Internet of Things: Cybersecurity in Small Businesses

Zobair Wali
Old Dominion University

Internet of Things: Cybersecurity in Small Businesses

Zobair Wali

Old Dominion University

November 20, 2021

Introduction:

Small businesses are the most vital part of a nation's economy. In today's world, as we are moving towards digitizing almost everything around us, cybersecurity is essential and vital for our digitalized world to function. Small businesses are no exception. All businesses collect, use, and store information. They store employees' information, tax information, customers' information, business transaction information, and all other operational information that is needed for a business to function. Without an appropriate cybersecurity program, these businesses are vulnerable and can be easily impacted by cyber incidents and malicious attacks. Businesses are putting resources to protect their systems against malicious attacks. Although small businesses, due to their limited budget, do not have enough resources to implement a continuous and flexible security program for the protection of their information systems. Therefore, small businesses are often called "soft targets" among hackers. Small business owners believe there might be no valuable information in their business to protect, but often hackers open their way from less secure systems toward the high-profile targets using small security gaps. Additionally, there are a number of factors behind cyber attacks on small businesses. Attackers are not often after profit. They might have intentions to disrupt the business due to negative rivalries and market competitions. Therefore, a pragmatic security program is a solution to address these needs and concerns. This research review will focus on technological and security concerns surrounding small businesses, financial impacts of cyber incidents on small businesses, and solutions to address security concerns in small businesses by proposing procedures to help protect information systems. The review encompasses a section for the research methodology, a literature review where the topic is broken down into subtopics, a discussion, and a conclusion to summarize the whole review.

Methods:

In the first phase of my research, I specified several keywords and terms for my research before examining any database and journal. These keywords and terms were including "Technology," "Security," "Information Systems," "Information Security," "Small Businesses," and "Cybersecurity". I used google scholar and Old Dominion University's library search tool to find my articles. I encountered problems with google scholar since most journals were not accessible for free and I found ODU's searching tool less intelligent than google in finding specified keywords across its database. Therefore, I used different searching techniques like using quotations around my keywords and, in some cases, using alternative keywords to make my search results smaller and more precise. Additionally, searching back the paid-articles that I found in google scholar in ODU's library search tool to check if the free version is accessible. In most cases, ODU's one search provided free access to paid-articles after logging in using my student ID. ODU's one search filters helped me to specifically search for peer-reviewed articles by using the peer-reviewed option. I examined 8 articles for my research review that are no older than 15 years. I chose research articles based on their recency and the credibility of the author in the cybersecurity field. Further, I read articles thoroughly to avoid redundant information for my research and profoundly focused on finding practical solutions in all articles for my research. I made sure their literature reviews included enough information to support their author's claims. Additionally, after reading the literature review, I examined the connection between the abstract and the literature review to check if they are relevant. Lastly, I focused on how the author came up with practical results to mitigate cyber incidents in small businesses. This way I came up with 8 articles that will support and solidify my research review.

Literature Review:

In order to make sure the research review is covering the most important aspects of cybersecurity in small businesses, the literature collected is divided into subsections to further elaborate on the topic.

Information Security and Small Businesses

Today, small businesses are facing sophisticated cyber threats that affect the whole business, individual computers, networks, and in some case several networks connected to each other in a region. Malware programs downloaded by the user, running behind the scene, without the user consent replicate themselves and quickly traverse around computers in a network for the purpose of stealing personal information or disrupting the flow of the business. However, businesses are taking actions against these types of cyber incidents, there are still security gaps that make their information systems vulnerable. This subsection of the literature discusses best practices to protect information systems.

As the internet changed the way businesses are working in today's world of digital interconnectivity by providing effective ways for businesses to function and compete, it also faces small businesses to cyber threats. A blended threat is a virus that can have multiple infection techniques and propagates through the Internet and network routines without human intervention. They often exhibit Trojan-like behavior. In the first half of 2003, over 60 percent of malicious code submissions were in the form of blended threats (Hilley, 2003, p. 1). Katulic and Clark discuss how the size of a company or business influences its cybersecurity program. One of the constraints of small businesses is that they generally do not have the diverse IT staff typical of larger companies. Many small business managers have little understanding of information security threats and risks and the associated business implications that can result.

Company size has been found to be a factor in whether or not a company will have an established security program, with smaller businesses less likely to have extensive security in place (Kotulic and Clark, 2004, p.1). There is a notion that most businesses are not investing in protecting their information systems until after an attack happened. Therefore, after concluding these security concerns, this literature introduces "best practices' as a methodology to provide basic security measurements in order to protect information systems. This practices are as followed:

1. Installing and properly configuring firewalls and Intrusion Prevention Systems IPS).
2. Updating software regularly.
3. Implement strong password policies.
4. Provide appropriate physical protection for the information system devices.
5. Train employees about different cyber threats.

Financial Impacts of Cyber Attacks on Small Businesses

Recognizing the growing cyber threat landscape, many

finance and risk officers are responding by increasing budget allocations for IT security programs and investing in cyber insurance. While these commitments may be necessary to improve protection against certain kinds of losses, if made in the absence of a more comprehensive cyber risk program, they can leave an organization unwittingly exposed to far more consequential financial damage. Leaders need to think more broadly about cyber risk and consider the true intent behind a potential cyber incident and understand that theft of data may not be the most damaging impact. (Mossburg, p.1) . Cyber attacks are becoming more sophisticated and widespread that they are being placed as one of the main financial loss factors in a business. Cyber incidents are becoming so widespread that some of the associated costs are

fairly well anticipated, and are increasingly accepted as part of the risk of doing business. Direct costs can include those associated with customer notification, post-breach assurance programs, regulatory fines, public relations, technical analysis and remediation, and litigation, to name a few of the obvious. (Mossburg, p.1). In a study, Deloitte explores some costs behind cyber attacks.

CLOSER COMPLIANCE SCRUTINY. Beyond fines tied to the immediate incident, a breach can trigger larger investigations that often lead to evidence of further violations, and more fines and remediation expense.

HIGHER CYBER INSURANCE PREMIUMS. Companies that have experienced a publicly disclosed breach are likely to face higher future premiums, whether for first-time coverage or renewal.

WAVES OF PR AND LEGAL COSTS. The full ramifications of a cyber incident may take time to surface. Duration of a breach can also impact some of the organization's most valued assets, its brand, and reputation. Legal fees and litigation can span months and years post-incident. For example, theft of PII could, months later, be associated with cases of identity theft, triggering new rounds of litigation.

INCREASED COST TO RAISE DEBT. In the Deloitte study, a comparison of companies that had, and had not, suffered cyber breaches suggests that on average, a breach causes a full-level downgrade in credit rating. When the study was conducted, the interest rate for a 10 year, A-rated U.S. corporate bond averaged 3.44 percent, with BBB pegged at 4.13 percent. In this case, being downgraded from A to BBB would subject the company to an additional $3.6 million in interest over the lifespan of a $100 million project.

IMPACTS TO CUSTOMER RETENTION, COST OF SALES, AND REVENUE.

Depending on the nature of the business, loss in customer or market confidence can have a range of consequences over time, and ultimately, a significant impact on the bottom line. Price reductions may be necessary to retain clients or customers. Consider the potential impact on third-party contracts or negotiating power with vendors. Significant reputation damage might negatively impact sales, causing either loss of revenue or extending the duration and cost of a sales cycle. (Deloitte, p.1).

Discussion:

The literature reviews technological and security concerns that surround small businesses and tries to find a consensus to present a practical procedure for protecting information systems in small businesses. The *Information Security and Small Businesses* section in the literature review identifies basic practical ways to protect information systems from cyber-attacks. Firewalls and Intrusion Prevention Systems (IPS) block traffics that is not explicitly allowed. Therefore, firewalls are the most helpful devices in protecting information systems. Along with firewalls, updating all the application software and operating systems will help to resolve security vulnerabilities in software. Using complex passwords comprised of different Alphanumeric and special characters add an extra layer of security. The next section of the literature review discusses the financial impacts of cyber incidents in small businesses. Small businesses due to their limited budget are often easier targets for cybercriminals and the financial impacts followed by these attacks are long-lasting and detrimental for businesses.

Conclusion:

In today's digital world, cybersecurity is one of the main challenges for companies to deal with in order to effectively function and keep their competitiveness. This literature expands

understanding of the importance of protecting information systems through implementing basic security practices and the financial consequences a small business will face in lack of a comprehensive security program. Although the topic of protecting information systems requires more research and discussion, this literature briefly discusses the causes, solutions, and consequences of cyber incidents in small businesses. The article listed financial challenges, steps that need to be taken, and resolution on how to address and recover from after-impacts of cyberattacks. There is a direct relationship between reducing negative financial impacts of cyber attacks and following NIST guidelines and standard codes. Many organizations have to carry the burden of regulatory fines and penalties after investigations due to the violations and illegal cybersecurity practices within their businesses. Therefore, Along with regulatory fines, following security guidelines will help businesses to mitigate the cost of cyber incidents impacts considerably.

Citations:

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management, 33*(3), 583-590.

Bangs, G. (2014, October). New ransomware and cyber extortion schemes hold businesses hostage. *Risk Management,* 61(8), 30-31.

Mossburg, E. (2015). A deeper look at the financial impact of cyber attacks. *Financial Executive,*

31(3), 77-80,4.

Corallo, A., Lazoi, M., Lezzi, M. (2020, January). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in industry. 114.* doi.org/10.1016/j.compind.2019.103165.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management, 22*(2), 7-19.

Muftic, S., Abdullah, B. N., & Kounelis, I. (2016, May). Business information exchange system with security, privacy, and anonymity. *Journal of Electrical and Computer Engineering, 2016* (2016),

1-10. doi.org/10.1155/2016/7093642

Tang, Y. (2014, October). A user authentication protocol based on multiple factors. *Journal of Networks, 9*(10), 2796-2804. doi: 0001759644; 10.4304/jnw.9.10.2796-2804

Doinea, M. (2009). E-business security architectures. *Informatica Economica, 13*(1), 137-145.