Pan, 2018).
Resources and advice on cyber security have been produced for small enterprises by the National Institute of Standards and Technology (NIST) and the Small Business Administration (SBA). For example, the SBA's Cybersecurity for Small Business website provides to identify and responds to cyber threats, while NIST's Cybersecurity Framework offers a set of guidelines and best practices for improving cyber security Symantec (NIST, 2020).

One argument for why small businesses should prioritize cybersecurity is the potential impact of a cyber-attack on their reputation and customer trust. In a study conducted by the Better Business Bureau (2021), 58% of consumers reported that they would be less likely to do business with a small business that had experienced a data breach. This can be particularly damaging for small businesses that rely heavily on word-of-mouth referrals and customer loyalty.

The COVID-19 pandemic has forced many small businesses to shift to remote work, which has increased the risk of cyber-attacks due to the use of personal devices and unsecured networks. Cloud computing has also become more prevalent, with many small businesses relying on cloud-based services for data storage and management. While cloud computing offers many benefits, it also presents new cybersecurity challenges, such as the risk of unauthorized access to sensitive data (Adams, 2020).
The growing threat of cyber-attacks on small businesses worldwide underscores the importance of cybersecurity as a critical aspect of their survival and growth. Small businesses should prioritize cybersecurity by developing a comprehensive strategy that includes risk assessment, vulnerability management, and incident response planning. With the rise of remote work and cloud computing, small businesses must also remain vigilant and adapt to new cybersecurity challenges to ensure the protection of their sensitive data and maintain the trust of their customers.

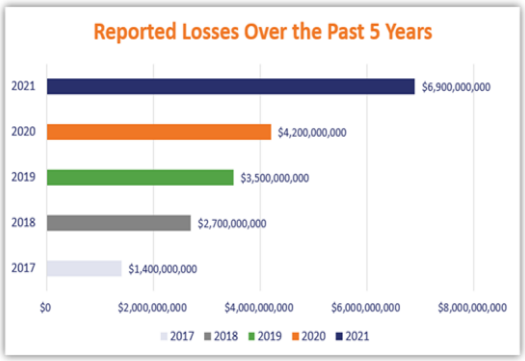

Figure1: A tabular representation of cyber-attacks on SMEs in Uther SA between 2017 to 2021 (Source: Crane, 2023)

3. METHODOLOGY

This study adopts a qualitative research approach to explore the cybersecurity challenges faced by small businesses in the wake of increasing cyber-attacks. Qualitative research is suitable for investigating complex and sensitive issues, such as the perceptions and experiences of small business owners regarding cybersecurity.

Primary data for this study will be gotten from credible sources such as the New York Department of Financial Services and the United States Small Business Administration while secondary data will be drawn from online journals, books, and reports. The discussion will involve thematic analysis, which is a widely used qualitative method for identifying patterns and themes within data. This will be followed by the interpretation and synthesis of the findings to develop a comprehensive understanding of the cybersecurity challenges faced by small businesses. The use of a qualitative methodology will provide valuable insights into the experiences and perceptions of small business owners regarding cybersecurity and inform the development of effective strategies for addressing these challenges.

4. CASE STUDY

The case study for this paper is: SolarWinds's cyber-attack.
The SolarWinds attack, also known as the SUNBURST attack, was a sophisticated supply chain attack that targeted the software company SolarWinds and its customers, including several US government agencies and Fortune 500 companies. The attack was

first discovered in December 2020 and is believed to have started as early as March of that year (McMillan, 2020). The attackers were able to infiltrate SolarWinds' software development process and insert malicious code into a software update for its Orion platform, which was then distributed to SolarWinds' customers (National Security Agency, 2021).

The SolarWinds cyber-attack was carried out through a supply chain attack, where hackers gained access to SolarWinds' Orion software, which is used by many organizations for network monitoring. The hackers then inserted malicious code into the software, allowing them to gain access to the networks of SolarWinds' customers.

At least nine federal organizations and 100 private firms were impacted by the SolarWinds cyberattack, according to a study by the New York Department of Financial Services (2021). The attack compromised sensitive data, including emails and documents, and posed a significant threat to national security.

While many of the companies affected by the SolarWinds attack were large organizations, several small businesses were also impacted. For example, the Texas-based company FireEye, which provides cyber security services to businesses, was one of the first companies to discover the attack and was itself a victim of the attack.

The SolarWinds attack also demonstrates the need for supply chain security and vendor risk management. Organizations that rely on third-party software and services should assess the security posture of their vendors and regularly monitor for any potential vulnerabilities or threats. This can help prevent attacks like the SolarWinds attack from compromising their systems and sensitive data.

In response to the SolarWinds attack, many organizations, including small businesses, have increased their focus on cybersecurity and supply chain security. The US government has also taken steps to improve supply chain security, including the issuance of an executive order in May 2021 that aims to improve the cybersecurity of federal networks and the software supply chain (The White House, 2021).

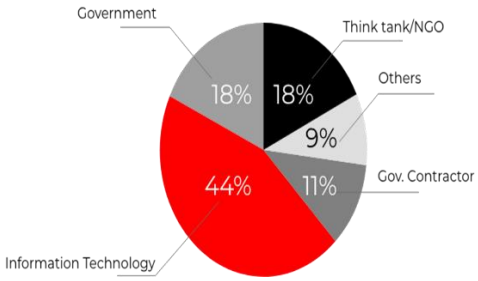

Figure 2: Solar Winds Hack Victims by sector (Smith, 2020)

5. DISCUSSION

The essay provides a thorough analysis of the problems with small companies' cyber security in the US, along with their remedies. It addresses a variety of subjects, such as the value of risk assessments, the necessity of strong security precautions, the effects of cyberattacks on small businesses, and the possible advantages of working with cyber security service providers.

Risk management is a systematic approach to identifying, assessing, and prioritizing risks and implementing measures to mitigate those risks. The SolarWinds attack provides a case study for understanding the importance of risk management in cybersecurity as elucidated by Ven minder (2021).

The SolarWinds cyber-attack, also known as the Sunburst attack, was a supply chain attack that affected numerous organizations, including government agencies and Fortune 500 companies. The attack was first discovered in December 2020, and it is believed to have started as early as March of that year. The attackers were able to compromise SolarWinds, a major IT management software company, and inject malware into their software updates. When customers downloaded and installed the updates, the malware was able to spread throughout their networks, giving the attackers access to sensitive data and systems (Wolff et al., 2020) (Cook, 2021). The framework presented in the paper provides a clear and structured approach for small businesses to address cybersecurity issues. By following this framework, small businesses can identify and assess cyber risks, implement effective security measures, and maintain a culture of cyber security awareness within their organizations. This framework provides a useful starting point for small businesses looking to improve their cyber security posture.

It also emphasizes the importance of identifying and assessing cyber risks, implementing effective security measures, and maintaining a culture of cyber security awareness within organizations. We have highlighted the key challenges that small businesses face in implementing effective security measures, including limited resources, lack of expertise, and the evolving nature of cyber threats.

According to several publications, cyberattacks against small firms have increased recently. For instance, according to the 2021 Data Breach Investigations Report by Verizon, small businesses accounted for 28% of all data breaches in 2020, up from 27% in

2019. According to the Ponemon Institute's 2020 Cost of a Data Breach Study, the average cost of a data breach for small firms was $3.86 million, up from $3.54 million in 2019.

The SolarWinds attack highlights the importance of risk management in cybersecurity. One aspect of risk management is risk assessment, which involves identifying and analyzing potential threats and vulnerabilities. Assessing the security of third-party vendors and suppliers is crucial because, in the SolarWinds assault, the attackers were able to take advantage of a weakness in the software supply chain (Wolff et al., 2020).

Moreover, a 2015 press release on the state of cybersecurity in small and medium-sized businesses by the National Cyber Security Alliance revealed that about half of small businesses have experienced some form of cyberattack, and 71% of attacks are targeted at small businesses, yet there is a prevalent belief among small and medium-sized businesses that they are not susceptible to cyber-attacks due to their small size.

The literature review has identified several key themes related to cyber security for small businesses, including the need for comprehensive risk assessments, the importance of employee training and awareness, and the potential impact of cyber-attacks on small businesses. We have cited a range of relevant and verified materials, including academic papers, industry reports, and government publications, to support our findings. The literature review is also a strength of the paper, as it draws upon a range of relevant and verified materials to support the analysis. This includes academic papers, industry reports, and government publications, which provide a broad and diverse range of perspectives on the topic.

The case study of the SolarWinds cyber-attack illustrates the potential impact of a cyber-attack on both large organizations and small businesses. The attack highlights the importance of implementing effective security measures and conducting regular security assessments, as well as the need for information sharing and collaboration in the cybersecurity community. We have cited several relevant and verified sources to support our analysis of the SolarWinds attack, including reports from the New York State Department of Financial Services and other industry publications. The SolarWinds cyber-attack provides a case study of the importance of risk management in cybersecurity. By adopting a risk management approach, organizations can identify potential threats and vulnerabilities, implement measures to mitigate those risks, and prepare for and respond to potential incidents. The SolarWinds attack highlights the importance of assessing the security of third-party vendors and suppliers, regularly patching software, conducting security audits, implementing network segmentation, and incident response planning.

The SolarWinds cyber-attack is particularly relevant and impactful, as it illustrates the potential impact of a cyber-attack on both large organizations and small businesses. The case study highlights the need for effective security measures and regular security assessments, as well as the importance of information sharing and collaboration in the cybersecurity community.
One potential area for further research is the specific challenges and solutions related to cyber security issues for different types of small businesses. For example, small businesses in the healthcare or financial services industries may face various cybersecurity risks and require different security measures than small businesses in other industries.

This paper highlights the importance of cyber security for small businesses in the United States and provides an analytical and qualitative framework for approaching cyber security issues. A range of relevant and verified materials to support the analysis were employed which includes academic papers, industry reports, and government publications. The case study of the SolarWinds cyber-attack demonstrates the potential impact of a cyber-attack on both large organizations and small businesses and serves as a reminder of the need for effective security measures and a culture of cyber security awareness.

6. CONCLUSION

Cybersecurity issues pose a significant challenge for small businesses in the United States. This paper has presented an analytical framework for approaching cyber security issues, which emphasizes the importance of identifying and assessing risks, implementing effective security measures, and maintaining a culture of cyber security awareness within organizations. It has also highlighted the key challenges faced by small businesses in implementing effective security measures, such as limited resources and lack of expertise.

The comprehensive literature review has identified several key themes related to cyber security for small businesses, including the need for comprehensive risk assessments, employee training and awareness, and the potential impact of cyber-attacks on small businesses. We have cited a range of relevant and verified materials to support our analysis.

The case study of the SolarWinds cyber-attack illustrates the potential impact of a cyber-attack on both large organizations and small businesses and serves as a reminder of the need for effective security measures and a culture of cyber security awareness. Several relevant and verified sources have been cited to support the analysis of the SolarWinds attack.

Small businesses must take cyber security seriously, as the potential impact of a cyber-attack can be devastating. Implementing effective security measures and maintaining a culture of cyber security awareness is crucial to protecting against cyber threats. By following the framework presented in this paper, small businesses can take a structured approach to address cybersecurity issues and better protect themselves against cyber-attacks.

Ultimately, the paper has provided a comprehensive overview of the challenges and solutions related to cyber security issues for small businesses in the United States. By taking a proactive approach to cyber security, small businesses may enhance their defences

against online dangers and make sure their companies are successful in the long run.

7. REFERENCES

[1] Adams, E., (2020). Top Threats to Cloud Computing: Egregious Eleven Deep Dive. Cloud Security Alliance. https://blog.securityinnovation.com/cloud-security-alliance-egregious-11

[2] Adhikari, U., T.H. Morris, and S.Y. Pan. (2018). Applying Hoeffding adaptive trees for real-time cyber-power event and intrusion classification. IEEE Transactions on Smart Grid 9 (5): 4049–4060. https://doi.org/10.1109/tsg.2017.2647778.

[3] Better Business Bureau. (2017) State of Small Business Cybersecurity in North America. https://www.prweb.com/releases/2017/10/prweb14798117.htm

[4] Celia P. & Patricia T. (2016). Small business information security: The Fundamentals. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf.

[5] Cook, S., (2021) Ransomware Marketplace Report Q1 2021. Coveware. [online] Available at: https://www.comparitech.com/antivirus/ransomware-statistics/ (Accessed: 28 February 2023).

[6] New York Department of Financial Services. (2021). Report on the SolarWinds Cyber Espionage Attack and Institutions' Response. [Online]. Available at: https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf

[7] National Cyber Security Alliance. (2015) Small and Medium-Sized Businesses Learn to Protect Their Digital Assets During National Cyber Security Awareness Month. [online] Available at: https://staysafeonline.org/resources/small-midsized-businesses-protect-digital-assets/ (Accessed: 01 March 2023).

[8] National Institute of Standards and Technology. (2020) Understanding the NIST Cybersecurity Framework. [online] Available at: https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf (Accessed: 28 February 2023).

[9] Ponemon Institute. (2020) 2020 Cost of a Data Breach Report. [online] Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf (Accessed: 28 February 2023).

[10] Ponemon Institute. (2021). The 2021 State of Threat Feed Effectiveness in the United States and United Kingdom [Online]. Available at: https://www.ponemon.org/userfiles/filemanager/9u0j2syx272onj9dkfpj/ (Accessed: 01 March 2023).

[11] Pratt M. K. (2022). 15 benefits of outsourcing your cybersecurity operations. Tech Accelerator. Retrieved from: https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations.

[12] PR Newswire. (2018). 43% of Cyberattacks Target Small Businesses. Retrieved from: https://www.prnewswire.com/news-releases/43-of-cyberattacks-target-small-businesses-300729384.html.

[13] Satish A. (2018) Security systems in smart buildings. https://www.researchgate.net/publication/326033055_SRI_RAMAKRISHNA_INSTITUTE_OF_TECHNOLOGY_COIMBATORE-10_An_Autonomous_Institution_Security_systems_in_smart_buildings

[14] Smith, B., (2020). A moment of reckoning: the need for a strong and global cybersecurity response. Microsoft Blog. Retrieved from: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ (Accessed: 02 March 2023)

[15] Symantec. (2019). Internet Security Threat Report. [Online]. Available at: https://docs.broadcom.com/doc/istr-24-executive-summary-en (Accessed: 28 February 2023).

[16] U.S. Small Business Administration. (2021). Protect Your Small Business from Cybersecurity Attacks. Retrieved from: https://proxy.www.sba.gov/blog/protect-your-small-business-cybersecurity-attacks

[17] Venminder. (2021). SolarWinds Data Hack is a Reminder Why Third-Party Risk Management is Important. [online] Available at: https://www.venminder.com/blog/solarwinds-hack-third-party-risk-importance

[18] Verizon. (2021) 2021 Data Breach Investigations Report. [online] Available at: https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report (Accessed: 01 March 2023).

[19] Wolff E. D., Growley K. M., Lerner M. O., Welling M. B., Gruden M. G., and Canter J., (2021). Navigating the SolarWinds Supply Chain Attack. Retrieved from https://www.crowell.com/files/20210325-Navigating-the-SolarWinds-Supply-Chain-Attack%20.pdf

