KEEPING SMALL BUSINESSES SECURE: A Cybersecurity Study

by

COURT COLLINS HUISH

Senior thesis submitted to the Integrated Studies Board of Utah Valley University in partial fulfillment of the requirements for a Bachelor of Science in Integrated Studies

BUSINESS MANAGEMENT AND COMPUTER NETWORKING

Orem, UT

December 2018

Thesis Approval Page

In partial fulfillment for a Bachelor of Science Degree in Integrated Studies with Business Management and Computer Networking emphases, we hereby accept this Senior Thesis written by Court Huish.

Defended: December 3rd, 2018

Thesis Mentor Signatures:

Alan W. Clarke — Alan Clarke, Integrated Studies

Mikki O'Connor — Mikki O'Connor, Assistant Dean,

Woodbury School of Business

Tahir Khan — Tahir Khan, Information Technology

Statement of Thesis and Project Summary

This paper will review the cyber threats and attacks that target small businesses, as well as discuss methods that managers can take to minimize and prevent breaches. The purpose of this paper is to provide an explanation on the impact of cyber-attacks on a small business, while informing on suitable practices and procedures that can be taken to protect data and network infrastructures. Looking further into the reasons small businesses are more prone to attacks and what those attacks are composed of will shed light on the severe problems these sectors of business face and what can be done to help.

This project will examine cybercriminal case studies affecting businesses, and scholarly literature in the forms of journals, periodicals, and conferences. It will focus on why small businesses are a specifically targeted, and the steps cybercriminals take to infiltrate them. It will also look at policy and procedures that small businesses practice that may put them at risk, and actions that businesses can take to better protect themselves against cyber-attacks. All of this will help me demonstrate the need that small businesses have for educating themselves on cyber threats, and changes that can be made to operations to better protect their network and data within.

This paper will interpret the technical data, as well as social and environmental forces that are critical to business. It will present information and practices that can be used by different departments of a business that will promote network security and data protection. Network and Executive Management departments must work together to prevent cyberthreats and allow the company to prosper.

This research will show that small businesses are a high risk for cyber-attacks, while providing the best solutions to implement to protect data and their network. Strengthening cybersecurity will require numerous variables like funding for technical solutions, building a security model or workforce, deploying security programs and software, providing support and training for internal staff as well as end-users, and implementing devices for network protection. It is important to have multiple points of protection to stop many of the inevitable attacks to their network. Managers with a proactive approach to cyber security will have fewer data breaches. Methods managers can use to increase cyber security in their business include staff training, implementing policies and procedures, purchasing cyber insurance, and conducting internal audits.

Literature Review

Cybersecurity is the practice of protecting against criminal or unauthorized use of electronic data, or steps taken to accomplish this. Cybersecurity is being implemented into all areas of life across the world. Corporations, governments, schools, and personal devices are being attacked everyday by cybercriminals that are looking to exploit network vulnerabilities. Nearly everyone will be affected by cyber-attacks at some point and need to understand the necessity for protection. To better understand the need for cybersecurity, one must know why and where these cyber-attacks happen, where they come from, and the reason behind them (Geer, 2015, p. 12; Balan, Otto, Minasian, and Aryal, 2017, p. 64).

Although "hacking" or cyber-attacks existed before 1990s, it is a good place to start in the history of cybersecurity to understand where it is today. In the first Gulf War, the United Stated demonstrated its dominance over the Iraqi army, and this dominance was broadcast over the news worldwide. This led to other countries investing in technologies to knock out satellites and penetrate cyber networks in the event of a future war with the U.S. Retired cyber warriors soon established cybercriminal groups who would later promote cybercrime worldwide as a business model. As cybercrime became more relevant, elite hackers joined forces to create "dumbed-down" resources to sell to aspiring hackers (Dunkel, 2017, p. 35). This has led to the modern day "virus or malware" that are a common component of hacking or cyber-attacks. The absence of adequate planning combined with advances in technology lead to weakness in a system or process. As technology advancements in networking and computing systems become more complex, hackers see a great degree of potential damage that can be accomplished through these weaknesses (Ghosh, 2004, p. 18).

Cyber-attacks have become an everyday event. In 2016, Cybersecurity studies found a significant level of high-risk security and severe threats to control systems. Many of these security vulnerabilities are due to outdated or improper equipment, absence of training, unestablished policies related to technology, and the nonexistence of data security enforcement legislation (Pelliccione, 2016, p. 12; Gordon, 2016, p. 184). As electronic information is being used more frequently for a wide variety of business and personal devices, it is also being stolen and manipulated at higher rates than ever before. Cybercrime has become so rampant with new technology that businesses have begun putting old, simple technology to use again. The old "analog" technologies that were put aside for faster, digital devices, are being re-implemented as they cannot be infiltrated by hackers (Lyons, 2014). In 2017, a new form of insurance became more widely used due to today's rampant slew of cybercrime, which is cyber insurance. Cyber insurance helps businesses after a cyber-attack or data breach by covering costs of legal defense fees, public relations campaigns, customer notifications and business interruptions. However, cyber insurance coverage has a variety of policies and small businesses need to work with insurance providers that understands their systems and practices. Businesses and organizations no longer have the luxury of being worried about a cyber data breach, they must now accept the fact that it will happen, and be prepared for a loss (Kerner, 2016; Rivera, 2018). To help small businesses, many insurance carriers have begun offering tailor-made coverage to meet lower-end budgets. The fact that the world needs insurance to protect themselves from a cybercrime is proof that no one is safe. No organization, big or small, that can hide from hackers that are actively trying to exploit the weaknesses in their network and systems (Murray, 2015, p. 18).

Although the internet has streamlined communication across the world, linking data from different countries almost instantly, it has come at an extreme cost for organizations that have fallen victim to cyber-attacks. If companies and organizations do not implement precautionary measures, they too run the risk of costly cyber-attacks. In recent years, news headlines have been riddled with accounts of cybercrime, not limited to any area of business, government, or the public sector (Arlitsch and Edelman, 2014, p. 48). In 2012, cyber-attackers infiltrated computers in embassies around the world, which included France, Belgium, Ukraine, China, Jordan, Greece, Kazakhstan, Armenia, Poland, Germany and the Soviet Union. Around the same time, it was reported that a Russian hacker group stole 1.2 billion usernames and passwords from over 420,000 different websites. A survey for a one-month period in 2014 showed 1.4 million cyber-attacks targeting financial data and banking software (Gaur, 2014). There have also been attacks on some "big name" corporations that occurred recently, which included Target, JP Morgan, and Home Depot, affecting millions of people. As more organizations put technology into use to better their daily tasks, business practices, and problem solving, more organizations will fall victim to cybercrime (Balan et al., 2017, p. 64).

Shockingly, no regulatory system exists to hold all organizations to an industry standard of protecting their network and data. This is because there is no agency regulating and forcing standard practices upon organizations. There are government and public groups that share information on standards of cybersecurity. Examples of these kinds of groups are ENISA (European Network and Information Security Agency) and EISAS (European Information Sharing and Alert System), who work to educate others on cybercrime (Balan et al, 2017, p. 64). Currently, the U.S. Congress does not have laws in place to enforce network security, but the Federal Trade Commission (FTC) is enforcing cybersecurity standards. Although the FTC can sue for lack of cybersecurity practices, there are no clear statements or guidelines of suitable cybersecurity policies and how to handle network threats. U.S. organizations would benefit from Congress passing legislation that would provide protections, resources and policy solutions to help support organizations without punishing organizations that do not have resources for change. This would be a large step for our nation and worldwide in preventing cyber-attacks; and if implemented correctly, it could lead to vast improvements in network security. (Worzala, 2017, p. 8; Gordon 2016).

Advances in technology change the way a company operates and the roles the employees play. Technology with higher functionality cuts out the need for humans performing tasks or processes, but also exposes vulnerabilities on a network or computer system. Small businesses are more often victims of cyber-attacks due to their lack of resources and willingness to use new technology. Small businesses often try to cut corners with free or low-priced software that can fulfill their needs while saving money. Unknowingly, this cheaper software can be easy to hack, letting cybercriminals wreak havoc on a network that may contain many security vulnerabilities (Harris, 2011, p. 12). The purpose of this paper is to examine cyber-attacks that are directed at small businesses and inform on suitable practices and procedures that can be taken to improve network and data security.

Introduction to Cybersecurity and Small Businesses

Technology has developed into a driving force in business, commerce, education, and social media. Never in history have humans depended so much on digital data spread across inter-linked networks, with the ability to access information at incredible speeds. Physical letters being mailed across the world have been replaced with electronic mail systems, letting users access their email messages within seconds. Consider the phrase, "With great power comes great responsibility" in terms of technology: when the world is making large strides in technological developments, there will be a higher level of responsibility to secure the data within. James Harris, network equipment manager at ZyXEL Communications, a large networking corporation, states that "more functionality breeds more vulnerability, and attackers have been quick to exploit weaknesses" (2011, p. 12). Unfortunately, many organizations do not take their responsibilities of security as serious as they should, ultimately leaving a door unlocked for hackers to steal their valuable information or the information of their customers.

As technology is being implemented in almost every sector of business, so are the security risks and threats that coincide with technological advances. Year after year, new reports describe increasingly advanced network security breaches and hacking efforts that were never thought possible. While the breaches are becoming more crippling to organizations, cybersecurity, which is the practice of protecting against unauthorized use of data, is on the rise. Although businesses are not subject by law to maintain certain cybersecurity practices, if they do not begin implementing policies and procedures to protect their data they will eventually be subject to an attack. A recent executive summary on cybersecurity by the Council of the Better Business Bureaus (BBB) directed to small businesses effectively allocating resources for cybersecurity, stated that small businesses "cannot afford to make mistakes when committing to such important and potentially expensive investments and need to be as effective as possible in the allocation of resources" (2017, p. 3).

The U.S. Small Business Administration (SBA) defines as small business as a business with a maximum of 250 to 1,500 employees, depending on the industry. They are privately owned corporations, partnerships, or sole proprietorships that have less revenue than larger businesses. Small businesses with less than 20 employees make up 89.6% of all U.S. business enterprises, and 23 million businesses in the United States have no employees at all and operate solely by the owner (McIntyre, 2018). For the purpose of this paper, small business is defined as business organizations within the employee range stated by the SBA that do not have enough resources to build advanced security systems reaching all areas of their organization.

Small businesses may have been able to get by with minimal cybersecurity in the past, but now they must implement better solutions to protect their data. In an article focused on cybersecurity threats, Darren Guccione, co-founder of Keeper Security, states "that cyber-attacks and data breaches within small sized businesses will increase dramatically in 2017" and businesses "need to invest in strong security defenses or risk going out of business" (Kerner, 2016, p. 1). A 2018 cybersecurity report performed by the IT and security company, Switchfast Technologies, points out a devastating fact, that

> for many businesses, these cyberattacks can be financially devastating — 60 percent of small businesses that suffer a breach are likely to go out of business within six months. From a loss of customers to a damaged reputation, small businesses have a lot to lose, and one in three business owners have no safeguards in place to combat a cyber breach. (p. 2)

Threat levels are tremendously high, and cybersecurity is now a necessity, rather than a practice implemented solely by tech savvy organizations.

Small businesses need to educate themselves and promote cybersecurity practices to keep their business and data safe. This paper will provide examples of security threats that small businesses face, and reasons why criminals attack them. The statistical data on incidents shows the importance of implementing cybersecurity at the small business level. The research will provide IT or system administrators and executive management approaches to building a better cybersecurity environment. My approach will be to provide examples of best practices to implement for protecting data and a network. By presentation benefits from proactive cybersecurity policies and practices as they relate to the business. Overall, my intent is to provide a small business with an explanation of why they are a high security risk to better understand the appropriate cybersecurity practices to implement.

Why Small Businesses?

Small businesses are a prominent example of the "American Dream". Many citizens of the world have flocked to this country for an equal opportunity at success and prosperity through hard work and determination. Although large companies and corporations can produce significantly more capital than their smaller competitors, small businesses make up a great portion of the nation's economy. Small businesses

> represent a majority of employers, create around two thirds of the nation's new jobs, employ about half of the nation's private sector work force, provide half of the nation's nonfarm, private real gross domestic product, and contribute a significant share of innovations, even in the economic recession. (Alexander, Truell, Woosley, and Zhao, 2011, p. 42)

The small business plays a big role in our nation's makeup and economy, affecting all walks of life in America. A recent report into cybersecurity states, "In 2016 alone, over 14 million American small businesses were breached by cybercriminals. And with over 30 million small businesses listed in America, that means 46 percent of all small businesses will likely become the victim of a cyberattack" (Switchfast, 2018, p. 2). With small businesses being an important part of our nation's makeup, it is beneficial to help this sector of business with knowledge on cyber-attacks and data breaches to provide them with tools to protect themselves.

Coinciding with small businesses is the rise of the technology empire over the past 30 years. Technology companies began as a small and niche business, which have grown into large, ever expanding, business networks that build upon old technologies to bring to life new ones. During the 1990s, the personal computer was becoming a household tool with the adaptation of the internet. As internet sites grew from a place where users simply read content, it transformed into today's web with sites sharing personal and confidential information. Users now submit their own content into web sites, share photos, and chat or edit documents together in real time. While technology has become a driving factor for conducting business, small businesses have been taking advantage of these technologies (Harris, 2011, p. 12).

One of the positive outcomes from advancements in technology is cutting down the time, manpower, and skill it takes to perform certain tasks. "These technologies have brought small businesses the same benefits as their larger counterparts. Online applications, advanced search capabilities, and real-time messaging technologies enable Small-to-Medium Sized Businesses (SMBs) to build scalable, highly-responsive technology infrastructures to support their businesses" (Harris, 2011, p. 12). With modern technology, small business can now compete with larger businesses that have far more resources. However, more access to technology only leads to more vulnerability for a cyber-attack. As time goes on, some of these small businesses may evolve into larger businesses that have much more complex processes, but correct practices in cybersecurity can never start too early.

The threat of cyber-attacks and hackers is not a new-found harm for businesses, although it coincides with the adaptation of computing technology. In 2000, President Clinton held a cybersecurity conference at the White House for the first time in history. It was focused on the rise of cyber-attacks and what is to be done to stop them. President Clinton announced an unprecedented amount of $2 billion for federal funding to research and invest in new cybersecurity technologies. He stated that cyber-attacks can be a "replay of what always happens" with changes to the ways communication is conducted, providing new routes for making money. He goes on to point out that in history someone always tries to take advantage of the new systems, and "we will figure out how to deal with it" (Hunker & Kelly, 2012, p. 1). The end statement of finding a resolution is notable, as cyber-crime and data breaches are progressively getting worse. Fast forward to the 2017, Matt Rosenquist, Cybersecurity Strategist, explained "that the same controls that provide auto assist to parallel park your vehicle can be hacked to force a car, or hundreds of cars, to accelerate to high speeds and turn abruptly, causing fatal accidents" (Dunkel, 2017, p. 37). This is just one example of how criminals can alter technology with intent to damage or destroy.

As more everyday home and work devices are becoming networked, the process of using the internet to pass data back and forth, more instances of cyber-attacks are occurring. The Serious Organized Crime Agency stated the global cyber-crime as of 2017, has surpassed narcotic trafficking in illicit revenues. Tom Kellermann, cyber intelligence expert, author, professor and Global Fellow leader, suggests that cybercrime has changed from the old-style burglary to what is now a digital home assault. He goes on to state that, "The economic security of the West is in jeopardy. Civilizing cyberspace must become a national priority" (Dunkel, 2017, p. 37).

In recent years, there have been cyberespionage campaigns involving viruses that penetrate Government and Embassy computers and systems. Infected computers for Government officials have been discovered in major countries across the world. Cybercriminals have found ways to infiltrate businesses that previously would not have been looked at as a target. They use tools to evade traditional antivirus programs and legacy firewalls, eventually gaining complete control over infected systems to steal critical data from companies. Cisco, a technology conglomerate that develops, manufactures and sells networking and telecommunications hardware, equipment and services, informed in their 2014 Security Report, that outdated software, incorrect code, abandoned digital properties, and user errors in organizations contribute to the enemy's ability to exploit weaknesses (Gaur, 2014).

Data breach incidents have become increasingly popular and exist for any level of user accessing an array of different websites. With data breaches, hackers will steal usernames and passwords that can correlate to an email address, used to access data behind closed doors.

> Such data breach revelation poses three main threats: first, personal and sensitive information has been put at risk and can be used by criminals. Second, the lost credentials could result in identity theft. Third, and potentially the most significant for businesses, attackers can impersonate legitimate users to gain access to organizational assets and confidential information. (Gaur, 2014)

Large companies containing more username and passwords are not the only target, many small or personal websites are also infiltrated. The 2018 cybersecurity report performed by Switchfast states that

> Despite common misconception, small businesses are prime targets for hackers because of their size. Thieves aren't concerned about how big a business is; as long as there is financial gain to be had from stealing, any company is fair game. (p. 2)

All businesses in the world, large or small, are dealing with cyber threats on an uncontrollable level, whoever has the least amount of protections in place will suffer the consequences. Small business can easily fall into this category, due to the nature of the business makeup. Many do not have the resources or knowledge to implement security that will adequately protect their network and data. Such limited level of resources pertains to capital, hardware implementation, expertise knowledge, staff training, and policies and procedures. Small businesses implement cybersecurity solutions that appear beneficial from advertising campaigns or a sales representative, yet many of these solutions are not providing adequate protection for networks or computer systems. Roger Schell, a Distinguished Fellow at the University of San Diego Center for Cybersecurity Engineering and Technology, states that

> Current approaches to cybersecurity are more focused on saving money or developing elegant technical solutions than on working and protecting lives and property. They largely lack the scientific or engineering rigor needed for a trustworthy system to defend the security of networked computers. (2016, p. 20)

Another factor to consider is the lack of executive level promotion for cybersecurity practices and policies. All of which puts a target on the back of any small business that exists in today's cyber world.

Reasons for Cyber-attacks

There is a common phrase used to remain ignorant or uninformed about situations, which is "What you don't know won't hurt you". This phrase will allow someone in a negative experience to not have a sense of responsibility, as a problem cannot be fixed if it is not known. At one point, this phrase could be used as computer users only had a limited number of features to work with. The internet was once a passive tool where users would simply read information, but now an unknowing click on the wrong image can infect your computer with a virus that lets a hacker access your computer to steal data. In an article by Elizabeth Leary, she reports that

> a survey of small-business owners by Nationwide found only 13% of respondents believed they had experienced a cyberattack. However, when owners were shown a list of specific examples of attacks, including phishing, viruses and ransomware, the figure of those reporting attacks increased to 58%. (2017)

Understanding the reasons why small businesses are targeted and do not have proper lines of defense are crucial to fixing the problems these businesses face.

There can be many problems that lead to small businesses experiencing cyber-attacks. A commonly mentioned practice is the lack of knowledge and training in all levels of a company. A networking professional or IT staff can implement hardware and software to protect against outside attacks, loss of data, and other occurrences that could harm a company. However, it only takes one user providing their username and password to the wrong person or website to start the process of a cyber-attack. A guide to cybersecurity published in *Business News Daily* describes that small businesses are

> easy to attack due to this complacent attitude [of unknown threats] and a lack of investment into cybersecurity measures. Since security breaches can be devastating to a

> small business, many SMB owners are more likely to pay a ransom to get their data back. (Rivera, 2018)

Although a lack of knowledge is clearly a cause, we see that the investment in training users to gain knowledge is a contributing factor.

More of our devices and work practices are being inter-twined with technology to help in a variety of ways. But as technology spreads to new areas, there must be hardware and software put in place to guide and protect these technologies. For example, if a business would like to implement a door security system to use name badges to unlock office doors, there would need to be a controller and management system for the devices governing the doors to lock or unlock, as well as staff trained on the system to manage it. Depending on how much capital a small business has, they may have to pick and choose which technologies to implement. If there is a lack of knowledge for cybersecurity, it will correlate to poor use of technology to protect a network, data and users.

The cybersecurity report by Switchfast shares some shocking statistics further proving that a lack of knowledge is leading factor in cyber vulnerability. Forty-four percent of small business leaders and 66% of small business employees connect to public WiFi to perform work tasks. Seventy-six percent of leaders and 69% of employees have not activated multi-factor authentication for their work email. Twenty-two percent of leaders and 19% of employees share their work email password with coworkers and assistants. Forty-four percent of leaders and 62% of employees use their work computers to log into personal social media accounts (2018, p. 7). Do you fall into any of these categories? Do you think that any of these examples would not harm the company you work for? If so, you are not alone, but may be contributing to the cybersecurity dilemma many of these companies are facing. As Switchfast points out, "Negligent employees remain the number one cause of data breaches at small businesses across America" (p. 6).

Another reason why small businesses experience cyber-attacks is the lack of money and resources. Untangle, a cybersecurity innovator for the below-enterprise market, surveyed more than 350 SMBs globally in 2018 to learn more about the current state of cybersecurity. They found the largest challenge for small businesses in relation to cybersecurity is budget constraints (at 47%). Many small businesses lack resources in the area of IT professionals that can help with implementing, training, and maintaining cybersecurity. This is primarily because not all small businesses deem it affordable to pay for an employee or consultant in this position. Also, the small business may not think it would or have been targeted by a cyber-attack and feel that security is not needed. The survey by Untangle goes on to mention that most small businesses are not able to handle security threats because

> more than 50% of businesses distribute IT security responsibilities across other roles, meaning those employees are pulling double duty. On top of that, less than 30% have a dedicated IT security professional on staff. While most SMBs (75%) have fewer than 5 physical locations and even less (60%) have fewer than 100 end-user devices to manage, IT security still remains a constant struggle for businesses with limited resources. (Untangle, 2018, p. 3)

Clearly more resources need to be put into protecting the businesses networking and data.

The small business report on cybersecurity by the Council of the Better Business Bureau stated that a lack of time is a significant factor for not implementing best practices for protecting a network. Lack of time had the same percentage as a reported factor to hinder cybersecurity efforts as did the lack of information (2017, p. 12). The Untangle survey also points out the burden of limited time and research to understanding new threats can plague small businesses (2018, p. 4). It is commonly said that time is money, and both are limited resources for a small business.

Another finding is how important it is for the stakeholders or board of the company to build a cybersecurity culture. They must understand and care about cybersecurity so that it trickles down into all parts of the business and to all employees. A recent article in *Security Magazine*, points out the senior executives need to be more committed to cybersecurity to better understand what is actually at risk. Small businesses

> tend to think that, because they aren't dealing in billions of dollars, cybercriminals won't bother attacking their networks. While they may believe they have less to lose to a cyberattack than these organizations, there is a greater risk that their business might not survive the fallout or clean-up. (Chevalier, 2018)

By promoting cybersecurity, executives may be saving their company from loss of data or records, and potentially from a threat that could bankrupt their business.

Also, to mention, is the threat of an inside attack. The Untangle survey breaks down areas that small businesses that contribute to cyber-attacks, and 29% of instances are caused by "rogue" employees that do not follow guidelines (2018, p. 4). A report dedicated to insider threats on businesses points out the three most common types of insiders that pose security threats: regular employees; privileged IT users and admins; and Contractors, services providers, and temporary workers or previous employees. Although these three areas can make up a large portion of staff, the intent is most commonly non-malicious, and accidental. Cybersecurity Insiders report that "The most common culprit of insider threat is accidental exposure by employees" (2018, p. 10).

For small businesses, there are many causes for cyber-attacks and reasons why the businesses are not prepared. Most notably the lack of capital the business is able to spend on cybersecurity, followed by its constraints on time to research and understand new threats. There is also an absence of manpower to monitor and manage security, and a limited amount of knowledge and training. Some of the smaller contributors are rogue employees, lack of policies and the use of personal devices that are not managed or monitored by the employer. Understanding why small business may be attacked is the first part to the issue, while the latter reveals the types of attacks small business face on a daily occurrence.

Type of Attacks on Small Businesses

Any small business can fall victim to a cyber-attack for several reasons, depending on the company makeup and what policies and practices they have in place. There are diverse forms of attacks, with completely different focuses and methods that hackers can use to steal information. As Andreas Rivera points out, "In almost every case, the end goal of a cyberattack is to steal and exploit sensitive data" (2018). Understanding the different threats that small businesses face will help to stop attacks from being successful. When executives are educated they can put trainings, new technology and hardware, as well as policies and procedures to use to better protect their company. As regular staff are trained and learn about the different threats they face, they can make better decisions and stop data breaches before a serious attack is at hand. Although there are many kinds of threats and attacks, the focus will be on those that are most commonly found in small businesses.

Malware

One of the most common threats that has been seen in all types of small businesses for past years is malware. "This umbrella term is short for "malicious software" and covers any program introduced into the target's computer with the intent to cause damage or gain unauthorized access" (Rivera, 2018). The survey performed by Untangle shows that 27% of small businesses have experienced a malware attack within the last 12 months (2018, p. 5). Malware can alter computer functions, delete personal or system files that can cause a system failure, and steal data and information. It also encompasses many other types of threats, some of which will be discussed, including: spyware, ransomware, worms, trojans, and even the common phrase "virus". Although malware can pose a serious threat to a computer system and come in many different forms, there is popular and effective malware removal software that is relatively low prices or free that small businesses can take advantage of.

Ransomware

Ransomware is one of the fastest-growing types of security breaches and can cause serious damage due to the amount of money businesses will pay. Ransomware is a type of malicious software that infects a computer's operating system and eventually demands a ransom. Typically, ransomware will lock the user out of the computer or certain files and demands money in exchange for access. There are certain attacks that threaten to publish private information if a specific amount of money is not paid (Rivera, 2018). The Untangle survey shows that 15% of small businesses experienced some sort of Ransomware within the last 12 months (2018, p. 5). The most devastating details with ransomware attacks is the capital lost in an attack. A CNBC article focusing on research into Ransomware, points out that,

> cost of a single ransomware incident (where an attacker encrypts a computer or network until a ransom is paid) can cost a company more than $713,000 on average, due to the costs of paying the ransom and related losses, such as value of lost data, the expense of improving infrastructure and repairing brand image. (Graham, 2017)

Phishing

One of the newer attacks that has become increasingly popular is phishing. The Untangle survey in 2018 shows that 33% of small businesses experienced a sort of phishing attack within the last 12 months, which was the highest of all cyber-attacks (p. 5). A brief description of a phishing attack is a message or any kind of communication imitating a trustworthy source, such as a bank or cell phone company, with purpose to deceive a business or user into providing sensitive information or passwords. In a journal article on cybersecurity, writers Kenning Arlitsch and Adam Edelman give a detailed explanation on this kind of attack,

> A phishing attempt often takes the form of a legitimate-looking email that claims to be from an organization or person that is familiar to the targeted user. Spear phishing takes this approach even further with targeted messages that are tailored for specific organizations or even to single individuals. The messages sometimes purport to alert the user to a problem with his/her account and request some action be taken. Sometimes personal or financial information is requested and surprisingly that approach still yields some success with gullible users. (2014, p. 50)

Phishing sites can imitate actual websites with very minimal difference, prompting users to login with their username and passwords. This can take the form of email, banking, social media, or any number of websites with a login page.

Denial of Service (DoS) Attacks

Small businesses can be easy targets for denial of service attacks as they typically do not think hackers will target them.

> In a typical DoS attack, a website, email, or network will be flooded with so many requests, or so much data, that it will cease to function. In a distributed DoS attack, an

> organization's computers may be taken over and used to attack a different target. That could mean hundreds or thousands of compromised computer networks are joined together to immobilize a single business. (Piper, 2014, p. 40)

Often a DoS attack will be implemented by hackers so those affected will focus efforts in one area, leaving other aresa of the network vulnerable. In an article about DoS attacks on small business, Joy Reo mentions,

> many small businesses assume that hackers target only high-profile companies, and use large-scale attacks that cripple a website or application. However, the truth is that a variety of organizations are victims of DDoS attacks, and research (from our Q2 - Q3 2017 DDoS Trends Report) has shown that most DDoS attacks are small, low-threshold attacks. (2018)

Advanced Persistent Threats (APTs)

Advanced persistent threats, or APTs, were once focused on larger businesses, but in recent years small businesses have seen a rise with these attacks. With APTs, attackers take their time to break into a network, and do this in many phases or with different routes in order to avoid detection. After penetrating the network, the attacker tries to continue undetected while establishing a foothold in the system. If a system breach is detected and repaired, the attackers have made other routes into the network readily available and can continue their attack (Rivera, 2018). Kaspersky, a cybersecurity company for small to large sized businesses, mentioned the following in relation to small businesses needing to protect themselves against APTs,

> APT is a method of attack that should be on the radar for businesses everywhere. However, this doesn't mean that small- and medium-sized businesses can ignore this type of attack. APT attackers are increasingly using smaller companies that make up the

> supply-chain of their ultimate target as a way of gaining access to large organizations. They use such companies, which are typically less well-defended, as stepping-stones. (2018)

Common Scams

There are a variety of "scams" that hackers or cybercriminals use to try gain access to information, certain systems, or the network for a small business. Depending on a company's makeup, these sorts of scams can cause serious issues for a small business, similar to any of the attacks already described. The FTC released detailed information on the different kinds of scams that small businesses face in May of this year. They listed a few notable tactics of scammers, which are important to help determine a scam and stop it before it leads to a full-fledged cyber-attack. The scammer tactics to watch for are: they pretend to be someone you trust, use intimidation and fear, create a sense of urgency, and use untraceable payment methods (2018). The next section will discuss the scams that are mentioned by the FTC that plague small businesses.

Fake Invoices and Checks

Scammers make up phony invoices that appear to be for goods or services that the business uses. They expect the person who is paying the bills will assume that the phony invoices are valid and pay the full amount. Depending on the makeup of the fake invoice, other critical data from the business can be passed along to the scammer as well. The FTC points out that "Scammers know that when the invoice is for something critical, like keeping your website up and running, you may pay first and ask questions later. Except it's all fake, and if you pay, your money may be gone" (2018, p. 5). Along with fake invoices are the use of fake checks. A scammer will overpay with a check, and then ask that the difference be sent to a third party.

There is usually some kind of story to explain the overpayment. The company will then deposit the check, but by the time the bank notifies the company that the check is bad, the scammer will already have the difference that was sent (p. 6).

Directory listing and Advertising Scams

Scammers try to talk someone at the company into paying for a nonexistent advertisement or a listing in a nonexistent directory. Often the scammers pretend to be from the Yellow Pages to establish credibility. They commonly ask the company to provide contact information for a "free" listing, or imply they are only confirming information for an existing order. After all of this, the scammers will send the company a large bill and use details or even a recording from a previous call to pressure the company into paying (2018, p. 5).

Utility Company Imposter Scam

Like fake invoices, scammers will pretend to be the gas, electric, or water company. They will create a sense of urgency by informing the service provided is about to be interrupted. The FTC mentions that,

> They want to scare you into believing a late bill must be paid immediately, often with a wire transfer or a reloadable card or gift card. Their timing is often carefully planned to create the greatest urgency – like just before the dinner rush in a restaurant. (2018, p. 5)

Government Agency Imposter Scam

Also, like fake invoices, is the government agency imposter scam where the scammers try to impersonate government agents. The phony agents will threaten to suspend their business license, impose fines, or take legal actions if the company does not pay certain taxes, government licenses or registrations, or other fees. Specific examples that the FTC lists are,

> Some businesses have been scared into buying workplace compliance posters that are available for free from the U.S. Department of Labor. Others have been tricked into paying to receive nonexistent business grants from fake government programs. Businesses have received letters, often claiming to be from the U.S. Patent and Trademark Office, warning that they'll lose their trademarks if they don't pay a fee immediately, or saying that they owe money for additional registration services. (2018, p. 5)

Tech Support Scam

The tech support scam starts with a call or fake pop-up message from a trusted company that informs the company there is a problem with their computers security. The scammers may ask you to pay them to fix a problem that does not exist or register the company for a phony computer maintenance program. The goal with this kind of scam is for the scammer to get money, as well as access to the computer that enables them to steal sensitive data (2018, p. 5).

Business Promotion and Coaching Scams

Scammers will try to sell non-existent business coaching and internet promotion services. They promise vast results and exclusive market research by luring companies with fake testimonials, videos, seminar presentations, and telemarking calls. The scammers will start with very low fees to intrigue the company, and later invoice for thousands of dollars. This can leave a small business without the help they were needing and hoping to receive, as well as a substantial debt (2018, p. 6).

Credit Card Processing and Equipment Leasing Scams

Credit card processing and leasing scams are directed at small businesses as they are looking for ways to save on costs. The scammers will promise lower rates for credit card processing, or even better pricing for leasing equipment. They deceptively use fine print, half-truths, and even lie to get a company to sign a contract with them. Scammers have been known to ask business owners to sign documents that are missing certain terms, or even change the terms after the fact. The FTC gives signs for this kind of attack, that the scammer will "refuse to give you copies of all documents right then and here, or will try to put you off with a promise to send them later" (2018, p. 6).

With so many reasons why businesses fall victim to cyber-attacks, and all the different threats that can occur, how can a business really know where they stand with their protection and if they need to invest more into their cybersecurity technology and practices? The answer depends on the current systems they are using, and how they are using them. There is a wide range of security that can be implemented today. A small business could completely protect itself at any time with guidance of a networking professional and money to purchase equipment and software. But really understanding how your current technology is being used, and the vulnerabilities associated is where the focus should be. James Harris, manager at ZyXEL Communications poses the following question:

> Modern internet security is an exercise in probability. It is impossible to guarantee 100% security – a determined hacker may still be able to gain access to a company's system. But the more points protection that a company covers, the more likely it is to fend off the majority of generic attacks on the Internet. Can you afford not to cover your bases? (2011, p. 14)

What Small Businesses Can Do

After investigating the reasons why small businesses are targeted and the different threats they face from attackers, the focus will now be on what small businesses should do to protect themselves. Small businesses need to be implementing solutions that focus on the importance of cybersecurity or else they will never get ahead of attackers. In a *Security Magazine* article, it is stated that "This means the systems they use should include ways to encrypt data, authenticate users and authorize access" (Chevalier, 2018). Promoting good cybersecurity practices, along with hardware, software, and knowledge will significantly help a to protect a small business. Other items that need to be focused on are training, implementing cyber insurance, expertise help, backup or restore systems, and a cost-benefit analysis tool for cybersecurity.

Small businesses are most prepared for threats when higher level management sincerely cares about the topic.

> Those that want to be successful should look to address cyber-security head-on. This means putting every employee on the front line of defense, by creating a culture of cyber-security. This begins with the board; every executive should be aware of the threats that the business is facing and the importance of maintaining robust cyber-defenses. It is then vital to ensure that your employees are properly trained and aware of the best cyber-security practices. The board should take it upon themselves to skill and re-skill employees to make them security experts in the business. If every employee is engaged in the culture of cyber-security, this will ultimately reduce the risk of a breach caused by human error. (Keegan, 2017, p. 17)

Cybersecurity needs to be promoted from the top of the company, so its importance is valued and practiced.

When high-level managers are educated in cybersecurity, they will strive to implement the best solutions to protect their data and networks, as well as train their staff. An area of cybersecurity that is becoming a focus for small business to reduce damage from attacks is detection. When threats are quickly detected, the overall impact and data recovery time is severely less. In a study by Verizon, it was found that 68% of breaches took months or longer to discover (Chevalier, 2018). The study done by Switchfast shows that high-level managers can significantly help with threat detection by promoting staff to speak up right away if they have been victim to an attack, and that they will not be punished.

> Above all, it's important for employers to remind employees they will not get in trouble for reporting a cyberattack, even if they were the cause of it. Everyone makes mistakes, and even the most tech-savvy employee is bound to have a misstep that results in an unintentional breach. By reassuring workers they won't be reprimanded for a cyberattack, small businesses will likely see the number of reported incidents rise, giving teams more time to respond to threats before they spiral out of control. In an IT security crisis, every second counts. (2018, p. 10)

Management really sets the tone as how far a small business will go when it comes to cyber threats. Small businesses that have proactive and supportive management will be better prepared for threats and learn from attacks to better protect their network and data.

Implementing hardware and software that focuses on cybersecurity will highly protect any small business and be a first line of defense against threats. The most important piece of hardware for network security is a trusted firewall. Firewalls create an added layer of protection by blocking unauthorized users from accessing a computer or network (Rivera, 2018). They can range from inexpensive with low-end features, to very sophisticated and costly. With the amount of threats in today's cyber world, businesses should stay away from the low-end model firewalls and spend a little more up front on a good firewall that will be more beneficial in the long run. Tony Howlett, author of Windows IT Pro, mentions the following about installing the proper firewall for your business, "you should treat your firewall appliance like any other OS, perhaps even more so because it guards the entrance to your network. Be sure to regularly review installed firewall appliances for required updates and maintenance" (James, 2012, p. 135).

Firewalls available today offer advanced built-in technologies, which used to be available only by separate devices called Intrusion Prevention Systems (IPS). Integrating these devices helps small business to reduce costs for devices and managing multiple systems. More importantly than installing a firewall, is properly configuring it to block unwanted outsiders from penetrating any weakness. Mangers should discuss their company's practices and procedures with a networking professional who can analyze the network and configure a firewall that best suites the company and their networking needs (James, 2012, p. 133). In comparison, what good is an expensive, quality piano, if it is not tuned correctly by professional piano tuner?

James Harris of ZyXEL mentions other devices that can be used with firewalls to add extra protection like email and web threat scanning, limiting web content for users, and searching for suspicious traffic on the network. These types of devices are called Unified Threat Management appliances. These devices use new technologies built on traditional firewall systems that inspect details of the network that regular firewalls cannot. Firewalls and added security appliances will significantly help a small business with network security by stopping attackers from penetrating computers or a network (2011, p. 13).

Small Businesses can also take advantage of different cybersecurity software that will greatly help with threat protection. Antivirus software is the most common, has existed for many years from various sellers, and can defend against many types of malware including: ransomware, spyware, worms, and trojan horse viruses. Antivirus programs can also be quite cost efficient, and even free depending on the features or protections the software offers (Rivera, 2018). Other software to mention is a network content filter, enabling companies to screen or block certain websites known to be harmful or inappropriate. This helps small businesses to control what content is viewed on their network and protects against sites carrying malicious content looking to infect unprotected computers. Software nowadays can also have built in firewalls, enabling protection at the software layer, in case a threat has made it past the physical network firewall (Switchfast, 2018, p. 8).

Another practice related to software that will greatly benefit a small business is keeping all software up to dare. Computers that are not updated are more prone to crashes, security breaches and cyber-attacks. Hackers specifically look for outdates systems with security vulnerabilities, leaving an outdates computer at higher risk for being attacked (Rivera, 2018). In a journal focusing on cyber peace for businesses, Scott Shackelford speaks on the importance of updating software as a top cybersecurity best practice. He writes, "Keep all software and operating systems up to date—especially Windows, but also programs like Adobe Reader, Flash, and Java, which are often convenient backdoors that can be closed through frequent updates" (2016, p. 544).

Small businesses should also be using up-to-date methods of encryption and authentication. Encrypting data helps protect sensitive information and improve the security of communication with users connecting to resources like servers. When data is encrypted, the data in the file is altered, only to be unlocked by a certain "key". If an unauthorized user attempts to read an encrypted file, they will not have access to this key, leaving the data unattainable. The way businesses control access to those encryption keys is through authentication. Authentication includes username/password combinations, tokens, certificates to identify trusted third parties, and other techniques. This allows small businesses to determine if a user, server or client app is who it claims to be, and then will verify access to programs or data, including encryption keys (Chavelier, 2018, p. 3). A recent authentication process known as "two-step user authentication" can be implemented into login processes to reduce the likelihood of password cracking. This feature will send a one-time code to a confirmed cell phone of the user attempting to login. The user then enters in this one-time code after their username/password to gain secure, authenticated access (Rivera, 2018).

Managers need to be proactive at providing information and training to all staff in areas of cybersecurity. The BBB surveyed the top factors that hinder advancements in cybersecurity and the lack of information and training were reported at 24% for small businesses (2018, p. 12).

> By increasing education and awareness and leaning on a service provider for proactive monitoring and response around cyber threats, small businesses can begin to improve their company's cyber hygiene habits and alleviate fears of a breach reaching the ears of customers. While it's important to install firewalls and filters to protect against internal threats, it's equally crucial for companies to strengthen resiliency among their employees. (Switchfast, 2018, p. 10)

Although it may take managers time and capital to get their staff trained, it will save more money in the long run from users not falling victim to a scam or attack. Higher level management must implement training and a knowledge-building approach to stay ahead of cyber threats.

Providing staff with knowledge and training does not have to be costly. The FTC has resources online dedicated for small business that provide knowledge about cybersecurity basics, physical security, ransomware, phishing, business email imposters, tech support scams, vendor security, cyber insurance, email authentication, and securing remote access. There are guides for employers on how to properly provide knowledge and trainings, as well as implement policies and procedures all focused on cybersecurity. There are also in-depth training materials on various subjects that can be ordered, as well as cybersecurity quiz options. This information can be accessed at: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (2018). Many hardware and software developers often offer a one time, or yearly training on their systems to keep their customers secure and up to date on correct practices. Small businesses need to take advantage of vendor trainings at any chance and can even hire a cybersecurity company to evaluate their business practices and offer training tailored specifically for that company. Training for staff should be researched by managers or those with a high understanding of the network and systems.

Although budget constraints make up a large portion of why small business cannot protect themselves, there is hope for budget friendly cybersecurity practices.

> On the cost-effectiveness side, only 42% believe that there is a limit to cybersecurity spending. Per the Gordon and Loeb Framework7 to Assess Cost Effectiveness of Cybersecurity – there is a point where a dollar invested in cybersecurity results in less than a dollar's worth of protection. (BBB, 2018, p. 7)

Gordon and Loeb have developed a model to help small businesses figure out how much they should invest in cybersecurity. The 5 steps for determining the Return on Cybersecurity Investment are summarized below:

> Step 1. Estimate Loss - For each information set in your organization, estimate the potential loss that you could incur in a cybersecurity breach. ($LOSS).
>
> Step 2. Estimate Risk - For each information set in step 1, estimate the probability of loss from a cyber breach of that data. (%RISK).

> Step 3. Identify Investments - For each information set in step 1, identify the potential investments that you could make in cybersecurity. ($INVEST).
>
> Step 4. Estimate Savings - For each potential investment in step 3, estimate the reduction in the probability of a cyber breach due to the additional cybersecurity investment. (%SAVE).
>
> Step 5. Calculate - Compare the investment cost ($INVEST) to the potential savings, where: Potential Savings = ($LOSS) X (%RISK) X (%SAVE). As long as the potential savings exceeds the cost of investment, then it is a cost-effective measure that should be implemented. (2018, p. 21)

This model demonstrates the likelihood of money loss due to cyber-attacks and is intended to help small businesses asses their risk and reflect on current practices and policies.

The last practice to mention that helps protect small businesses is cyber insurance. This is a new form of insurance that businesses can purchase to help to cover damages in case of an attack. Andreas Rivera references a survey by insurance company Hiscox, that "only 21% of small business have some form of cyber insurance, and 52% indicating they have no intention of acquiring any" (2018). Rivera mentions this is because most small businesses think cyber insurance is intended for large companies, and many insurance carriers are offering specific coverage for smaller businesses with smaller budgets but similar risk-exposure levels. He also discusses that small businesses need a combination of first- and third-part coverage. First-party coverage includes costs incurred because of a breach, such as legal expertise and customer or public relations campaigns. Third-party coverage protects from breaches that expose sensitive information resulting in affected parties suing for losses (2018). Small businesses that purchase cyber insurance understand that even with training, hardware, and software, one data breach could have devastating effects. They must also consider the cost to implement cyber insurance and research the best available options for their company. For a company to meet their cyber insurance policy, certain policies and procedures must be in place or else the company may lose coverage for the attack or data breach. Small businesses need to go over all details with their insurance company first and be prepared for their due-diligence processes after an attack. Cyber insurance is a final safeguard a business can implement to dismiss financial responsivity for the loss of sensitive data.

Looking Forward

Small businesses are a significant part in our nation's makeup, workforce, economy, and even a slice of the American dream. Due to a rise in technology used to compete with larger corporations and a sense of being too insignificant, small businesses have been experiencing a high level of cyber threats and attacks. The lack of knowledge, training, professional resources, time and capital that small businesses face leave them at the mercy of cybercriminals. Small businesses must confront attackers that are highly skilled in manipulating identities, data, and professional services. Although resources may be limited, the time has come for all small businesses to invest in their cybersecurity practices and policies.

By increasing awareness and knowledge, along with adding new technologies that search for and block cyber threats, small businesses can start improving their practices and policies associated with cybersecurity. Training and providing staff with resources on proper cybersecurity practices can be inexpensive and will be more successful when promoted from top-level managers down. Firewalls and filters that block network threats are a must, along with antivirus tools and a proactive approach for updating all operating systems and software. With cyber insurance, small businesses can feel a sense of peace knowing they have protection for damages of stolen data.

No matter the industry, all small businesses need to spend time and resources evaluating their current state of cybersecurity. To ensure protection, staff needs to be engaged in protecting the network and data by promoting a culture of carefulness and preventive practices. By evaluating current risks, adopting a cybersecurity path, training and implanting new age technologies, small business can be prepared for today's security threats and ward off any level of attack.

References

Alexander, M., Truell, A., Woosley, S., & Zhao, J. (2011). A Vulnerability Assessment of the U.S. Small Business B2C E-Commerce Network Systems, *The Delta Pi Epsilon Journal*, 53(1), 45-52. Retrieved from http://ezproxy.uvu.edu/

Arlitsch, K., & Edelman, A. (2014). Staying Safe: Cybersecurity for People and Organizations. *Journal of Library Administration*, 54(1), 46-56. doi:10.1080/01930826.2014.893116

Balan, S., Otto, J., Minasian, E., & Aryal, A. (2017). Data Analysis of Cybercrimes in Businesses. *Information Technology and Management Science*, 20(1), 64-68. doi:10.1515/itms-2017-0011

Chevalier, M. (2018). Small and Mid-Sized Businesses Need to Focus on Cybersecurity. Retrieved from https://www.securitymagazine.com/articles/89202-small-and-mid-size-businesses-need-to-focus-on-cybersecurity

Council of the Better Business Bureau. (2017). State of Cybersecurity Among Small Businesses in North America. Retrieved from https://www.BBB.org/stateofcybersecurity

Cybersecurity Insiders. (2018). Insider Threat: 2018 Report. Retrieved from https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Dunkel, D. (2017). The Cyber 101 Discussion: Whether you are a security executive, integrator or manufacturer, a cyber discussion is much needed in your organization. *Security Magazine*, 54(8), 34-38. Retrieved from http://ezproxy.uvu.edu/

Federal Trade Commission. (2018). Protecting Small Businesses: Scams and your small business. Retrieved from https://www.ftc.gov/tips-advice/business-center/small-businesses

Gaur, P. (2014). Global Cybersecurity Threats Landscape. Retrieved from https://www.pcquest.com/global-cyber-security-threats-landscape/

Geer, D. (2015). Six Key Areas of Investment for the Science of Cybersecurity. *Futurist*, 49(1), 10-15. Retrieved from http://ezproxy.uvu.edu/

Ghosh, S. (2004). The Nature of Cyber-attacks in the Future: A Position Paper. *Information Systems Security*, 13(1), 18-33. Retrieved from http://ezproxy.uvu.edu/

Gordon, J. (2016). Like a Bad Neighbor, Hackers Are There: The Need for Data Security Legislation and Cyber Insurance in Light of Increasing FTC Enforcement Actions. *Brooklyn Journal of Corporate, Financial & Commercial Law*, 11(1), 183-208. Retrieved from http://ezproxy.uvu.edu/

Graham, L. (2017). Ransomware can cost firms over $700,000; Cloud computing may provide the protection they need. Retrieved from https://www.cnbc.com/2017/08/04/cloud-computing-cybersecurity-defend-against-ransomware-hacks.html

Harris, J. (2011). Defending the Network Several Times Over. *Network Security*, 11(1), 12-14. Retrieved from http://ezproxy.uvu.edu/

Hunker, J., & Kelly, T. (2012). Cyber Policy: Institutional Struggle in A Transformed World. *I/S: A Journal of Law and Policy for the Information Society*, 211(1), 212-243. Retrieved from http://ezproxy.uvu.edu/

James, J. (2012). Hardware Firewall Appliances for SMBs. *Windows IT Pro*, 18(5), 133-138. Retrieved from http://ezproxy.uvu.edu/

Kaspersky. (2018). What Is an Advanced Persistent Threat? Retrieved from https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Keegan, M. (2017). It Takes Just One Mistake for a Company to Be Hacked. *Computer Fraud and Security*, (17)1, 16-18. Retrieved from http://ezproxy.uvu.edu/

Kerner, S. (2016). 17 Security Experts Share Predictions for the Top Cyber-Trends of 2017. *Eweek*, 1-2. Retrieved from http://ezproxy.uvu.edu/

Leary, E. (2017). Local Businesses: A Target for Next Cyberattacks. Retrieved from https://www.cnbc.com/2017/10/13/local-businesses-a-target-for-next-cyberattacks.html

Lyons, S. (2014). Typewriters Are Back, and We Have Edward Snowden to Thank. Retrieved from https://www.washingtonpost.com/posteverything/wp/2014/11/12/typewriters-are-back-and-we-have-edward-snowden-to-thank/?utm_term=.1e8d4c2d9303

McIntyre, G. (2018). What Is the SBA's Definition of Small Business (Any Why)? Retrieved from https://www.fundera.com/blog/sba-definition-of-small-business

Murray, D. (2015). Cyber-attack is a business risk for big and small. *Wenatchee Business Journal*, 15(8), 18. Retrieved from http://ezproxy.uvu.edu/

Pelliccione, A. (2016). 2016 CYBERSECURITY STUDY: High to Severe Control System Threat Levels. *Control Engineering*, 63(12), 12. Retrieved from http://ezproxy.uvu.edu/

Piper, A. (2014). Businesswide Cybersecurity. *Internal Auditor*, 71(3), 38-43. Retrieved from http://ezproxy.uvu.edu/

Reo, J. (2018). DDoS Protection: A Big Need for Small Business. Retrieved from https://www.corero.com/blog/868-ddos-protection-a-big-need-for-small-business.html

Rivera, A. (2018). Cybersecurity: A Small Business Guide. Retrieved from https://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html

Schell, R. (2016). Cyber Defense Triad for Where Security Matters. *Communications of the ACM*, 59(11), 20-23. Retrieved from http://ezproxy.uvu.edu/

Shackelford, S. (2016). Business and Cyber Peace: We Need You! *Business Horizons*, 59(5), 539-548. doi:10.1016/j.bushor.2016.03.015.

Switchfast. (2018). Small Businesses Are Thinking Too Simply About Their Cybersecurity Strategies. Retrieved from https://cdn2.hubspot.net/hubfs/1747499/Content%20 Downloads/Switchfast_SMB_Cybersecurity_Report.pdf

Untangle. (2018). 2018 SMB IT Security Report. Retrieved from https://www5.untangle.com/smbitsecurityreport2018

Worzala, C. (2017). Cybersecurity Must Be A Priority for Everyone. *Hospitals & Health Networks,* 17(7), 8. Retrieved from http://ezproxy.uvu.edu/