12-2021

BEGINNING THE INFORMATION SECURITY JOURNEY FOR SMALL AND MEDIUM ENTERPRISES THROUGH BUSINESS CONTINUITY PLANNING AND INFRASTRUCTURE AUTOMATION

Aaron Chamberlain

BEGINNING THE INFORMATION SECURITY JOURNEY FOR SMALL AND MEDIUM ENTERPRISES THROUGH BUSINESS CONTINUITY PLANNING AND INFRASTRUCTURE AUTOMATION

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

---

by

Aaron Chamberlain

December 2021

BEGINNING THE INFORMATION SECURITY JOURNEY FOR SMALL AND MEDIUM ENTERPRISES THROUGH BUSINESS CONTINUITY PLANNING AND INFRASTRUCTURE AUTOMATION

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Aaron Chamberlain

December 2021

Approved by:

Dr. Nasrin Mohabbati, Committee Chair, Information & Decision Sciences

Dr. Conrad Shayo, Committee Member

Dr. Javad Varzandeh, Department Chair, Information & Decision Sciences

ABSTRACT

Technology has become an essential component of enterprises, driving productivity, innovation, and defining entire processes and product categories. However, these advances come with additional risk; the devices that drive an enterprise can fail at any time or be attacked by malicious actors. Larger enterprises have learned to deal with these risks, but small and medium-sized enterprises (SMEs) have been largely left behind. This project sought to investigate the cybersecurity-related problems SMEs experience and what SMEs can do to solve them. In addition, the project examines the types of information security incidents that occur within SMEs and their financial preparedness for such security incidents. The literature findings are that SMEs lack financial preparedness for information security and natural disasters, lack an effective company culture that generates and keeps, and need a more technical or operational approach to improve information security performance. Given these observations, cost-effective solutions are presented for Incident Response Testing, Business Continuity Planning, Employee Training, and DevSecOps Automation. Suggested areas of future research include developing Infrastructure Automation strategies for SMEs, focusing on employee training and validation processes. Additional real-world data about information security breaches must also be brought forward and analyzed to assess business risk correctly.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

Problem Statement

Technology has brought dramatic increases in productivity and innovation within enterprises. Entire industries such as retail have evolved with their technological advancements. Small and medium-sized enterprises (SMEs) are now seeking to remain competitive by utilizing technology in the same way. However, SMEs often lack human capital and financial resources to create and maintain Information Systems in the same way as large enterprises (Heidt, Gerlach, & Buxmann, 2019). These limitations increase the risks taken by SMEs, stressing their ability to operate (Kaukola, Ruohonen, Tuomisto, Hyrynsalmi & Leppänen, 2017). Therefore, SMEs need unique solutions that fit within the scope of their industries while also remaining affordable and realistic time investments.

Objective

The objective of this project is to conduct a literature review to discover the issues that SMEs face when implementing Information Security practices, summarize prevailing recommendations, and produce additional adaptable and affordable recommendations SMEs could use to increase their resilience to information security incidents.

Research Questions

This project aims to answer the following questions:

1. What risk factors do SMEs take on with Information Technology?
2. What are the financial consequences of an information security incident within an SME? How does it affect their overall business finances?
3. What adaptable and low-cost tools exist to develop cultural and technological maturity?

This project is organized as follows: Chapter one provided basic information and the objectives of this research project. Chapter two covers definitions of small and medium enterprises and information security risk. Chapter three summarizes the information found in the literature review process and the prevailing opinions of experts in the field. Chapter four discusses the financial status of small and medium enterprises along with the cost of information security breaches. Chapter five discusses solutions that have been shown to reduce the cost of information security incidents. Finally, chapter six presents conclusions and discusses areas for further research.

CHAPTER TWO

SMALL BUSINESS AND INFORMATION SECURITY RISK

Distinguishing Small, Medium, and Large Enterprises

Enterprises exist in many different forms and sizes; they are mission and vision-driven with specific strategic goals. An enterprise can be run by a single person to earn a side income, or it can be run with the vision of becoming the largest company in the world. The term enterprise is used more often than business in academic literature, but they are usually interchangeable. There are several different methods for defining small and medium-sized enterprises. Within the US, the Small Business Administration has created size standards based on several criteria, including the type of business you are entering. A business is considered small if it has an average gross annual income below a specified threshold for three years. For example, if the business offers Interior Design Services, Code 541410, the average must fall under $8.0 Million USD to be considered small. For Custom Computer Programming Services, Code 541511, they must fall under $30 Million USD (Small Business Administration, 2019).

While this definition is specific and could provide insight for certain types of analysis, it presents several issues. Primarily, it remains a standard for only the US and would require non-trivial data processing to verify that businesses interviewed or sampled in a study qualify as small or medium-sized. In addition, while the business categories transcend borders, the currency does not and

would require all studies to specify exchange rates used. This system would also require researchers to intimately know the classification codes to discern the difference between a consultancy that produces software and one that does project management. Worse, if businesses participate in more than one category, it requires the business to estimate the percentages of their output in each category and be classified by the largest category. Each of these issues presents an element of a system that has difficulty reaching an international scale.

This project will be using an alternative method where the business is classified by the organization's size. Of the academic literature observed that mentioned their criteria, all followed the Organization for Economic Co-operation and Development (OECD) definition. These standards also vary between regions, but this classification is trivial to adjust. For example, the United States and Canada define small businesses as having less than 100 employees and medium businesses with between 101 and 500 employees (Innovation, Science and Economic Development Canada, 2020). The OECD covers European countries, which defines the same limits as 10-49 and 50-249, respectively (OECD, 2017). In the 2016 US Annual Survey of Entrepreneurs, 99.7% of businesses have fewer than 500 employees (United Census Bureau, 2016). More specifically, 98.2% of US businesses have less than 100 workers, and 89.0% of US businesses have fewer than 20 employees. These statistics are similar within other nations; in the EU, 93% of enterprises have fewer than ten

employees (European Commision, 2019). These statistics indicate that the world economy still relies heavily on small businesses.

Defining Risk

Information security (IS) risk is the probability of data loss, exposure, or failure of a system due to an attack or other vulnerability. This project centers around mitigating Information Security risks for small to medium-sized enterprises (SMEs), so each enterprises' unique needs must be considered. Some enterprises inherently carry little to no IS risk. For a small local cookie store, their entire digital footprint might only be social media and point-of-sale devices. While each of these could be compromised and carries risk, they carry little monetary or reputational cost. Other small businesses might be the complete opposite. Consider businesses like small dentists, law firms, and other medical professionals. These professional businesses are run by a person knowledgeable and experienced in their industries, has valuable data and personally identifiable information (PII), but might not immediately consider their IS risk. Given this, the problems and solutions addressed in this project are directed at businesses that stand to lose the most, as opposed to every small and medium business.

A common paradigm to understand the purpose of Information Security is the CIA triad, representing the Confidentiality, Integrity, and Availability of an information system. Confidentiality represents the desire to keep confidential information private. For example, if the private home addresses of a web store's

customers are published publicly online, this represents a failure in confidentiality. Integrity represents the desire to keep accurate information to benefit the business goals. A failure here can come in many forms, either malicious or unintentional. If, for example, the hard drives on an important database server fail with no backups, nothing can be done; the valuable information is now gone. Finally, availability defines the downtime constraints of a system, or when it can be offline and inaccessible to its users. For a company's primary website, it should be online at every moment and never shut down. For a database used only by in-office staff, the availability can be significantly less, down to just the time staff perform their daily jobs.

Each corner of the CIA triad holds a critical value for businesses. A failure in any one of them will result in business losses of some kind. It can present itself as employees not being able to complete their jobs, lost labor, damage to reputation, and many other ways. Despite having typically considerable financial repercussions independent of how the damage manifests itself, many small businesses do not consider the CIA triad. They may not document how the computers were set up; they may not take regular and reliable backups; they may follow security best practices that prevent malicious attackers. Medium-size businesses typically begin to sort out some of these issues, such as backups, but staffing issues hold them back from solving all of them. Consider a typical SME with 80 employees; 54 percent will have two total employees for IT and Information Security roles, with 46 percent having either one employee or

outsourcing this role (Asti, 2017). Anyone familiar with the role will know this is just enough staff to keep things working. So, what causes businesses to ignore the risks?

One of the most significant factors is underreporting information and communication of the risks. Currently, no federal laws require a company to disclose cyber incidents, but US lawmakers are attempting to pass such regulations (Cyber Incident Notification Act, 2021). The SEC does require disclosure for publicly traded companies when they "...materially affect company's products, services, relationships with customers or suppliers." (Security and Exchange Commission, 2018). According to the Wilshire 5000 Index, there are only 3,544 public companies in the US as of June 30, 2021 (Wilshire Advisors LLC, 2021). Thus, of the 30.4 million U.S. companies, those legally required to declare cyber security events are a tiny minority, approximately 0.01% of companies.

No official number regarding underreporting can ever be produced since it would require the entire data set of issues to be present in the first place. However, the 2019 ISACA State of Cybersecurity report found that 50% of professionals believe enterprises underreport cybercrime, even when required to do so (ISACA, 2019). Another research paper concludes that publicly traded companies only disclose incidents themselves when they suspect with 40% certainty that investors already know (Amir, Levi & Livne, 2018). While enterprises do this to prop up their stock prices, the same researchers found that

stock prices dropped further when third-party groups disclosed data breaches. Two possibilities account for this: either the third-party disclosed breaches were much worse in nature, or the public perceived the business as less honest and trustworthy when they did not announce it themselves. Several research papers have concluded that CEO's social influences significantly influence their visibility of Information Security dangers and their support of those efforts within their organizations. (Barlette & Jaouen, 2019; Ozgen & Baron, 2007).

A 2019 Keeper Security report estimates that 66 percent of all SMBs were hacked in that year (Keeper Security, 2019). What types of attacks are they seeing? It turns out that they are not spared from the same types of attacks as larger enterprises, although they might see them at different rates. Spear-phishing is a targeted attack, usually against a single employee believed to hold power, such as a system administrator. An attacker will target that single identified employee rather than blasting out many emails to an entire company. The 2014 Symantec Internet Security Report noted that 41 percent of SMEs were targeted by spear-phishing attacks. (Symantec, 2014). However, in another report, Symantec noted that SMEs were 20 times less likely to be affected (Symantec, 2015).

Reconciling these two facts reveals that while SMEs are targets, they are not deliberate or planned targets. Instead, they primarily fall victim to mass scanning operations that immediately attack systems that have known vulnerabilities. Many of these vulnerabilities can be mitigated by keeping track of

security announcements and updating systems as needed, yet this proves to be a challenging task for small businesses. A Ponemon Institute report conducted for ServiceNow found that 60% of respondents stated their breaches were caused by an unpatched system, despite an update being available (ServiceNow, 2020). Of that 60%, 62% said they were unaware that they were vulnerable. Given the high likelihood of an attack, perhaps SMEs do not acknowledge the risks because they do not understand the financial implications. After proceeding with the literature review, chapter four will address the finances of SMEs.

CHAPTER THREE

LITERATURE REVIEW

While new trends in information security are always emerging, a vast wealth of knowledge can be gained from every generation of information technology. The research process was primarily conducted using California State University's OneSearch tool to find peer-reviewed articles and publications that treated the same topic. The OneSearch tool accesses all types of library content from other linked databases, including sources from other California State University libraries (John M. Pfau Library, 2021). Additional information was pulled from industry sources where the sample size seemed large enough, had academic merit, and had a purpose beyond marketing.

Table 1: OneSearch Internet Results

Database Source	Search Words	Number of Hits	# of Relevant Articles Selected / Used	Authors
Default / All OneSearch Databases	SMB Information Security	29,737	32 / 8	• Abazi • Goucher • Heidt, Gerlach, & Buxmann

				• Henson & Garfield • Kaila • Khan, Tanwar, & Rana • Nilaykumar & Balakrishnan • Pérez-González, Preciado & Solana-Gonzalez
Default / All OneSearch Databases	SME Information Security	97,294	32 / 8	See above.
Default / All OneSearch Databases	SME Business Continuity Planning	9,765	87 / 5	• Goodwin • Kim & Amran • Lucey • Lucey & Lyons • Merchant, Kumar & Malik • Wedawatta & Ingirige

Default / All OneSearch Databases	SME DevOps	414	6 / 1	• Mohamed
Default / All OneSearch Databases	SME Failure	69,371	73 / 7	• Dewaelheyns, Van Hulle, Van Landuyt & Verreydt • Gupta, Barzotto & Khorasgani • Kosmidis & Stavropoulos • Milošević, Mihajlović & Stojanović • Schalck & Yankol-Schalck • Williams • Youssef, Mohamed & Abdeslam

Table one summarizes the library search results. The first research query was for “SMB Information Security” and “SME Information Security,” which returned 29,737 and 97,294 results, respectively. The only OneSearch filter used

was to produce results only containing articles. This means that all databases were searched by default. During the library search, it became clear that the preferred academic term for SMB was SME, so all further research utilized this acronym. From this selection, the top 100 articles were reviewed, finding 32 that matched the project objectives. After further analysis of the abstracts and content, only eight articles were deemed relevant for the project. The project provides a complete content review and presents the findings below. “SME Business Continuity Planning” was searched next, producing 9,765 results. Again, the first 100 results were reviewed, finding 87 that matched the project objectives. Using the same analysis methods, only five were deemed relevant. Finding the appropriate or common academic terminology to produce articles that discussed DevOps practices in SMEs was challenging. “SME DevOps” produced the highest number of results, 414, while also being consistent with my research. The first 100 results were also reviewed here but only produced six results. Of those six results, only one covered similar research. It is abundantly clear from this search that IT automation has yet to reach SMEs. Finally, “SME Failure” was searched, producing 69,371 results. After again reviewing the first 100 results, 73 matched the project objectives and seven were found to be relevant. Each topic will now be briefly reviewed, however a complete summary of each of these relevant results can be found in Appendix A.

Starting off, the subject of “SME Information Security” was broad but helped to define common issues researchers are finding, and the suggested

resolutions. The most commonly cited issue was that organizations had the desire to increase security (Heidt, Gerlach, & Buxmann, 2019; Henson & Garfield, 2016), but they did not believe they had the resources (Heidt, et. al., 2019), or didn't want to spend money (Henson & Garfield, 2016) without compliance requirements forcing them to do so (Goucher, 2011). Some authors present organizational solutions, such as viewing each information system member as an asset to understand return on investment (ROI) on employees and technology (Abazi, 2018). Pérez-González, Preciado & Solana-Gonzalez suggest that to build an information security culture, organizations should avoid contracting these responsibilities and make related decisions in the open (Pérez-González, et. al., 2019). Others present more straightforward technical recommendations like protecting cloud environments and data, using Multi-factor-authentication (MFA) (Kaila, 2018), or mitigating SQL Injections and Cross-Site Scripting (Nilaykumar & Balakrishnan, 2012). Some authors also chose to balance both sides like recommending the development of a Business Continuity Plan (Kaila, 2018).

Since it had been recommended in several places, I was interested in understanding the overall discussion surrounding Business Continuity Planning (BCP). Just as with my previous search, the common theme of lacking resources quickly arose (Lucey & Lyons, 2009). Kim and Amran discuss how traditional methods of developing a BCP can require large human and monetary capital that SMEs do not possess (Kim & Amran, 2018). Other researchers chose to focus

on issues likely to affect SMEs, such as outgrowing immediate family ownership (Merchant, Kumar & Malik, 2018) or extreme weather events (Wedawatta & Ingirige, 2016). In the case of extreme weather events, SMEs are typically less prepared because they operate in a smaller geographic region and disasters can affect supply chains and processes outside of their typical boundaries (Wedawatta & Ingirige, 2016). Overall, Lucey provides the most straightforward summary of Business Continuity Planning (Lucey, 2006). They start by summarizing its importance, the difficulty of producing one with traditional methods, and then provide a unique method specialized for SMEs that cannot invest significant amounts of time towards the process (Lucey, 2006).

From my research into “SME DevOps”, it became clear that both academia and business at large have not benefited from infrastructure automation. Of the very few results that were produced, many read as specific implementations of a technology that might not be transferrable to another organization (Kenner, 2019). Others focused solely on software development practices (Mishra & Otaiwi, 2020), of which many SMEs take no part. The paper “DevOps Shifting Software Engineering Strategy – Value Based Perspective” held the most value since it presents a simple model for evaluating the success of DevOps adoption within an organization (Mohamed, 2015). They suggest that the primary purpose of DevOps practices is to foster communication between departments that would have previously worked in silos (Mohamed, 2015). Their

measurements for success are communication, automation, governance, and quality.

Finally, the research behind “SME Failure” is showing very active progress to understanding the failure scenarios for Small and Medium Enterprises. In general, the research has been focused on breaking up the large group Small and Medium Enterprises into small groups via size (Gupta, Barzotto & Khorasgani, 2018) or other discrete variables (Milošević, Mihajlović & Stojanović, 2019). Newer statistical and machine-learning models have come into play (Schalck & Yankol-Schalck, 2021) that have been able to determine self-ownership and region of operation as critical factors for SMEs. Some factors like industry sector have been found to not affect business viability (Williams, 2014). Overall, the research suggests revenue to be a strong indicator of success (Gupta, et. al., 2018; Milošević, et. al., 2019; Youssef, Mohamed & Abdeslam, 2020), with some suggesting its value is determinant on the size of business (Gupta, et. al., 2018; Williams, 2014). While not often considered, the research suggests that when used to build and retain human capital, large relative wages increased an SMEs chance of survival (Dewaelheyns, Van Hulle, Van Landuyt & Verreydt, 2021; Kosmidis & Stavropoulos, 2014).

After the literature review process was complete, I began to have a good idea of the issues affecting SMEs (Research Question 1), and solutions for the same issues (Research Question 3). However, while there is sufficient academic research surrounding SME finances (Question 2), they did not all seem to have

high confidence that their solutions could be generally attributed to SMEs. Thus, in the following chapter, I will continue the analysis of SME finances through other reputable, non-academic sources.

CHAPTER FOUR

SMALL BUSINESS FINANCES

Understanding the financial situations of the average small business is critical to correctly forecasting how an information security failure of any kind will affect business outcomes. Finding the leading causes of small business failure was harder than anticipated. The academic literature summarized above was able to produce some results, but not yet with high confidence. Since academic research can often be locked behind paywalls, I wanted to see what common internet search engines would present on this topic.

Searching the topic “Why Small Businesses Fail” produced an overwhelming number of results. Many of the top results are from other businesses hoping to provide consulting services, and write blogs to suggest they know how to resolve issues. A particular statistic can be found plastered around the internet, unattributed, stating, “82% of businesses fail because of poor cash flow management skills/poor understanding of cash flow.” A recent source of this information is a Business Insider Article (Desjardins, 2017). However, tracing back this research, it is created by US Bank in 2002 from a proprietary data set (Hagen, 2002). Not only does this make it difficult to verify, but it also has some obvious bias coming from a bank from who would make money providing business loans.

Luckily, the Federal Reserve Banks have come together to produce the Small Business Credit Survey (SBCS) for the past five years. It is taken annually

in the third and fourth quarters and features responses from 5,000 to 8,000 businesses, depending on the year. Pertinent to this analysis, the SBCS report uses the same size restrictions in their definitions of small business defined previously; an SME contains 1 to 499 employees. While it is also a small sample size compared to the audience it represents, it remains one of the most extensive annual datasets. The 2021 SBCS has been released but has heavy influence from COVID-19 related issues. Thus, the 2019 and 2020 surveys provide the best look into recent ‘normal’ business statistics. They found that 66 percent of small businesses faced a form of financial challenge (Federal Reserve Banks, 2020). Forty-three percent noted the issue was paying operating expenses. When asked what would happen if revenue was lost for two months, 86 percent stated they would need to supplement funding or cut costs. More specifically, 17 percent would need to close their business if that revenue was lost.

Looking at the financial costs of an information security incident reveals that most small businesses cannot afford to fail. According to Coveware, the average business will have 23 days of downtime following a ransomware attack (Coveware, 2021). This high number shows that recovery is not a simple task. Businesses not only have to get their systems rebuilt under time constraints to keep their employees productive but also perform analysis, quarantine systems, determine the scope of data taken, and report to the proper governing bodies. Coveware also reported an increase in duplicate attacks on businesses, with attackers replicating attempts if the business managed to recover without paying

the ransom (Coveware, 2021). A single attack will burn roughly half of the financial runway that most SMBs will have. given the average downtime

These large numbers demonstrate both the severity of the situation and the lack of reporting on the topic. Popular media has begun to treat the issue, but primarily because it has become a political issue. In September, CNN ran an article on Information Security on average every four days, with five of the eight articles mentioning the acting president Joe Biden. According to Risk Based Security, they estimated some 3,932 publicly reported breaches occurred in 2020 (Lohrmann, 2021). The news could report on dozens of business closures every day if they wanted to, but it would make for constant, tiring news. So instead, they report on the more sensational headlines, such as “Company shuts down because of ransomware, leaves 300 without jobs just before holidays” (Cimpanu, 2020).

The Arkansas-based company in question was named “The Heritage Company.” The Heritage Company was primarily a telemarketing firm that ran fundraising campaigns for charities or collected political market research. Sometime around October 2019, the company’s servers were compromised, locking out nearly every system (Cimpanu, 2020). They were able to slowly recover over time thanks to the owner funding the company while it remained unprofitable. When they finally realized they were likely to never get back up to speed, the owner sent a letter before Christmas that the company would cease

operations. They instructed employees to call a phone number on January 2nd to see if they could return to work, but they never did (Cimpanu, 2020).

The Heritage Company story was carried by several local news outlets (Briggs, 2020; Brooks, 2020) and several IT-focused publications (O'Donnell, 2020), but none carried updates after the initial letter from the CEO, Sandra Franecke. Searching for additional information yields ghost towns. Their website has been turned into a podcast aggregation website, their Linkedin and Facebook pages remain active but have not been updated since 2020. Despite the tragic nature of the incident, the timing around major US holidays likely meant few heard the news, making no change on the behavior of SMEs in practice. Between the actual probability of an attack and the financial likelihood of failure, SMEs are in dire need of practical, real-world, affordable solutions.

CHAPTER FIVE

BIG SOLUTIONS FOR SMALL BUSINESS

Within Information Security, academic literature can be categorized by their approaches: human, behavioral, technological, environmental, or organizational. Each of these approaches can produce valuable insight depending on each enterprise's exact needs, however, I contend that SMEs should focus on the human, technological, and organizational aspects of their enterprise first. I contend that SMEs have greater control over these elements than the others, and that they may also be the most neglected in an unconscious effort to just produce anything of value. The literature reviewed previously either suggests business culture is the critical component of maturing an Information Security program (Saban, Rau & Wood, 2021; Sadok, Alter & Bednar, 2020; Pérez-González, Preciado & Solana-Gonzalez, 2019) or solutions of a more practical and technical nature (Kaila, 2018; Khan, Tanwar & Rana, 2020). In reality, both are requirements for successful Information Security programs: supportive executives and a team with the correct technical background.

From what we have observed thus far, small to medium enterprises ignore their information security risks because they are difficult to enumerate and quantify. Resolving risks involves first finding and knowing what issues are present within the organization, determining the cost when risk is exploited, and the cost to mitigate the risk. For many small businesses doing their own IT work, creating a list of risks can be difficult. Many companies are willing to sell SMEs

the most expensive, shiny solution possible, but it often is not the correct solution for small businesses. Instead, the most significant cost-saving and critical components are the most affordable and unattractive solutions. According to IBM, Incident Response Testing, Business Continuity Planning, Employee Training, and DevSecOps sit in the leading factors that reduce the cost of a system failure (IBM Security, 2020).

Incident Response Testing

Incident Response Testing is multi-faceted and is focused on having a documented, repeatable, and tested plan for dealing with an incident. These tests can be done in real-world settings, but this method can require additional hardware to avoid taking down existing business-critical systems. Since many small businesses do not have this, the next best thing is to carry out tabletop simulations. A tabletop simulation involves getting every core stakeholder of the response plan in the same room and talking through the plan. When someone notices that a step might be missing or is easy to get wrong, the group discusses it, updates the incident response plan, and ensures that it can be done as written. While it will take time away from other critical business operations, IBM suggests that it will reduce the cost of a ransomware attack by $295,267 USD on average (IBM Security, 2020).

A common failure in incident response planning happens with backups. Often, organizations just assume their backups will be there when the time comes. However, in the case of ransomware, it is increasingly becoming more

common to see it seek out backups as the primary target with the actual systems following it. When this happens, it leaves little option but to completely rebuild everything or pay the attackers. So-called “offline” backups can help to mitigate this partially. For example, an enterprise can save data to magnetic tape drives, requiring a high upfront investment. They could also have a system that only periodically comes online to sync with a primary backup server and then is taken back off the network. The final critical component of backup systems is testing. Ideally, the enterprise will create an automated method of restoring from backup and verifying it can produce a working system. In this way, staff can regularly verify the backups without taking too much time from their regular work.

Business Continuity Planning

According to IBM, Business Continuity Planning is the second most significant factor in reducing the cost of a cybersecurity incident (IBM Security, 2020). Business continuity planning can be seen as a superset of incident response planning. It goes beyond just the steps of how a system will be restored to a functioning state. It typically states which business processes are most critical, which produces the most value, or will result in lost productivity. It identifies what can be done to make the primary systems redundant and highly available and keep an organization functioning during an incident. It should be clear why a business continuity plan carries so much value. If a business has genuinely put no thought into this type of plan, they will start to create it on the fly as the incident unfolds. It is critical information that is needed to focus the efforts

of staff and ensure that they are working on a single critical problem instead of solving everyone's problems.

A Business Continuity Plan is not a document, especially one that only gets brought out in times of disaster or to be updated. It forms the basis of how an organization will make decisions. Lucey, an expert in the field, authored a critical article for our recommendations, pointing out that many business continuity processes came from large businesses and benefited them most (Lucey, 2006). Traditional methods take a lengthy analysis period and cost hundreds of thousands of dollars to find an enterprises' problems and risks. Lucey's article suggests a newer methodology that will be summarized here but should be referenced for detailed procedures. The first proposed step is to form a Business Continuity Committee (BCC). The plan will be developed by a small committee representing every critical business function and lead by anyone besides IT leadership (Lucey, 2006). These individuals will meet for about 10 hours total to develop the proposed annual plans to further the organization's plan and resilience. A first meeting is carried out to go over the process with the committee.

The second step is to define internal and external interruption scenario classes. An external interruption scenario is anything the business cannot control, such as an ISP Networking failure or an earthquake that destroys property. An internal interruption is anything the business can control, such as IT networking or the loss of critical employees. A project manager interviews key

staff members, executives, and outside suppliers to create a list for the committee. A second BCC meeting is held to review this document (Lucey, 2006). The third step is to create a list of strategies and tools to avoid interruption or lower the probability of failure. The project manager classifies each strategy or tool with an A, B, C ranking system, where A is very important, B is important, and C can be deferred. A third BCC meeting is held to agree on the findings and establish them as final priorities (Lucey, 2006). The fourth step involves the project manager going back and determining if the solutions are already implemented within the organization. The unimplemented solutions establish a list of areas with gaps that need to be filled. A fourth meeting with the BCC agrees on this list (Lucey, 2006). With this information, the project manager creates a list of priority items that can be performed in the coming year, finds out the funds and resources available to accomplish the project. Each project is placed on a calendar, and a final, fifth BCC meeting is held to formalize the projects (Lucey, 2006).

While it might sound like a fair amount of work, Lucey’s work is quite a simplified and approachable way to establish a business continuity plan. This ongoing process will help to slowly mitigate the business's risks without hiring expensive consultants to carry out the analysis. Using a committee from the start is also an effective strategy to reduce work that must be brought back, getting consensus on the process from the first meetings. Especially in smaller enterprises, this process will also find areas where they have little employee

overlap. This risk of knowledge loss is unavoidable within SMEs, so the next section is dedicated to what businesses can do to increase employee training and knowledge bases.

Knowledge Loss and Employee Training

The critical nature of knowledge loss becomes immediately visible when reviewing SME employee makeup. Again, 89% of US enterprises have fewer than 20 employees. By losing a single employee, five percent of the average SMEs' workforce has left. How much knowledge loss occurs depends on business practices. For example, if they are a team member with five others, each doing the same task, no knowledge loss occurs, a new employee can come in and learn from the remaining four. However, if there was only one employee, it could result in a total knowledge loss, precisely the situation most SMEs face with their IT department. Therefore, SMEs must be highly diligent about ensuring documentation is being created for all work being done by their IT employees. Hopefully, the system documentation will provide enough context for their replacement to come in and pick up where they left off.

There are several reasons an enterprise might use a Managed Service Provider (MSP) for its IT solutions. The ability to mitigate the risk of knowledge loss ranks in the top reasons. MSPs have it in their best interest to follow standard best practices so that if an unfamiliar staff member is assigned to their client, they are not wasting time rebuilding a knowledge base of unique configurations. On the other hand, using an MSP can increase the latency to

solving an urgent issue because of the time it takes them to contact them and apprise them of the situation. Finally, it is worth noting that another staff member should have sufficient IT knowledge to ensure that the previous staff is properly disabled from all systems. Disabling unused credentials will prevent unauthorized access from terminated staff, eliminating the possibility of numerous damaging situations.

Enterprises can reduce their risk of knowledge loss through efforts to keep employees longer. Turnover rates are positively related to an employee's job satisfaction and organizational commitment. (Igbaria & Greenhaus, 1992) Chandler and Mcevoy noted that SMEs that increase their training programs would see lower employee turnover and associated costs (Chandler & Mcevoy, 2000). Younger, educated employees are even more likely to benefit from this training and career focus. If the path towards new positions and higher pay is not abundantly clear, this age group will begin to look for those opportunities elsewhere. Thus, managers within SMEs should focus on each employee. If organization roles do not yet exist, employers should work with the employee to see their vision of the enterprise. Where appropriate, employers should allow them to help expand the organization in that direction.

Infrastructure Automation

Finally, a middle-ground cost mitigation factor is utilizing DevSecOps principles. DevSecOps principals center around fostering communication between departments and building systems jointly. Each syllable represents a

potential department or business operation that can be tied together; development, security, and operations. The origins of DevOps can be traced back to the late 2000s where the Development and Operations teams had opposing goals. Developers had recently adopted agile practices to produce new changes quickly, while operations teams maintained uptime of the service by resisting large changes (Yitbarek, 2018). The principles allowed these teams to communicate and push the developers' changes rapidly, but with reasonable surety that it would work on production systems. Unfortunately, these principles have been pushed aside for a more straightforward marketing paradigm meant to push software and well-defined solutions. In many companies, they formed a DevOps department without applying the principles to all aspects of the organization.

This marketing-driven definition for DevOps has added many knowledge requirements to a DevOps engineers' plate. The knowledge requirements form a very high bar that in turn has driven up the cost of salaries. So not only are the salaries of engineers expensive, but so is the software that they use. The high associated costs have traditionally prohibited small businesses from automating anything in their IT infrastructure. Medium-sized businesses have begun adopting these practices, while large companies like Google or Apple have already begun to move to new phases of that journey, with technologies like Kubernetes and Software-Defined Networking. This section aims to demonstrate

the need for automation, even on a small scale, and discuss how SMEs can overcome those price hurdles.

Unlike the other recommendations addressed thus far, automation can either shape business growth or reduce operational costs. While the IBM study suggests DevOps practices as a mid-level threat reduction mechanism, adopting DevOps principles can bring other organizational benefits. A common misconception is that an enterprise needs to do in-house software development to benefit from DevOps, which is not true. In this regard, it makes the complexity of server automation even more accessible, with a shifted focus to repeatable server configuration, stability, and security compliance. DevOps principles achieve these goals by increasing the reliability, stability, resilience, and security of an enterprise's servers (Mohamed, 2015).

For SMEs, their automation journey should begin focusing on how to automate server configurations. If a server were manually configured, it would need to be configured by hand again in any incident. They should ask questions like: How do we automatically set up the AD server? How can we automate a web or outlook server installation? This type of automation provides many benefits. Perhaps the most important, it will allow for testing updates without fear. Often, organizations do not patch their critical systems and web services because they do not have the confidence that an update will work. By having automation in place, they can quickly create a replica of the production server configuration and test there, gaining confidence in the process. This type of

automation also benefits from being self-documenting. Often, when a server is configured manually, the employee must also find the time to write out what was done. Then problems arise, such as never returning to update the document when configurations change or misplacing the document altogether. When automating configuration, the configuration files tell the whole story of what is on the server.

The next question to ask is who will be doing this work. As we already pointed out above, employee retention is positively related to training and career growth (Chandler & Mcevoy, 2000). Considering this, employers should seek to have their current staff trained to become automation engineers. If this is not possible, another possible solution is to use a Managed Service Provider (MSP) to work on areas of their business that would otherwise demand a high price tag. Indeed, this appears to be what is happening. According to the 2019 Global State of Cybersecurity report by Keeper, SMBs have slowly brought MSPs into the mix, with 32% of businesses now reporting they use one. (Keeper Security, 2019) On the MSP side of operations, if they have not already, automation has the potential to reshape their business. While it takes more time upfront to automate things, the time to stamp out automated systems becomes very minimal. The reduction in implementation phases would allow them to theoretically take on more customers and lower prices to work with other organizations.

Choosing a Software Solution

Suppose a business chooses not to delegate this responsibility. In that case, an enterprise needs to look at the criteria for choosing software and determine whether such software exists. Each enterprise will have unique needs, but the following four criteria will walk us through choosing software to begin a SMEs automation journey. Price should be the first factor to consider. Ideally, it should be free with few, if any, restrictions with optional purchases for support or software as a service (SaaS) platform. The next three factors all relate to our previously discussed issue of knowledge requirements and employee retention. Second, the software should be capable of being installed and configured within a short timeframe, with little previous knowledge. While this reduces the need to have previously trained employees, it also benefits disaster recovery efforts. I have personally spent days configuring specific software packages. I can only imagine the disaster that would ensue if it became a critical piece of infrastructure without automation to recreate it. Third, the automation software should use no proprietary or domain-specific languages (DSLs). DSLs have many downsides: they require employee training or paying more for staff with previously existing backgrounds. They also lock enterprises into the software, forcing them to rewrite everything if they leave the platform. Finally, the existing user base and the overall sentiment to the software should be considered. These attributes directly relate to the possibility of finding employees that are both willing and capable of delivering solutions to an SME.

With these criteria in mind, we will look at the industry-standard software stacks and evaluate the use of each in an SME environment. Puppet, Chef, Ansible, and SaltStack will be evaluated due to their ubiquity. Each of these solutions is open source, meaning that it is free to download and change as needed, with the option to pay for SaaS versions or additional support. Each of these solutions, except for Chef, has the option of using an agent-less architecture. Each computer does not need to be configured to speak with a controlling server with agent-less architectures, reducing the installation and configuration period. However, the agentless versions of Puppet and SaltStack carry some limitations and are not the typical configuration within the industry. In those environments, the agent-less mode fills in gaps for some devices such as networking equipment. Puppet and Chef configuration files are written in their own DSLs, which is a superset of the Ruby programming language. Ansible and SaltStack share a similar design, with modules and other code written in standard Python. However, the user-facing configuration files are written in YAML, a markup language that is easy to read and write. Based on the outlined criteria, SaltStack and Ansible remain in the top two choices, with the remaining question being the number of potential candidates for either job position.

Finding the installed userbase of either system is difficult, but we can look at other community measures to estimate users. On Github, a website for code collaboration where each project is stored, ‘stars’ are used to bookmark a project and follow the work. Ansible (ansible/ansible) has 49,900 Stars and SaltStack

(saltstack/salt) has about a quarter of those users, at 11,900 Stars. Using Google search engine, “Ansible” produces 11.5 million results, while “SaltStack” produces only 822,000. Finally, we can look at the number of Job Positions for either technology on Indeed, a website for employers to list job openings, and job seekers to apply to them. Within the United States, “Ansible” produces 20,137 Job Openings. “SaltStack” produces a list of only 1,020 job openings in the same region. Thus overall, since it meets every criterion, Ansible is recommended for SMEs beginning to automate things.

CHAPTER SIX

DISCUSSION, CONCLUSIONS, AND AREAS FOR FURTHER STUDY

Throughout this project, we have gone through a wide range of academic and professional literature and reporting, sifting the information to find solutions that will present the most immediate benefit to a Small to Medium-Sized Enterprise (SME). It has been shown that while SMEs often have financial limitations, they are not incapable of following through on the most effective risk reduction methods. Through business continuity planning and incident response testing, all essentially free exercises, they can reduce their risk footprint by understanding what needs to be done. The project has also shown that accessible and affordable solutions are available to small businesses looking to automate the deployment of their IT infrastructure. Such automation can lead to stable and reliable environments and can also be reproduced quickly in the case of any information security incident. Enterprises should adopt these information security principles to increase their resilience and chance of survival significantly. The evidence overwhelmingly suggests that if SMEs fail to do so, it is only a matter of time before an information security incident endangers their enterprise.

This project opens up several possible areas for future research. I would like to see additional datasets and analysis in the areas where it is currently lacking. A more direct implementation plan for Infrastructure Automation would be of great benefit to SMEs, including how to train and retain skilled employees. A great deal of work also remains obtaining real-world data about information

security breaches. Methods need to be derived to either directly obtain or estimate the number of SMEs affected by these issues. Without a correct sense of danger, the appropriate resources will never be assigned to address the issues.

APPENDIX A

SUMMARY OF SELECTED ARTICLES

Author(s)	Article Title	Year	Summary
Abazi	An approach to Information Security for SMEs based on the Resource-Based View theory	2018	Abazi suggests SMEs should view Information Security as a collection of resources. This view will allow SMEs to more easily visualize their return on investment and invest in security and employees.
Dewaelheyns, Van Hulle, Van Landuyt & Verreydt	Labor Contracts, Wages, and SME Failure	2021	The researchers use discrete regression models to determine if wages are related to SME failure. They found it can be both positively or negatively related, depending on the businesses motivations. The researchers found that when used to build human capital and retain talent, SMEs were more likely to survive.

Goodwin	Contingency planning; SMEs failing to plan for business continuity risks, survey shows.	2005	Discusses how many businesses have no business continuity plans in place but would also be materially affected if staff were unable to come into work.
Goucher	Do SMEs have the right attitude to security? Computer Fraud & Security	2011	Goucher shows that for SMEs without compliance requirements, Information Security spending is low. Suggests these SMEs should still improve security posture to maintain reputation.
Gupta, Barzotto & Khorasgani	Does size matter in predicting SMEs failure?	2018	The researchers use financial variables to predict the likelihood of either financial distress or failure (bankruptcy). They found that Micro and Small firms fall within typical estimates,

			EBITDATA and cash flow have negative effects on the probability of financial distress. However, the coefficients were different between each size category and cannot be attributed to SMEs as a whole.
Heidt, Gerlach, & Buxmann	Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments	2019	In-person interview process with SME leaders suggests that SMEs may be aware of information security risks. However, they do not believe they have the resources to accomplish their goals.
Henson & Garfield	What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security?	2016	Another research group showing that SMEs had positive attitudes towards Information Security, but did not want to spend

			money on improving it. Suggest misinformation may play a large role in lack of investment.
Kaila	Information Security Best Practices: First Steps for Startups and SMEs	2018	Kaila develops a new lightweight framework for SMEs beginning investment in Information Security. They make suggestions such as using MFA, ensuring SaaS products have security agreements, and to have a business continuity plan.
Khan, Tanwar, & Rana	The Need for Information Security Management for SMEs	2020	The research team provides unique recommendations specifically to HR departments of SMEs, such as creating and enforcing non-disclosure agreements. They also suggest training

			on how to mitigate phishing attacks since their departments contain all employee's PII.
Kim & Amran	Factors Leading to the Adoption of Business Continuity Management (BCM) in Malaysia	2018	Kim and Amran make several conclusions on Business Continuity Management (BCM) adoption. They note that the complexity can be difficult to adopt for SMEs since it can require large human capital investment. They suggest that the larger an enterprise gets, the more they will benefit from BCM.
Kosmidis & Stavropoulos	Corporate failure diagnosis in SMEs: A longitudinal analysis on alternative prediction methods	2014	Full text unavailable. Researchers suggest that human capital plays a much larger role in the

			viability of SMEs compared to large corporations.
Lucey	Why traditional business continuity thinking does not work for SMEs: A new approach for managers and their advisers	2006	Lucey develops a novel methodology for implementing a Business Continuity Plan (BCP). They lay out a linear project strategy more suitable for SMEs due to decreased time investment.
Lucey & Lyons	Corporate Defense Insights. Dispatches from the Front Line	2009	Question and Answer session between the two authors. Lucey describes many methods SMEs can utilize to become more resilient. These methods include redundant systems, fault tolerance, load balancing. They note, like others, that the biggest challenges to business are

			knowledge, skills and budgets.
Merchant, Kumar & Malik	Factors Influencing Family Business Continuity in Indian Small and Medium Enterprises (SMEs)	2018	The researchers focus uniquely on family-owned businesses in India. They focus on succession planning, and how to grow an SME beyond family limits.
Milošević, Mihajlović & Stojanović	Dominant factors of SMEs failure: Multigroup confirmatory factor analysis	2019	The researchers classify external and internal factors affecting the financial distress and business failure of SMEs. The major internal weakness was lack of capital. As external factors, they found an unpredictable business environment and lack of institutional protection to play the largest roles.

Mohamed	DevOps Shifting Software Engineering Strategy – Value Based Perspective	2015	Mohamed develops a model of how to evaluate the success of DevOps practices within an SME. This success is measured by the maturity of communication, automation, governance, and quality. They suggest the main value of DevOps is to bridge gaps between teams that otherwise work in silos.
Nilaykumar & Balakrishnan	Cyber Security Scenarios and Control for Small and Medium Enterprises	2012	The researchers create a list of common Information Security vulnerabilities found within SMEs and the controls for proper mitigation. They cover issues such as phishing, SQL Injection, XSS, Insider

			Attacks, and Wireless Network Breaches.
Pérez-González, Preciado & Solana-Gonzalez	Organizational practices as antecedents of the information security management performance	2019	The researchers focus on the political and organizational aspects of an SME. They suggest that contracting Information Security will harm the development of a security culture. Conversely, making security decisions and activities public to all employees will benefit the culture.
Schalck & Yankol-Schalck	Predicting French SME failures: new evidence from machine learning techniques	2021	The researchers applied several estimation methods to French SME data consisting of financial and nonfinancial variables. They find that self ownership is the highest correlation to failure, with

			the second being related to the region of operation. This means that both financial and environmental variables play a role in business success.
Wedawatta & Ingirige	A conceptual framework for understanding resilience of construction SMEs to extreme weather events	2016	The researchers discuss the predictability and effects of extreme weather events (EWEs), particularly in the UK. They focus on how EWEs affect issues beyond the SMEs typical geographic boundaries, affecting supply chains and the construction process as a whole.
Williams	Resources and Business Failure in SMEs: Does Size Matter?	2014	The study uses a large dataset of UK based SMEs to determine business failure factors among SME size classifications. They

			found that industry sector did not have a large impact on failure for small or medium businesses and must compete equally. However, revenue plays a larger role for Small Enterprise survival as opposed to medium size enterprises. This indicates that at a certain size, they needed to organize more effectively and utilize the resources to their advantage.
Youssef, Mohamed & Abdeslam	Determinants and Predictors of SMEs' Financial Failure: A Logistic Regression Approach	2020	The researchers analyze a subset of SMEs that were customers of a Moroccan bank. They found that three years out, seven variables can identify sound and failing SMEs: autonomy

			ratio, repayment capacity, interest to sales, return on assets, asset turnover, days in accounts receivable, and duration of trade payables. Two years out, only five of the variables were needed to discriminate. In general, failing SMEs have higher debt and low profitability.

REFERENCES

Abazi, B. (2018). An approach to Information Security for SMEs based on the Resource-Based View theory. *International Journal of Business & Technology*, *6*(3), 1–5. https://doi.org/10.33107/ijbte.2018.6.3.06

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, 23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Asti, A. (2017). Cyber Defense Challenges from the Small and Medium-Sized Business Perspective. SANS Library Whitepaper. https://sansorg.egnyte.com/dl/ab0OXRBfck/?

Barlette, Y., & Jaouen, A. (2019). Information security in SMEs: determinants of CEOs' protective and supportive behaviors. *Systèmes d'information & management, 24*(3), 7–40. https://doi.org/10.3917/sim.193.0007

Briggs, Z. (2020, January 3). *Shuttering telemarketing company hit by "cyber attack" wishes employees "Happy New Year."* KATV. https://katv.com/news/local/shuttering-telemarketing-company-hit-by-cyber-attack-wishes-employees-happy-new-year

Brooks, H. (2020, January 2). T*he Heritage Company still closed and fighting cyber attack.* Fox 16. https://www.fox16.com/news/local-news/the-heritage-company-still-closed-and-fighting-cyber-attack/

Burhan, M., Salam, M. T., Hamdan, O. A., & Tariq, H. (2021). Crisis management in the hospitality sector SMEs in Pakistan during COVID-19. International *Journal of Hospitality Management, 98*. https://doi.org/10.1016/j.ijhm.2021.103037

Chandler, G. N., & Mcevoy, G. M. (2000). Human Resource Management, TQM, and Firm Performance in Small and Medium-Size Enterprises. *Entrepreneurship Theory and Practice, 25*(1), 43–58. https://doi.org/10.1177/104225870002500105

Cimpanu, C. (2020, January 3). Company shuts down because of ransomware, leaves 300 without jobs just before the holidays. *ZDNet.* https://www.zdnet.com/article/company-shuts-down-because-of-ransomware-leaves-300-without-jobs-just-before-holidays/

Coveware, Inc. (2021). Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound. https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

Cyber Incident Notification Act of 2021 (2021). https://www.warner.senate.gov/public/_cache/files/4/2/422a0de2-3c56-4e56-a4be-0e83af5b0065/F90B3C493BA4FAB09E546FAF40E4B116.alb21b95.pdf

Desjardins, J. (2017, August 2). Here's why small businesses fail. Business Insider. https://www.businessinsider.com/why-small-businesses-fail-infographic-2017-8?international=true&r=US&IR=T

Dewaelheyns, Van Hulle, C., Van Landuyt, Y., & Verreydt, M. (2021). Labor Contracts, Wages and SME Failure. *Sustainability (Basel, Switzerland), 13*(14), 7864–. https://doi.org/10.3390/su13147864

European Commision. (2019). *Small and medium-sized enterprises: an overview*. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20191125-1

Federal Reserve Banks. (2020). *2020 Report On Employer Firms. Small Business Credit Survey.* https://www.fedsmallbusiness.org/medialibrary/FedSmallBusiness/files/2020/2020-sbcs-employer-firms-report

Goodwin, B. (2005, September 29). *Business continuity warning for SMEs*. ComputerWeekly.Com. https://www.computerweekly.com/news/2240075329/Business-continuity-warning-for-SMEs

Goucher, W. (2011). Do SMEs have the right attitude to security? *Computer Fraud & Security, 2011*(7), 18–20. https://doi.org/10.1016/S1361-3723(11)70075-6

Gupta, J., Barzotto, M., & Khorasgani, A. (2018). Does size matter in predicting SMEs failure? *International Journal of Finance and Economics, 23*(4), 571–605. https://doi.org/10.1002/ijfe.1638

Hagen, J. (2002, December 13). Top Reasons Why Businesses Fail. Fox Cities SCORE. https://web.archive.org/web/20030711152742/http://www.foxcitiesbusiness.com/score/whybusinessesfail.htm

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers, 21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Henson, R., & Garfield, J. (2016). What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security? *Athens Journal of Business & Economics, 2*(3), 303–317. https://doi.org/10.30958/ajbe.2-3-5

IBM Security. (2020). *Cost of a Data Breach Report 2020.* https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

Igbaria, M., & Greenhaus, J. (1992). Determinants of MIS employees' turnover intentions: a structural equation model. *Communications of the ACM, 35*(2), 34–49. https://doi.org/10.1145/129630.129631

Innovation, Science and Economic Development Canada. (2020). *Key Small Business Statistics – 2020.* Retrieved from https://www.ic.gc.ca/eic/site/061.nsf/eng/h_03126.html

ISACA. (2019). *State of Cybersecurity 2019, Part 2: Current Trends in Attacks, Awareness and Governance.* https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619

John M. Pfau Library. (2021). OneSearch User's Guide: Introduction. Retrieved on September 20, 2021 from CSUSB: https://libguides.csusb.edu/onesearch.

Kaila, U. (2018). Information Security Best Practices: First Steps for Startups and SMEs. *Technology Innovation Management Review, 8*(11), 32–42. https://doi.org/10.22215/timreview/1198

Kaukola, J., Ruohonen, J., Tuomisto, A., Hyrynsalmi, S., & Leppänen, V. (2017). Tightroping between APT and BCI in small enterprises. *Information and Computer Security, 25*(3), 226–239. https://doi.org/10.1108/ICS-07-2016-0047

Keeper Security, Inc. (2019). *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses.* https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf

Kenner, B. T. (2019). Too Agile? - DevOps Software Development Challenges in a Military Environment. ProQuest Dissertations Publishing.

Khan, M. I., Tanwar, S., & Rana, A. (2020). The Need for Information Security Management for SMEs. *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 328–332. https://doi.org/10.1109/SMART50582.2020.9337108

Kim, L. L., & Amran, A. (2018). Factors Leading to the Adoption of Business Continuity Management (BCM) in Malaysia. *Global Business and Management Research, 10*(1), 179–196.

Kosmidis, & Stavropoulos, A. (2014). Corporate failure diagnosis in SMEs: A longitudinal analysis based on alternative prediction models. *International Journal of Accounting and Information Management, 22*(1), 49–67. https://doi.org/10.1108/IJAIM-01-2013-0001

Lohrmann, D. (2021, January 21). 2020 Data Breaches Point to Cybersecurity Trends for 2021. *Government Technology.* https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-data-breaches-point-to-cybersecurity-trends-for-2021.html

Lim, A. (2019). *Applying Multi-disciplinary Systems Engineering (SE) Approach to Minimizing Information System (IS) Vulnerabilities*. ProQuest Dissertations Publishing.

Lucey, K. A. (2006). Why traditional business continuity thinking does not work for SMEs: A new approach for managers and their advisers. *Journal of Business Continuity & Emergency Planning, 1*(1), 65–79.

Lucey, K., Lyons, S. (2009). Corporate Defense Insights. Dispatches from the Front Line. p. 52 Retrieved from https://www.continuitycentral.com/seanlyons.pdf

Merchant, P., Kumar, A., & Mallik, D. (2018). Factors Influencing Family Business Continuity in Indian Small and Medium Enterprises (SMEs). *Journal of Family and Economic Issues, 39*(2), 177–190. https://doi.org/10.1007/s10834-017-9562-3

Milošević, Mihajlović, I., & Stojanović, A. (2019). Dominant factors of SMEs failure: Multigroup confirmatory factor analysis. *Serbian Journal of Management, 14*(2), 345–360. https://doi.org/10.5937/sjm14-23536

Mishra, & Otaiwi, Z. (2020). DevOps and software quality: A systematic mapping. *Computer Science Review, 38*. https://doi.org/10.1016/j.cosrev.2020.100308

Mohamed, S. I. (2015). DevOps Shifting Software Engineering Strategy – Value Based Perspective. *IOSR Journal of Computer Engineering. Volume 17, Issue 2*. Version IV, 51-57

Nilaykumar K. S., Balakrishnan, V. (2012). Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informatica Economica, 16*(2), 58–71.

O'Donnell, L. (2020, January 3). Ransomware Attack Topples Telemarketing Firm, Leaving Hundreds Jobless. Threatpost. https://threatpost.com/ransomware-attack-topples-telemarketing-firm/151530/

OECD. (2017). *Entrepreneurship at a Glance 2017.* Retrieved from https://www.oecd-ilibrary.org/docserver/entrepreneur_aag-2017-en.pdf

Ozgen, E., & Baron, R. A. (2007). Social sources of information in opportunity recognition: Effects of mentors, industry networks, and professional forums. *Journal of Business Venturing, 22*(2), 174–192. https://doi.org/10.1016/j.jbusvent.2005.12.001

Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. (1C.E.). Organizational practices as antecedents of the information security management performance. *Information Technology & People (West Linn, Or.), 32*(5), 1262–1275. https://doi.org/10.1108/ITP-06-2018-0261

Saban, K. A., Rau, S., & Wood, C. A. (2021). SME executives' perceptions and the information security preparedness model. *Information & Computer Security*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ICS-01-2020-0014

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security, 28*(3), 467–483. https://doi.org/10.1108/ICS-01-2019-0010

Schalck, & Yankol-Schalck, M. (2021). Predicting French SME failures: new evidence from machine learning techniques. *Applied Economics, 53*(51), 5948–5963. https://doi.org/10.1080/00036846.2021.1934389

Securities and Exchange Commission. (2018, February 26). *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* [Press Release]. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Servicenow. (2020). *Costs and Consequences of Gaps in Vulnerability Response.* https://media.bitpipe.com/io_15x/io_152272/item_2184126/ponemon-state-of-vulnerability-response-.pdf

Small Business Administration. (2019). *Table of Size Standards*. Retrieved from https://www.sba.gov/document/support--table-size-standards

Symantec. (2014). *Internet Security Threat Report 2014. Volume 19.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf

Symantec. (2015). *Attackers Target Both Large and Small Businesses.* https://docs.broadcom.com/doc/istr-attackers-strike-large-business-en

United States Census Bureau. (2016). *Annual Survey of Entrepreneurs (ASE) - Company Summary: 2016 Tables. Sector, Gender, Ethnicity, Race, Veteran Status, and Employment Size of Firm*. Retrieved from https://www.census.gov/data/tables/2016/econ/ase/allcompanytables.html

Wedawatta, G., & Ingirige, B. (2016). A conceptual framework for understanding resilience of construction SMEs to extreme weather events. *Built*

Environment Project and Asset Management, 6(4), 428–443. https://doi.org/10.1108/BEPAM-06-2015-0023

Williams, D. A. (2014). Resources and Business Failure in SMEs: Does Size Matter? *Journal of Business and Management, 20*(2), 89–. https://doi.org/10.6347/JBM.201407_20(2).0005

Wilshire Advisors LLC. (2021). *Wilshire Index Fact Sheet. https://assets-global.website-files.com/60f8038183eb84c40e8c14e9/6132007be5f0a49e7a5f652a_ft-wilshire-5000-fact-sheet.pdf*

Yitbarek, S. (Host). (2018, February 13). DevOps_Tear Down That Wall (No. 4) [Audio podcast episode]. In *Command Line Heroes.* Red Hat, Inc. https://www.redhat.com/en/command-line-heroes/season-1/devops-tear-down-that-wall

Youssef, Z., Mohamed, O., & Abdeslam, E. M. (2020). Determinants and Predictors of SMEs' Financial Failure: A Logistic Regression Approach. *Risks (Basel), 8*(107), 107–. https://doi.org/10.3390/risks8040107