Cybersecurity Failures of Small and Medium-Sized Businesses: Circumventing Leadership Failure

by

Paul Dent

A Capstone Project Submitted to the Faculty of

Utica College

August 2021

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

Cybersecurity is a rapidly changing field that challenges many businesses to keep up. This failure to keep up with rapid cybersecurity changes is even more true in the small and medium enterprises (SME) that comprise a significant portion of employment domestically. With SMEs' failing to implement cybersecurity strategies they will continually remain at risk. There are several factors that influence cybersecurity planning, including technology, processes, and people. This research found that many SMEs have limited technology and staffing resources to stay ahead of the evolution of cyber-attacks and the tools and techniques to combat these threats. This lack of technology and resources is often due to the lack of funding to implement these technologies and a severe shortage of qualified cybersecurity-trained individuals. The research found that cybersecurity is not an area that is easily quantified, and, in turn, the leaders of SMEs do not invest in it. The research also showed that these leaders need to change their perception on cybersecurity, which will allow them to prioritize its significance in their business. Future research is recommended on SMEs' use of technology, understanding of cybersecurity, culture, and leadership to better understand the gaps leading to failures of SMEs to create cybersecurity strategies.

Keywords: Cybersecurity, Doctor Donnie Wendt, small business cybersecurity, SME cybersecurity, organizational culture

Acknowledgments

Firstly, I would like to thank my wife, Heidi, who encouraged me to take on this program. The timing was great as it was just before the pandemic began; it gave me something to learn, focus on and keep busy during this awful time in all our lives. To Alex and Kirby for listening to all my cliché cyber jokes and starting a sentence with “As a cybersecurity professional…”. I also want to thank all the professors who made the classes very interesting, which made me want to stick with the program. Finally, Dr. Donnie Wendt who had to deal with my writing software that did not track changes and migrating to Word, to helping me write more scholarly, as it has been 30 years since college and APA was not something used in my major.

Table of Contents

Statement of Problem

Cybersecurity is an important aspect of business in today's global environment for organizations of all sizes. Large organizations continue to make media headlines as the consequences of cyber breaches tend to significantly impact a larger population. Attacks aimed at exploiting vulnerabilities existing in information systems, including critical infrastructures, have increased. These vulnerabilities have led the attack landscape to include strategic industries, such as utilities, healthcare, transportation, and the financial sector (Lopez et al., 2020). These large-scale attacks have been well-publicized in the last few months with Colonial Pipeline and JBS Meatpacking (Ikeda, 2021). The recent attacks led the Mid-Atlantic region of the United States to panic at the gas pumps and caused a temporary disruption to the meat supply chain. In addition, the cyberattacks had significant financial impacts; the organizations paid $4 million and $10 million in ransom, respectively (Ikeda, 2021). While large enterprises and government institutions make the headlines, small businesses are not exempt from cyber risk.

According to a U.S. Small Business Administration Office of Advocacy report (SBA, 2020), 31.7 million small businesses represent 99.9% of United States businesses. Attacks on small and medium enterprises (SMEs) happen exponentially more often and at a higher rate than more prominent organizations that make the national news (Aguilar, 2015; Verizon, 2021). In a data breach, SMEs are conceivably at a higher risk than large enterprises (Selzinck & LaMacchia, 2018). Most small and medium enterprises operate with minimum personnel, capital, and reserves and focus on technology funding for operational and marketing purposes (Thrive Analytics, 2020). However, a lack of resources for cybersecurity measures does not excuse the SMEs' responsibility to protect their customer and employee data. The cost of cybersecurity failures can result in the demise of SMEs (Selzinck & LaMacchia, 2018).

Nevertheless, SME leadership continues to ignore cybersecurity as a priority and misunderstand their risk exposure.

SMEs face many challenges to ensure their information is secure as they collect, process, and store sensitive information (Talu, 2020). Without the proper security protocols and technology in place, sensitive information can become compromised. Enterprises of all sizes could face severe adverse economic outcomes due to compromised data (Talu, 2020). In addition, cyber weakness, lack of national relevance, and economic impact make SMEs appropriate targets that will not send up a national alarm (Lopez et al., 2020).

The lean operations of small businesses provide increased exposure. An SME attack aims to disturb or interrupt the SME's basic structure, having a considerable impact on the entity and the continuity of business service that are sometimes essential (Lopez et al., 2020). In fact, oftentimes, SME cyber-attacks offer criminals an opportunity with minimum threat. These attacks are well-studied actions that offer a significant benefit with low risk for the criminals due to their international nature, adaptability, mobility, and opacity (Lopez et al., 2020). The availability and accessibility of technology have grown exponentially over the last few decades, creating increased opportunities and challenges for SMEs.

Technology and Small Business

The use of the internet and internet-connected devices or the Internet of Things (IoT) has become a proven necessity for all businesses to keep up with the competition. The Fourth Industrial Revolution (4IR) has led to an overwhelming increase in the utilization of technology, including robotics, artificial intelligence (AI), the IoT, and augmented reality (AR) (World Economic Forum, 2020). Because of the tremendous increase in internet and internet-connected device usage, businesses are more susceptible to cyberattacks than ever before. When a business becomes more dependent on the internet, the potential for a cyberattack increases exponentially to the business (Radanliev et al., 2020). The increased exposure presents challenges for SMEs because of their need to locate and connect with their customers online. The internet functions as a bridge for businesses to understand their customers, develop new products and compete in new markets or segments.

SMEs can leverage the internet to reach additional and larger markets and communicate globally to their clients, vendors, and employees. This accessibility helps SMEs to grow, compete globally, and enter the market agilely. Furthermore, continual advances in technology will allow for more efficient work (Gafni & Pavel, 2019). SMEs use the internet and computer-based tools in daily routines, often without being attuned to the cyber threats, and may lack preparation in the advent of a cyberattack (Gafni & Pavel, 2019). The developers of applications and devices have not, for the most part, moved to *security-by-design*, which is integrating cybersecurity technologies and design during the development process (World Economic Forum, 2020). As a result, cybersecurity is typically an afterthought as it may slow down the development and, ultimately, delivery of products to market. The knowledge and resources needed for cybersecurity and cyberattack plan development may not be readily available, or the SME leadership may not know where to find resources to help them plan (Gafni & Pavel, 2019).

Unlike their larger counterparts, SMEs differ in their approach to and use of information technology, creating additional exposure to cyber risk. Many SMEs use basic information systems and do not require robust information systems, have limited resources and human capital, and rarely have an information technology (IT) department or an IT support analyst for basic technology needs (Lopez-Nicolas & Soto-Acosta, 2010)**.** The assumption is that SMEs are not alert and are potentially unprepared to handle cyber-attacks (Gafni & Pavel, 2019). There are many daily technology tools that provide cyber concerns that SMEs must be aware of, such as maintaining a website, migrating to cloud computing, using e-commerce, or simply sending and receiving emails. While migrating to cloud computing presents cyber concerns, research suggests that SMEs should be migrating to the cloud as a cyber-hacking preventative measure (Hamdar, 2021; Saber, 2016). When researching and implementing technology tools, leadership should use caution to mitigate potential opportunities for a possible cyber-attack. Unfortunately, the increase in internet activity has gained the attention of old school (Mafia) criminal organizations, which have created new stealthy groups of cybercriminals (Bhattacharya, 2015). Therefore, SMEs using the internet and information systems in their business must prioritize cybersecurity procedures as cyber criminals continue to grow.

According to Verizon Enterprise (2018), SMEs were targeted by over 50% of all cyberattacks, while Moschovitis (2018) found that 43% of cyberattacks targeted SMEs. According to the 2019 National Small Business Association (NSBA) survey, there is an advanced risk for SMEs becoming victims of cyber-crime. The survey determined that 35% of SMEs admitted to being a victim of a cyber-attack (National Small Business Association, 2019). According to HISCOX Insurance, the cost of an attack on an SME averages $25,612 (HISCOX, 2021). Many SMEs are challenged with cash flow management; adding additional financial exposure can be fatal. The motivations of hackers are not always financially based; some hackers attack based on revenge or for fun. Small businesses are often considered soft targets that can provide the attacker money, information, revenge, or a potential portal to access and attack a larger company (Paulsen & Toth, 2016). SMEs need to understand cybersecurity and the potential impact for their organization to prioritize and plan effectively.

Cybersecurity in SMEs

A recent SBA survey found that 88% of small business owners felt their business was susceptible to a cyberattack (SBA, 2021). Businesses that have faced an attack face an uncertain future as 60% go out of business within six months of the attack (Moschovitis 2018). Unfortunately, many of these businesses are unable to cover the expense of professional IT solutions or personnel. Additionally, they have a perceived limited amount of time to devote to cybersecurity, and more importantly, they do not know where to begin (SBA, 2021). Compared to large organizations, the ambiguity of not knowing where to begin leads SMEs to go longer before realizing they have been hacked (Verizon 2021).

During the past year, many SMEs shifted their working environments from the office to the home. With the lack of knowledge and technical expertise, 2020 became a record year for credential thefts by cybercriminals. According to Verizon (2021), phishing increased by 11% and ransomware by 6%. The main entry points became accessible through social engineering, and 61% of data breaches were due to credential theft (Verizon 2021). A significant void exists with the level of experience regarding cybersecurity and the amount of relevant cybersecurity information the SME executive leadership has. This limited amount of information awareness limits informed decision-making regarding cybersecurity (Cleveland & Cleveland, 2018).

Organizational Culture

Leadership drives decision-making and organizational culture. Strategic decision-making is set by organizational leadership and drives the tactics needed for executing strategy. Small and medium enterprises are increasingly turning to technology for operational and sales support (Thrive Analytics, 2020). A small business leaders' lack of IT knowledge is a proven predictor of adopting IT, which can influence prioritization (Rohn et al., 2016). SMEs that use the internet and internet-connected technology often lack a culture prioritizing security that will enhance business and consumer confidence (Moschovitis, 2018). Organizations effectively communicating the customer value leads to increase perceived quality and positive awareness and reinforcement of the brand, helping the company to build brand equity (Aaker, 2009). A culture focused on cybersecurity and protecting consumer and employee data helps to boost confidence. This boost in confidence can help SMEs build a positive brand reputation helping them to create stronger brand equity with their customers and survive a data breach (Kshetri, Voas, Kshetri, & Voas, 2018). A cybersecurity culture is achievable by hiring the right people and providing ongoing training. The tools and cybersecurity knowledge necessary for SMEs' leaders, managers, and decision-makers to manage cyber threats may not be easily found or accessible through known avenues (Gafni & Pavel, 2019). Few organizations can validate their cybersecurity culture when tested (Paulsen, 2016). The information typically available to the public is related to significant corporate cyberattacks or complex systems not used by SMEs (Gafni & Pavel, 2019). This lack of technical knowledge, tools, and accessible information can adversely impact SME owners' prioritization of cybersecurity. Understanding the influence of a cybersecurity culture on consumer brand perception may also help SME owners' prioritization of cybersecurity planning.

Hiring the right people and providing ongoing training is an important part of building a cybersecurity culture. Organizations of all sizes require executive oversight of technology tools and processes. SMEs with limited resources are often unable to hire a chief information security officer (CISO). With a shortage of at least 2 million trained employees in the cybersecurity field, finding an employee with even a minimum amount of cybersecurity knowledge is a challenge. A staffed position responsible for cybersecurity is needed to protect a company effectively.

Without a CISO, a cybersecurity program is at risk of never getting off the ground. The role must have the power and authority to assemble the required resources to allow an information security program to succeed while considering the variety of factors that can negatively impact the program's implementation (Cleveland & Cleveland, 2018). A difficult challenge for SMEs, which are already lean organizations, is that they will typically lack a cybersecurity leader. The absence of a cybersecurity leader makes it increasingly difficult for SMEs to understand the technical aspects, have the business skills, steadfastness, and team-building skills needed for proper planning (Cleveland & Cleveland, 2018). Additionally, SMEs that do not have a leader focused on cybersecurity are challenged with seeing relevant cyber threats in the media, which will motivate their prioritization of security programs, time, and capital required for effective prevention. Conversely, SMEs that have a cybersecurity culture, with their organizational creativity, flexibility, and adaptability, can change the landscape of cybersecurity (Paulsen, 2016). By adopting a cybersecurity culture and leadership focused on cybersecurity, SMEs can create a competitive advantage over larger organizations. Unfortunately, most SME leadership perceptions about cybersecurity limit this opportunity.

One of the glaring issues with SMEs is the culture of the business, the lack of one, or the potential that the leaders do not know what their culture is (Moschovitis, 2018). Many SMEs have the mindset of growth at all costs. The singular focus on a growth mindset many times results in the leadership neglecting or forgetting other business priorities, especially when it comes to cybersecurity (Moschovitis, 2018). Many SMEs do not have their organization in alignment with technology and business operations. A lack of proactive security culture is a common denominator in SMEs and hinders alignment. Many studies have highlighted multiple examples where leadership is failing regarding cybersecurity practices (Benz et al., 2020;

Moschovitis, 2018; Paulsen, 2016; Sweeney, 2016). To create a cybersecurity-driven organization, SME leadership needs to focus on the attitudes, assumptions, beliefs, and values of their employees (Da Viega, 2016) and align with security goals (Huang & Pearlson, 2019).

Perceptions and Priorities

According to the Small Business Administration (SBA) (2018), there are over 30,000,000 SMEs that comprise almost half (47.5%) of the workforce and economic input (43.5%) into the overall economy of the United States. Representing a significant portion of economic input, SMEs, like large corporations, need to protect their intellectual property, client information, and finances from cyber criminals. SMEs are falling behind in their effort to combat cyberattacks. SMEs lack emphasis on protecting their data and systems through cybersecurity methods and tactics. Sixty percent of all targeted cyberattacks in 2014 (Aguilar, 2015) and 56% in 2020 (Verizon, 2021) were focused on SMEs. SME technology leaders are concerned about IT disruption (Martins, 2020). The statistics highlight the need for SME leadership to prioritize cybersecurity.

The lack of prioritization by leaders may cause confusion and lack of direction related to cybersecurity needs. While cybersecurity is one of the most critical challenges for all SMEs in today's technical arena, today's executive leadership face challenges that prior leaders did not (Cleveland & Cleveland, 2018). Many SMEs do not have information technology or cybersecurity teams. However, whether publicly traded, privately held, large or small, size does not alleviate the potential cyber risk.

Purpose Statement

The purpose of this research was to investigate leadership failure to implement cybersecurity plans and policies in small and medium enterprises. This research evaluated why

SME leadership has not prioritized cybersecurity plans and assessed tactics to increase adaptation and incorporate a cybersecurity strategy. This research aims to encourage SME owners and leadership to prioritize cybersecurity and outline a framework to create and maintain a cybersecurity plan and implement technology solutions to help thwart potential cyberattacks.

Research Questions

1. How does small and medium enterprises (SMEs) leadership define cybersecurity and its role in day-to-day operations?
2. How does business culture influence the outcome of a cybersecurity strategy and the implementation tactics required?
3. What communication strategies and tactics are needed to increase awareness and urgency for leadership to implement cybersecurity measures?

Literature Review

This research evaluates the struggle that SMEs face with cybersecurity. This paper looks explicitly at organizational culture and leadership failures that prevent SMEs from implementing effective cybersecurity protocols. The first part of this chapter looks at how technology is used in SMEs and what is the overall outlook with technology implementation. The second section defines cybersecurity and details how the government and the private sector define cybersecurity. This section also looks at the impact cybersecurity plays on an SME. The third section looks at the vital role organizational culture plays in a successful cybersecurity program within SMEs. The leadership of SMEs sets the culture and strategy of the business, and they are the ones who drive the adoption of programs in their organization (Reynolds et al., 2020). The type of personalities and traits the leaders possess are essential factors for success. The final section looks at the perceptions and priorities inside the SME. The prioritization of strategies and tactics has significant impacts on the sustainability of the firm.

Technology and Small Business

Consumers lead digital lives and expect to interact with businesses through technology. Therefore, integrating technology in business operations is no longer a competitive advantage; it is an essential business function. The accessibility and advancement of technology have enabled SMEs to compete by leveraging technology. The affordable cost and freemium versions of digital technology offer SMEs the ability to access new markets and target new customers relatively economically. Technology opens new markets and new prospective employees for small and medium businesses with less than 1,000 employees, providing a greater opportunity to compete. Deloitte (2019) found that small businesses with high engagement with technology experienced four times the revenue growth of those that did not. Continual advances in technology will allow for more efficient work (Gafni & Pavel, 2019).

An International Data Corporation (IDC) (2020) report forecasted technology spending by SMEs to reach $100 billion annually in 2021. The report covered nine regions, 53 countries, 40 technologies, and four company size segments ranging from 1 to 999 employees. SME spending encompasses hardware, software, and IT services, with a continual pattern of growth. In addition, SME executives continue to expand into cloud-based services, according to the report, with 62% confirming that they currently use cloud-based services. The SME leader's rationale included accessibility, increased security, and reliability.

Increasingly, small-business owners rely on technology to start and scale their businesses. Technology plays an essential role in running a small or medium enterprise, including leveraging human capital, managing finances, and optimizing the supply chain. When it comes to leveraging human capital, according to the U.S. Chamber of Commerce (2018), 62% of small businesses surveyed rated digital and social media skills as more important than education when hiring. Additionally, 84% utilized at least one digital platform to provide information to their customers. Recent research by Thrive Analytics (2020) found that 35% of US small businesses plan to increase their technology budgets in the next year. The motivation of these organizations included time savings and cost reduction. While organizations are increasingly investing and using technology, it presents significant opportunities and challenges for SME executives.

Organizationally, SME executives are the decision-makers when it comes to capital investments. A small business owner's independent decision-making may simplify and accelerate decision-making. A leader's attitude toward technology correlates with the adoption of technology in a company. SME leaders are used to making their own decisions and may not seek the counsel of outside board members (Woods et al., 2012). However, their access to decision-making information from business associations correlates to an increased willingness to adopt new technologies. While seeking outside counsel may correlate with an increased willingness to utilize new technologies, other factors may suppress that willingness. The propensity to introduce status quo bias (i.e., preference for maintenance of existing resources) may increase important decision-making arenas, such as investment in new technology for business operations (Woods et al., 2017).

The benefits of technology adoption outweigh the risks. Entrepreneurship and technology readiness traits correlate with technology adoption (Reynolds et al., 2020). Research has found that SME executives can improve company performance by integrating company processes supporting IT and remaining involved in implementing a cloud-based enterprise resource planning (ERP) solution (Hamdar, 2021). Executives that have incorporated technology in planning and business management have improved business performance and are empowered to expand to more areas and countries (Kiradoo, 2021).

Many SMEs use basic information systems and do not require or desire robust information systems. Small firms typically are at an advantage because of their ability to be agile in the market due to their lean operational structure. Competitive strengths created from the ability to be flexible in responding to the market can also create a weakness. SMEs are challenged with limited resources and human capital and rarely have an IT department or an IT support analyst for basic technology needs (Lopez-Nicolas & Soto-Acosta, 2010). Leadership and organizational culture are important for technology usage in an SME.

Increasingly SME executives are exhibiting more technology-driven leadership styles.

Seventy-seven percent of US small business owners are regular technology users for personal reasons, such as online shopping or consuming digital media (Deloitte, 2018). Forty-one percent of SME executives expect to increase technology spending, with a specific concentration on the Internet of Things (IoT) and mobile payment systems (Martins, 2020). SME executives, through technology, can advance their digital skills and comprehension of the effective use of digital channels for customer engagement. SMEs that have computer-savvy leadership influence the amount of digital engagement of the organization. SME leaders that prioritize technology adoption expect the benefits of increased sales. While growth is a high priority for SME executives, surprisingly, improved communications, flexibility, and lower business costs are lower priorities for technology adoption (Deloitte, 2018). SME leadership priorities offer an important contribution to organizational technology adoption and usage.

Even with this growing technology adoption in SMEs, the adoption of cybersecurity technology is not as widespread. Cybersecurity is not a priority for many SME leaders (Benz & Chatterjee, 2020). Few leaders can comprehend the threats and do not see their business as a target. Leadership does not consider security-related activities and technology to add any tangible value to the bottom line (Benz et al., 2020). These leaders trying to understand what security technology is available to their organization and is affordable is like them trying to understand a foreign language. Even if they can understand what technology to purchase, such as firewalls, intrusion detection systems, and intrusion preventions, they will need to find the resources to implement them (Kaila & Nyman, 2018). These challenges add to the lack of understanding of the definition of cybersecurity, and how it can be applied to their business is a challenge (Kaila et al., 2018).

There is a large array of hardware and software technology that an SME can implement on their network to help protect them from a cyberattack. These cyber protection solutions include firewalls, intrusion detection systems, and tokens for authentication. These devices and software applications play a significant role in protecting companies from attacks. Unfortunately, most of these items are not easily installed and configurable to work effectively on the organization’s network. Without the appropriate staff to configure the firewall, route the network traffic flow, and implement a trustworthy design, the firewall is not of much use (Pfleeger & Pfleeger, 2012). The use of malware and antivirus software, on the other hand, is relatively easy to install and use right out of the box. SMEs may not realize that these applications can play a pivotal role in their initiation of a cybersecurity plan. The lack of understanding of what cybersecurity entails presents additional challenges for SMEs.

Cybersecurity Defined

Cybersecurity is a broad overarching term that can have many definitions. Cybersecurity is a rapidly developing field; research has monitored and evaluated scholarly and industry practices to successfully create new definitions (Craigen et al., 2014; Schatz et al., 2017). Cybersecurity includes protecting people, processes, and technologies through confidentiality, integrity, and availability (Craigen et al., 2014; Toth & Patterson, 2016). Craigen et al. (2014) defined cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems for occurrences that misalign de jure from de facto property rights." This definition involved practitioners, academics, and graduate students and is still fairly broad. The National Institute of Standards and Technology (NIST) further defined cybersecurity as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (Paulsen, 2016, p. 2). More recent research streamlined the definition to provide more clarity; "the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity, and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of cyber environment and its users" (Schatz et al., 2017, p. 66). As technology evolves and compounds, so does the definition of cybersecurity; "the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity, and availability of data and assets used in cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of cyber environment and its users" (Schatz & Wall, 2017, p. 66). Organizational culture, leadership, size, and industry can influence the perceptions and priorities of cybersecurity.

Cybersecurity impacts multiple departments organizationally, which may explain the broad definition. Without a clear definition, cybersecurity can cause organizational issues concerning strategies and objectives (Schatz et al., 2017). This lack of definition becomes more apparent in SMEs as they lack the resources to build definitions, plans, and ultimately a defense. The return on investment to many SME leaders is often unknown, and the lack of knowledge leads to the leader not implementing a strategy. Research suggests that cybersecurity incorporates technology, events, strategies, processes, procedures, human interactions, and security (Craigen et al., 2014). Cybersecurity as a field is advancing, often causing disagreements between the public and private sectors. There is a mixture of rules, regulations, and statutes regarding developing solutions to cyber-threat risks. For example, multiple federal, state, local, and private organizations are involved in some aspects of electric grid cybersecurity protection, regulation, or emergency response. These agencies include the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), NIST, Department of Homeland Security (DHS), Department of Energy (DOE), state public utility commissions, local utility boards, and others (Hébert, 2013). Smaller organizations tend to have the strain of small IT teams, and inadequate security budgets are frequently at a significant disadvantage in dealing with cyber threats effectively (Howard, 2018; Stasiak, 2018).

Organizational Culture

Leadership actions and organizational culture determine the involvement of humans, strategies, and processes. The failure of SMEs to recognize the cyber threats their businesses face is of great concern. Organizationally, it is no longer a competitive advantage to use technology but an essential part of conducting business. The more a business becomes dependent on the internet, the potential for a cyberattack increases exponentially (Radanliev et al., 2020). SMEs recognize the role technology plays in their sustainability. The assumption is that SMEs are not alert and are potentially unprepared to handle cyber-attacks (Gafni & Pavel, 2019). However, in a recent Insight study, 55% of small business owners feel that their current technology solutions are actually "a hindrance to incorporating or adopting new technologies." Most small business owners (65%) feel that IT disruption will influence their tech spending decisions. Close to 75% of technology influencers in SMEs are concerned about IT disruption (Martins, 2020). SMEs are encouraged to utilize cybersecurity frameworks so that executives have a better understanding of the firm’s overall security readiness, understand, and have a process implemented to evaluate their technology strategy on a consistent basis. The evaluation process recommends monitoring and evaluating the organization's cybersecurity culture and understanding that this process is constantly adapting and evolving to the rapidly changing technological environment (Georgiadou et al., 2020).

Leadership, culture, availability, accessibility, and communication of cybersecurity information present a fundamental gap between large and small enterprises. All organizations require leaders to achieve their goals and objectives and serve the expectations of their customers. Leadership is what drives the strategy and culture of an organization. Individuals focused on goal achievement through the influence of others can also be defined as leaders (Tubbs, 2006). Literature has identified a multitude of leadership styles, from micromanagement to servant leadership (Cleveland & Cleveland, 2018). As leadership styles influence the organization's success, they are influential in an organization's cybersecurity strategy and execution. The involvement of others beyond cybersecurity professionals in discussions around technology and cybersecurity will drive a cybersecurity culture (Huang & Pearlson, 2019). A leader focused on building a cybersecurity culture will prevent the haphazard execution of cyber training, communication, and performance management (Huang & Pearlson, 2019).

Technology adoption and, importantly, the adoption of cybersecurity within an SME typically falls on the owner or CEO. Executives and small business CEOs should examine their internal traits, which may increase the odds of technology adoption compared to external traits(Penz et al., 2017; Reynolds et al., 2020). The trait narcissism supports an environment for a technology-driven leader that is often strong with innovation speed, innovation novelty, and product safety performance (Kashmiri et al., 2017). There are considerable, although weak, effects of influences such as the CEO attitude, length in position, ability to innovate, and outside pressure on IT adoption (Hameed and Counsell, 2012). However, outside pressure (customers, competition, and direct industry growth) greatly influenced the leader’s and, ultimately, the SME’s adoption of technology (Reynolds et al., 2020). The two most significant traits needed for a technology-driven culture are entrepreneurial mindset and technology readiness (Reynolds et al., 2020). The entrepreneurial mindset leads to an entrepreneurial company. The entrepreneurial company engages in an innovating product or market segment, is dedicated to the business risk, and is at the forefront of showing innovation and a proactive mindset and aggressively competing (Penz et al., 2017). The leader's ability to take these sources of influence and apply them organizationally is crucial to cybersecurity adoption. The adoption of a cybersecurity culture, innovation, and dedication can help SME leaders to build a strong brand reputation which is beneficial for cybersecurity challenges (Kshetri, Voas, Kshetri, & Voas, 2018).

Cybersecurity is one of the most critical challenges for all SMEs in today's technical arena, and today's executive leaders face challenges that prior leaders did not (Cleveland & Cleveland, 2018). Leadership styles are key to the response tactics utilized for cyberattacks (Cleveland & Cleveland, 2018). A leadership style that prioritizes cybersecurity can mitigate exposure. A leader who is forward-thinking and is not afraid to spend the time and money to build a cybersecurity program will not be an easy target for an attacker. This is where Kashmiri et al. (2017) pointed out that the narcissistic style would be a benefit, as the leader is focused on himself and the success of their business. Once an attack is identified, prevention tactics are irrelevant (Cleveland & Cleveland, 2018) and influence customer perceptions of the company (Kshetri, Voas, Kshetri, & Voas, 2018).

While information technology systems play a significant role in the response, leadership soft skills are equally important. Even with robust and resilient controls in place, the global nature of information technology systems makes the response in the moments after a cyberattack much more than technological. SME leaders are typically not trained or astute at recognizing various factors, including behavioral, cultural, contextual, and organizational influence response (Auffret et al., 2017). A cybersecurity-driven culture is a combination of technology and investments in the people and processes of an organization (Huang & Pearlson, 2019). Small businesses that adopt recommended practices can build competitive advantage by increasing customer trust and mitigating risk through technology investments and security practices (Raghaven et al., 2017).

Small businesses are often intimidated by cybersecurity; however, all stakeholders must view it as part of the business strategy (Paulsen & Toth, 2016). SMEs must consider risk assessments and the creation and continual review of their security policies and procedures. However, most small businesses are unclear in their risk evaluations and understanding of cybersecurity recommendations (Paulsen, 2016). These risks and potential threats can include personnel, environments, accidental data loss, or intentional destruction of data. According to the NIST (2021), the most common threats to information security include environmental, business resources, and hostile actors. Therefore, leadership can define their risk by understanding the type of threat, potential vulnerabilities, the potential of occurrence, and the resulting impact (Paulsen & Toth, 2016).

The research highlighted multiple examples where leadership fails regarding cybersecurity practices (Benz et al., 2020; Moschovitis, 2018; Paulsen, 2016; Sweeney, 2016). Leadership styles and traits are vital in how an organization responds to a cyberattack. Very few organizations can validate their cybersecurity culture when tested (Paulsen, 2016). Company culture is an essential piece to the overall success of the business. The culture of a business, the lack of one, or the potential that the leaders do not know their culture is a glaring issue for SMEs (Moschovitis, 2018). A cybersecurity culture is the way online information is utilized, intentionally and unintentionally, which promotes or inhibits individuals, organizations, or governments' safety, security, privacy, and civil liberties (Da Viega, 2016). Unfortunately, the benefits of a cybersecurity culture are not apparent to many small business owners who are more focused on making payroll and profits. When culture is not essential or is an afterthought in an organization, any strategy for cybersecurity will quickly fade away. "Culture will eat strategy for lunch any day of the week" (Moschovitis, 2018).

A cybersecurity culture is achievable by hiring the right people and providing ongoing training. To mitigate the risk of a cyberattack, a leader's ignorance is not a prevention technique, which is often the scenario with SME leaders (Benz et al., 2020). Cybersecurity planning incorporates many facets and can be overwhelming to small business leaders already dealing with scalability and operations, especially during and post-pandemic. For executive leadership and boards of directors to be responsible for developing policy and regulations regarding the organization's cybersecurity efforts, a greater understanding of the field and the threats need to be prioritized. A prioritized cybersecurity culture provides the internal leadership with clear direction on the approach to cybersecurity. Managers can support and strengthen a cybersecurity culture through their decision-making around performance, control, and governance systems (Huang & Pearlson, 2019).

SME leaders are overly confident about the level of cybersecurity preparedness and defense planning in their organization. A study found that 95% of the surveyed SME IT leaders believe they have an above-average security disposition (Bisson, 2017). Unfortunately, the reality is quite different. The National Center for the Middle Market (2016) survey found that over half of SME companies surveyed do not have a cybersecurity strategy or use an out-of-date cybersecurity strategy, and half of SME IT leaders are unaware of where the best place to start to build a strategy (Kaila et al., 2018). Since the 2016 survey, this failure has improved with the National Center for the Middle Market (2018) survey, showing 62% having cyber risk management as an active part of their business. However, the survey also showed that leadership is failing, with only 49% rating their technical teams as good, and 13% have faith in their leaders to guide the technical team and business through an incident. Additionally, the SMEs surveyed say it is uncommon for their organizations to conduct a thorough cyber-risk assessment. Not conducting proper cyber practices may be due to IT and business leadership teams not being of the same mindset when it comes to cybersecurity risk management (Sweeney, 2016).

The tools and cybersecurity knowledge necessary for leaders, managers, and decision-makers of SMEs to manage cyber threats may not be easily accessible through known avenues (Gafni & Pavel, 2019). Even with risks identified and security prioritized, it is still necessary for leaders to understand and implement cybersecurity throughout the company (Sweeney, 2016). Leadership must champion any cybersecurity review and plan, in addition to understanding them (Sweeney, 2016). The people responsible for cybersecurity must be part of new organization initiatives from the beginning; this allows security to become part of the organization and not an afterthought (Sweeney, 2016).

A proactive stance is essential for risk mitigation in organizations and a recommended practice for cybersecurity culture. Leaders who understand business functions are fundamental to the effectiveness of a cybersecurity system implementation plan. Risk management generally falls under the leadership team's responsibility in an organization as most SMEs do not have a structured board of directors as in a publicly traded organization (Klimosky, 2018).

Organizations with a culture focused on security will help mitigate risk as many criminals still use established methods that are preventable. Gartner, a global market research firm, recommended that organizations with as few as 150 employees staff a cybersecurity leader. Government and businesses need to work together proactively and hold each other accountable for creating cybersecurity programs (Hathaway & Stewart, 2014; Kosseff, 2019). NIST provides guidance on recommended practices for training staff and programmatic steps for the business (Paulsen and Toth, 2016). The accessibility of coherent frameworks can help SMEs to grasp better and prioritize their cybersecurity strategies. Regardless of size, organizations should adopt cybersecurity strategies to include organizational training and increased data protection via cloud computing (Huang & Paulsen, 2019; Saber, 2016).

Perceptions and Priorities

Small business leadership involves managing the day-to-day business. Management involves the coordinating of people's behavior, responsibilities in the organization, defining and directing goals, objectives of the company, the people, and the strategy. Each of these factors influences the performance of the organization. The leadership in small firms directs and manages the business goals and managerial priorities. Additionally, owners must balance their ownership control tendencies. When small business leaders understand their influence and authority and lead in a participative way, their organization operates in a more professional way and achieves more substantial sales growth (Morched & Jarbouri, 2020; Wang & Poutziouris, 2010). With increased performance, the firm and leadership are met with more diverse needs, departments, priorities, and populations. Leadership must create an awareness of certain tendencies, such as loyalty, task orientation, single-mindedness, and lack of skills, that may prevent their ability to scale (Cukier et al., 2021; Hamm, 2002). Their ability to understand these tendencies can help them stay focused on their organization's health and welfare

Small enterprise leadership perceptions and priorities influence the firm's strategy. Leaders that focus on cost and flexibility strategies tend to have a positive impact and are predictors of firm success, but quality and delivery strategies have not been found to have a significant impact (Haleem and Jehangir, 2018). The amount of leadership focus on cost and flexibility can be correlated to the firm’s future success. Therefore, cybersecurity practices and culture can impact leadership prioritization and firm strategy if they are focused on cost. However, when it came to quality, flexibility, and delivery strategies, there is no difference found between high and low-priority importance (Haleem and Jehangir, 2018). Leadership priorities can be impacted by daily distractions as well. Issues that were imposed or required monitoring tend to attract management attention away from traditional business operation decisions (Dandridge and Sewell, 1978, Moschovitis, 2018). Rohn et al. (2016) used the social comparison theory and the rare events bias theory to suggest a leader’s self-efficacy leads to the incorrect assumptions of their business environment, which includes information security. The small business leaders drive the organizational strategy and rely on internal forces; however, they may also compare to others to reduce their uncertainty. Their lack of understanding of the broad reach of cyber-attacks can result in rare events bias. Strategic focus can also impact leadership priorities. While the focus on cost has a positive impact on performance, the relationship between cost management practices and SMEs' strategic priorities is mediated by entrepreneurship competency (Amir et al., 2016). Communication is a key characteristic of leadership and essential for defining strategy and vision for the organization. There are seven key communication priorities that are important factors in entrepreneurial leadership (Darling and

Beebe, 2012). Of these, the ability to intentionally focus, behave inclusively, and purposefully trust are key attributes that will help to prioritize cybersecurity planning. Leaders that set an example by participating and prioritizing cybersecurity activities influence employee involvement (Huang & Pearlson, 2019). The role of cost, communication, and leadership styles influence priorities. The relationship between leadership and staff is alterable by communication and perceptions.

The U.S. Small Business Administration (2016) stipulated that small-business owners constitute 99.9% of all firms in the United States, employ 48% of the private sector employees, and provide 41.2% of the total US private-sector payroll. Hiring staff is a high cost and finite resource for SMEs. Little has changed in the last decade; in 2007, employees were considered critical for competitive positioning and product quality (Lawrenece, 2007) and remains a key concern for small businesses today (NSBA, 2019). In addition to people, the NSBA's (2019) results showed that innovation was also a key concern for small firms. The expansion of the use of technology by small businesses presents a new challenge for firms when prioritizing appropriate security precautions (NSBA, 2019, Thrive Analytics, 2020). In the NSBA 2019 survey results, a majority of respondents felt vulnerable to a cyber-attack, though only 24% of respondents felt they had a high understanding of handling cybersecurity issues. People are often one of the most significant risks for data breaches (D'Arcy and Lowry, 2019; Da Veigaa, 2016). Small firm leadership focuses on addressing initial challenges, and subsequent changes follow one of the three emergent themes for surviving beyond five years in business: owner networking, business planning, and marketing differentiation (Turner and Endres, 2017). Training is an important attribute for cybersecurity-prioritized firms (Kaila et al., 2018).

While scaling an organization is a daily challenge for leadership, leadership has supported the increase in technology adoption for automating tasks, generating leads, and decision making. The increased spending and utilization of technology by SMEs and the influence of the executive team create gaps or vulnerabilities in the organization. Most small businesses are unclear in their risk evaluations and understanding of cybersecurity recommendations (Paulsen, 2016). One tactic to reduce gaps and vulnerabilities is through training. Firms implementing a leadership training framework tend to increase sales growth and operate more professionally than those that do not undertake leadership training (Wang and Poutziouris, 2010). Expanding a leadership training framework to include cybersecurity training will help SMEs to begin adapting to NIST framework suggestions for cyber planning. The NIST framework provides a tool for organizations to use as a baseline to measure their cybersecurity program and identify potential gaps. While not meant to be a prescriptive standard, it may evolve to create a standard of cybersecurity care (Shackelford et al., 2015; Shen, 2014).

While leadership can create opportunity with technology, there are challenges in their approach as well. Organizations with leadership lacking funding or knowledge to adopt technology and digital processes or keep up with the rapidly changing environment run an increased risk of cyber-attacks. A small business leader's lack of IT knowledge is a predictor of adopting IT, which can influence prioritization coinciding with social theory and rare events bias (Rohn et al., 2016). Small firms are often lean organizations with minimal IT support, leaving much of the strategy and execution to the leader.

Since many SMEs do not have a CTO on staff and are challenged with finding staff with minimal cybersecurity knowledge, CEOs must determine their technology entry points and alignment with corporate strategy (Moschovitis, 2018). As they scale the organization, the leaders must implement cybersecurity and technology training to move towards a cybersecurity culture and risk mitigation strategies. Cybersecurity training is an important factor to incorporate into the organization's training framework and is an essential part of cybersecurity culture (Huang & Pearlson, 2016; Moschovitis, 2018). Small business owners that adapt their businesses and are open to learning and implementing cybersecurity strategies may prevent the demise of their business from cyberattacks (Phillips, 2020).

The SMEs' lack of understanding of cybersecurity implications, lack of access to peer resources, and minimal news coverage of cyberattacks targeting small and medium organizations adversely impact leadership cybersecurity planning as compared to larger organizations. Cybersecurity in SMEs is often an afterthought or one not broached. While many small business leaders have the best intentions, the prominent threats and weaknesses distract their focus. Many small business executives fail to prioritize their cybersecurity planning due to the lack of tangible evidence. Tangible evidence may never come, and many times the attack has been underway for six months or more before leadership becomes aware of the attack (Thrive, 2020**).**

In larger organizations, teams and leaders are dedicated to cybersecurity planning. A study of chief technology officers (CTO) priorities in larger global organizations identified three key activities: aligning technology and corporate strategy, shaping technology entry and exit points, and assembling data to support the need for funding for technology development. CTO priorities are related to technology transition points, major technological and business disconnects (van der Hoven et al., 2012). Today's CTOs must be versatile in their skill set to work across the organization and provide the strategies and tactics needed to execute within the company (Perri, Farrington, Johnson, & O'Connor, 2019)

In addition to technology and training, firms must plan to prioritize cybersecurity in their firm’s culture. Several factors are necessary for small firms to adopt a cybersecurity culture. Firms that focus on leadership training and a learning orientation create opportunities while mitigating their exposure to cyber risk. Small businesses that embrace a leadership training culture that addresses people, processes, and systems, including leadership strengths and weaknesses, long-term strategic vision, business opportunities and threats, a documented training program, and periodic evaluations, have an increased opportunity for more robust firm performance (Wang & Poutziouris, 2010). Understanding the internal beliefs, values, and attitudes combined with external influences and organizational mechanisms can drive a cybersecurity culture (Huang & Pearlson, 2019). Small business owners that embrace a learning mindset and are open to learning and implementing cybersecurity strategies may prevent the ultimate collapse of their business. The endorsement of recommended practices can build a competitive advantage by increasing customer trust and mitigating risk through technology investments and security practices (Raghavan et al., 2017).

Summary

This research analyzed why SMEs leaders are failing with cybersecurity. The leadership for many SMEs is responsible for implementing new strategies organizationally, including cybersecurity. The research showed that the organization's leaders play an essential role in implementing cybersecurity (Rohn et al., 2016). One of the discoveries highlighted the many misunderstandings with regards to cybersecurity. These misconceptions lead to many SME leaders avoiding cybersecurity and going with the *ignorance is bliss* mindset (Benz et al., 2020). Additionally, cybersecurity is not standard information technology and is rapidly changing (Craigen et al., 2014; Moschovitis, 2018; Schatz et al., 2017; Toth & Patterson, 2016). This fast pace of change should fit into the SME’s wheelhouse, but research has shown that it does not (Cleveland & Cleveland, 2018; Paulsen, 2016; Radanliev et al., 2020).

Leadership has a hard time finding where to turn for information that may help them with policies related to cybersecurity (Paulsen, 2016). When SME leadership can locate information, there is a chance the leaders will not find the appropriate staff to help them define and implement a cybersecurity program and the required technology (Moschovitis, 2018). Additionally, small and medium firms struggle with the lack of funding and cost-benefit. This lack of funding can cause struggles with training the users inside the company on appropriate avoidance techniques (D'Arcy et al., 2019).

Many leaders feel that their organization is ready for a cyber-attack; however, studies have shown otherwise (Gafni & Pavel, 2019; Talu, 2020). Many inside the company who are responsible for a cyber program do not know where to access resources to begin (SBA, 2021). Leaders need to be proactive and entrepreneurial-oriented with strong beliefs to solve their organizations' cybersecurity needs (Kashmiri et al., 2017).

Discussion of Findings

The purpose of this research was to investigate leadership failure to implement cybersecurity plans and policies in small and medium enterprises. This research evaluated why SME leadership has not prioritized cybersecurity plans and assessed tactics to increase adaptation and incorporate a cybersecurity strategy. This research aims to encourage SME owners and leadership to prioritize cybersecurity and outline a framework to create and maintain a cybersecurity plan and implement technology solutions to help thwart potential cyberattacks.

1. How does small and medium enterprises (SMEs) leadership define cybersecurity and its role in day-to-day operations?
2. How does business culture influence the outcome of a cybersecurity strategy and the implementation tactics required?
3. What communication strategies and tactics are needed to increase awareness and urgency for leadership to implement cybersecurity measures?

This research evaluated the struggles that most SMEs face regarding cybersecurity and where leadership is failing. Numerous factors, including lack of IT staff, lack of resources, lack of knowledge, flawed strategies, misperceptions, and lack of priority, have led to the challenges most SMEs face today. SME leadership has failed to implement adequate cybersecurity protocols. This research found multiple factors to address and answer why SMEs are challenged with cybersecurity techniques, strategies, and planning. These factors include technology, understanding what defines cybersecurity, organizational culture, and leadership perceptions and priorities. The factors were evaluated against existing literature to determine the following findings.

Technology and Small Business

As SME leaders focus on firm optimization, they are increasing their technology spending. This research evaluated the role that technology disruptions play in the increase of technology spending decisions. Cybersecurity is one such technology disruption in the current business environment. Research has shown that SMEs have adopted many different technologies to help optimize and run their business. These technologies house essential user data like payment information and personal contact details, enabling the purchase and sales processes. Sensitive customer data housed in these technologies must be protected to mitigate exposure to cyber threats, instill trust, and protect the business' reputation. SME leadership must understand the potential exposure with each process and technology that involves touchpoints with customer data and the potential for a data breach with each technology adopted by the organization.

With more consumers spending their time online and more companies moving online due to the global pandemic, SMEs were forced to adapt and move online. This pivot changed how SMEs approach their business strategy and incorporate IT and highlighted the need to prioritize cybersecurity. Creating and implementing a cybersecurity plan will lead to additional expenses for an organization. This expense forces the organization into additional technology decision-making investments and management. Previously, research has shown that spending on security has been viewed as an input without output to the businesses (Paulsen, 2016). Organizations moving towards more online commerce have interrupted *normal operations* and require more funding for technology investments to maintain a competitive stance in the marketplace (Martins, 2020). This increased spending may act as a hindrance to creating or adopting a cybersecurity plan. Unfortunately, the increased integration of technology in day-to-day operations underscores the importance of creating a cybersecurity plan. This technology integration creates additional challenges for SME leaders managing other factors, like the inadequate budget for additional technology and security, lack of staffing, and other immediate customers, vendors, or staffing issues (Georgiadou et al., 2020).

While research has shown that SMEs are increasing their technology spending, they remain limited in their staffing of IT departments and cybersecurity support. Typically, the IT or information systems department is responsible for implementing and managing cybersecurity (Moschovitis, 2018). The IT departments are responsible for building and maintaining the network and systems to keep the business running. Therefore, without a designated cybersecurity department, the SME may remain exposed without someone planning and watching for cyber threats. Individuals responsible for cybersecurity support are essential for analyzing possible security threats and assessing the security risks (Raghavan et al., 2017). Having a designated individual that is responsible for cybersecurity is a best practice. This individual can assess the organizational infrastructure and aid in designing robust security mechanisms to protect the organization. Risk assessment and mitigation are essential for an organization's success, especially in the current technological environment. Without risk assessment teams or designated individuals, the potential for business success is at risk.

Businesses must fight to stay competitive in today's global environment and achieve this by integrating technology solutions for optimizing operations, sales, and services. Due to the increased use of technology, SMEs cannot avoid cybersecurity. SMEs must maintain their integrity by ensuring that their customer and employee data is always secured.

Another factor influencing SME adoption of cybersecurity planning is inadequate security budgets. A growing trend among many SMEs is the issue of security being an afterthought. When budgeting for the resources to run their businesses, SMEs do not consider security in the category of essential resources. The financial and resource limitations mitigate their prioritization to budget for the security and make them hesitant to incur additional technology expenses. Specialized tools need implementation, and specialized personnel is a must for the implementation. The implementation process requires special attention and the continual training of employees on cybersecurity (Sweeney, 2016). The tools and staff needed for this specialized attention are expensive. As a result, for SMEs to implement cybersecurity, they must first allocate a budget to it (Sweeney, 2016).

Cybersecurity Defined

Small and medium enterprises are not fully educated about cybersecurity. This research investigated the various interdisciplinary definitions for cybersecurity. Though many definitions have been given that are acceptable by government, scholars, and businesses, most SMEs lack the awareness or ability to define cybersecurity. Small and medium enterprises would benefit from understanding the definition, "the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity, and availability of data and assets used in cyberspace," by having a better understanding of the various components contributing to cybersecurity (Schatz et al., 2017, p. 66). As a result, SME leadership must understand and have prior knowledge about cybersecurity (Georgiadou et al., 2020). It is only a matter of when and not if that SME leadership will need to protect their organizational data and understand the importance of cybersecurity. Furthermore, this research suggests that leaders learn about cybersecurity and how to implement it or rather invest in it through the creation of a cybersecurity plan and ongoing organizational security training (Huang et al., 2016).

Small and medium enterprises are challenged with limited resources (capital, technology, knowledge) and the lack of human capital. Many SMEs tend to focus on maximizing their profits, reducing expenses, and deferring acquisition of assets and other aspects of business that do not offer a near-term tangible return. Leadership tends to focus on spending on the business operations, which offer quicker returns to increase company profits. Additionally, SMEs are limited in their sources of capital, often using personal savings and credit cards or personally guaranteed loans from financial lenders. The increased personal risk exposure of investing in technology and assets drives their focus on clearing their debts. This exposure can have an adverse effect on their investment and expenditures with no returns. There is the potential for SMEs to optimize operations and staffing resources so that they can focus on allocating resources to cybersecurity planning. Some businesses do not see the importance of designated cybersecurity staff as they do not see the long-term value because they are focused on their immediate returns. Despite having IT departments, cybersecurity is an addition that requires special attention. Designated cybersecurity individuals increase the organization's chances for sustainable success and can assist the organization in gaining a competitive advantage by earning customer trust. Small and medium enterprises strive to have sustainable and profitable businesses.

Organizational Culture

The research shows that an organization with a healthy culture accomplishes its plans and strategies. Having a strategy provides a guide for execution goals and tactics. However, strategies are at risk without the proper culture, "culture will eat strategy any day of the week" (Moschovitis, 2018). SME executives are responsible for setting the strategy and culture for the organization. Leadership, through their actions or inactions, drives culture. The firm’s culture is the foundation for every plan, process, goal, or tactic that the organization tends to follow. Most organization's employees will work towards fulfilling the organization's requirements or work within the set guidelines by the organization. These guidelines work as the internal traits and establish the culture of the organization.

An organization must have a good strategy involving people, tools, processes, and planning to implement cybersecurity, but if the organization lacks a cybersecurity culture, the strategy will fail (Paulsen, 2016; Sweeney, 2016). First and foremost, SME executives need to set internal processes and procedures for technology, be responsible for staff oversight, ensure continual training of staff, and establish an implementation plan. To effectively communicate the organizational strategy, a leader must be influential. The two most essential traits of an influential leader are entrepreneurial mindset and technological readiness. The technological readiness mindset establishes that an SME with computer-savvy leadership influences an organization's digital engagement (Reynolds et al., 2020). An influential leader will ensure that the organization integrates technology through investments, adoption, and use. Investing in technology will build a competitive advantage; thereby, creating a business cybersecurity culture powered by technology.

When an organization establishes cybersecurity culture the strategic plan to implement cybersecurity will mitigate resistance or fear of failure. The integration of people, processes, technologies, and prioritization of cybersecurity will address the glaring issues facing SMEs. One such issue is the misperception that cybersecurity does not add value. Most SMEs tend to invest in items related to operations that drive more immediate profitability. Cybersecurity is often viewed as a function that does not drive the organization's income, making it difficult to implement in the organizational workflow (Sweeney, 2016). Cybersecurity planning and implementation are expensive, and an organization must incur additional expenses to execute on cybersecurity strategy. Cybersecurity tools are an added expense and may require specialized knowledge to adopt and manage. The added expense and non-tangible return on investment make it difficult for SMEs to see its importance. However, cybersecurity is a long-term strategic initiative that drives future returns for the organization. SMEs must secure and protect customer-sensitive data to earn customers' trust. The best way to protect online user data is by leveraging proper cybersecurity planning. A cybersecurity culture drives brand equity through the increased trust of customers and employees. Brand equity helps organizations with long-term sustainability with increased word-of-mouth and brand loyalty (Aaker, 2009). The increased brand equity translates to revenue through increased consumption and customer retention. Organizations with a cybersecurity culture build a brand reputation that is influenced by their customer's perceptions of their cybersecurity practices (Kshetri, Voas, Kshetri, & Voas, 2018). SME leadership must understand the value that a cybersecurity culture offers for the long-term viability of their firm.

Attacks on SMEs happen significantly more frequently and at a higher rate than more prominent organizations that make the national news (Aguilar, 2015; Verizon, 2021). The company's response to the cyberattack influences customer trust and the organization's brand equity (Kshetri, Voas, Kshetri, & Voas, 2018). As more SMEs move operations online, their exposure to cyber-attacks increases.

The lack of understanding of customer and employee touchpoints can lead to unpreparedness for cyber-attacks. This research has provided insights that most SMEs lack knowledge of cybersecurity. SMEs fail to recognize their exposure to cyber-threats, while others do not see the importance of cybersecurity planning and implementation. The combination of these factors highlights the SMEs’ lack of preparedness to handle cyber-attacks. When SMEs have embraced a cybersecurity culture and have strong operational technology support focused on security, they will be better prepared to handle the inevitable cyber-attack and post-breach response. Their proper cybersecurity planning will better position the organization for future exposure and response and build more substantial brand equity, leading to greater success opportunities. Having a cybersecurity plan in place means the security team analyzes potential threats, completes a thorough risk assessment and is better prepared to handle a cyber threat. SMEs face many challenges to ensure their information is secure as they collect, process, and store sensitive information (Talu, 2020). When an SME understands cybersecurity, prioritizes cybersecurity support, and plans for when an attack happens, it will achieve a stronger competitive position in the marketplace.

The most critical priority for SMEs is to adopt a cybersecurity culture. To achieve this, firms will need to hire the *right* people. According to Paulsen (2016), the *right* people constitute technical-oriented staff or rather the qualified cybersecurity personnel. Technical and cybersecurity personnel may be more expensive to hire. Additionally, SMEs will need to combat ignorance to their risk exposure. Leadership must assume that they are already at risk of cyber-attacks or threats. By focusing on potential exposure, SMEs will prioritize implementing cybersecurity strategies, protecting assets, maintaining a firm reputation, customer retention, and building brand equity.

Perceptions and Priorities

This research has evaluated SME organizational perceptions and priorities. SMEs tend to prioritize what they know (self-efficacy) and how they perform compared to others (social comparison) depending on their perceptions (Rohn et al., 2016). Leadership perceptions about technology will influence their prioritization of technology investments (Reynolds et al., 2020).

Additionally, SMEs tend to fail to prioritize cybersecurity due to the lack of instant or tangible returns. This perception leads to a lack of prioritization, adoption, and management of technology.

Another glaring issue that SMEs face is their ignorance of exposure. A popular opinion among many SMEs is their misperceptions about exposure to cyber threats. SMEs are focused on the day-to-day operations of their businesses and do not see the type or amount of data exposed to create a cyber threat (Phillips, 2020). When a cyberattack happens to a business, it is not instantly seen or felt by the organization. It may take as long as six months before the attack's impact can be felt, and when it is uncovered, it is too late.

SMEs prioritize spending on tools, technologies, and inventory that results in quicker returns, grow their business, and support their operations (Rohn et al., 2016). In fact, in a data breach, SMEs are conceivably at a higher risk than large enterprises (Selzinck & LaMacchia, 2018). For SMEs to prioritize technology, leadership will need to change their perceptions about technology. Leadership must understand the strategic view of long-term operational efficiencies, customer retention, staff engagement, the potential for risk mitigation, and the result of a cybersecurity plan to generate long-tail returns for the organization. To manage cybersecurity exposure, SMEs must prioritize technology and training employees on cybersecurity-related issues (Rohn et al., 2016). Leadership must prioritize operational technology support (departmental or individual) through planning and investments. As the SME organization grows, the need to protect assets (people and data) from cyber-attacks increases exponentially.

Future Considerations

Future research should focus on developing frameworks to reflect the typical technologies utilized by SMEs using simplified terminology based on the NIST framework (the current framework is 54 pages and will be glossed over by a busy SME leader). This simplified framework would create a more task-oriented structure for small businesses to implement and scale. Using banks or the Chamber of Commerce to offer a cybersecurity analyst to help these companies get started with an initial program may be what is needed to kickstart cybersecurity programs in SMEs. This program could be funded by the federal or state government, the SME's financial institution, or an insurance provider. As lean organizations where strategic decision making is established by a single or select few leaders, creating a more task-oriented framework that is delivered free of charge can help reduce the decision-making burden and help leadership delegate tasks across the organization. This suggested methodology can also help drive a cybersecurity culture with the firm's employees participating in the overall security planning and execution, helping them feel more engaged with the organization. This task-oriented framework may support the small firm with limited funding for technology and support staff by implementing a cross-training framework and additional responsibilities as defined for employees, minimizing additional staff requirements, and adding skill development. By starting with a task-oriented framework, SMEs can move forward with the cybersecurity plan.

Conclusion

This research investigated why SME leadership is failing with cybersecurity. Several factors were examined regarding SMEs: technology, how cybersecurity is defined, organizational culture, and leadership perceptions and priorities. These factors provided additional insight to support what resources are available for SMEs, the challenges and opportunities for leadership, and existing frameworks available that can support the planning and organizational culture of cybersecurity. A suggested framework can help reduce the research and planning component of cybersecurity; thereby, mitigating prioritization failure of the SME leader's never-ending short- and long-term decision-making responsibilities.

SMEs are competing in an increasingly digital and global environment. They are increasing their investments in technology yet are limited in resources (financially and operationally) to support those technology investments. SMEs are focused on quick returns for technology investments, investing more in operational efficiencies and cost-saving strategies than in the intangible investment of security.

The research evaluated the organizational priority of cybersecurity, confirming that many SMEs fail to see the importance of cybersecurity. SME leadership struggles with limited resources for cybersecurity awareness and education. As seen with technology, SME leadership frequently sees cybersecurity as an investment that does not add value to their bottom line. These leaders fail to recognize the threats that they might be exposed to in their daily operations. Most SME leaders wrongly assume that due to their size or industry that they are not exposed to any threats (Gafni et al., 2020). As the findings revealed, any organization operating online is at risk of cyber threats. While there are many definitions of cybersecurity, it is also a rapidly changing and growing landscape. This high rate of change within the broadly defined field and the headlines focused on large institutions and enterprises have led to a misunderstanding for SMEs on the definition of cybersecurity.

Another factor that influences leadership failures in cybersecurity is organizational culture. SME leadership is responsible for implementing significant organizational capabilities, not limited to cybersecurity (Rohn et al., 2016). It is evident that there is a disconnect between cybersecurity and the leadership of SMEs, resulting in a lack of planning and implementation of cybersecurity (Benz et al., 2020). While SMEs are known for being flexible and agile in their business practices and adapting to changing environments, research has shown that this does not apply when it comes to cybersecurity (Paulsen, 2016). A good organizational culture is essential for implementing an effective cybersecurity plan (Paulsen, 2016). Without an engaged culture, any cybersecurity strategy will face challenges. Leadership drives organizational culture, and SME leaders face challenges with decision-making based on their limited resources for consultation or focus on self-reliance (Selzinck et al., 2018). Leadership that is open to adopting new technology, having an open-door policy with regards to engaging staff in cybersecurity discussions, and having a culture of accountability are the ones that help to drive a cybersecurity culture. Those organizations with a cybersecurity culture will be better prepared for the growth of cybersecurity attacks, build stronger brand equity, retain customers, and engage employees.

According to the research, most SMEs lack an IT department or support staff. While investments in technology are increasing, SMEs are focused on operational technology rather than security. SME leadership failure to prioritize security investments will lead to cybersecurity failures. As SMEs increasingly move online, they must protect their organizational and customer data privacy. Limited resources are not an excuse for lack of prioritization, nor a defense should a data breach result. SME leadership believes they are prepared to handle cyber threats, but research indicates that they are not.

Additionally, leadership's failure to see the value of cybersecurity and the risk potential is a major determinant for the lack of cybersecurity planning and implementation. The lack of knowledge of risk exposure and cybersecurity, in general, makes it difficult for SME leaders to identify the necessary resources and where to access those resources (SBA, 2021), which may explain their lack of prioritization. Research also confirmed that the type of leadership has a direct impact on cybersecurity and technology planning. Two factors support cybersecurity preparedness: leaders with an entrepreneurial mindset and technological readiness (Reynolds et al., 2020). The combination of mindset and proper cybersecurity planning is essential in today's digital environment

References

Aaker, D.A. (2009). Aaker's brand equity model. *European Institute for Brand Management.*

Abdul Hameed, M., & Counsell, S. (2012). Assessing the influence of environmental and CEO characteristics for adoption of information technology in organizations. *Journal of Technology Management & Innovation*, 7(1), 64–84. https://doi.org/10.4067/S0718-27242012000100005

Aguilar, L. (2015, October 19). *The need for greater focus on the cybersecurity challenges facing small and midsize businesses*. SEC. https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html

Akhtar, S., Sheorey, P., Bhattacharya, S., & Kumar V. V., A. (2021). Cyber security solutions for businesses in financial services. *International Journal of Business Intelligence Research*, *12*(1), 82–97. https://doi.org/10.4018/ijbir.20210101.oa5

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Amir, A., Auzair, S. M., & Amiruddin, R. (2016). Cost management, entrepreneurship and competitiveness of strategic priorities for small and medium enterprises. *Procedia-Social and Behavioral Sciences*, 219, 84-90.

Auffret, J., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., Stein, F., Sokol, L., Allor, P., & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, *17*(01), 1740001. https://doi.org/10.1142/s0219265917400011

Benz, M., & Chatterjee, D. (2020). Calculated risk? a cybersecurity evaluation tool for smes. *Business Horizons*, 63(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Bhattacharya, D. (2015). Evolution of cybersecurity issues in small businesses. *4th Annual ACM Conference on Research in Information Technology*. https://doi.org/10.1145/2808062.2808063

Boletsis, C., Surridge, M., Halvorsrud, R., Pickering, J. B., & Phillips, S. C. (2021). Cybersecurity for SMEs: Introducing the human element into socio-technical cybersecurity risk assessment. *Computer Vision, Imaging and Computer Graphics Theory and Applications*, *3*, 266–274. https://doi.org/10.5220/0010332902660274

Burrell, D. (2020). Understanding the talent management intricacies of remote cybersecurity teams in covid-19 induced telework organizational ecosystems. *Land Forces Academy Review*, *25*(3), 232–244. https://doi.org/10.2478/raft-2020-0028

Cleveland, S., & Cleveland, M. (2018). Toward cybersecurity leadership framework. *Association of Information Systems*, (49). https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1048&context=mwais2018

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Cukier, W., McCallum, K. E., Egbunonu, P., & Bates, K. (2021). The mother of invention: Skills for innovation in the post-pandemic world. *Public Policy Forum, Diversity Institute, Future Skills Centre*. https://www. ryerson.ca/diversity/reports/MotherOfInvention_EN. pdf.

D'Arcy, J., & Lowry, P. (2019). Cognitive affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. https://doi.org/10.1111/isj.12173

Da Viega, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI Computing Conference (SAI)* (pp. 1006-1015). IEEE. https://doi.org/10.1109/SAI.2016.7556102.

Dandridge, T. C., & Sewall, M. A. (1978). A Priority Analysis Of The Problems Of Small Business Managers. American Journal of Small Business, 3(2), 28–36. https://doi-org.proxy195.nclive.org/10.1177/104225877800300204

Darling, J. R., & Beebe, S. A. (2007). Enhancing entrepreneurial leadership: A focus on key communication priorities. Journal of Small Business & Entrepreneurship, 20(2), 151-167. https://doi.org/10.1080/08276331.2007.10593392

Deloitte. (2019). *Connecting small businesses in the us 2018* [PDF]. deloitte.com. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-connected-small-businesses-Jan2018.pdf

Falkner, E., & Hiebl, M. R. (2015). Risk management in SMEs: A systematic review of available evidence. *The Journal of Risk Finance*, *16*(2), 122–144. https://doi.org/10.1108/jrf-06-2014-0079

Federal Communication Commission. (n.d.). *Cybersecurity for Small Business*. FCC.gov. https://www.fcc.gov/general/cybersecurity-small-business

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management*, *7*(1), 14–26. https://doi.org/10.36965/ojakm.2019.7(1)14-26

Gallup & Marlar, J. (2018, April 25). *Why phone and web survey results aren't the same*. Gallup.com. https://news.gallup.com/opinion/methodology/233291/why-phone-web-survey-results-aren.aspx

Georgiadou, A., Mouzakitis, S., Bounas, K., &amp; Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, (2020). https://doi.org/10.1080/08874417.2020.1845583

Global Cyber Alliance. (2020). *GCA Cybersecurity Toolkit Backgrounder: Know What You Have Toolbox* [PDF]. https://gcatoolkit.org/wp-content/uploads/2021/04/Backgrounder-know-what-you-have-2001.pdf

Haleem, F., & Jehangir, M. (2018). High performers vs low performers SMEs, from competitive priorities perspective. *Pakistan Journal of Social Sciences* (PJSS), 38(1), 181–198. https://www.bzu.edu.pk/PJSS/Vol38No12018/PJSS-2018-I-12.pdf

Hamm, J. (2002). Why entrepreneurs don't scale. *Harvard Business Review*, 80(12), 110.

Hathaway, M. (2012). Leadership and responsibility for cybersecurity. *Georgetown Journal of International Affairs*, 71–80. http://www.jstor.org/stable/43134340

Hathaway, M., & Stewart, J. N. (2014). Taking control of our cyber future. *Georgetown Journal of International Affairs*, 55–68. http://www.jstor.org/stable/43773649

HISCOX. (2021). *Hiscox-cyber-readiness-report-2021* [PDF]. Hiscox Insurance https://www.hiscox.com/sites/default/files/content/documents/Hiscox-Cyber-Readiness-Report-2021.pdf

Howard, L. S. (2019, October 2). *SMEs underestimate cyber risks which could prove 'fatal': allianz report*. Insurance Journal. https://www.insurancejournal.com/news/international/2018/02/21/481113.htm#

Huang, K., & Pearlson, K. (2019, January). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019. https://doi.org/10.24251/HICSS.2019.769

Ikeda, S. (2021, June 7). *Are ransomware attacks on critical infrastructure becoming a cybercrime trend? Meat processing giant JBS, Colonial Pipeline may only be the beginning*. CPO Magazine. https://www.cpomagazine.com/cyber-security/are-ransomware-attacks-on-critical-infrastructure-becoming-a-cybercrime-trend-meat-processing-giant-jbs-colonial-pipeline-may-only-be-the-beginning/

International Data Corporation. (2020). Worldwide small and medium business spending guide. IDC. https://www.idc.com/tracker/showproductinfo.jsp?containerId=IDC_P35112

Kshetri, N., Voas, J.M., Kshetri, N., & Voas, J. (2018). Hackings Brand-Equity Nexus. *Computer,* 51(3), 74-77

Kaila, U., & Nyman, L. (2018). Information security best practices: First steps for startups and SMEs. *Technology Innovation Management Review*, 8(11), 32e42. https://timreview.ca/article/1198

Klimoski, R. (2018). Critical success factors for cyber security leaders: Not just technical competence. *People + Strategy*. 39

Kosseff, J. (2019). *Cybersecurity law* (2nd ed.). Wiley. https://doi.org/10.1002/9781119517436.ch6

Lawrence, W. W. (2007). Small business operations strategy: Aligning priorities and resources. *Journal of Small Business Strategy*, 18(2), 89–103. https://libjournals.mtsu.edu/index.php/jsbs/article/view/93

Lechner, C., & Gudmundsson, S. (2012). Entrepreneurial orientation, firm strategy and small firm performance. *International Small Business Journal: Researching Entrepreneurship*, *32*(1), 36–60. https://doi.org/10.1177/0266242612455034

Lopez, M., Lombardo, J., Lopez, M., Alba, C., Velasco, S., Braojos, M., & Fuentes-Garcia, M. (2020). Intelligent detection and recovery from cyberattacks for small and medium-sized enterprises. *International Journal of Interactive Multimedia and Artificial Intelligence*, *6*(3), 55. https://doi.org/10.9781/ijimai.2020.08.003

Lopez-Nicolas, C., & Soto-Acosta, P. (2010). Analyzing ICT adoption and use effects on knowledge creation: An empirical investigation in SMEs. *International Journal of Information Management*, *30*(6), 521–528. https://doi.org/10.1016/j.ijinfomgt.2010.03.004

Malecki, F. (2020). Optimising storage processes to reduce the risk of ransomware. *Network Security*, *2020*(5), 6–8. https://doi.org/10.1016/s1353-4858(20)30055-6

Morched, S., & Jarboui, A. (2020). Is business performance linked to organizational culture? a study from tunisian smes through subjective measures. Qualitative Research in Financial Markets, 13(1), 59–81. https://doi.org/10.1108/qrfm-01-2020-0005

Moschovitis, C. (Ed.). (2018). *Cybersecurity program development for business*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119430018

National Small Business Association. (2019). *2019 Technology & small business survey* [PDF]. NSBA. https://nsba.biz/wp-content/uploads/2019/06/Technology-Survey-2019-1.pdf

NIST. (2021). 2019 technology & small business survey [PDF]. https://www.nist.gov/system/files/documents/2021/01/13/Getting-Started-NIST-Privacy-Framework-Guide.pdf

Patterson, J. (2017). *Cyber-Security policy decisions in small businesses*. (Publication No. 10680962 [Doctoral dissertation, Walden University]. Walden Dissertations and Doctoral Studies Collection.

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, *49*(8), 92–97. https://doi.org/10.1109/mc.2016.223

Perri, S.T., Farrington, T., Johnson, S. & Colarelli O'Connor, G. (2019) Today's Innovation Leaders, Research-Technology Management, 62:1, 20-29, DOI: 10.1080/08956308.2019.1541726

Pfleeger, C. P., & Pfleeger, S. L. (2012). Analyzing computer security. Upper Saddle River, NJ: Prentice Hall.

Phillips, I. J. (2020). *Maintaining small retail business profitability by reducing cyberattacks*. (Publication No. 28024279) [Doctoral dissertation, Walden University Walden Dissertations and Doctoral Studies Collection.

Radanliev, P., De Roure, D. C., Nurse, J. C., Mantilla Montalvo, R., Cannady, S., Santos, O., Maddox, L., Burnap, P., & Maple, C. (2020). Future developments in standardisation of cyber risk in the internet of things (iot). *SN Applied Sciences*, *2*(2). https://doi.org/10.1007/s42452-019-1931-0

Reynolds, S., Cotrino, F., Ifedi, C., & Donthu, N. (2020). An exploratory study of executive factors that lead to technology adoption in small businesses. *Journal of Small Business Strategy*, 30(2), 1–16.

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business infosec posture using social theories. *Information & Computer Security*, *24*(5), 534–556. https://doi.org/10.1108/ics-09-2015-0041

SBA. (2018, April 25). *Small businesses drive job growth in the U.S..: The U.S. small business administration.* sba.gov. https://www.sba.gov/advocacy/small-businesses-drive-job-growth-us

SBA. (2020). *US small business economic profile* [PDF]. USBA Office of Advocacy. https://cdn.advocacy.sba.gov/wp-content/uploads/2020/06/04144224/2020-Small-Business-Economic-Profile-US.pdf

SBA. (2021). *Stay safe from cybersecurity threats*. sba.gov. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2017.1476

Selzinck, L., & LaMacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law*, *13*(2), 217–253.

Shackelford, S.J., Proia, A., A., Martell, B. & Craig, A.N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Tex. Int'l LJ,* 50, 305 http://search.ebscohost.com.ezproxy.utica.edu/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=tsh&AN=108372861&site=ehost-live.

Shen, L. (2014). The NIST Cybersecurity Framework: Overview and Potential Impacts. *Scitech Lawyer,* 10 (4), 16-19. http://proxy195.nclive.org

Shriver, S., & Williams, B. (2018). Situational leadership and cybersecurity. *Leader to Leader*, *2019*(91), 44–49. https://doi.org/10.1002/ltl.20409

Heffes, E. M. (2009). Small-business priorities.(strategy)(brief article). Financial Executive, 24(3), 10. https://go-gale-com.ezproxy.utica.edu/ps/i.do?p=AONE&u=nysl_ce_uticacol&id=GALE%7CA198234193&v=2.1&it=r&sid=oclcSreenivas, K., & Jyothi, T. P. (2020). Strategic approach for improving market share in micro, small and medium enterprises lending - a case study. *South Asian Journal of Marketing & Management Research*, *10*(11), 111–114. https://doi.org/10.5958/2249-877x.2020.00091.0

Stasiak, K. (2018, July 26). *Middle-market companies underestimate cybersecurity risks*. Industry Week. https://www.industryweek.com/leadership/article/22026028/middlemarket-companies-underestimate-cybersecurity-risks.

Stone, K. (2021, February 2). *2021: What's ahead from NIST in cybersecurity and privacy?* NIST. https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

Talu, S. (2020). Strategic measures in improving cybersecurity management in micro and small enterprises. *International Scientific and Practical Conference on Digital Economy*, 522–528. https://doi.org/10.2991/aebmr.k.201205.087

Thrive Analytics. (2020, January 27). *Small Businesses Expand Technology Budgets in 2020*. https://thriveanalytics.com/small-businesses-expand-technology-budgets-in-2020/

Toth, P. R., & Patterson, C. (2016). *Small business information security: The fundamentals* (No. NIST Internal or Interagency Report (NISTIR) 7621 Rev. 1). NIST. https://doi.org/10.6028/NIST.IR.7621r1

Tubbs, S. L. & Schultz, E. (2006). Exploring a taxonomy of global leadership competencies and meta-competencies*. Journal of American Academy of Business,* Cambridge, 8(2), 29-34

Turner, S., & Endres, A. (2017). Strategies for enhancing small business owners' success rates. *International Journal of Applied Management and Technology*, 16.10.5590/IJAMT.2017.16.1.03

U.S. Chamber of Commerce. (2018). *Examining the impact of technology on small business: How small businesses use social media and digital platforms to grow, sell, and hire* [PDF]. https://www.uschamber.com/sites/default/files/ctec_sme-rpt_v3.pdf

U.S. Small Business Administration (SBA). (2016). *Frequently asked questions*. Sba.gov. https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf

van der Hoven, C., Probert, D., Phaal, R., & Goffin, K. (2012). Dynamic technology leadership. *Research Technology Management*, 55(5), 24–33. https://doi-org.proxy195.nclive.org/10.5437/08956308X5505073

Verizon. (2021). *DBIR 2021 data breach investigations report smb snapshot* [PDF]. https://enterprise.verizon.com/resources/reports/2021-dbir-smb-snapshot.pdf

Wang, Y., & Poutziouris, P. (2010). Leadership styles, management systems and growth: Empirical evidence from UK owner-managed SMEs. *Journal of Enterprising Culture,* 18(3), 331–354. https://doiorg.proxy195.nclive.org/10.1142/S0218495810000604

Wong, M. (2020, June 29). *A snapshot of a new working-from-home economy*. Stanford News. https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy/

World Economic Forum. (2020). *The global risk report 2020* [PDF]. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346 USA