Developing a Framework to Help Small Organizations Improve Their Cybersecurity Posture

A Capstone Paper

Shane DelMonaco

Department of Cybersecurity, University of Maine at Presque Isle

For Fulfillment of COS 485: Cybersecurity Capstone

Professor Seth Michael Woodman

August 22, 2025

Abstract

The dramatic increase in global cybersecurity threats over the past half-decade has led to increased attention to products, services, and guidelines dedicated to cyberdefense. Government sectors and private enterprises have realized their position as major targets for cyber threats, whether they be from internal or external sources. The rapid evolution of cybersecurity needs is further shown in the growth of the cyber-defense industry, with a compound annual growth rate of 11.3% projected for the next ten years. With the rise of powerful technologies such as Artificial Intelligence, Machine Learning, Quantum Computing, Cloud Computing, and virtualization, a further sense of unpredictability shadows the tech industry and its customers. But while we may not be able to predict where technology will go tomorrow, we can be certain that a qualified workforce to secure and analyze it is no longer an option. Cyber threats continue to expand and intensify year by year, and new technologies seem to assist threat actors rather than avert them. While national governments are realizing the depth and breadth of new Advanced Persistent Threats (APTs) and large corporations are learning the financial devastation a data breach or ransomware attack can bring, there seems to be a lack of security understanding and coverage for the most vulnerable targets in our economy: small businesses, public institutions, and local governments. This capstone project will highlight the serious implications cyber-attacks can have on these entities through a combination of historical research and analysis of emerging trends. I will then develop a comprehensive framework that will address these security concerns in an easy-to-understand and implement fashion. By completing this project, I hope to help everyday citizens and entrepreneurs find an accessible solution for securing themselves and their assets in an increasingly dangerous digital landscape.

Table of Contents

Chapter 1: Information Technology in 2025

Technology Evolution

The 2020s have seen a rapid and profound expansion in the evolution of digital technology. Year by year, new grounds continue to be broken in areas such as cloud computing, artificial intelligence, machine learning, virtualization, and Big Data technologies. It can be surreal to remember that twenty years ago, Windows XP was the hottest new operating system on the market, and 8 gigabytes of memory was a luxury for a home computer. Here in 2025, Windows 10 will reach its End of Life (EOL) in October, and consumers can pick computers with anywhere from 16 to 64 gigabytes of memory.

The rapidly evolving technology sector has had a significant impact on the world's bustling markets. Artificial intelligence, while still far from perfect, is creeping its way into workplace operations and changing the way human workers interact with their daily tasks. Many businesses have shifted their focus away from an on-premises network infrastructure and towards a scalable, cloud-based infrastructure. Big Data technologies help corporations collect unbelievable amounts of raw data and break it down into sharp insights to help better understand their customers. For many, these developments in technology are coming so fast, it can be hard not to get in a state of anxiety over it all.

Impact of the COVID-19 Pandemic

A substantial factor in the evolution of digital technology was the COVID-19 Pandemic of 2020-23. The winter and spring of 2020 saw businesses, schools, and government offices shut down their in-person workplaces and quickly move to an internet-based work environment. Office Local Area Networks were quickly replaced with Virtual Private Networks for home use,

meeting rooms were replaced with Zoom and Microsoft Teams calls, and local file shares were replaced with cloud collaboration software. The learning curve that this new way of work brought was jarring for many at first, but nobody can deny that individuals and businesses got more and more used to these new technologies as the months and eventually years progressed.

The migration of thousands of users to the Internet over the past half-decade has opened lots of new opportunities to grow workplace skills and efficiency. However, it has also opened many new opportunities to the darker side of the digital landscape. Cybercriminals have greatly evolved the sophistication of their exploits and have found lots of new targets for their attacks. Evolving technologies like artificial intelligence have assisted cybercriminals in finding easier and more convincing methods to infiltrate their targets. With these advancements in cyber threats, business and personal users on the Internet are being forced to confront the large gaps many of them have in quality cybersecurity.

Evolution of Cybersecurity Threats

Since the dawn of computing, threat actors have created new ways to exploit gaps in security and assurance. One may think back to the early threats to enterprise technology such as Stuxnet, Code Red, Conficker, and MyDoom. Or one may remember frightening alerts from Microsoft Security Essentials or Avast Antivirus notifying them that malware had been found on their machine. Like physical crimes, cybercrimes are not going away and are only going to expand and intensify as more people and resources become reliant on the Internet. The past five years, especially, have seen unbelievable growth in the frequency and severity of cyberattacks. Many of the most vital members of our economy have suffered as a result.

Perhaps the most common yet destructive threat targeting Internet users is phishing. It is imperative today that all serious businesses provide email addresses and mailboxes to their employees. On top of this, most people use their own personal email addresses in addition to their work email addresses. Phishing is a major threat to both. Billions of phishing emails are sent daily, trying to convince end users to execute their payload through methods like impersonation, baiting, and pretexting.

The social engineering tactics present in phishing emails are often easy to spot upon close inspection, but the threat actors rely on the base instincts of their victims to not think twice and act on the scenario presented in their email. Malicious file attachments containing trojan horses or keyloggers are staples of phishing emails, but threat actors may also direct their targets to impersonation webpages where they are asked to enter important credentials.

Phishing emails often serve as an early stage in a much more sophisticated attack. IBM reported in its 2024 Cost of a Data Breach report that phishing attacks account for nearly 30% of all global data breaches (IBM, 2024). They also reported in their X-Force 2025 Threat Intelligence Index that phishing attacks are responsible for 33% of cloud-related cybersecurity incidents (IBM, 2025).

The ever-growing efficiency of artificial intelligence has further aided threat actors in crafting their phishing emails. According to the cybersecurity company HoxHunt, there has been a 49% rise in phishing attacks since 2021, which aligns steadily with the evolution of AI platforms (Baker and Cartier, 2024). AI tools can aid threat actors in improving realism and spelling/grammar in their emails. More realistic logos and illustrations can also be created with

these tools. As AI gets more accessible and sophisticated, we can expect phishing emails to grow in number and sophistication.

Phishing often acts as a delivery method for destructive payloads. These could range from keyloggers to macro viruses to Potentially Unwanted Programs (PUPs). The malicious software that has gained the most attention in recent years is ransomware. By 2031, it is predicted that this breed of malicious software will cost the world $275 billion a year (Morgan, 2023). Ransomware consists of highly sophisticated programs that find their way onto users' workstations through email attachments or drive-by downloads. Once executed, they encrypt all the victim's files, rendering them unreadable. The attackers will then present an ultimatum to the victim, usually a demand for payment within a specified time frame in return for the decryption of their files. If the victim does not answer the demand, the attacker often threatens to destroy the private key for their encrypted files, rendering them permanently unreadable. It should be noted that there is no guarantee that the attacker will decrypt the files even if the ransom is paid by the victim.

Since the early 2010s, many ransomware strains have resulted in serious global crises with millions of dollars in damage. In late 2013, the Crypto Locker Ransomware first appeared. Many will recall the menacing pop up on their desktop with the red background and the header "Your personal files are encrypted!". Crypto Locker used RSA public-key cryptography and demanded payment in Bitcoin or pre-paid cash vouchers for decryption. By the time Crypto Locker was isolated in June 2024, it had accumulated around 500,000 global victims and extorted an estimated $3 million in ransom payments (Ward, 2014).

Crypto Locker was upstaged in May 2017 when an even more destructive strain of ransomware called WannaCry appeared on the Internet. This sophisticated ransomware used a stolen exploit from the NSA called EternalBlue that took advantage of the insecure SMBv1 protocol on Windows networks (CLOUDFLARE, 2017). WannaCry encrypted victims' files with a combination of the RSA and AES algorithms and demanded a ransom of $300 to be paid in Bitcoin. WannaCry was largely neutralized a few hours after the initial outbreak by the discovery of a kill switch that halted the propagation of the software. By the time its reign of terror was stopped, WannaCry had infected at least 300,000 machines and caused up to $4 billion in financial loss (Berr, 2017). Ever since the days of Crypto Locker and WannaCry, thousands of different ransomware strains have come and go on the Internet with varying levels of success and destruction.

Businesses are the prime targets for ransomware attacks and are the ones to suffer the most from a successful infection. Many ransomware strains are built to target a specific industry or business. Ransomware software often has worm capabilities, meaning they quickly spread to other hosts on a network after their initial infection. The quick propagation can cause full infection before an Incident Response team can react. The fact that all user files, from Microsoft Office documents to QuickBooks files to AutoCAD drawings, are encrypted means that workplace efficiency is grinded to a complete halt. In many cases, management decides to pay the ransom demanded by the attacker to get their files decrypted rather than wait for eradication efforts that may or may not be successful. Data Security firm Varonis found in a 2024 study that the average ransom payment has grown to $2.73 million and that an average downtime of 24 days can be expected after an infection (Sobers, 2023).

While ransomware may be the most frightening and destructive cyber threat facing an average business, there are plenty more to be on the lookout for. Another common piece of malicious software that can be unknowingly downloaded by employees is the Remote Access Trojan, usually referred to by its acronym RAT. This malware uses trojan capabilities, meaning it disguises its true purpose within a seemingly legitimate program such as an important email or program. When the "legitimate" program is executed by the end user, a malicious payload is actually executed. This payload grants a connection back to the attacker, allowing them to create a session to remotely access and control the victim's host. With this access, the attacker can exfiltrate important data or embed other malicious services to persistently access the system. If a RAT is sophisticated enough, it can lay dormant in a system without being detected by the victim.

Some businesses and institutions may be targets for more direct attacks aimed at disrupting their operations for reasons of vendetta, operational damage, or activism. A go-to-attack for these cases is the Distributed Denial of Service Attack. This entails an attacker or group of collaborating attackers overloading target network resources with packets until the extreme volume causes the resources to cease functioning. Such network devices could include routers, web servers, switches, and domain controllers. According to Sentinel One, an average of 44,000 DDoS attacks were launched daily in 2023 alone (*Key Cyber Security Statistics for 2025*, 2025).

The common aim of these threats is to disrupt the confidentiality, integrity, or accessibility of business resources in some form. Many threat actors aim to disrupt all three. This is why it is useful to have a plan for incident response, including containment and eradication, ready to enact at any given time. However not all cyberattacks come in the form of visible,

highlighted incidents. Over the past few years, businesses and government organizations have been coming face to face with a rising new style of attack known as the Advanced Persistent Threat (APT).

An APT is a more advanced, sophisticated form of cyberattack often used by nation state actors and large cybercrime groups. These threats aim to infiltrate a target network and remain undetected for long periods of time, during which they escalate their privileges and execute payloads to achieve objectives. The point of an APT is to evade conventional detection methods and play the long game with its objectives. Cybersecurity teams must closely observe network activity and pinpoint deviations and abnormalities to detect an APT. Identifying and sharing the Tactics, Techniques, & Procedures (TTPs) of APTs helps organizations stay informed of the threat and prioritize prevention methods.

Several large APTs have received spotlight in recent years due to the size of the responsible groups and the sheer sophistication of their attacks. APT28 has been attributed to a division of Russian Military Intelligence and is sometimes referred to as “Fancy Bear”. Active since the mid-2000s, Fancy Bear targets a variety of sectors including aerospace, energy, and government. Since Fancy Bear is aligned with Russian geopolitical interests, main targets have included the United States and Western European nations, although they have been tracked globally. Fancy Bear is known for effectively using phishing emails and websites to gain their foothold, then slowly compromising network resources and exfiltrating large amounts of data over time (MITRE, 2017).

On the other hand, APT 32 originates from a much smaller nation state actor, Vietnam, yet it is just as dangerous. Associated names for APT 32 include SeaLotus and OceanLotus, and

its targets include the private sector as well as foreign governments and journalists in Southeast Asia (MITRE, 2024). APT32 appears to be very politically motivated. Like APT28, it uses phishing attacks to gain access to infrastructure, then manipulates system binaries and PowerShell scripts to create backdoor access to systems.

One vulnerability that many APTs take advantage of is the Zero-Day Attack. Every industry has their own set of applications that are necessary and trusted for workplace use. However, no software is perfect. Many times, software is shipped with vulnerabilities that are unknown, even to their producers. Skilled attackers can discover these vulnerabilities and create exploits for them before the producers are even aware of their existence. Therefore, both the producers and customers have "zero days" to prepare for an exploit of the vulnerability. It often isn't until several customers have become victims of the exploit before the software company releases a patch for the vulnerability.

In the past, organizations mainly had to focus on the security of their on-premises digital resources, network hardware, servers, and workstations. However there has been a large expansion of the digital frontier to include cloud computing and web applications. While cloud and web resources have brought some major improvements such as lowered costs for deployment and increased ease of use for employees, they have also brought in an entire new batch of security issues to be on the lookout for. NIST Special Publication 800-215 reports that over 75% of network traffic now takes place inside a LAN, or between servers hosting microservices. This has made securing enterprise networks more difficult, since traditional security controls like firewalls and intrusion detection systems focus on north-south traffic that originates from outside the local area network (Chandramouli, 2022). These implementations

aren't enough anymore. Security now needs to be brought to the per device, per user, per application, and per session level.

With companies holding large amounts of important data in the cloud, attackers have more evident targets for data breaches. Exploiting something as simple as poor access controls on cloud resources can lead an attacker to large amounts of important data. Many of the largest cloud providers such as AWS and Microsoft Entra push for their customers to enact strong security policies as a result. However, there is not much a cloud provider can do when it comes to actual applications built and deployed by the cloud customers themselves.

Many public and private organizations today utilize web application stacks with database integrations to host their resources. Some in the service industry host E-Commerce applications on their websites to allow for online purchasing. Database management systems such as MySQL and Microsoft SQL Server help provide this functionality. They serve content to the web frontend, but serious vulnerabilities can be introduced if the integration is not done properly. Attackers can take advantage of SQL Injection vulnerabilities in web applications, which entails entering a malicious SQL query into a web form, resulting in sensitive data being unintentionally retrieved and displayed. Another common web attack is Cross Site Scripting (XSS) which involves an attacker passing a malicious script to a web server, resulting in the script being executed in other users' browsers. Attacks like these highlight the necessity of properly developing and sanitizing website and web application code before opening them to the public internet.

This is just scratching the surface of the multitude of cyber threats facing organizations and individuals in the modern world. It can feel overwhelming for any one person, let alone an

organization of people, to try and stay safe with so many dangers facing their infrastructure and data. It can be difficult to find experienced personnel to take on the task of securing these assets. Not to mention that many businesses do not wish to spend the money on security personnel and systems. With all these difficulties, it is no wonder that cyberattacks continue to grow at an unprecedented rate.

Government & Regulatory Action

The past several years has also brought the concepts of cyberwarfare and cyberterrorism to the public conscience. These two concepts, which once sounded like science fiction to many, are now very real threats to national security and the security of the organizations inside them. While it is one of the stealthier subgenres of cyberattacks, nation-state-sponsored attacks are increasing and can impact everything from critical infrastructure functionality to election integrity to data confidentiality. But the growing concern of cyber warfare produces another problem relating to decentralized technology, and that is that it is difficult to define responsibility for attacks. World governments can construct and dictate cyberattacks themselves, but at the same time, any capable citizen of the same nation can launch their own destructive attack, leaving the question of whether a cyberattack was state-sponsored or not hard to answer for victim countries. For example, in late 2017, a coalition of the United States and the United Kingdom formally asserted that North Korea was the party responsible for the WannaCry ransomware. However, Pyongyang denied any connection and as of 2025, has not been fully confirmed as guilty of the attack (Volz, 2017).

This growing implementation and complexity of digital technology and corresponding cyber threats has led to an increase in attention from the private sector, public sector, and

government sector alike. Third-party cybersecurity firms such as CrowdStrike and Palo Alto have risen in the market by providing cybersecurity solutions to organizations of various sizes and sectors. Government agencies continue to tailor their standards to suit emerging technologies, such as the National Institute of Standards and Technology who regularly releases and updates their Special Publications, providing in-depth recommendations for securing various forms of technical infrastructure. In 2018, President Donald J. Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018, which created the Cybersecurity and Infrastructure Security Agency as a sub-agency of the Department of Homeland Security.

Throughout its short existence, CISA has sought to centralize many components of the nation's cybersecurity posture. Keeping up with emerging trends, CISA has sought to bring precautions such as multi-factor authentication and shared threat intelligence into the mainstream. CISA also stepped-up federal focus on the security of Industrial Control Systems (ICS) and the digital components of United States elections. More ambitious pursuits by CISA include working to lower the financial impact of ransomware attacks on victims, as well as implementing cyber defense into international agreements and diplomacy.

Recent political developments have raised concerns over the longevity of CISA. The same day as President Trump's inauguration for his second non-consecutive term, CISA Director Jen Easterly stepped down from the position. Since that date of January 20, 2025, the director position has been fulfilled by Acting Director Bridget Bean. In addition to the uncertainty over its leadership, CISA has seen a large-scale decrease in its workforce relating to President Trump's attempts to shrink the size of the federal government as well as his personal resentments over CISA's dismissal of his claims of election fraud in the 2020 United States Presidential

election. As of May 27, 2025, CISA has seen an exodus of at least ten top officials, as well as lingering threats of steep cuts to its funding by the Trump Administration.

The recent destabilization of federal cybersecurity agencies presents a question to business owners and local governments: can centralized federal cybersecurity resources be relied on going forward? This question has a lot to consider. Americans can generally rely on their government to protect them from physical threats from adversaries, mainly due to the visibility and centralization of something as powerful as national militaries. Questions have long been raised surrounding federal reliance on less centralized issues of national security, notably immigration concerns and organized crime. The use of technology across the country is even more decentralized and nuanced to the use case, and cyberthreats are so unpredictable and stealthy, that I think one can reasonably conclude that federal security of the digital landscape is an imperfect, uphill battle, certainly not one that can be conducted in fractured government agencies.

However, the huge landscape and accessibility of Internet resources means that organizations and individuals can look elsewhere for cybersecurity consultancy. The Internet is full of third parties providing comprehensive cybersecurity advice and solutions to the public. Open-Source Threat Intelligence Feeds, best practices guides, and threat alerts can all be easily found, with hundreds of different and unique sources for each area. Even though many government and regulatory agencies continue to keep their sources free and accessible, the NIST Special Publications can be found online with a simple search.

Organizations and the individuals associated with them do not have expendable schedules, however, and embracing third-party cybersecurity sources requires varying levels of

knowledge in the topics. As a result, it is more common for management to opt to hire a dedicated cybersecurity professional either in-house or outsourced to handle the issue. This is far from a easy resolution, as the accessibility for seasoned cybersecurity professionals can be bleak depending on the area. Another blunt reality is that most business owners and executives do not see a financial incentive for investing in cyber defense. Security hardware and applications are quite expensive, and it can be difficult to justify spending on them while security remains satisfactory for the organization. This often results in management opting to keep security at a stable baseline that only implements necessary defensive techniques while also saving costs. This approach of "just secure enough" will work fine until it isn't secure enough. With the rapid increase in threats and exploits, nobody can settle for a base level of security for long.

Any student of cybersecurity or information assurance will be told from the get-go that one hundred percent security is not attainable. A skilled professional may be able to produce security levels of ninety-nine percent, but year by year, this is becoming difficult to achieve. The impossibility of obtaining full security, combined with the financial incentives to keep spending on cyber defense technologies at a minimum, makes it clear why so many businesses, governments, and non-profit organizations never seem to be ready for the next big cyberattack. This is a way of thinking that I don't see disappearing anytime soon, even after the next, more destructive version of WannaCry hits.

Problem Statement

I have spent my entire life in small towns and cities in Maine, a very large and spacious part of the United States. Most of our part of the state is made up of small towns and cities

woven together, broken up by a larger city like Bangor or Houlton. Being such a small area, our economy consists of many small businesses, many of them family-run.

There is a great sense of community that comes out of supporting these businesses. It is nice to know the owners on a personal level and feel like you are directly contributing to the community economy. Without the community and economic growth created by our small businesses, there is no doubt that we would be much worse off. In addition to the very small mom-and-pop-style businesses in my area, there are many small-town offices and public departments staffed by a small number of town workers.

There are several issues that come with having such small businesses and offices populate your area. Staffing and finance are always major considerations, as they would be for any business. I have long wondered about the status of cybersecurity present in these institutions and have noticed many troubling procedures with their digital landscape.

As we explored in the previous section, receiving any sort of cohesive guidance on cybersecurity measures is an uphill battle for even large enterprises. The complexities of implementing a stable defensive infrastructure can be overwhelming for businesses with hundreds of staff members. The task is probably even more difficult for businesses with 100 or fewer employees.

I have often found that small to medium-sized businesses and organizations suffer from one of the most toxic mindsets in the modern world. They feel that they are “too small” to be targets of cyberattacks. When the news is full of reports on major Fortune 500 breaches and government compromises, an owner of a four-person gas station likely sees no reason why they should ever have to worry about the issue. Cybersecurity is present in larger enterprises and

government agencies if nothing else than to satisfy governance and regulations. It is a blunt reality that most organizations don't care about cybersecurity and what to spend as little as possible on it. Since small businesses often don't fall under the umbrella of regulations that large corporations do, they are even less interested in implementing proper cybersecurity measures.

Everybody needs to know that threat actors do not discriminate in their targets. Their exploits can be deployed as many times as they want, meaning they will likely not turn down a ripe target if it's there, regardless of size. Business owners need to know that their data is the most valuable digital asset they have, and anybody with data is a vulnerable target for cybercriminals. Systems like web applications, social media pages, and Point of Sale (POS) systems have become increasingly accessible to businesses of all sizes, and these systems produce a lot of data. Whether it be customer credit card payments, accounting software files, or passwords to company systems, possessing any amount of data is a danger in today's digital landscape.

However, it is sympathetic when you realize that many businesspeople in today's economy do not know where to start with cybersecurity. Your average person today likely has only basic desktop computer skills and doesn't understand how exactly cyberattacks work. A lot of times in these organizations, it isn't a matter of not caring about security, but a matter of not having the ability to implement it. There are more immediately pressing issues on the mind of any business owner, so security often gets pushed to a permanent background.

With government advisory departments in disarray and high-end security consultants often being out of financial reach, there seems to be a severe lack of guidance for small businesses and community organizations for cybersecurity. I feel that the most vulnerable

members of our economy and government deserve a solid and easy framework to guide them on their institution's security. That is what I will produce with this capstone project. I will first analyze the nuances of business technology use and the various threats facing that technology, then break down the common security oversights that continue to enable threat actors. After this analysis, I will present my framework to help our country's small business and community organizations ensure the best possible security for themselves, their employees, and their customers.

Chapter 2: Understanding Small Business Cyber Threats

Literature Review

The expansion of technology and the threat of cyberattacks has led to a wealth of published technical writing. An upside of dealing with cybersecurity is that the core concepts of a good cybersecurity program apply regardless of environment. This is why the NIST SP 800 series is so renowned. The cybersecurity topics covered by these publications are relevant regardless of what size organization is reading them.

Where popular frameworks like NIST fail, in my opinion, is when it comes to explaining concepts and controls. The major frameworks are presented with the assumption that the reader is familiar with IT and particularly cybersecurity. Their clear target audience is dedicated IT and InfoSec departments in medium to large sized enterprises and agencies. There is a lack of a comprehensive framework that assumes the reader is a complete beginner with no cybersecurity knowledge and only a few employees.

Most of the data I gathered on where small business owners stand in regard to cybersecurity came from brochures published by cybersecurity firms. These brochures were short and usually tailored to your average small business employee. They included the basic best practices like setting strong passwords and updating software.

I also reviewed many news articles detailing cyberattacks that impacted organizations on the smaller side of the economy. When I compared the provided root causes of some of those incidents with the language used in the brochures, I found that my thesis was heavily supported. Your average small business in a developed country has extremely basic knowledge of cybersecurity and settles for the basic practices they are given in documents like industry

brochures. Even thinking about consulting comprehensive cybersecurity advice like that provided by NIST is far beyond them.

Methodology

Something I found very helpful in pursuing this project was the wide availability of statistics surrounding this topic. With so many statistics available, a great deal of this project was produced using quantitative data as a backbone. Major cybersecurity firms such as CrowdStrike and Fortinet have numerous write-ups and data sheets with statistics regarding the specific niche of cyberattacks targeting small businesses. I was able to check the accuracy of this data by comparing it with statistics from other sectors. Financial services sectors have also released information regarding cyberattacks, allowing me to compare and correlate the data across different companies and different industries.

However, this project was more about understanding the nuances of cybersecurity and its relationship with small businesses. Therefore, I used lots of qualitative data to help develop this project. This mainly took the form of press releases and news articles found around the web from various national and community sources. These articles were unbelievable helpful, as they often gave some information about the root causes of various cybersecurity incidents. The articles also often provided interviews with the victims of these incidents. This data was extremely helpful in gaining an understanding of where the average small business owner is with understanding cybersecurity.

While collecting data for this project, I encountered some difficulty on finding expert opinions on specific incidents. My research mostly turned up either expert technical journals on specific cybersecurity topics, or statistics and news reports regarding individual incidents. I had

some difficulty bridging the gap, finding detailed analysis of the incidents themselves from cybersecurity experts. I am confident in my knowledge of intermediate level cybersecurity, so much of the root cause analysis surrounding the example real world cyber incidents is my own.

Technology Landscape of Small Businesses

Constructing a framework to aid small businesses with their digital security first requires an understanding of what business technology implementations look like in 2025. While your average local business usually cannot afford to purchase the highest-end servers and networking gear, they can expect to be able to purchase and implement reasonable technical measures.

Businesses of all sizes, from two employees to two hundred, universally prefer Microsoft Windows as their enterprise operating system. Windows sits at a stable 70% of the desktop operating system as of this writing in July 2025 (StatCounter, 2025). It's no surprise that Microsoft Windows remains the dominant operating system. It is simple to set up and generally comes pre-installed on workstations from all major PC vendors. Business software for all major industries is usually released with the expectation that it will be installed and run on a Windows machine. Microsoft has helped keep its rapport with business by releasing business-friendly features and products to help IT staff better integrate the OS with the workplace.

However, you are likely to come across a decent number of businesses using Apple macOS machines in their workplace. OSX holds about 10% of the market share as of this writing. There are many factors that go into the business preference for Windows PCs over Mac machines. Apple products are known for their high prices, combined with the fact that a lot of business software is not programmed for release on OSX. Windows is just the easier and more convenient option for workplace deployment.

In the business environment, the real use of technology rests with the actual tasks that employees perform on their machines. A publication from the United States Chamber of Commerce reports that small businesses using the most technology in their operations are the most likely to experience growth each year (Small Business, 2024). The publication finds that the most used piece of technology in small businesses is social media platforms such as Facebook, Instagram, and TikTok. Digital payment programs have also been steadily implemented into business operations, with many customers performing transactions through software such as Google Pay, Apple Pay, and Venmo. The other top technologies used by small businesses include accounting software, marketing platforms, point of sale systems, and productivity platforms.

Technology implementation is expected to help fuel better growth and small business success moving forward. Intuit's 2025 Small Business Index finds that increased digitalization of businesses increases productivity and correlates with higher sales revenue and entrepreneur confidence (QuickBooks, 2025). Artificial intelligence continues to be a key standout among emerging technologies. Having a tool to automate processes such as writing documentation, creating marketing materials, and analyzing datasets is very appealing to your average small business owner who may want to cut down their workload to the more pressing issues. The National Small Business Association reported earlier this summer that 76% of small businesses are either currently using AI tools or looking into using them in the future (NSBA, 2025, June 12). Just how drastically AI will change the economic landscape as it develops and further integrates remains something to pay close attention to.

Successfully implementing technology into the workplace is only part of the responsibility held by business owners. Technology needs to be securely implemented as well,

and oftentimes this is the area where business management falls short. A publication from Sparklight Business reports that small businesses are the targets for a third of cyberattacks and spend an average of $690,000 recovering from a cyberattack (One, 2020). If small businesses hope to keep growing their presence in the American economy through technology, they are going to need to start taking cybersecurity more seriously.

Incidents of Interest

The potential damage resulting from cyberattacks has not been lost on many small-to-medium-sized business owners. The past five years alone have many high profile cyberattacks affect organizations across various sectors, sizes, and locations. A common theme is present in almost all of them; the victim organizations were lacking in multiple critical areas of cyberdefense.

While conducting my research into cyber incidents of interest, I decided to start by looking into incidents within a local context. Living in rural Maine all of my life, I am familiar with many of the small businesses powering local communities like mine. I have seen some of the security practices in place in these organizations and have been concerned by what I have found. My concerns were validated when I came across some local cybersecurity incidents resulting from some of the same misconfigurations I observed.

The most disturbing case I came across was in the 2021 ransomware attack on the Presque Isle Police Department. On April 18, 2021, a server belonging to the municipal government of Presque Isle was compromised, and the Presque Isle Police Department was hit with a sophisticated ransomware attack. The malware in question was determined to be associated with an organized crime group utilizing Avaddon Ransomware, a Ransomware as a

Service (RaaS) family that surfaced in 2019 (Tomaselli, 2021). A Presque Isle official reported that the infection stemmed from a link in a phishing email. It was reported that this same attack simultaneously hit the Washington DC Metropolitan Police Department. The threat actors not only demanded a ransom for the decryption of PIPD's files, but they also threatened to dump all private data collected in the attack onto the Deep Web. This stolen data, which included Personally Identifiable Information (PII), could be dumped on a public site or possibly auctioned off for profit. The threat actors behind the attack claimed that the data seized from PIPD included victim statements, criminal case reports, and confidential records and identifications of individuals associated with the police (Tomaselli, 2021b).

While this infection clearly showed a lack of security precautions in some surface areas, PIPD had an important component of network security in place that prevented the incident from having an even larger impact. PIPD was able to restore its access to the seized data from its daily backup solution. Backups are one of, if not the most critical, implementations providing organizations with assurance against cyber threats. Backups, and then backups of backups, can be the difference between going out of business and being able to recover after a cyber-attack.

Presque Isle's city government assured the public that not only had they been able to restore data, but that they had also been in contact with the FBI to report the incident. In addition, the threat actors behind the ransomware attack had also been in contact with city leadership, putting the pressure on them to act before the leakage of their data began. The attackers gave PIPD an ultimatum of 240 hours to pay the ransom. To drive home their point, the attackers leaked a Presque Isle domestic violence police report containing names and addresses on the deep web. They also showcased a numbered countdown until the time expired on their website.

The 240 hours came and went with PIPD holding firm on not paying the ransom. The cybercrime group held firm on their ultimatum and dumped the data seized from PIPD on the deep web. According to Bangor Daily News, the major newspaper of Maine's 2nd Congressional District, this data comprised of, "200 gigabytes of data dating back to the 1970s". Among the most sensitive of the leaked data was 15,000 emails, police reports, and witness statements. The total number of leaked files was reported to be 135,000.

This incident showed how cyberattacks do not discriminate in their targets. In the event of a nuclear war, targets like Washington, DC or New York City would be prioritized. Presque Isle, Maine, would not be a high-ranking target. Here, however, PIPD was hit with the same attack as the Washington DC Metropolitan Police. Nobody is immune, regardless of population or national stature.

Another example of ransomware impacting organizations providing critical infrastructure also occurred in the summer of 2021, this time in both Limestone, Maine and Mount Desert Island, Maine. Limestone is located less than thirty miles from Presque Isle. It was reported that the initial attacks occurred during April in Mount Desert Island and on the Fourth of July in Limestone.

Employees reported that they were met with the same threats as the police department: pay the ransom or your organization's data will be published on the deep web. Mount Desert Island officials reported that the attack caused a three-day denial of service for their workstations. No Industrial Control Systems were affected due to their analog methods of connection (Lampariello, 2024). A Limestone forensic investigation determined that the ransomware attack on their systems entered through a host running Windows 7. This host was

directly connected to the plant's SCADA system (Wood, 2021). Right here, we can narrow down an all-too-common cybersecurity error: utilizing legacy systems. Windows 7 reached its end of life on January 14, 2020, over a year before the incident at Limestone. Organizations using critical ICS and SCADA systems often rely on legacy operating systems due to their compatibility with the systems, which may not be possible on newer hardware and operating systems. Many of these ICS and SCADA systems cannot tolerate downtime, meaning the operating systems hosting their control software are unpatched. Organizations being stuck with legacy systems that cannot be upgraded, while at the same time providing a major security vulnerability, is an all-too-common issue, even in today's digital world where Software as a Service platforms continue to grow.

In a stroke of luck, the ransomware attacks on the Limestone and Mount Desert Island plants were largely unsuccessful. Limestone had an overheating alarm disabled by the attack, an issue which plant staff were able to catch and mitigate quickly. No PII was compromised, and no ransom was paid from either facility. The Mount Desert Island facility reasoned that they could restore their network from backups, eliminating the need to pay the ransom. While these Maine plants were able to escape relatively unscathed, other wastewater plants across the country have not been so lucky. Some plants have been infiltrated so deeply that attackers were able to adjust chemical controls on water systems to dangerous levels. This right here is just a glimpse into how cyberattacks could be leveraged as a weapon against the public.

It has been reported that the wastewater ransomware attacks also originated from phishing emails. This is no surprise, as phishing and other forms of social engineering make up most entrance points for cyberattacks, especially ones involving malicious software. This attack method is a classic that has been utilized since the early days of personal computing and shows

no sign of losing its power. Business IT teams and government agencies alike have worked on stepping up user training and education for employees on how to identify phishing attempts and mitigate them. However, this seems to only go so far, as the quality and persuasiveness of phishing emails grows at the same pace. It is recommended that organizations implement both user training and email filtering services to help mitigate malicious emails. But email is such a difficult beast that the threat surface frequently remains wide open despite these controls.

The ease and speed with which these ransomware attacks were able to infiltrate their targets highlights the dangers of having even one notable security vulnerability present. The tactics, techniques, and procedures of ransomware keeps it as one of the most effective attacks in the wild today. A survey by CNBC and Momentive found that 51% of small business owners hit by ransomware ended up paying the ransom (Rosenbaum, 2021). Ransomware has grown into a sort of black-market product with the rise of Ransomware as a Service, a model that allows third parties to purchase ransomware software from a threat group and deploy said ransomware against a target of their choosing.

Ransomware attacks often serve as tool for a much larger objective for threat actors. A 2025 Data Breach Investigations report from Verizon Business found that ransomware was present in 75% of small business data breaches they investigated (Verizon, 2025, pg. 10). Most of us are familiar with the large data breaches affecting large corporations. However, the effect of a data breach on a small business can be much more devastating than ones on larger corporations with cyber insurance and legal backup. The Verizon report documented 3,049 incidents among businesses with less than 1,000 employees, with 2,842 of those incidents resulting in confirmed data exposure (Verizon, pg. 12). An even more chilling statistic comes from Cybercrime

Magazine, which found that 60% of small businesses close within six months of experiencing a major breach (Johnson, 2019).

One of the most tragic examples of this occurred in the UK this July. A transportation company known as Knights of Old (KNP) had its internal data completed encrypted and rendered unreadable by attackers. The root cause of the breach fell upon one employee who was using a password so simple, the attackers were simply able to guess it without need for brute force. The results were devastating, with the attackers crippling every workstation, server, backup, and disaster recovery method (Tyson, 2025). This incident highlights potential worst-case scenarios that can arise from the simplest security misconfigurations. KNP quickly disintegrated due to the breach, with 500 of their trucks being taken off the road and 700 individuals losing their jobs. This example stands out to me as one of the best examples illustrating the domino effect of weak cybersecurity practices.

The threat of data breaches goes beyond the walls of a small business itself. Management can pursue the most rigorous cybersecurity defenses available, but a key risk still remains. Businesses of all sizes rely on supply chains to effectively present their goods and services. Your average small business has accounts with larger companies for tasks like ordering, inventory, and business promotion. When creating one of these relationships with a vendor, business owners place a large amount of trust in them by providing them with personal data like names, office addresses, credit card info, and tax information. The security of this data is passed from the hands of business to the hands of the vendor.

In 2019, the financial provider Capital One experienced a data breach that resulted in the exposure of personal data for over 100 million customers. Reports indicate that the breach

occurred in March of 2019 but wasn't brought to Capital One's attention until a third-party penetration tester noticed the root vulnerability (CERT-EU, 2019). On July 19, Capital One announced the data breach and revealed that the compromised data included credit card application data, credit card scores, transaction information, balances, and Personally Identifiable Information (PII) of the customers affected, both individuals and business entities.

The cyber threats present in supply chains have been further amplified by the continuing rise of cloud computing, specifically the widespread use of Software as a Service products. Back in say, 2006, you were likely to come across an employee workstation that ran many software programs installed locally on the operating system with communication limited to the office LAN. In 2025, you are likely to see more business software running in cloud environments, some managed by the local organization and others completely managed by third parties. The fact that complete security over company data is now removed from business network perimeter and placed on various cloud platforms across the Internet creates more risk for business owners.

As the 2019 Capital One Breach was investigated, it was discovered that the incident reached higher up in the supply chain to involve Capital One storage buckets in the Amazon Web Services (AWS) cloud. Even more shockingly, it was discovered that the threat actor responsible for the breach was a former employee of AWS itself and managed to retain access to the servers hosting CapitalOne data even after her employment with AWS ended (Pepitone, 2019). The employee discovered a vulnerability in the Web Application Firewall (WAF) placed in front of the Capital One buckets and used the flaw to obtain service credentials. Eventually, they were able to escalate their privileges and obtain access to large volumes of customer data (Fier, 2019). The threat actor was identified as Paige A. Thompson, 30, of Seattle Washington. In 2022,

Thompson was sentenced to time served and an additional five years of probation plus supervision of computer usage (United States Attorney's Office, 2022).

The Capital One incident further illustrates the domino effect of cybersecurity incidents that can start up high at large multinational corporations and eventually trickle down to impact even the smallest of entities. A small rural mom and pop stored using a Capital One business credit card could have had their credit information published for anyone to see due to security vulnerabilities they had nothing to do with.

A similar supply chain and cloud software incident occurred this past winter and hit close to home for me. This cyber crisis involved a data breach of the K-12 software provider PowerSchool, stemming from an external attack that remained undetected in the provider's systems for nine days (Reed, 2025). Numerous Maine K-12 schools utilized this software and were impacted by this breach, along with thousands of other PowerSchool customers across the globe.

The Maine Department of Education calculated that at least nine Maine school districts were affected by the breach. This breach became an immediate public concern due to the intimate nature of the compromised data. An estimated 30,000 Maine residents were affected, with compromised PII including contact information, Social Security numbers, and some medical information (GovTech, 2025). Students and teachers were among the affected individuals, making up an estimated 19-20% of Maine's K-12 enrollment (Lampariello, 2025). Even more frighteningly, some affected school districts reported that data regarding previous students was compromised as well. The Yarmouth School Department reported that attackers were able to gather information dating back twenty years (Lampariello).

Educational facilities, both public and private, are an especially concerning entity when it comes to cybersecurity. Education is a coercing target for threat actors due to the large amount of data processed throughout schools. At the same time, many schools do not have the budget for high end security, nor the manpower to implement and monitor said security. This results in education being a vulnerable sector and an easy target for cyberattacks.

The Capital One and PowerSchool examples have illustrated how small-to-medium sized businesses and public organizations can become victims of major cyberattacks through supply chains. However, small businesses are not always the victim in supply chain based cyberattacks. Sometimes, businesses can unknowingly become perpetrators and spread malicious activity to larger entities.

Perhaps the best-known real-world example of this involves a small HVAC contractor called Fazio Mechanical Services. Some readers might find it unbelievable if I told them that in 2013, this small HVAC contractor became the first domino in a cyberattack that infiltrated one of the largest retailers in the United States and resulted in the PII of over 40 million people being exposed. But the story is true, and it highlights some of the worst mistakes any entity can make in regard to security.

In December of 2013, Fazio Mechanical was doing contracted work for Target, a staple retailer in the American economy. This required the company to connect its own computer systems to Target's network. Threat actors looking to infiltrate Target performed reconnaissance on Target's entire network landscape and identified Fazio Mechanical's systems as being the easiest entry into the network. Their computers reportedly had lax security controls in place, with

only a free anti-malware program protecting their operating systems (Steinberg, Stepan, & Neary, 2021, pp. 2).

Taking the opportunity to pounce, the attackers deployed the ever so classic phishing email, eventually convincing one of Fazio Mechanical's users to download a sophisticated piece of malware known as Citadel. With Citadel, threat actors harvested credentials from the user's browser and used them to sign into a web application that allowed Fazio Mechanical to upload invoices. While studying the web application, the attackers found a critical security mistake on Target's part. There was no restriction on file uploads, meaning executable files could be passed to the application in addition to documents. By uploading a malicious web shell to the portal, the attackers were able to gain remote access to Target's internal network (Steinberg, Stepan, & Neary, pp. 3). From here, they were able to escalate their privileges and eventually, compromise the private data of over 40 million Target customers.

All of these cases I studied during this investigation led me to the conclusion that there are two major issues facing small businesses when it comes to cybersecurity. The first involves the actual cybersecurity controls and policies within the businesses themselves. There is a clear lack of internal precautions regarding phishing attacks, malware, data protection, and proper backup solutions. Small businesses are in desperate need of a comprehensive, easy to understand framework to address these issues from within. Bringing forward options to resolve such issues is going to be one of the key goals of this framework.

The second issue I noticed during this research is much more insidious and unfortunately, difficult to address. The transformation of the digital landscape since the COVID-19 pandemic has resulted in a large exodus from perimeter-based computing environments towards a complex

environment of cloud and web-based applications. This decentralized environment makes security more difficult, since business owners are now vulnerable to attacks impacting supply chains that they themselves have little control over. Implementing security controls for these environments is going to be just as much of a priority in this framework.

My desires for this new framework are ambitious and are going to require careful selection of wording and selection of tools. I want to cover every category of modern technology that can possibly be found in everyday local businesses, and present security controls for them. To do this effectively, I have decided that I must break down the major security errors I have observed throughout my research to get the best understanding of what needs to be done.

Chapter 3: Dissecting Root Causes of Cyberattacks on Small Businesses

Legacy Infrastructure

A frequent culprit behind many major business cybersecurity incidents is the use of legacy software and systems. The fast evolution of operating systems, particularly Microsoft Windows, can put small business owners in a difficult spot regarding their software and hardware. Tasks like controlling chemical levels, mixing paint, and creating ID cards require highly specialized software. Often, when software is purchased for a task, there is little desire to upgrade it if it works as desired. Continuing to use the same program prevents the financial need for upgrades and prevents workers from having to learn a new interface or process.

The top operating systems tend to have a mixed record with legacy systems. Many pieces of software released in the Windows XP era continue to function well on Windows 7 and even 10 or 11. However, utilizing legacy software and systems presents a major security hole, especially if exposed to a public network like the Internet.

In many cases, it can be difficult to find modern versions of highly specialized or niche software. This presents a complicated situation, as business owners may be forced to abandon their current configuration and find new software. There are also new licensing costs and training requirements to consider. When faced with these roadblocks, it simply makes more sense to stay with a legacy program that works and is understood by staff.

The legacy infrastructure issue is going to continue to create problems. The release of Windows 11 has highlighted a lot of issues with both legacy software and hardware. Windows 11 has stringent hardware requirements for installation. An end user must have a Trusted Platform Module (TPM) version 2.0, a minimum of 4GB of RAM, a 64-bit system architecture, and UEFI firmware with Secure Boot (Microsoft). In the 2025 PC market, these specifications are pretty standard. However, many end users are still using older systems from as far back as Windows Vista and even XP eras. These users will not be able to upgrade to Windows 11 even if they want to. The only options are to buy a new system or continue using an insecure operating system on old hardware. For many small businesses, neither option is desirable or even feasible.

Wi-Fi Security Gaps

If you take a walk down the main street of your hometown and open the Wi-Fi settings on your phone, you are bound to see accessible networks. You can usually identify to whom the

networks belong by their Service Set Identifiers (SSIDs). You may even come across a few networks with no password required for connection.

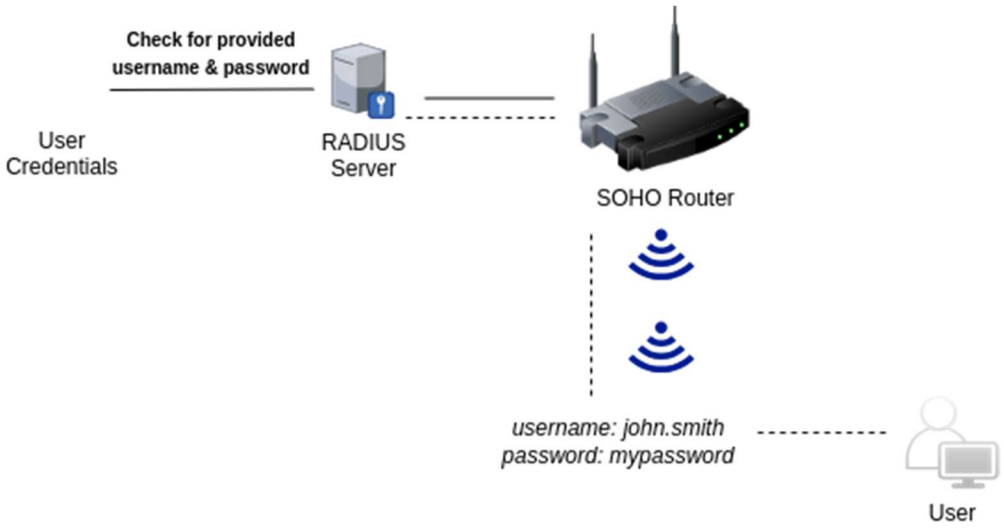
Cybercriminals often use this same tactic to find vulnerable networks to attack without needing to enter the target facility. This is known as “Wardriving”. Even if you are operating in a remote area, having your Wi-Fi network broadcast outside of your facility can be dangerous. It is recommended to turn down the Wi-Fi transmission power so that it is only accessible by the necessary parties. Further security can be added by turning off the SSID broadcast completely, removing the identifier that could direct an attacker towards your organization.

These additional security controls are pointless if there is no authentication present on the Wi-Fi to begin with. Consumer grade SOHO routers direct their owners to set up pre-shared key authentication, but business management might opt to keep at least one Wi-Fi network open for guest access or just for convenience. Having no authentication is an immediate critical vulnerability, especially if the same Wi-Fi network is used for both employees and guests. Having unfettered access to a business network provides attackers with an easy stepping-stone to start sniffing network traffic as part of active reconnaissance. Eventually, further vulnerabilities in the network will reveal themselves and attackers can begin preparing exploits to take advantage of network assets. This can be avoided by simply configuring Wi-Fi with secure authentication using at minimum WPA2-PSK out of the box.

When it comes to Guest Wi-Fi authentication should still be present regardless of how tempting it is to leave the network open. Setting a simple password on the guest Wi-Fi and advertising it inside the business facilities ensures that authorized visitors and third parties are able to access it while limiting access by unauthorized personnel. Many facilities, such as hotels,

restaurants, and schools, implement a Captive Portal. This sends end users to a webpage in a private subnet where they must sign in with credentials and complete tasks like accepting Terms & Conditions or completing a CAPTCHA, before being granted Guest Wi-Fi access.

For optimal network security, businesses should look into implementing 802.1X authentication through WPA2/WPA3-Enterprise. In a network with 802.1X authentication, usernames and passwords are provided to each employee, rather than a single pre-shared key. Credentials are stored on a RADIUS server connected to the wireless access points. When an individual initiates a connection, they are asked to provide their personal credentials which are then validated by the RADIUS server. Access is then either accepted or denied.



WPA2-PSK remains the minimum recommended wireless standard for security. Many routers still present the possibility to use Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA1) as protocols. Using these should be strictly avoided, as they are outdated protocols with weak encryption algorithms and lots of vulnerabilities.

WPA3, has been around since 2018 and should be considered for use in business networks moving forward. WPA3 uses advanced security features such as stronger encryption algorithms and unique private key exchanges between clients and servers. The likelihood of common Wi-Fi attack methods like Brute Force and Dictionary attacks is heavily reduced through WPA3.

Securing a business's wireless network is an easy first step in the broader scope of network security. Easy inroads can be closed to attackers by implementing basic best practices, all of which can be configured with the click of a few buttons on an access point's firmware page. However, network security is a much broader field than just Wi-Fi and must be addressed at deeper layers to ensure the confidentiality, integrity, and availability of critical business resources.

Lack of Network Segmentation

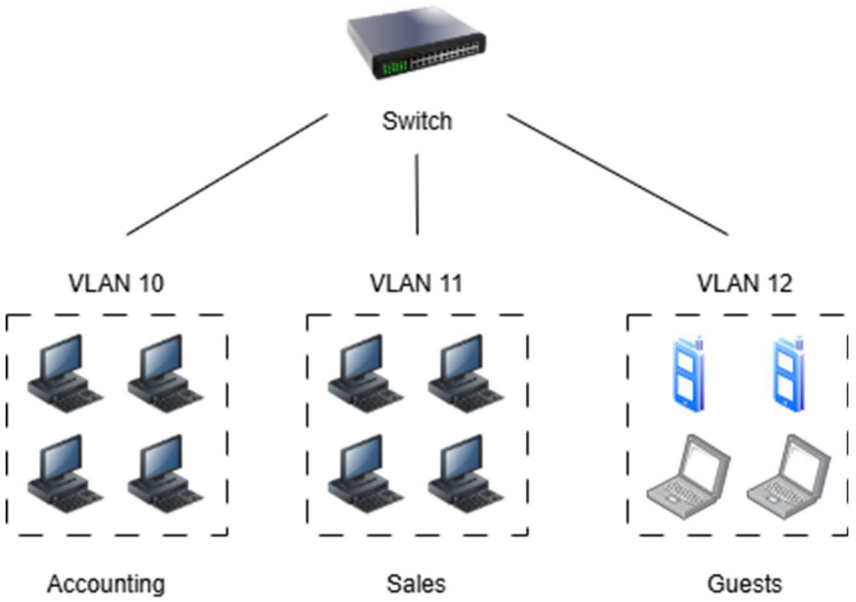
It is common to find businesses using a single network to host all of their data and services regardless of sensitivity levels. Having important business data such as financial information and trade secrets communicating over the same network as employees searching for free games and streaming services poses an immediate threat to the security of the business resources. The threat becomes even more severe when Personally Identifiable Information (PII) of customers begins moving through the network. No longer are you dealing with simple security risks, now you are opening your organization up to legal consequences in the case of a data breach.

Network segmentation is a strategy that can help reduce the attack surface of a business network and segregate data and services based on categories and sensitivity levels. Segmentation

can be employed at both physical and logical levels. It can be employed right out of the box by grouping workstations in the business facilities based on criteria such as their assigned department. A floor can be dedicated to the Financial Department, another to Human Resources, and another to Management. This means that each department has immediate physical access only to resources in their own department.

However, when we refer to network segmentation, we are usually referring to segmentation at the logical level. A common and highly recommended implementation of logical network segmentation is Virtual Local Area Networks or VLANs. When a network is created and hosts are connected to the same network switch, they exist in the same broadcast domain. This means that all hosts can communicate with each other through broadcast messages.

VLANs allow us to create smaller broadcast domains on the network and assign resources to each broadcast domain based on specific grouping criteria. We could create VLAN 2 for Finance computers and VLAN 3 for Marketing computers. Devices can be assigned to VLANs regardless of their proximity to other devices in their respective department. Once hosts are assigned to a specific VLAN, they are restricted to communicating with the other hosts in the VLAN. This significantly shrinks the attack surface of a network, since every host is no longer communicating on the same broadcast domain.

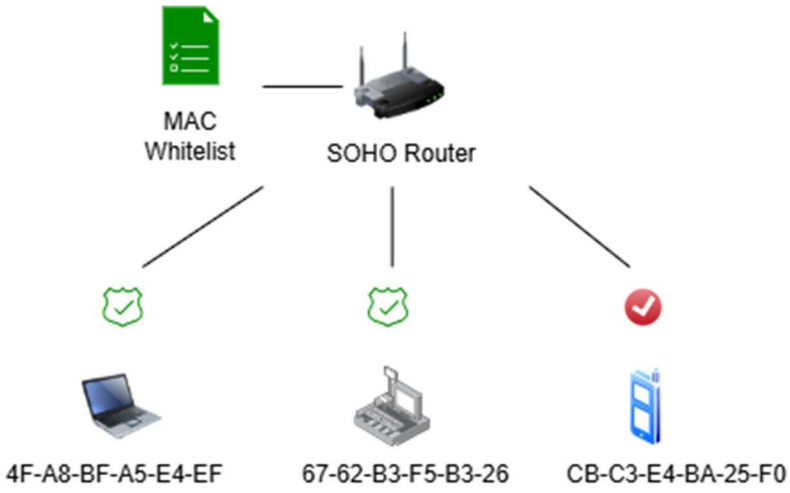


Creating VLANs requires the use of a Managed Switch. Switches may look the same to your average buyer, but they aren't created equal. Most SOHO routers have a switch built in on the backside. Depending on the size of your business, you may not implement any switches outside of this. The problem is that these switches are Unmanaged Switches, meaning they simply plug and play and don't support VLAN assignment or other advanced switching features. Managed Switches on the other hand allow administrators to configure features such as VLANs. If you and your organization want to implement segmentation through VLANs, you first have to look into purchasing one or more managed switches, which are generally quite pricey.

Additional Network Security Controls

Further network security features can be implemented at the routing and switching layer, some of which can be implemented even on basic SOHO routers and unmanaged switches. For example, MAC address filtering is a strategy where network devices are configured with Allow Lists or Blacklists based on MAC addresses. Every single network-capable device has a MAC address burned into its network card that uniquely identifies it. By taking note of these addresses,

administrators can inventory which devices belong to them. Then they can configure their network to allow only those addresses to connect. Whitelisting is the preferred option, as it allows the implementation of Implicit Deny. This is a strategy where all MAC addresses are blocked by default, and administrators whitelist devices on an as-needed basis.



Port Security is a security control that goes hand in hand with MAC filtering. Often when we configure a network, we end up not using every single switch port. Many office buildings use wall jacks for physical connections to networks, many of which end up being left open. This presents an immediate vulnerability, especially if these ports reside in the open or areas easily accessible to anybody. An attacker can quickly connect a device to an open port and use that access to either perform network reconnaissance or begin targeting devices with exploits. MAC address filtering takes care of part of this threat, but Port Security takes it a step further by allowing administrators to disable unused ports. This way, power is only provided to ports in use and those unused will be nonfunctional until they are enabled for legitimate reasons.

Wi-Fi routers may present the option to enable wireless access on a set schedule. The wireless networks can be configured to run during work hours during the week and then turn

themselves off after work hours and on the weekends. This feature completely removes the attack surface for hours when little to no network activity should be occurring to begin with. Implementing the scheduling option needs to be weighed beforehand. There are potential negatives associated with it, such as errors occurring on network servers when access is removed.

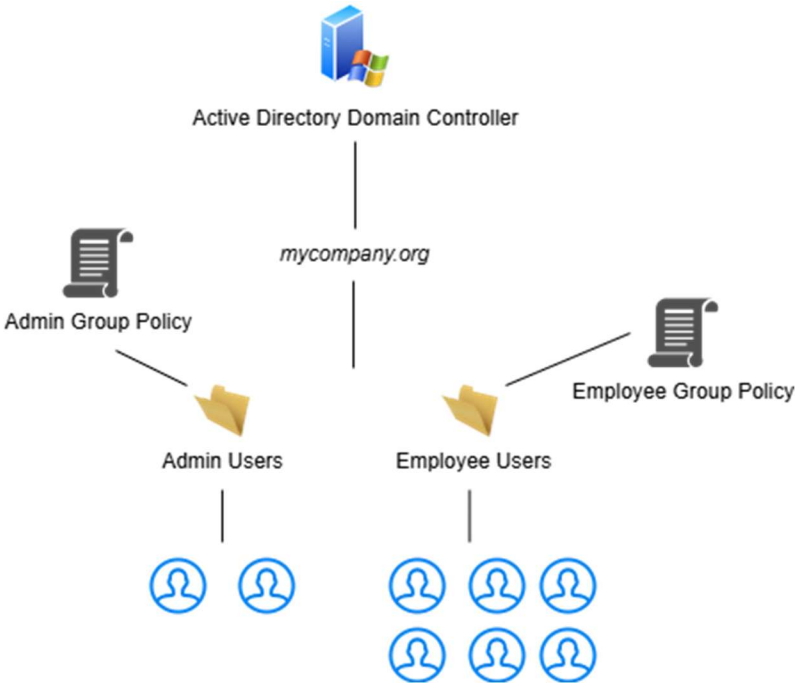
Flawed Access Control

Access control is a basic concept that applies to many areas in everyday life. We only want ourselves and maybe our spouses to have access to our personal bank accounts. We only want our immediate family to have keys to our homes. And we only want trusted employees to have the codes to unlock our office doors.

Digital assets need access controls in the same ways. Businesses store lots of data traversing various sensitivity levels. Without access controls in place, a network becomes the wild west where anybody of any standing can access any data they can get their hands on.

I have frequently observed basic access control failures in small businesses. By far the most prevalent is employees being assigned a Windows workstation with their own Administrator-level account. This is an understandable mistake since by default, Windows setup directs you to create an account with Administrator level permissions. However, assigning an admin level account to all users gives an uncomfortable amount of control to employees. With an admin account, there is no restriction on configurations an employee can make to their workstation. Any program they like can be downloaded and executed, the registry can be edited, settings can be changed, and unapproved connections can be initiated.

This issue is common in organizations with less than ten workstations. Larger organizations often implement a service known as Active Directory, a Microsoft service that enables the creation of a dedicated company domain with company computers joined to it. Within the domain, administrators can assign specific policies, access controls, and configurations to all devices under the domain's jurisdiction. Active Directory is a powerful tool that can harden assets at the most granular level. Users and computers can be subdivided into containers and groups according to a preferred organizational layout. A tool called Group Policy allows administrators to assign thousands of different permissions and configurations to these containers and groups.



The issue is that Active Directory is a pricey implementation, as it requires the purchase of a Windows Server license. In a business with ten or less employees, it is tough to justify the cost. This is unfortunate since centralized configuration and security is significantly more difficult without an Active Directory domain. If implementing an Active Directory domain is not

feasible, the best practice is to give every employee a standard Windows account and keep administrator accounts reserved for system maintenance and approved elevation tasks.

I have seen the consequences of unchecked administrator access several times. In one of the organizations I have worked for, an Active Directory domain is used for organization and access control. However, the access management policy still allows all employees in all departments to execute and install programs of their choosing without any need for privilege elevation. This has led to many employees downloading and installing Potentially Unwanted Programs (PUPs) either on purpose or through a bundle provided with another piece of software. PUPs vary greatly in their severity, but they are known for overloading users with adware, scareware, unnecessary toolbars, and spyware in extreme cases. PUPs are known for establishing persistence mechanisms in workstation registries and temporary file locations. This results in them being automatically reinstalled even after the user has supposedly uninstalled them.

Throughout this past summer, I have been part of Incident Response procedures for several cases of PUPs. Another employee and I found a sophisticated bundle of PUPs installed on an employee workstation that was exfiltrating user information and allowing a scam center to target the employee via phone and browser messages. After investigating the infection, we were able to highlight the bundle of programs causing the incident. All of this was enabled by a simple oversight in access control.

Access controls go far beyond the endpoint level; they should be incorporated into all areas of an organization's network infrastructure. Routers and switches allow administrators to create Access Control Lists (ACLs) for network segments. This allows networking devices to

allow or deny traffic based on their IP addresses. Combining MAC filtering with Layer 3 ACLs is a great strategy to harden access controls on business networks.

Another common piece of infrastructure in business environments is file servers for collaboration and sharing of projects and documents. In today's landscape, you are almost certain to encounter a hybrid deployment of on-premises and cloud file shares. File and directory-level permissions are perhaps the most common and vital use cases for access control. All major operating systems and cloud hosting platforms have access control list capabilities baked in. Data owners can get extremely granular with permission assignments. They can be based on users, groups, and subgroups. It is important to keep a record of permissions assignments and changes to ensure no oversight in access control.

Access management is a complex beast that requires regular auditing and tuning to ensure the utmost security. While assigning permissions and managing access may seem to be a tedious task, it is essential in a world where digital identities are replacing the perimeter as the primary digital assets.

Poor Authentication Practices

Everybody is familiar with the concept of a username and password. It is your sole guardian to ensure you have control of your digital assets. These days, everybody has many different applications and services that need secure passwords. The idea of creating multiple passwords is repulsive to most people, since it requires them to keep a record of each one. As a result, many people fall into the trap of using one password for every website and service. The danger of this approach goes without saying. Once the password is compromised for one

application, it is just a matter of applying it to others before an attacker has access to every user account of note.

This basic reality isn't lost on lots of digital users today. Many users do create unique passwords for each application. However, remembering them all remains an issue. As a result, you are bound to see many users employing insecure techniques for remembering passwords. The yellow sticky note strategy is one that I have seen constantly in professional environments. However, this is a dangerous practice, as attackers only need to employ simple shoulder surfing or dumpster diving to obtain notes containing passwords. In other cases, users will keep their passwords written in a simple text file on their computer desktop. This is also a risky practice. If the workstation is compromised, an attacker can extract or take a photo of the password list.

Password Manager services have emerged to address the inherent difficulties with storing passwords. Services like LastPass and Bitwarden offer subscription-based services where end users can store and organize passwords in a digital vault. The users only need to memorize a single password for the vault itself. The password managers offer desktop applications and browser extensions that will autofill the passwords when specific applications are accessed, as well as update passwords automatically when changes are made.

Deploying password managers in a business environment can be an excellent way to make the entire issue of password storage simpler. However, it is important to keep in mind that core vault passwords need to be strong and secure, since if a vault password is compromised, an attacker has automatic access to all other passwords. Additionally, it is important to be wary of the reputation of different password managers when selecting one. The products are not immune to compromise.

LastPass experienced a security incident in late 2022 in which hackers infiltrated the company's development environment and exfiltrated sensitive data. The stolen data contained credentials that enabled them to access third-party storage containing LastPass password vaults (Kapko). The incident was a major blow to LastPass's reputation and caused many customers to take their passwords elsewhere. So, while a password manager may aid organizational security, it can present large risks of its own. It is up to business management to educate their staff on the pros and cons of password managers and decide whether they are a good investment for the company.

When it comes to passwords themselves, the debate continues as to what constitutes a "strong" password. These days, applications set password requirements that involve mixing uppercase and lowercase letters, numbers, and special characters. This has remained best practice for a while now, but there have been some recent changes in recommendations for passwords. NIST is now recommending longer, more memorable passwords rather than complex ones (NIST, 2024). Rather than encouraging employees to make overly complex passwords, encourage them to create passphrases with 15 or more characters. These passphrases should be easy to retain and unique to the user, with some special characters or numbers thrown in at specific points.

One of the most useful technologies that has emerged in recent years is Multi-Factor Authentication (MFA). With MFA, users must provide two or more authentication methods to the AAA server to be permitted access. To meet the proper definition of Multi-Factor Authentication, these authentication methods must be taken from two of the following categories: Something You Have, Something You Know, and Something You Are. A username and password combo fulfills "Something You Know" and is commonly used as the first authentication method. We

could then combine it with a fingerprint or face scan for “Something You Are”, or a mobile push notification or a cryptographic smart card for “Something You Have”.

Many organizations have adopted the “Something You Have” category as their primary second factor. Apps like Duo Mobile are attached to accounts and provide users with a “One Time Passcode” or SMS Push Notification when they attempt to authenticate. The account owner must enter the passcode or accept the push before being authenticated. This strategy enables authentication to be spread across two separate devices, one that should only be possessed by the legitimate user.

A more expensive option for MFA is the deployment of smart cards. Smart cards hold a unique cryptographic private key that is unique to each user. When the user attempts to authenticate to a resource, they will be asked to physically connect their smart card. The private key on the card will be combined with their public key stored on the resource. If the combination is the correct one, the user will be granted access to the resource. Companies like YubiKey manufacture these unique cryptographic devices that can be used as authentication methods for many different applications.

If an organization does not want to take on the extra financial burden of purchasing unique keys, it can instead opt to use the “Something You Are” category. Networks running Windows systems can utilize Windows Hello, a built-in service that includes options for biometric authentication methods like facial recognition and fingerprint scans. In environments that utilize Windows Active Directory or Microsoft Entra ID, this might be the more sensible option.

Implementing MFA on all resources should be a requirement in modern small business networks. With advancements in computing power, cracking complex password hashes is becoming easier, and using a single username and password for authentication is going to become more and more unstable. Deploying a reputable and properly managed MFA solution adds an extra layer of safety by creating a roadblock that can only be passed with a unique personal attachment.

Weak Encryption

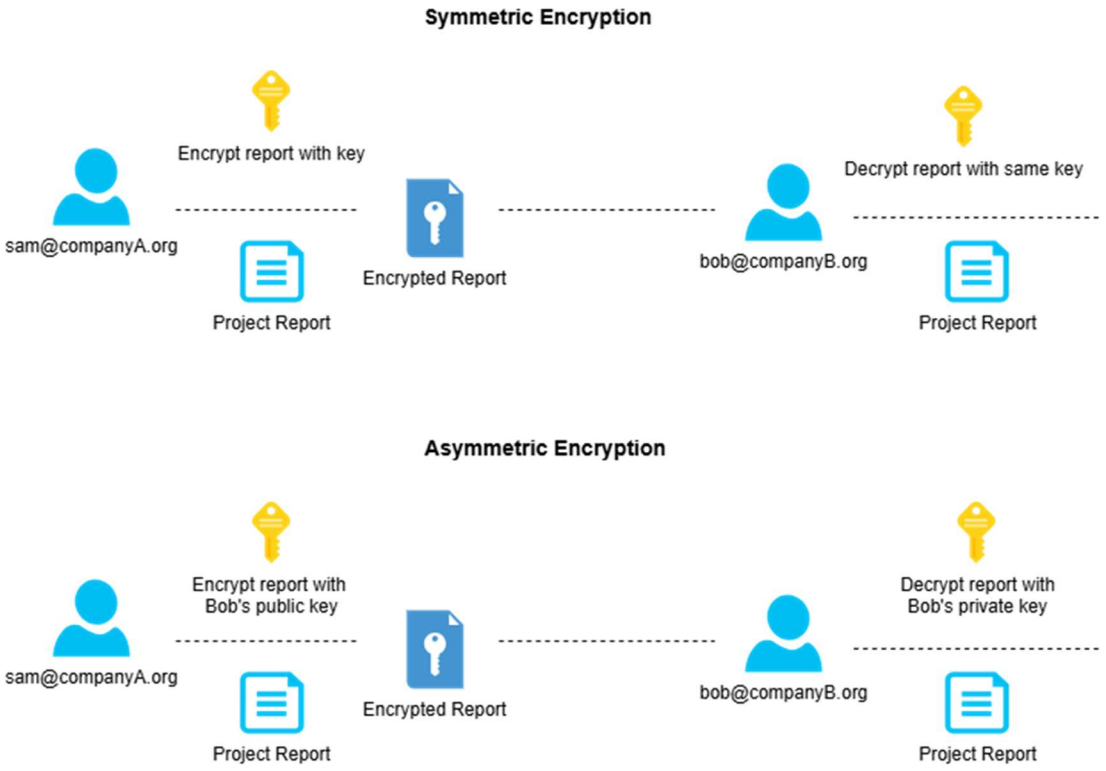
Data is perhaps the most valuable asset possessed by any organization today. More often than not, when a threat actor picks you for their target, it is your data that they are after. The amount of data present on the Internet has skyrocketed in recent years, and the emergence of new threats targeting that data has kept pace. To counter these threats, organizations need to embrace extra precautions like data encryption.

Encryption is the long-standing practice of taking a valuable piece of data and rendering it unreadable through a special cipher. A key exists to convert the unreadable text back to its original form, and that key is only known by approved entities. Encryption has a large presence within cybersecurity.

Business networks can implement encryption in a variety of ways. Encryption is often applied to data resting on storage devices, known as “data at rest”, and on data being transmitted across networks, known as “data in transit”. Encryption can be applied in two forms: symmetric and asymmetric.

Symmetric encryption entails using the same cryptographic key for both encrypting and decrypting data. All parties involved in communication are aware of the key and only need to

apply the key when receiving or sending data. Asymmetric encryption on the other hand, uses two keys: a “public key” and a “private key”. When a user wants to send out a piece of data, they encrypt it using the recipient’s public key, which is allowed to be known even on an unsecured network. The data can only be decrypted using the recipient’s private key, which should only ever be known by the recipient.

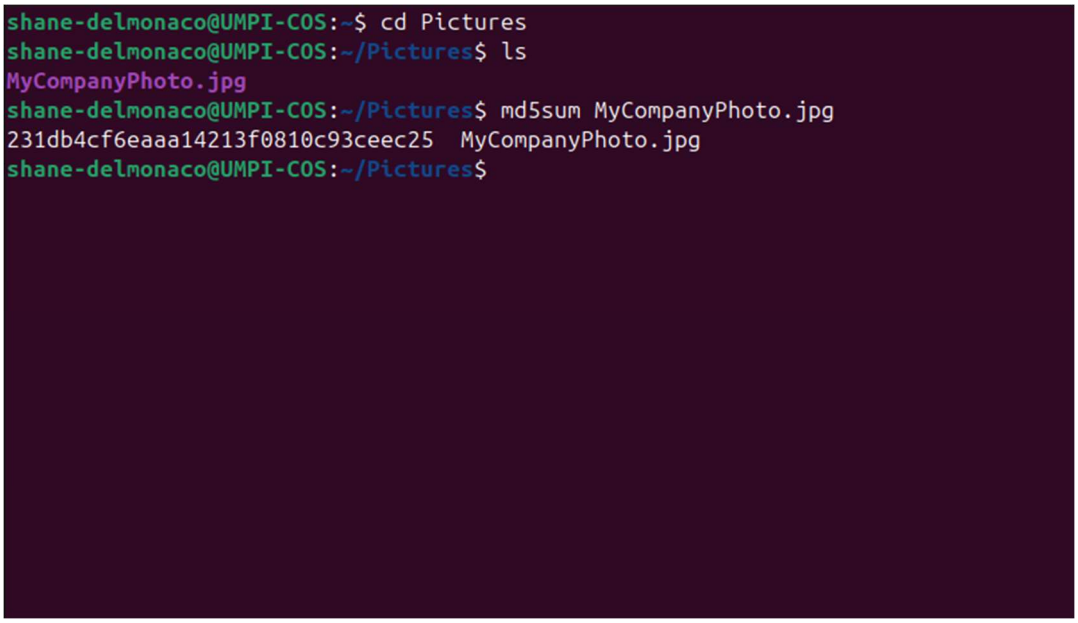


Encryption has many practical applications in a business environment. Often, we use encryption on our networks without actually knowing. I previously discussed the importance of using a reputable and modern protocol for wireless security, such as WPA2 or WPA3. Older wireless standards like WEP and WPA are still available but should not be used because of the insecure encryption algorithms they use. WEP uses an RC4 cipher, which employs static keys, meaning the same key is used for every packet transmitted.

WPA was released as an improvement to WEP, using Temporal Key Integrity Protocol (TKIP) and extra security measures like Message Integrity Checking (MIC). WPA also uses dynamic keys, meaning a new key is used for each packet. While it is an improvement over WEP, WPA has also had weaknesses revealed. TKIP is no longer considered secure and the encryption of WPA communication is now quite easy to break.

WPA2 is the recommended standard for most wireless networks today. It uses Advanced Encryption Standard (AES), a robust symmetric encryption algorithm with larger key sizes for encryption. WPA3 should still be considered going forward, as it uses even more robust encryption with larger key sizes.

Besides network communications, encryption is necessary at other levels of the network. Hashing is an encryption method that takes a piece of data and converts it into a string of characters that are globally unique to that data. If anything, part of the data is changed, even something small, the hash value changes. Hashing allows you to ensure the integrity of data. This has a wealth of practical uses in business environments. Confidential data can be hashed to ensure its integrity remains intact during daily operations. If new third party software is being downloaded for deployment, you can usually retrieve the software hash from the vendor, then compare it with your own generated hash to ensure you do not have an altered copy.



Hashing a simple image file with the MD5 algorithm.

Encryption can be implemented at the drive level to secure business data located on storage disks. The Professional, Enterprise, and Education editions of Microsoft Windows provide a tool known as BitLocker. BitLocker is a great security measure to implement on Windows systems regardless of company size. The program can encrypt either the used disk space, or the entire drive. BitLocker then stores the decryption key on a device's Trusted Platform Module (TPM), on a removable storage device, or in the cloud. If a device is stolen, the thief will be unable to retrieve data from the hard drives without the BitLocker key.

The rabbit hole of encryption continues to expand and intensify by the year. Algorithms once considered strong are being cracked, and faster computers are allowing for more complex ciphers and keys. Quantum computing is an industry with a lot of hype behind it, and as it expands, it is going to become more difficult to securely encrypt data. This is why it is essential to stay up to date with cryptography and adjust your business's use of encryption with the times.

Software Controls & Patching

Every small business is guaranteed to use several software programs in their daily operations. Whether it is locally installed or cloud Software as a Service implementation, software processes large amounts of data daily. Software can be used to aid in every facet of business, including decision-making, archiving, and digital transformation. Microsoft 365, QuickBooks, AutoCAD, Tableau, Photoshop, and Dropbox are just a few pieces of software you may find in business environments.

Since most work is done through software, it is imperative that attention is given to the security of the programs. Too often, it seems that people believe workstation security stops at the operating system level. This couldn't be further from the truth. Even the most high-end software can be full of vulnerabilities, giving attackers an entry point into the system and beyond.

A common mistake present in business environments involves the use of Microsoft Office macros. Macros are functions that can be enabled in office documents, allowing specialized calculations to be performed. Macros have long been a common source of viruses yet are still frequently necessary for workloads.

To combat malware stemming from macros, a business should employ a Principle of Least Privilege, keeping macros disabled by default and only enabling them for employees who absolutely need them to complete their job. On workstations that need them enabled, ensure that antivirus software is present and up to date. Organizations with a larger budget for security should look into deploying an Endpoint Detection & Response (EDR) program. These programs are more thorough and comprehensive than simple antivirus, they can investigate workstations

on a deeper level, catching anomalies and suspicious behavior present in small programs such as macros.

Web browsers are usually the most widely used software on any computer. They are the gateway to the public Internet, enabling communication and research for anybody with a connection. This means that browsers can lead you directly to the newest and most destructive cyberthreats and serve as an entry point into your system. Therefore, it is best to implement proper security measures in web browser settings. This is generally simple to do on a browser, whether it be Google Chrome, Firefox, Brave, or Microsoft Edge. Pop ups should be disabled to prevent adware, cookies should be limited to only those necessary, and browser password storage should be turned off in favor of a dedicated Password Manager application.

Each piece of software has its own configurations and purposes, so security personnel will need to meet programs where they're at for security controls. However, every program needs patching, and one of the most dangerous things someone can do is leave software unpatched. I have seen this mistake made plenty of times on business computers, and it can have dire consequences. Management should at least turn on automatic updates for all programs or implement a centralized patching system for pushing out updates on a schedule. The online package manager Ninite allows updates or multiple common programs to be downloaded and pushed out in a single package.

Exposed Ports & Services

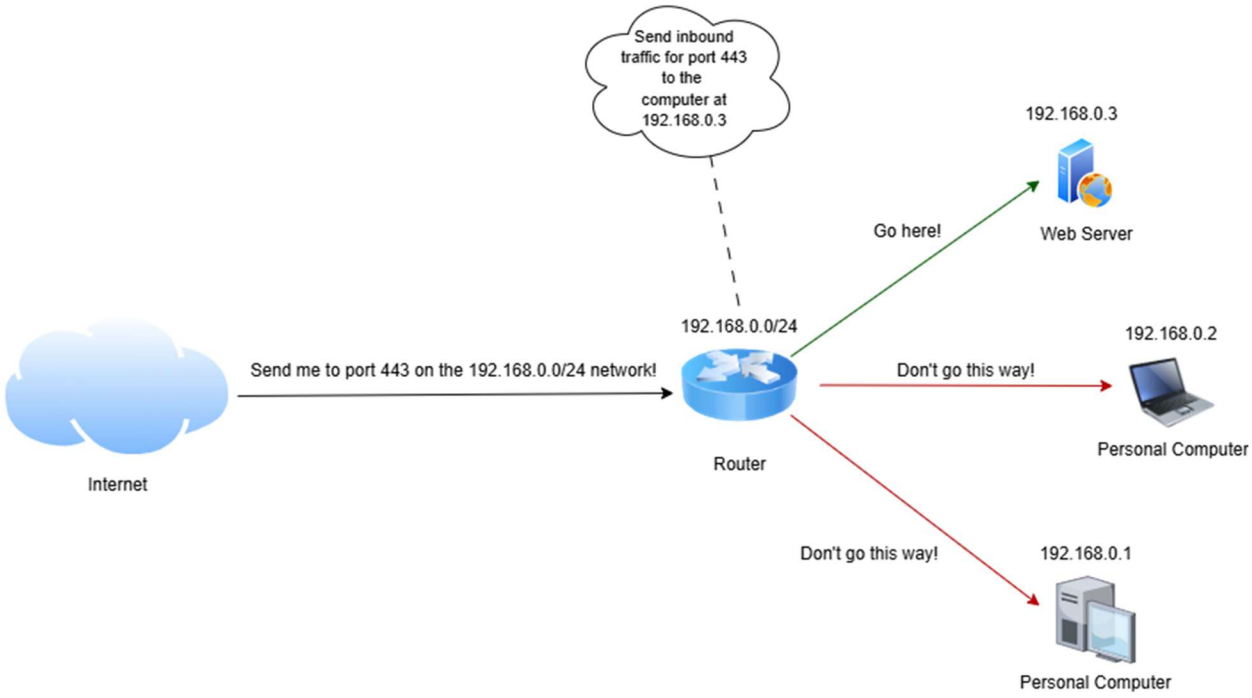
Realistically, every modern local area network is configured with a firewall solution. Larger organizations typically employ multiple dedicated hardware firewalls across their network infrastructure, allowing for granular traffic control. Even if a network doesn't have their

own dedicated firewall, basic SOHO routers contain a built-in firewall functionality. In the year 2025, not having a firewall is out of the question. It is a universal necessity that should not be questioned. Even if a person doesn't know whether or not they have a firewall, they likely do since it is a functionality baked into consumer brand routers.

Firewalls are meant to be configured to meet the end user's needs. Firewalls use "rules" to tell the device what kind of traffic should be let into the network and what traffic should not, as well as what traffic should be let out and what should not. The accepted strategy for firewall configuration is to "Allow Outgoing, Deny Incoming". This basic configuration makes the playing field simple. Users on the LAN can contact any services they want on the open Internet, while anybody outside trying to enter the network is blocked.

This only works for so long however, since two-way communication is necessary for communication with services on the Internet. The firewall will need to be configured to allow ingress traffic from valid ports and protocols. HTTPS, HTTP, DNS, SSH, SMTP, IMAPS, POP3S, and SFTP are widely used ports that are generally safe to open. Most consumer grade SOHO routers come with necessary standard ports already open.

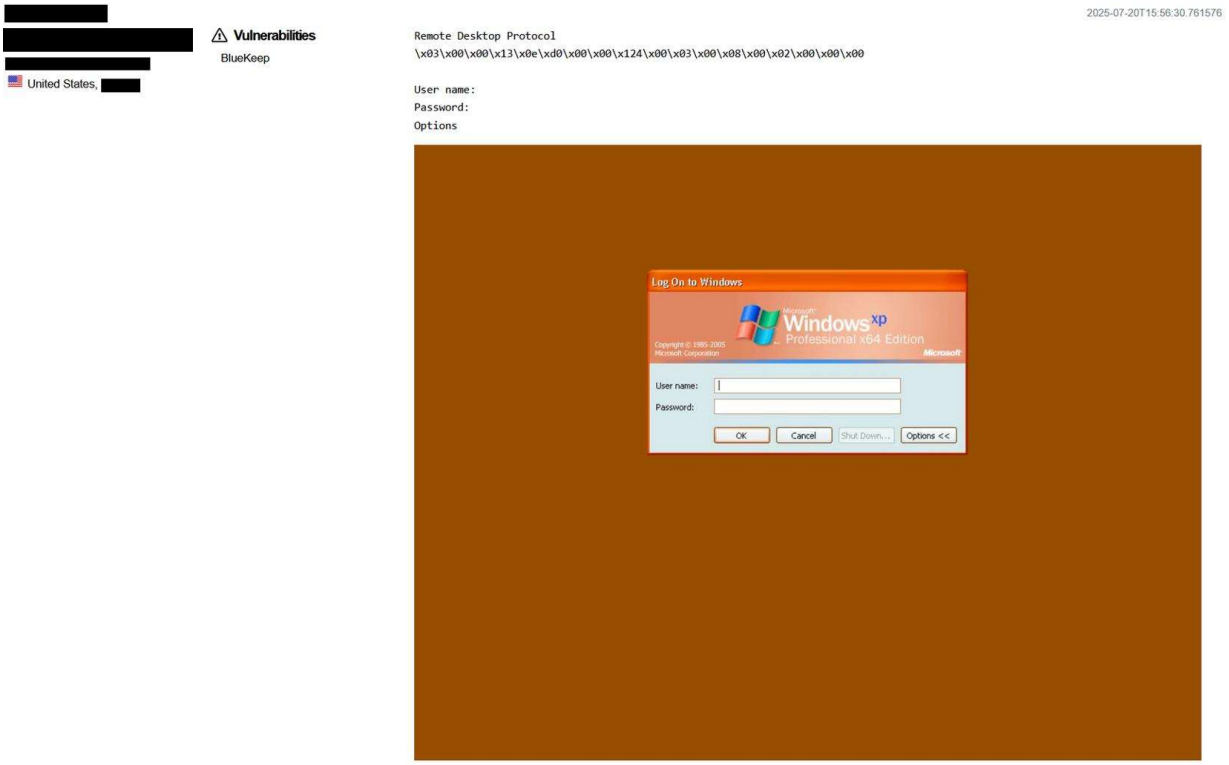
This is all well and good, but an organization can get into stormy water when it decides to start using Port Forwarding to open access to LAN resources that should not be open. Port Forwarding is the process of configuring a router/firewall to direct all traffic for a certain port/protocol to a specific device on the internal network. This is necessary to allow public networks to access resources like a website hosted on a web server. Think of it as a door kept open to the public that directs them to a specific room for a specific task.



Port Forwarding is dangerous if done incorrectly and should only be done for services that need to be publicly accessible. Ports should also only be forwarded to machines residing on a dedicated network segment for hosting public services and public services only. Under no pretext should a publicly accessible server be located on a network segment that is also hosting sensitive internal data.

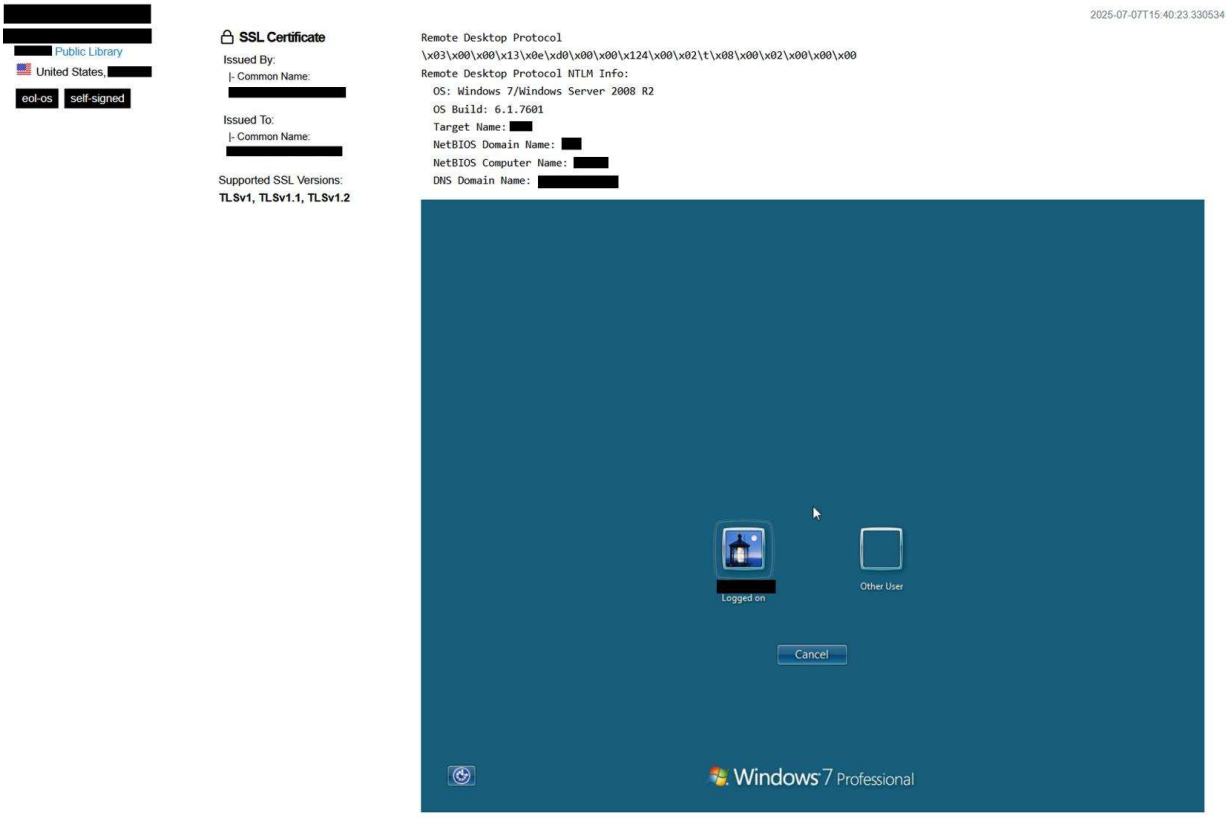
Unfortunately, more often than not ports are left open to the public Internet, allowing outside forces to see internal resources that were never meant to be seen by others. An organization may forward port 3389 for Remote Desktop Protocol to a work desktop to allow an employee to connect from home. Or they may open port 554 to view security camera feed from away. The problem is that not only can authorized users connect to and view these resources, but everyone else can too!

In this case, we don't need to wait for a public example to arise to prove this is dangerous. Shodan.io is a search engine focused on indexing publicly accessible servers that can be viewed by anybody using a specific search syntax. From webcams to desktop computers to media servers, anything left open and unsecured on the Internet can be found. While this may feel illegal, it is not and the information gathered on this website falls under the umbrella of Open-Source Intelligence (OSINT).



In the above screenshot (sensitive information on the location of entities has been redacted), we see an exposed RDP running on port 3389. As if this wasn't bad enough, we clearly see that the machine is running Windows XP Professional. XP reached its end of life on April 8, 2014. Its days have long passed and today the operating system has a reputation for its weak security due to its end of support.

Shodan will list any well-known vulnerabilities it identifies a subject as being exposed to. We can see that this machine is vulnerable to BlueKeep, a critical vulnerability that allows an attacker to use RDP for remote code execution. Instances like this are begging to be compromised by threat actors. A seasoned black hat hacker would see the IP address, the operation system hosted, and the detected vulnerabilities and quickly be able to develop a blueprint for deploying an attack.



In this second screenshot from Shodan, we see that this machine belongs to a public library and is connected to an Active Directory domain. The machine is running Windows 7, which reached its end of life on January 14, 2020. Like XP, Windows 7 is now known for its security vulnerabilities. An attacker who comes upon this machine could deploy their methods of attack specifically for Windows 7. Since this machine is domain connected, an even greater risk

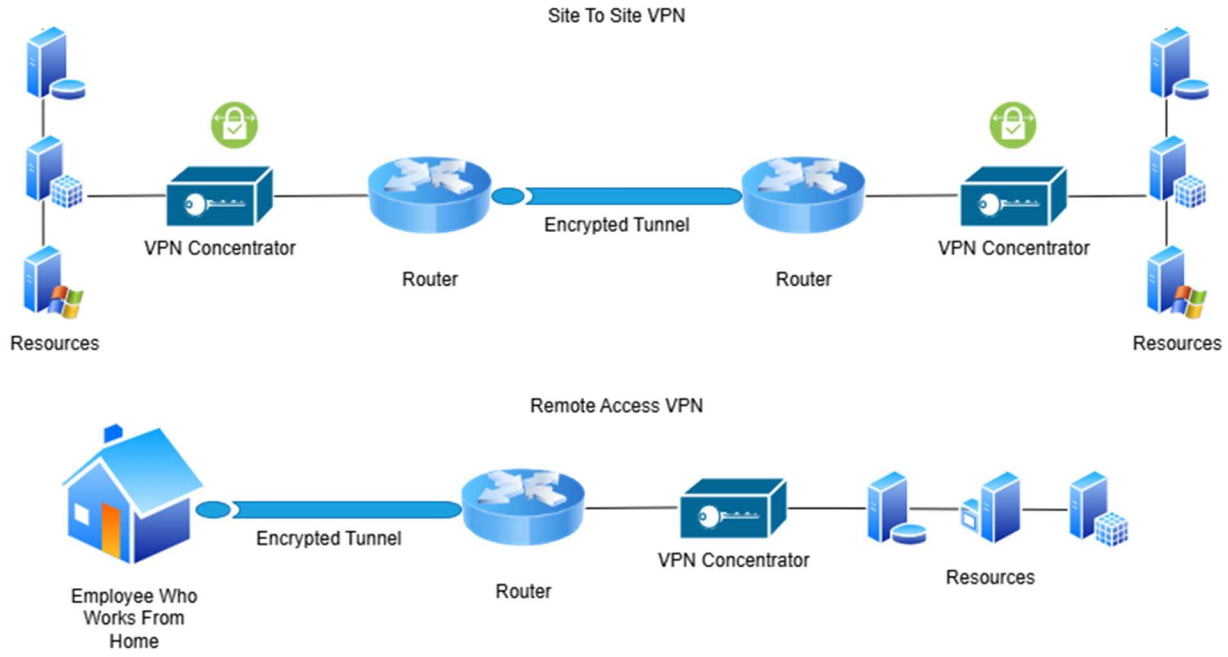
is presented. An attacker who compromises this exposed machine would then be presented will a clear path for lateral movement to other domain machines. They could also pursue privilege escalation and go after the domain controller itself, thus gaining access to credentials and network-wide administrative controls. Since the machine in the screenshot is running Windows 7, it would not be unreasonable to assume that the domain controller is running an outdated version of the Windows Server operating system as well.

Exposed ports and services are one of the most blatant misconfigurations an organization can make with cybersecurity. It is an easily avoidable mistake. Organizations should always follow implicit deny when deploying firewalls. No ingress traffic may pass unless it is from a port or protocol explicitly allowed by a firewall rule. If an organization is on the smaller side of the spectrum and uses a SOHO router, using the default configuration is generally acceptable.

In situations where it is imperative that certain services be accessed by employees from remote networks, a company Virtual Private Network (VPN) solution is recommended. A VPN is a security implementation that creates a secure encrypted tunnel passing from one private network over the Internet to another private network. Users can perform tasks and access resources on the distant private network with all of their traffic passing safely through the encrypted tunnel, meaning threat actors on the Internet cannot see the traffic and breach its confidentiality or integrity.

VPNs come in two general forms: site to site and remote access. A site-to-site VPN directly connects two LANs at the gateway level, allowing wide area connections between the end device on each LAN. A remote access VPN allows users to connect to one private network remotely as long as they have a proper configuration file and are vetted by an IAM system.

Remote Access VPNs are the more likely fit for small businesses, although a business could greatly benefit from a site-to-site VPN if they have multiple branch offices.



The issue with VPNs is that they are a complex beast to understand and set up. There are multiple VPN protocols, including SSL VPNs, Point to Point Protocol VPNs, Layer 2 Tunneling Protocol VPNs, and Internet Protocol Security VPNs. Each protocol has a different method of operation and requires different configurations. A more accessible solution for a small business looking to implement a simple VPN is OpenVPN. This is a free system that may be easier for the average business owner to implement.

Regardless of the chosen protocol, setting up a VPN allows users to securely access internal resources like servers, cameras, and printers. Opening and forwarding ports on the core router is no longer required, eliminating a severe risk. However, it is important that anyone wishing to implement a VPN solution treads with caution and seeks professional assistance if they do not know what they are doing.

Nonexistent Backup Solutions

If there is one lesson to take home from the security incidents in Chapter 2, its that proper backups make all the difference. However, I remain baffled at the number of small businesses that do not have any backups configured. Specifically in cases involving ransomware, having backups can be the difference between recovery and going out of business.

Narrowing down exactly how to create and retain backups can be a difficult task. For businesses with ten or more workstations and the money available, a Network Attached Storage (NAS) device can be bought and configured to host backups created by built in operating system backup utilities. For businesses with just two or three workstations, a simple USB drive or SD card can be used instead.

However, this solution, while easy, can fall short in the event of an actual cyberattack. Many pieces of malicious software, especially ransomware, attack all attached storage on a victim workstation, not just local files. This means that the effects of ransomware can spread to the NAS or USB drives themselves, rendering the entire point of the backups pointless.

A more painstaking yet effective method of backups is the offline backup. This utilizes either external hard drives or tape drives that are connected to devices on a backup schedule, then removed and kept in a secure location until the next backup or cases of recovery. This method can also be easy for small businesses with only a few workstations, but it requires staff to remember to complete the task. In a business with ten or more workstations, it is not a feasible solution.

To have the best possible backup solution in place, a business needs to follow what is known as the 3-2-1 Rule. For the 3, rather than keeping one single copy of enterprise data, an organization should keep three independent copies. These days, having one single backup solution is not enough. Compromise of the backup is a very possible threat, especially if your local backups are network attached. The 2 of the 3-2-1 Rule specifies that you need to keep two separate copies of backups on two separate storage mediums. More often than not, this will take the form of a local on site-backup and a cloud backup. The 1 of the 3-2-1 Rule further encourages this by specifying that one copy must always be held off-site. A small business with only a few workstations could find it difficult to justify the cost of a cloud service. Instead, they could make a local copy to two external hard drives, then store one in a safe at the owner's house or a locked filing cabinet.

With increases in ransomware and data breaches, it isn't crazy to start making three copies of backups. When dealing with cybersecurity, you have to assume that the worst possible scenario can occur anytime on any day. It is advised to make as many backups as a company sees fit in their environment, as long as at least one is being stored in a location far from the office facilities. Cloud services like AWS S3 offer cloud storage that can be provisioned to a customer's need at affordable prices. Just be aware that cloud storage has its own security requirements. Without proper access controls in place, the cloud can be an even easier method of exfiltration for threat actors.

Insider Threats

An organization can implement all the best network defenses on the market and make several backups a day. This will give them solid protection. However, at the end of the day, all

the defensive technologies in the world cannot defend against insider threats. Insider threats can take many different forms. A disgruntled employee who has just been laid off can copy important project notes or trade secrets to external storage and take the storage device home to sell or send to competitors. Aless tech savvy employee could accidentally send sensitive information to a malicious actor. An employee could use a company computer to access illegal content, bringing an undesired law enforcement presence to business facilities.

The blunt reality is that many people in the workforce today, even younger generations, are not familiar with all the cyber threats ready to take advantage of them. It is imperative that any organization implements security awareness training for staff. This training does not have to be deep; it just has to make staff aware of what threats could look like and the appropriate actions to take when encountering one.

It is bad practice to expect employees to be aware of all the newest threats. While employee training is a good precaution, separation of duties and principle of least privilege is necessary to protect assets when an employee compromise does come. Many organizations have made a push to embrace a “Culture of Security”. Employee training should include security precautions when describing every task to be performed with business technology. Familiarize employees with common cyberattacks and their Indicators of Compromise and encourage them to share knowledge with other employees.

The surface for threats targeting individual employees is growing more sophisticated by the year. Even if employees are educated to identify phishing emails, they may come across an email that is so well written and convincing that they may not even assume it is a malicious email. AI driven phishing emails are going to become harder to identify going forward. Another

piece of new technology that can wreak havoc in the workplace is the “Deep Fake”. This artificial intelligence driven technology allows users to create visually realistic digital imitations of real people, down to their voices and mannerisms. Cybercriminals could develop a Deep Fake of company management to send to employees to pretext an attack. While AI based social engineering may sound like the creative work of a science fiction author, it is quickly becoming reality. Business leadership should passively keep an eye on artificial intelligence developments moving forward, as the social implications of new technologies will likely have unpredictable effects on internal security.

Management should never give employees the benefit of the doubt and expect that all insider threats will emerge from employees being taken advantage of by outside threat actors. Employees themselves have just as much capability to be the threat actors, and no oversight should be passed over, no matter how reliable the employee is. Perhaps the most common scenario that comes to mind is that of the disgruntled employee, who is released from employment, and just before vacating the premises, wrecks some kind of havoc on digital infrastructure. This could include sabotaging the integrity of data, copying data for unauthorized public exposure, or even corrupting the availability of workstations or servers.

Mitigating the chances of this risk occurring involves having a comprehensive onboarding/offboarding policy in place. Onboarding processes should involve having all access and scope clearly defined before the employee is even hired. This information should be compiled into a user account policy that has all the necessary permissions ready. This way, when an employee is hired, their account can be quickly deployed. There should also be the opposite policy ready to be deployed at all times. An offboarding policy should remove all privileged access from the user and take their account out of commission as soon as their employment

expires. A clean onboarding and offboarding policy is a necessity to prevent disgruntled employee attacks. In smaller organizations, the process could be as simple as having the IT department disable the employees' Active Directory account the day of their leaving.

A final insider threat that unfortunately is very possible is employees using company information systems to access and/or distribute illegal materials. There have been many cases of employees distributing pirated material, accessing or distributing child sexual abuse material, or engaging in illegal market transactions, all on devices owned by their employer. Incidents such as these have the potential to bring a law enforcement presence to the workplace. This could result in a bad public relations image for the company.

Log collection may not be a top priority for small business owners, but it is a practice that makes incident response much easier when the time comes. Collecting Windows Event logs, Internet search history, and communication between network devices can give management and law enforcement a blueprint for investigating illegal misuse of the Internet. Many security standards require organizations to retain their logs for a set amount of time. While the overhead of purchasing additional storage for these logs may be unappealing, the payoff will be immense in the case of a law enforcement investigation into any activities performed by bad actors on your network and information systems.

Administrators can and should implement measures to discourage illegal misuse of networks and devices from the get-go. Every organization should have an Acceptable Use Policy (AUP) in place. This policy lays out the expected behavior to be exhibited when using company information systems. The policy should also lay out in fine print potential consequences for misuse of the systems. Administrators can also implement content filtering at the DNS level to

blacklist unnecessary, malicious, and illicit Internet content inside the business LAN. There are several open sources to provide secure DNS and content filtering, such as OpenDNS. While there are plenty of ways around content filtering, implementing it will set a strict line in the sand for employee use of company Internet access.

Internet of Things (IoT)

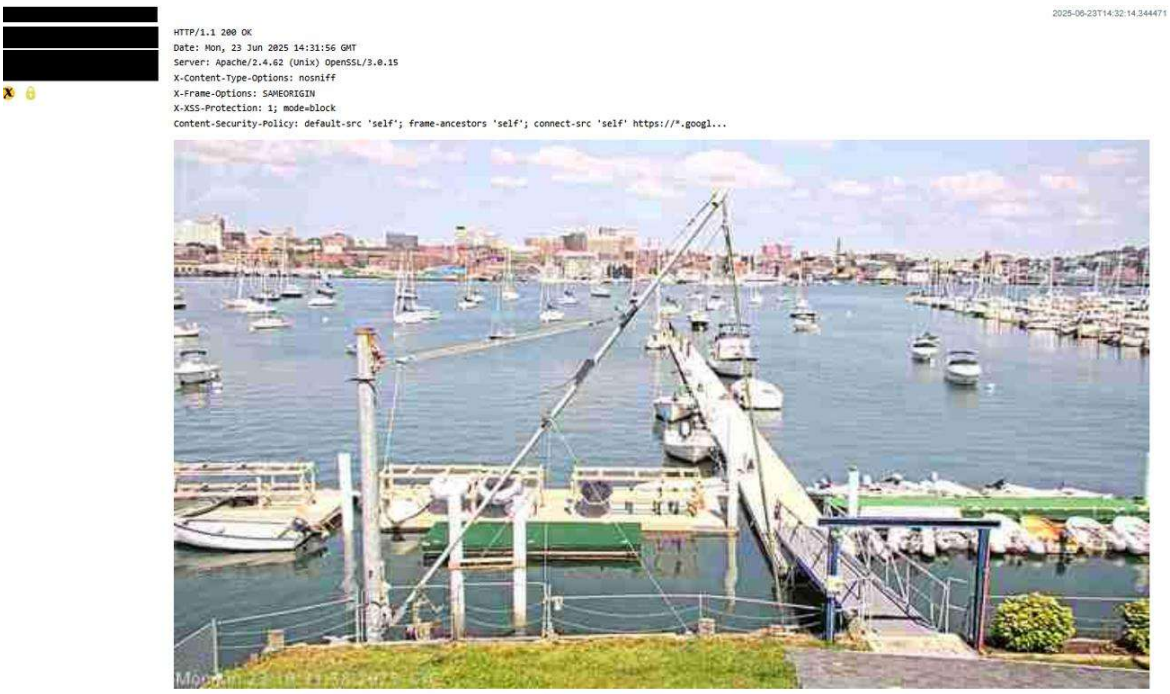
One of the new technologies that has hit the markets in the last decade is the constantly improving Internet of Things, commonly referred to as IoT. Microcontrollers, sensors, and wireless networking have allowed individuals to control their everyday appliances remotely from a screen. Light switches, HVAC appliances, refrigerators, and thermometers are just some of the small devices that can perform simple daily tasks for you. Business management may implement IoT devices to control facility lighting and heat around the clock. Industrial organizations are increasingly taking opportunities for IoT automation of many of their complex manufacturing components. The world of IoT is not perfect, but it presents some great opportunities.

Perhaps the most evident example of IoT's imperfection is the lack of security in IoT devices. Global cybersecurity firms have frequently sounded the alarm on the large number of vulnerabilities present in smart devices. The relatively new presence of IoT devices means that patches for vulnerabilities are usually not available out of the box and need to be discovered and developed. IoT devices are very susceptible to Zero Day attacks for this reason.

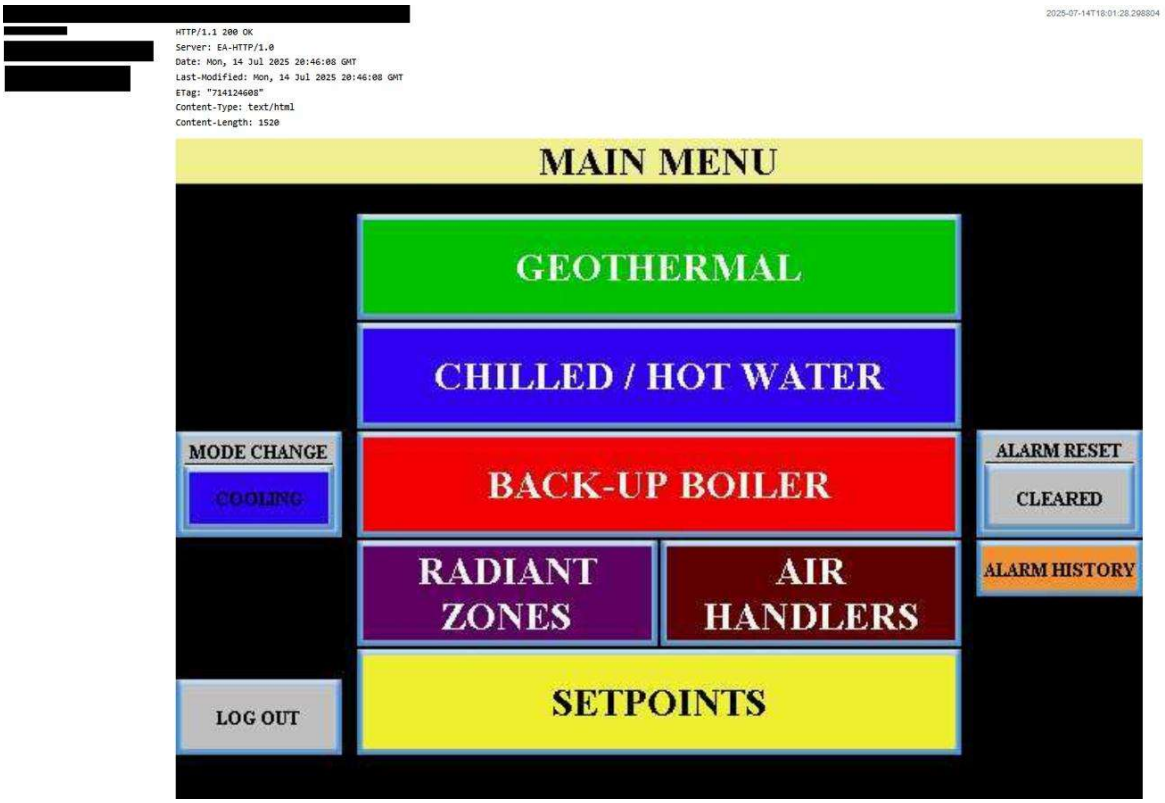
Organizations should always isolate their IoT devices by assigning them to their own dedicated VLAN. Some IoT devices are more closely integrated with the organization than others. Industrial control sensors pose a much larger risk than the break room ice cube maker. To help break the threat down further, create multiple VLANs to assign IoT devices to according to

their sensitivity level. Administration should closely follow the security developments of the IoT devices they have implemented and reassign the devices to different VLANs according to the evolution of their security.

The vulnerabilities present in security cameras are probably the most well-known IoT risk. In this day and age, most small businesses have at least one security camera present. Many of these devices provide the ability to be remotely monitored and accessed. However, this can open a gaping hole right into a network. Combine this with the fact that your average SOHO network will likely place the cameras on the same network as their company data makes them one of the most dangerous pieces of technology used by small businesses. Some users may forward certain ports on their router to the camera interface as a way to access their company cameras from afar. This is a terrible idea, as not only can threat actors use the port as an entry point to the network, but the camera feed can become accessible to the entire Internet. Using shodan.io, we can search for port 554 and find a wealth of open security camera feeds.



Any organization that needs to access security cameras from remote locations should keep their cameras behind their firewall and use a VPN solution to access the network and then the cameras. This goes for all devices that need to be accessed remotely. Many times, ICS controllers and SCADA systems are also opened to the open Internet in an attempt to make remote access and control easier.



There should never be any circumstance in which a critical system residing on a private network segment is port forwarded to the Internet. Some machines such as web servers need port forwarding to serve their function. In such cases the systems should reside on a dedicated network segment for riskier services, known as the Demilitarized Zone (DMZ).

Even when confined to their own bubble, IoT devices still pose security risks. A common mistake made by users is forgetting to change the default credentials on devices. Users might be

convinced that strong credentials are not necessary for smart devices, but it is essential to always change default credentials on any device that has them. If an attacker enters a network segment through any means, they can find out default IoT credentials and pivot to those devices.

The issue of IoT security is a complex one that crosses over into many other areas of cybersecurity, such as legacy system integration and zero-day vulnerabilities. IoT security is an issue that isn't going away and is only going to get more relevant in the future as more appliances begin employing sensors and microcontrollers. Any organization that uses any IoT device should focus on proper segmentation, keep up to date with vendor patch releases, and integrate compensating controls such as a dedicated Intrusion Detection/Prevention System for IoT segments.

Physical Security Vulnerabilities

A business team can purchase all the hottest new security equipment from all the top vendors they want, but it means nothing if basic physical security measures are not implemented. Physical security risks are among the most under-discussed when it comes to developing a cybersecurity plan. If an attacker breaches a facility physically and steals hardware, they have their target right at their fingertips and can take the time to dissect the stolen asset. Even if data residing on the hardware is encrypted, attackers can try to break the encryption since they are no longer under the pressure of maintaining access.

There are some very basic physical security measures that can be implemented to provide up-front security for any organization. Locks are the most obvious. While traditional locks with dedicated keys may suffice, any organization should look into upgrading to a digital locking system. Digital locks with dedicated PINs are an option. Different PINs can be set for different

doors, and these PINs can be distributed to employees following the Principle of Least Privilege. However, in an organization with more than ten employees, this solution can become difficult to manage and the likelihood of PINs becoming compromised increases. Organizations should look into implementing an NFC locking system that uses smart cards to validate user identities and privileges. The Principle of Least Privilege becomes easier to implement and manage in this case, since each user is authenticated and authorized individually rather than by one valid key or PIN. NFC locking systems are on the pricier side of the spectrum but nonetheless should be heavily considered.

Lock placement needs to be carefully planned to guard the most critical business assets. There should be a lock placed at all entrances to the facility. A lock should also be deployed at any network closet door. Make sure to employ the principle of least privilege when defining access controls for the locks. Non malicious incidents can arise from something as simple as a janitor sweeping a network closet and accidentally disconnecting a few cables in the process.

Locks should be accompanied by security cameras. Today, IP security cameras are affordable and should be implemented by any business regardless of size. A camera should be placed above every entrance and on every physical side of the office building. Administration can then be as loose or stringent with interior camera deployment. There should at minimum be a camera in any public entrance and above any network closet door.

There are many models for security cameras that have different placements in mind. Dome cameras make sense for large interior areas while bullet cameras are recommended for guarding exterior entrances. Pan, Tilt, Zoom (PTZ) cameras are a more flexible option that work in a variety of interior and exterior locations.

Even with these standard security measures, physical security incidents can still arise through clever maneuvering by threat actors. Tailgating and piggybacking are common social engineering techniques that pose large risks to organizations with frequent in and out traffic. In a tailgating attack, an attacker discretely follows an authorized person into a secure location. A piggybacking attack occurs when an attacker is let into a secure location by an authorized person who assumes the attacker is another authorized person. For example, an attacker could put on a generic handyman outfit and carry a toolbox with them, convincing the authorized person that they are a contractor performing a job for the organization.

Tailgating and piggybacking can be mitigated by regularly informing employees about the dangers of letting people onto the premises, even if they appear legitimate. Remind employees to carefully observe those around them and not let anybody through a locked door under any circumstances. A major defense against tailgating and piggybacking is implementing a mantrap door. This is an entrance that employs two interlocking doors along with sensors to ensure that only one person enters the building at a time. This may not be financially feasible for small businesses.

Any organization that has a publicly accessible entrance area presents an inherent risk to staff and assets occupying the front desk. A forceful attacker could easily come onto the premises and hold staff at gunpoint before walking out with a piece of technology. Placing cable locks on computer hardware is an inexpensive way to make this task more difficult for attackers. Since hardware is locked into a physical connection, walking out with the hardware becomes significantly more difficult. At the very least attackers will be tied down into the task, providing time for incident response and/or law enforcement to engage. For optimal security, organizations

should apply cable locks to all computers in their facilities, not just those in publicly accessible areas.

Cloud Misconfigurations

Businesses everywhere have transitioned many of their technological needs to cloud platforms, benefiting from features such as easier configuration, reduced costs, high availability, and options for scaling resources. Platforms such as Amazon Web Services, Microsoft Entra, and Google Cloud have made it easier for organizations to host almost any resource, from web applications and servers to identity management and access controls.

Many risks come with utilizing cloud platforms. Since cloud user interfaces are accessed on the Internet rather than on a private network, a compromised administrator password could give an attacker access to the dashboard for managing cloud resources. This is why it is highly recommended to use multi-factor authentication for all cloud accounts.

Cloud resources have become major sources of data breaches. This issue can stem from a fundamental misunderstanding of how permissions are assigned in the cloud. Cloud services utilize roles and security groups that often have a specific method of application that is unique to the cloud interface. Learning how to navigate this can be a learning curve for a small business owner trying to spin up a few basic cloud instances. Luckily, most major cloud services offer built-in tools to help audit cloud permissions, such as AWS IAM Access Manager.

A common mistake often left unaddressed by users new to the cloud relates to the section on Exposed Ports & Services. Cloud instances are defended by virtual firewalls that are configured with security groups to allow necessary connections. A cloud user could accidentally allow too much unnecessary access to certain ports. A common bad practice is to allow unlimited

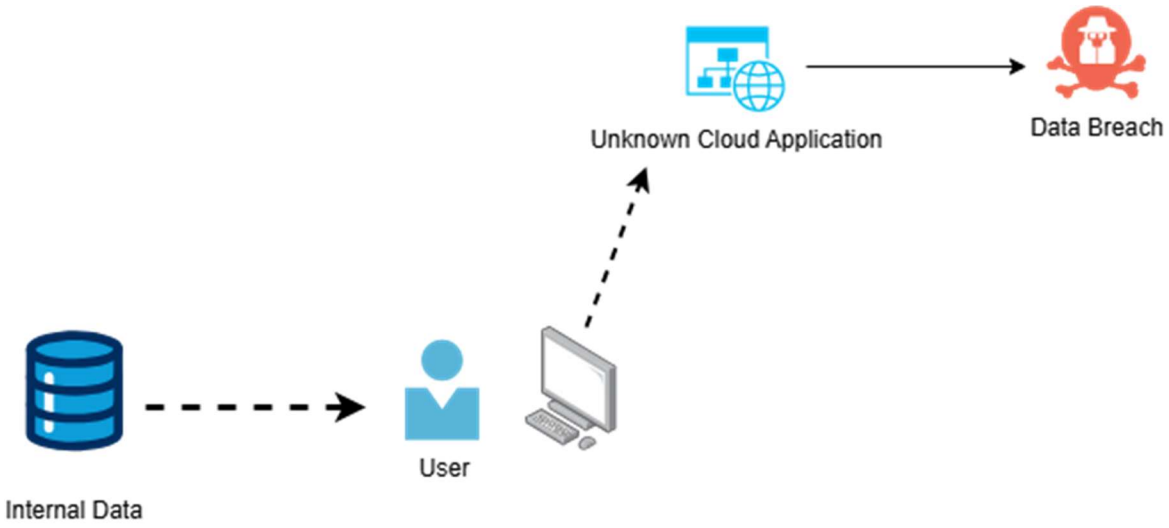
ingress access to a cloud server through SSH. When configuring SSH rules, administrators should allow access to an approved subnet of IP addresses rather than all networks.

As a business grows in size and expands its workloads, it may begin using multiple cloud platforms to provide different services. For example, they may use AWS to host a website, Microsoft Entra ID to provide Identity & Access Management, and Google Suite to provide productivity tools. Managing multiple cloud instances can become a managerial nightmare, as administrators are tasked with controlling access and setting centralized permissions.

The Cloud Security Alliance, in their publication "Top Threats to Cloud Computing 2024", highlights that "Different cloud providers have unique systems, which can lead to mistakes and security gaps", and that "without a deep understanding and management strategy for multiple systems, the risk of misconfigurations and inconsistent security policies is significant" (Cybersecurity Insiders, 2024, p.14). Any organization looking to migrate services to the cloud needs to carefully review the vendor's interface and IAM process before moving forward. Implementing a change control process to carefully document actions in the cloud is also recommended to avoid confusion during provisioning and management.

The post-pandemic world has seen a shift away from the strict use of company technology, which is residing behind a network perimeter. You are more likely to see the previously mentioned scenario, where a business uses a variety of cloud and web applications from various vendors. The lack of any real core perimeter is what enables many data breaches to take place, since there is no centralization of access controls or permissions. This issue is known as Shadow IT.

Two threats stand out regarding unsupervised cloud usage, those being Un-Sanctioned App Misuse and Sanctioned App Misuse. The Cloud Security Alliance defines Un-Sanctioned App Misuse as “when employees utilize cloud applications and resources without corporate IT and security’s specific permission and support, leading to Shadow IT”, and Sanctioned App Misuse as “when organizations cannot monitor how their approved applications are being used by insiders or targeted by external threat actors, often through methods like credential theft, SQL injection, and DNS attack” (Cybersecurity Insiders, p. 43).



Both of these issues can create serious trouble for organizations, as their data escapes their hands. However, the issue is complex, as employees may be encouraged to utilize Internet resources at their discretion to improve the efficiency and quality of their work. Concerns over internal data usage can be mitigated by implementing a Data Loss Prevention (DLP) solution to monitor and control attempts to send internal data to an external source. This would prevent employees from sending data to any entities that are not approved.

It is becoming unavoidable to utilize cloud services in today’s digital landscape, and the complexities of implementing cloud infrastructure with on-premises infrastructure can be

overwhelming. Caution is urged at every step of the cloud migration process. Security best practices should be followed at every stage, especially regarding identity management and access control.

Web Vulnerabilities

Building a public website for your business is one of the classic appeals of the Internet. A well-designed website enables an organization to inform the public about its mission and sell products and services. Web development has significantly evolved over the past decade and has expanded its reach with simple-to-use drag-and-drop Content Management Systems, such as Wix, Squarespace, and WordPress. Building a website is no longer reserved for those with knowledge of web frameworks and markup languages. Anybody can do it now.

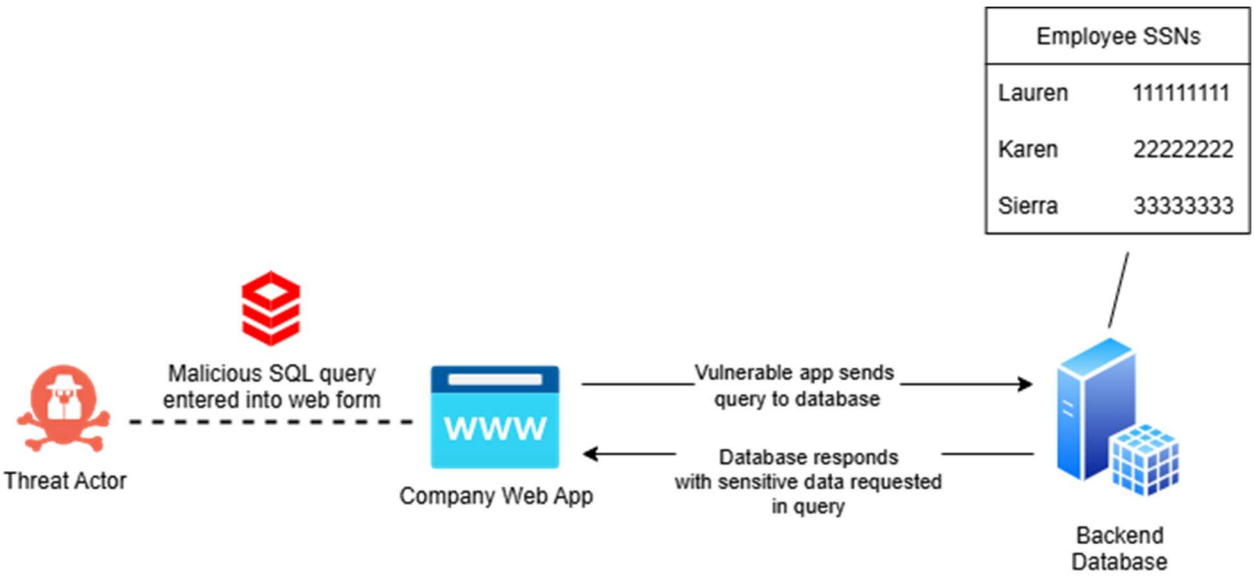
When building a website, organizations should follow the same precautions as other cloud platforms. Strong passwords and multifactor authentication should be enabled for webmaster accounts. Plugins for web backends should be updated regularly. WordPress plugins have historically been known for their vulnerabilities. The image of a compromised and defaced website likely evokes a shudder among business owners, as such a public display of compromise can do serious damage to public relations. Websites are a well-known target for Internet hacktivists, a category of threat actor that seeks to push a political or social message in public displays. While a small business may logically not be as large of a target for hacktivists as a multinational oil corporation, it is important to be wary.

The expanding surface of cloud computing has also led to greater use of the Internet for hosting infrastructure via web applications. One is likely to find company web portals connected to databases hosting customer data and scheduling programs, as well e-commerce websites

transmitting financial data between a customer's browser and an organization's database. Web application vulnerabilities have risen to become a major focus in cybersecurity over the last decade and have shifted the attention of threat actors towards exploiting them instead of on-premises infrastructure.

During the development of this capstone, a major security crisis occurred involving web application compromise of the new app known as "Tea". This dating app created an environment for female users to have discussions about various men in the dating scene. The app quickly shot to number 1 on the Apple App Store, but almost immediately, security vulnerabilities were uncovered, and a data breach occurred. It has been reported that users from the website 4Chan exploited an Insecure Direct Object Reference (IDOR) vulnerability to access a simple, unencrypted database containing information on the app's registrants (Yu and Kindelan). The uncovered data included user's profile photos, Real ID/Driver's License information, and media data from user posts (Collier and Yang). This incident proves that any web-based application that gains traction is going to have threat actors crawling all over it waiting to pounce on vulnerabilities.

The Open Web Application Security Project is a well-known standard in cybersecurity that regularly updates and lists a List of "Top Ten" vulnerabilities in web applications. As of 2025, the top vulnerabilities are as follows: Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable & Outdated Components, Identification & Authentication Failures, Software & Data Integrity Failures, Security Logging & Monitoring Failures, and Server-Side Request Forgery (OWASP).



An organization developing in-house web applications should embrace a security-focused development process that aims to mitigate the Top 10 vulnerabilities at every stage of development. An organization outsourcing web application development to a third party should include security measures in the Service Level Agreement (SLA) with the third party. The term DevSecOps has emerged as the software development approach that incorporates security considerations at every stage of development. Major security flaws found in applications can trickle down to the core design, often resulting in the application needing to be scrapped and rebuilt from scratch. By employing DevSecOps, security can be kept at the bottom line, thus lessening the chances for major issues in the future.

The smallest of organizations often decide to use social media accounts like Facebook, Instagram, and TikTok for their public engagement rather than websites. This is a sensible decision for most, as small businesses usually want to keep most of their engagement in the local community and don't see the return on investment for purchasing web hosting. Business owners

need to be aware that security best practices apply to social media, too. They are placing their trust in a large corporation that may or may not have the privacy of their data as a top priority. Separation of duties managing social media accounts should be implemented, and all employees with an account should use strong passwords and multifactor authentication.

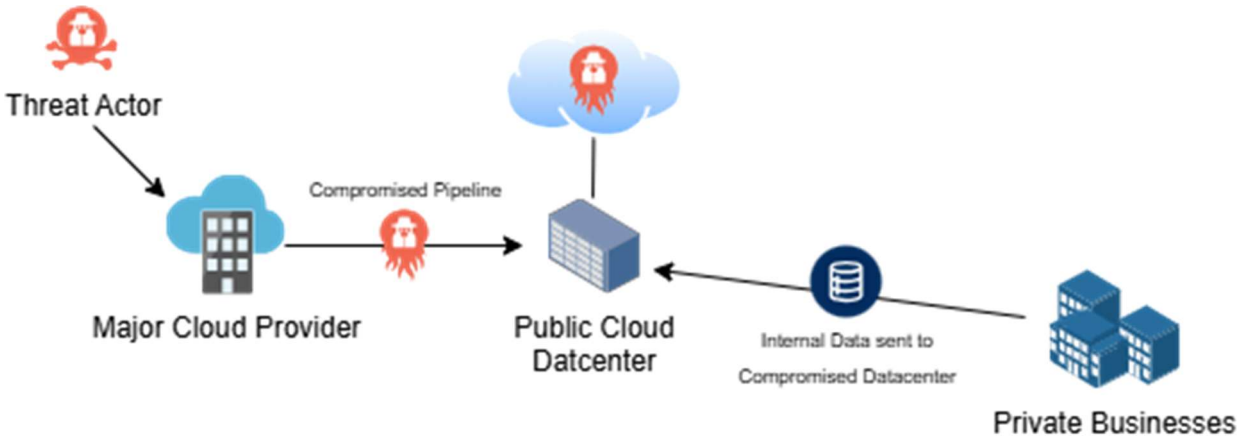
Supply Chain Attacks

The shift towards digitalization of the economy has highlighted the need for basic security standards across all industries. While one sector of the economy may have the best security practices enabled, it means very little if the data they receive from another member of the supply chain has already had its confidentiality or integrity violated. This issue becomes more apparent when dealing with global supply chains consisting of nation-states that may have varying security governance practices in place.

At first glance, your average small business owner may shrug this issue off, as they do not feel that they are a major member of any mainstream supply chain. However, I must continue to emphasize that threat actors do not discriminate based on size. Any person and any organization can access and use digital resources regardless of size or stature. The 2024 PowerSchool breach perfectly illustrates this, as the breach impacted even some of the small rural school departments in my home state of Maine.

Supply chain risks in cybersecurity are an issue that ties in very closely with the expansion of web applications and cloud computing. A classic perimeter-bound network with on-premises systems is more immune to supply chain attacks since most digital resources exist in a single location, with most of the control belonging to the in-house network administrators. In today's landscape, organizations are forced to embrace a "shared responsibility" model between

themselves and service providers, whether it be for Software as a Service, Platform as a Service, or Infrastructure as a Service products. The shared responsibility model is an agreement that trust will be placed in the provider for a certain level of security, and the rest will be handled by the customer.



Even in organizations using only desktop programs, trust is still being given to vendors. Unpackaging and deploying a .msi file across an organization is often done with the assumption of full integrity of the program. There is always the possibility that the software was modified at some point in the supply chain and that a malicious or corrupt program is now being spread. A good precaution against this risk is to verify the hash of software before deployment. Many software vendors, especially on the open-source side, provide a hash value with the program installation file. The integrity of the program can be verified by generating a hash value on the user's end and comparing it with the value provided by the vendor. Even the smallest change in the program's integrity will result in a completely different hash value.

The cybersecurity risks regarding supply chains are still evolving, and we have yet to see the true capabilities of supply chain threats. Data privacy and security governance are still lacking in many corners of the world, further fueling uncertainties regarding integrity and

privacy. This can leave business owners feeling helpless, as they no longer have control over the root causes fueling cybersecurity incidents. Following best practices can help reduce the chances of compromise via third parties. Keeping a proper asset inventory of software versions and hash values ensures no unapproved software is used. When involving third parties with an internal network, make sure to incorporate security requirements in Service Level Agreements. Perhaps the most useful precaution is keeping up with threat intelligence to catch supply chain issues early and incorporate necessary compensating controls.

Chapter 4: Considerations for a New Framework

Key Objectives

Through the previous real-world incidents, I have presented and the breakdown of their mistakes, I have highlighted that there is a real need for some comprehensive cybersecurity framework for small to medium-sized businesses and organizations to follow. It is evident that federal cybersecurity advice is not reliable for long-term protection, and a lot of it goes over the heads of entrepreneurs opening businesses with just two to a hundred employees.

Using the data and insights gathered from the previous chapters, I am going to apply them towards developing an accessible and easy-to-understand cybersecurity framework for the most vulnerable members of our economy to follow. From local health clinics to mom-and-pop stores to local churches, this framework will narrow down requirements and present recommendations and playbooks for keeping security at the forefront.

NIST SP 800-215 states, “Any enterprise-wide secure network that consists of on-premises and cloud-hosted applications should be based on an established security framework”. (Chandramouli, 14). The document further outlines five network configuration areas that make up basic security functions. Those are: Device Management, User Authentication, Device Authentication and Health Monitoring, Authorizing Applications/Service Access, and Preventing Attack Escalation. Indeed, these areas make up the basic threat surface of any organization that processes, stores, and analyzes data. This framework aims to highlight the most accessible technologies and methods for security in each of those listed areas. Measures will also be highlighted regarding data security and physical security best practices.

The changing digital landscape, much of which has been brought on by the pandemic, has

resulted in necessary recalibrations on where major security measures should be focused. Organizations now operate in a world where assets are decentralized and don't operate behind one set perimeter. Cloud computing and microservices have led to major changes in enterprise security architecture. Out of this have risen two new strategies to keep up with the current state of cyberthreats: Zero-Trust Architecture (ZTA) and Defense In Depth (DiD).

The insights I gathered while writing Chapter 2 of this capstone left me with the conclusion that small organizations have taken advantage of the new cloud centric technologies for efficiency and results, meaning that your average small business has no clear network perimeter. Developing a framework focusing on securing a basic LAN with ingress and egress traffic would only be addressing a fraction of the problem. Therefore, I want to develop this framework with heavy regard for decentralized assets, as well as the core tenets of Zero Trust Architecture and Defense In Depth.

It is important to remember that the first and foremost goal of this capstone project is to build a framework that is as accessible as possible. The guidelines and solutions I present will be directed at a target audience of average entrepreneurs who are not well-versed in the ins and outs of cybersecurity. This task will involve compressing the amount of technical jargon used and explaining concepts in a way that is easily understandable to those outside of the tech industry. The final web application hosting this framework will include links, guidelines, and even automation tools to do as much legwork as possible for those who want to implement this framework. It is important to remember that my goal is not to teach business owners cybersecurity from the ground up, but to provide coverage to as many users as possible before it is too late.

Zero Trust

NIST SP 800-215 identifies over 75% of network traffic as belonging to either an east to west or server to server traffic flow. This means that the majority of network communication no longer occurs between large network segments guarded by perimeter security devices. Instead, traffic now occurs between servers and nodes within networks themselves, and between microservices hosted at various locations across various networks.

The use of microservice computing has transformed and enhanced many aspects of enterprises. However, these transformations have made security a more difficult task. With the average business technology landscape now heavily decentralized, security precautions need to be moved to applications, sessions, and identities themselves. To move towards such implementations is to chase a “Zero-Trust Model”.

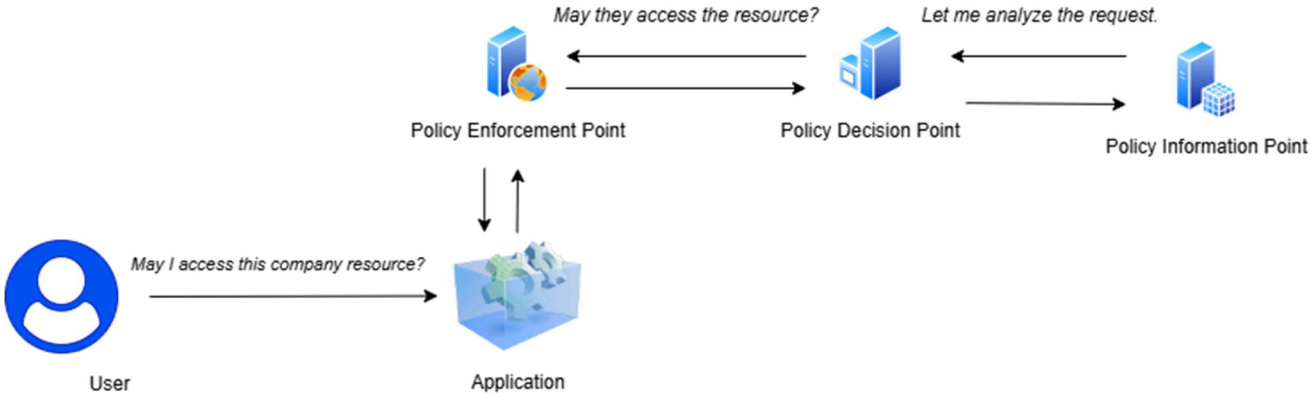
Zero trust is not a specific, one and down infrastructure implementation, rather it is a goal that needs to be continuously improved upon. NIST SP 800-207 defines zero trust as following a premise that “trust is never granted implicitly but must be continually evaluated”. The generally accepted tagline of Zero-Trust Architecture is “never trust, always verify”. In a zero-trust environment, anything that produces, distributes, or stores data needs to be considered a resource. Regardless of where the resource sits, whether on a company LAN or on a cloud platform, security measures need to be implemented to continuously evaluate and validate the resource.

In zero trust, security controls placed in front of resources make decisions to grant or deny access on a per-session basis. This is a reversal of the traditional perimeter-based security model where resources were validated once at the perimeter, then allowed permanent access to

other resources behind the perimeter as long as they passed validation checks. Resources now need to be continuously validated throughout a session to ensure their integrity has not been compromised while the session takes place.

As opposed to the standard username and password combo, Zero Trust utilizes more granular policies to make decisions on a resource's validity. Behavioral and environmental attributes are factored into the decision-making process. This could include analysis of the requested asset location, and the time-of-day access is requested. Analysis of the state of each asset is also factored in, including review of software versions, anti-malware status, and host firewall status.

The process of granting or denying access in a Zero Trust environment involves communication between various components, namely a Policy Decision Point (PDP), Policy Information Point (PIP), and Policy Enforcement Point (PEP). These components are not necessarily physical devices like firewalls and routers, but logical components. They could be combined into a single piece of infrastructure or exist as separated processes with the ability to communicate. Each component essentially serves as a "checkpoint" in the validation process. The PDP takes contextual information from the PIP to help make its decision to grant or deny access, then passes its decision to the PEP which hands down the decision, then monitors allowed assets throughout their session. The PEP can terminate the session between the asset and resource if needed, and then have the PDP re-evaluate the asset's validity.



What exactly will a Zero Trust environment look like in this framework, which is geared towards organizations at the lower and less complex end of technology? As I've stated, Zero Trust is not a device or service purchased and installed within a network. It is a series of configurations and improvements that are hardened regularly, with the ultimate goal of ensuring "never trust, always verify". Since the target base of this new framework will be organizations with not much technical training or capital to spend on upgrades, I want to avoid recommending expensive and complex zero-trust solutions. Instead, the framework will make use of security enhancements built into everyday technology platforms. These enhancements are often not enabled for convenience's sake but implementing them will provide an extra level of security that could be considered "in the spirit of a zero-trust architecture".

Administrator accounts on Windows devices are given free rein to install applications and modify settings simply because they are inherently trusted as the administrator. To add a level of Zero Trust, we could require elevation on the desktop for every single account, administrator or not, and require them to provide credentials each time they invoke privileged access. The administrators are still acknowledged as the device admins, but they are required to prove it regularly because after all, "never trust, always verify".

Small security fixes like this bring a level of zero trust into even the smallest business environments. While working within these restrictions may take some getting used to, they are essential to keeping up with the growing trend of zero trust architecture.

Defense in Depth

Another modern concept that will have a heavy influence on this framework will be Defense in Depth. Like Zero Trust, Defense in Depth emphasizes a move away from inherently trusting anything inside an organization's network perimeter. Instead, it acknowledges the vulnerability of all digital assets and seeks to apply multiple layers of security to them. Controls applied to digital assets can be a range of physical, technical, and administrative controls.

Defense in Depth also emphasizes integrating people and operations capabilities into security processes, according to the National Institute of Standards and Technology (NIST, 2024). Creating this safety net of security controls allows an organization to have a level of fallback if one security control is compromised. For example, an organization could implement an email spam filter, DKIM & SPF, and heavy user security training. If a phishing email is sent to the organization, even if it manages to bypass the spam filtering and DKIM/SPF, the user training will allow the recipient to properly identify the email as a phishing attempt and quarantine it.

This framework will try to implement multiple security controls in each area to satisfy Defense in Depth.

Artificial Intelligence

Artificial Intelligence has grown in the mainstream since 2023 and continues to show promise with new developments each year. In the world of cybersecurity, AI is a double-edged

sword. With the increasing sophistication of LLMs, attackers can craft better written, more convincing phishing messages. As access to AI continues to grow, you can expect to see a decline in the obvious grammatical and spelling errors present in hastily written phishing emails.

Threat actors can also use AI tools to seamlessly provide them with scripts and programs to use in various phases of the cyber kill chain. The time needed to prepare for an attack is significantly cut down since writing and testing programs are no longer necessary. The correctness of these AI produced tools will always be up in the air, but overtime results are going to get more and more reliable.

But while AI may assist threat actors, it can just as effectively assist cyberdefense teams. AI has shown promise in being able to effectively identify phishing attempts in emails, even picking up on nuances that may go over the heads of human users. The input of AI tools shouldn't always be trusted, however. I tested ChatGPT and Microsoft Copilot against a series of phishing emails I received in my University of Maine mailbox and had mixed results. Some emails were correctly identified as malicious, and the tools elaborated on their decision. However, there were a few emails that were obviously malicious, and the tools flagged them as safe with murky reasoning for their decisions.

The potential of AI in cybersecurity remains to grow and progress, but for the time being it can serve as a useful tool in the workplace. As noted in the U.S. Chamber of Commerce report on the use of Technology in Small Business, small business owners have already began utilizing the benefits of AI to increase productivity and efficiency. Therefore, this framework will implement AI when possible, to keep consistent with current trends.

Technical Jargon

One of the key issues in cybersecurity that I wanted to remedy in this project is the inaccessibility of many frameworks when it comes to technical knowledge. The majority of mainstream cybersecurity frameworks are written in a way that is clearly targeted at established information security professionals working in a dedicated IT department, either on-premises or outsourced.

The key demographic of this framework is the small businesses which only have a few employees and are unlikely to have any sort of dedicated IT department. All of the tasks outlined in this framework can be done by the business owners and management themselves, no professional IT staff required. This means that this framework needs to be as light on the technical jargon as possible.

There is no escape from using the appropriate terms, as it is a cybersecurity framework. Concepts need to be explained properly. But rather than simply bringing up concepts and expecting the audience to have prior knowledge, I will present technical concepts with definitions and analogies surrounding them. This will help the framework audience maintain at least a basic understanding of certain technologies and terms.

Software Accessibility

One of the most common reasons cited by business owners as to why they don't invest in cybersecurity measures is the price tag associated with much of the technology. High end routers and firewalls, antivirus programs, intrusion detection and prevention systems, and identity and access management solutions can simply be non-feasible for your average small business. This is a shame, as it ends up blocking entire sectors of the economy from getting the help they need.

For this framework I want to recommend as much open-source software as possible. While high end market tools still remain an end goal, most small businesses need to have immediate options for specific tasks. By recommending open-source tools, I aim to present pragmatic solutions for tiding up security misconfigurations quickly. As long as they meet the standards for security, the organization leadership can utilize the open-source tools for as long as they like. The ultimate hope will be that they can financially prepare for implementing proprietary tools further down the road.

Relevant Technology

It is important to remember that the target audience of this framework is the owners of small businesses and community organizations. This project was specifically inspired by my experiences with cybersecurity in small businesses in rural Maine. This framework is not strictly limited to that region, however. The recommendations and guidelines provided have universal application in any small business across the world. Whether a business is operating out of a storefront, or fully online as a side hustle, the same cybersecurity best practices apply.

Building a framework targeted at small businesses also requires consideration of what technologies are typically used in those environments. Many cybersecurity frameworks are targeted towards larger enterprises with employees numbering in the thousands. These organizations are going to have vastly different infrastructure in place than your local mom and pop store.

Small businesses typically have some basic network setup, usually comprising of a SOHO router with Wi-Fi networks enabled. Employees typically use personal computers in their workflows but lack any kind of centralized identity and device management. More and more

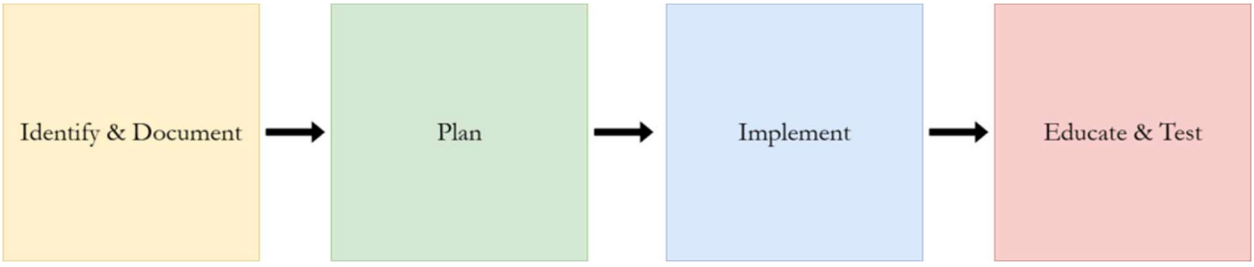
small business workflows are taking place entirely online and within cloud platforms. Google productivity tools, QuickBooks online, social media pages, and an email client may be the only software used. In a business with just one or two employees, a web browser and some printer drivers may be the only desktop software required.

I have made careful note of these nuances throughout the development of this capstone. I have carefully tailored security controls towards the technologies that are more likely to be found in small business environments. It would be pointless to focus an entire document on securing large Oracle databases, since these are realistically not going to be found in a small local business. On the other hand, social media pages and cloud storage platforms are likely to be found in these environments. I have eliminated unnecessary technologies from the framework and focused on the ones that matter to most small businesses. This will keep the scope of the project on track and eliminate information that will end up having no real application to the framework's core audience.

Chapter 5: Unveiling the Framework

Structure

To align with my objective of keeping the framework straightforward and easy to follow, I narrowed it down to four stages. The four stages are “Identify & Document”, “Plan”, “Implement”, and “Educate & Test”. The stages represent specific long-term goals for building a solid cybersecurity program within a small business. Underneath each stage is a series of documents and tutorials for accomplishing various tasks related to the particular stage.



Stage 1: Identify & Document directs business leadership to identify the technology surface of their organization. Systems, software, and identities are established as the major assets of the organization. The framework documentation directs the organization to create an inventory of these assets. By doing this, the organization will have data to consult when deciding what strategies and technologies need to be implemented. This data will then be further enriched by a Risks Assessment and a Gap Analysis, also to be performed in this stage.

The first stage also facilitates the creation of an internal cybersecurity team. This team can be arranged at the business leadership’s discretion. However, a mix of perspectives is recommended for the best insights. Management, financial advisors, Subject Matter Experts (SMEs), and some lower-end staff are highlighted as the cornerstone individuals to include in the

team. This team will be responsible for regularly discussing the state of organizational cybersecurity and planning any new implementations.

Stage 2: Plan is where the business leadership and the cybersecurity team prepare individual controls and technologies to be implemented into the workplace. Heavy emphasis is placed on drafting cybersecurity policies, a vital piece of governance that is often missing in small businesses.

Guidelines to writing an Acceptable Use Policy, Disaster Recovery Plan, Password Policy, BYOD Policy, and Remote Access Policy are included in this stage. Stage 2 also directs business leadership to plan for new technology platforms being brought into their organization for backend infrastructure. This includes assessing options for identity and access management platforms and cloud-based infrastructure. The framework makes no mandates on implementing specific infrastructure, but it does encourage readers to weigh the pros and cons of implementing certain solutions in their organization.

Further tasks under Stage 2 include defining backup solutions and specifying conditions for creating maintenance windows. All tasks under Stage 2 are aimed at creating a holistic understanding of the cybersecurity program throughout the organization. By directing business leadership to preconfigure policies and share infrastructure changes ahead of time, the framework helps organizations avoid some of the chaos and confusion that can erupt from implementing sudden technological changes.

Stage 3: Implement is the meat of the framework and the stage that contains the most documentation. This is the stage where all the planned changes to the organization's cybersecurity infrastructure are configured. Recommendations and tutorials are provided for

hardening everything from Windows workstations to Point of Sale Devices to Zoom Meetings. The framework makes no assumption on what devices an organization is using, so I tried to cover as many different possible pieces of technology as possible. The different controls and configurations in this stage vary in difficulty and expense. Some configurations involve some form of a financial transaction, such as subscriptions for password managers and the purchase of physical security devices. Other controls are simple fixes that are built right into common hardware. The documentation on Router and Wi-Fi Hardening directs users to take advantage of advanced security settings already present in most consumer grade routers. The hope for this stage of the framework is that businesses can start small by embracing configurations that already apply to their existing infrastructure. From there they can expand their knowledge of cybersecurity equipment and possibly start looking into new and advanced devices or tools.

Stage 4: Educate & Test is the final stage and is less extensive in its documentation. This is because educating the workforce and testing controls is a repetitive process that involves repeating the steps over and over again and using trial and error. This stage consists of less tutorials and more ideas for the end users to better implement cybersecurity preparations into the workplace. There are demonstrations on how AI tools can be used to enhance analysis of suspicious behavior, as well as ideas for tabletop exercises and simulations to keep staff prepared for a cyberattack.

While the framework is arranged sequentially by stages, it is not meant to be a checklist where all the tasks in each stage are completed and never returned to. Cybersecurity requires constant supervision and improvement. Some tasks in one stage may require a return to a previous stage to consult a specific document or policy made there. Business leadership may get to the Implement stage and decide they need to return to the Plan stage to better organize

deployment of a specific technology. The framework expects regular re-iterations overtime, as the digital landscape changes and new threats and defenses emerge.

Presentation

I thought long and hard about how I wanted to go about presenting this framework. I toyed with the idea of presenting it in book form, with each framework stage broken down into individual chapters. However, I decided that a visual medium would be more accessible to the target audience. Somebody looking for a quick tip on hardening their Windows 11 machine is going to instantly disregard an answer if it requires sifting through a ton of pages.

I decided on a website for the presentation medium. A website would allow me to post all the documentation I created while still providing an easy to navigate interface. I believe this takes away some of the aversion one may have to a long, dense technical manual. Instead, end users can see the breakdown of each framework stage and quickly pick out the documents that best apply to their needs.

Building websites is a skill I have utilized on and off ever since I started working in IT. I taught myself HTML in 8th grade and learned how to build websites from the ground up. However, for most of my web-based projects, I have opted to use Content Management Systems to build websites instead. I decided on WordPress as the CMS for this capstone project. I have had great experiences with WordPress in the past and I am fond of the level of customization enabled through different plugins.

Web Backend

Opportunities exist to create websites on online Content Management Systems and have them hosted by the CMS itself. Wix, Squarespace, and even the .com version of WordPress are

examples of this service. However, I wanted more control over the website for this project and also wanted to utilize the new Cyber Range for the UMPI Department of Cybersecurity.

Throughout the spring and summer of 2025, the UMPI Department of Cybersecurity began construction on a virtualization lab for hosting large amounts of infrastructure for classroom instruction, testing, and student projects. Server configuration and security management has always been one of my specific interests in the world of IT, so I decided to spin up my own instance of WordPress on an Apache Web Server.

I created a basic virtual machine on the UMPI Cyber Range and configured it with 32GB of RAM and a 100GB hard drive. These specifications are ample for the basic needs of the website as they currently stand. I chose Ubuntu Server as the server operating system due to its reliability, large amount of user support, and ease of configuration and management.

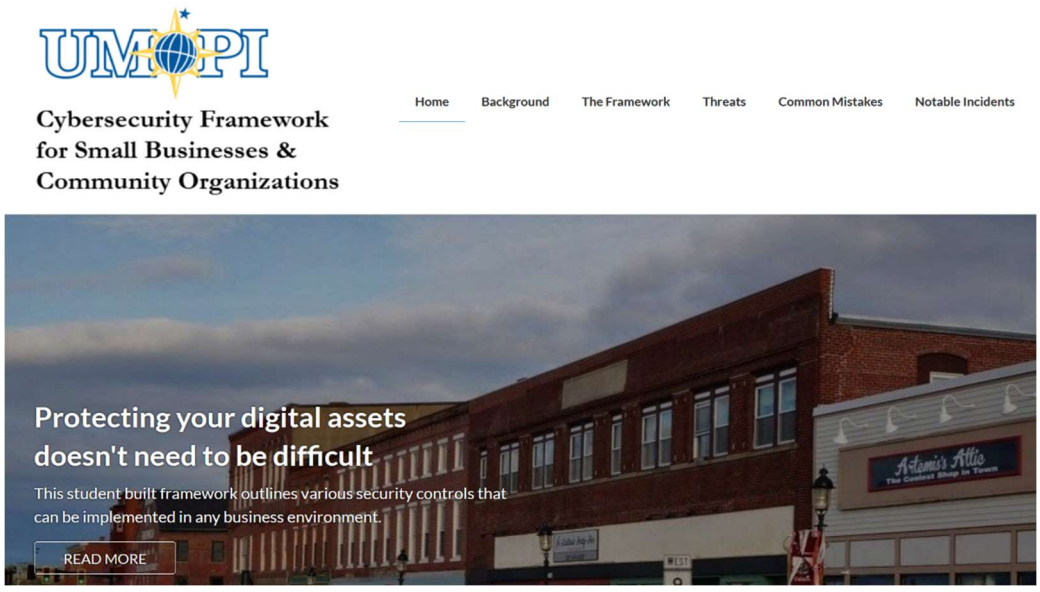
After Ubuntu Server finished installing, I immediately installed and configured the Apache Web Server and the WordPress CMS. Once I finished configuring the WordPress website management dashboard, I logged in and immediately began construction on the framework

website. I spent a decent amount of time comparing different WordPress themes, before ultimately deciding on the Lightning theme by Vektor, Inc. Within a few days, I had the basic shell of my capstone website built.

Before delving too deep into the development of the actual website, I took the time to apply some security controls to the Ubuntu/Apache web server. These controls included hiding exposed server information, creating cron jobs to automatically update the server, and restricting access to web directories. I also configured snapshots of the Ubuntu virtual machine and setup my WordPress CMS to automatically backup to my University of Maine Google Drive.

Homepage

For the framework, I wanted a clean page that would appear instantly welcoming to users who may be looking for basic cybersecurity help. In keeping with the theme of this being an UMPI project, I titled the website "UMPI Cybersecurity Framework for Small Businesses and Community Organizations". This allows the project to continue its associate with the UMPI Cybersecurity Program.



Below the main navigation bar, I included a banner with text reiterating the mission statement of the project: “Protecting your digital assets doesn’t need to be difficult”. I made sure to emphasize that this framework is a good fit for any business owner with minimal capital and technical expertise.

After the banner, I implemented some of the most interesting statistics I found while doing research for the project. These are displayed through colorful shapes to catch the viewer’s eye. The goal of displaying these statistics is to inform the viewer about the dangers of leaving their organization unsecured and encourage them to explore the framework further.

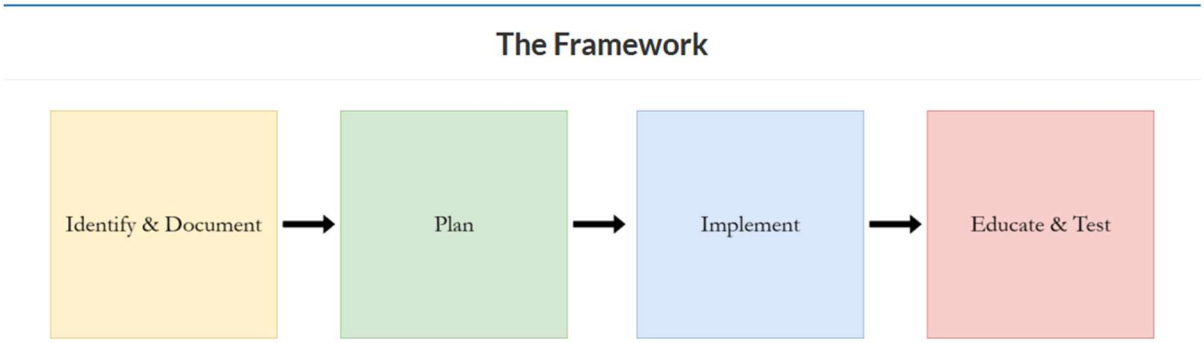
The next section provides further pretext by emphasizing the correlation between increased digital transformation of business and the increase in cybercrime. The write up shows sympathy for the issues facing small business owners regarding their cybersecurity posture. It closes by further emphasizing the usefulness this framework may have for individuals in their position.

Digital transformation of the economy and the increase in cyber threats go hand in hand

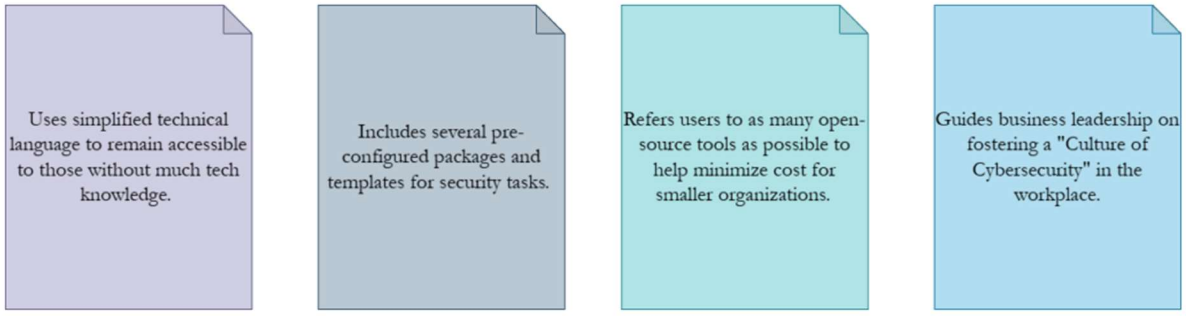
Organizations of all sizes are embracing technologies like cloud computing, artificial intelligence, and the Internet of Things to improve their productivity and efficiency. However, not everybody knows how to implement security controls for their information technology, and many remain in the dark about the risks presented by much of their technology. Not only this, but taking the initiative to implement cybersecurity measures can be daunting and confusing to many business owners.

This framework was built to provide easy to learn, yet comprehensive guidance on cybersecurity measures for small business owners who are concerned about the safety of their assets and reputation.

The framework is presented in the next section. The visuals for the stages are displayed with arrows to symbolize the progression of the process. The framework appears straightforward, with no technical jargon in the stage names. They only contain simple words that clearly define what topics each stage covers.



Immediately following the framework, I provided some illustrations giving the reader key points regarding the benefits of using this framework. Again, they highlight the ease of use, consideration for technical inexperience, and referral to as many free tools as possible.



While this framework aims to be as user friendly as possible, it also seeks to educate its users further about cybersecurity concepts that are essential knowledge in today's digital landscape. I used draw.io to create small illustrations of the concepts combined with small, basic descriptions of what they are. The cybersecurity concepts I highlighted are: The CIA Triad, Zero Trust, Defense In Depth, the Cyber Kill Chain, and the Pyramid of Pain. These five concepts are the ones I feel have the most relevance in understanding the current state of cybersecurity in a business context. Every control and guideline provided in the framework has an end goal that falls under one or more of these concepts.

The key concepts section closes off the homepage for the website. I added a basic footer containing basic information about the ownership of the website. I also added links for viewers to further explore UMPI and its Cybersecurity program. When I completed the framework, I understood that many users are going to want more as they improve their cybersecurity program and expand their knowledge. I decided it was a professional gesture to include links to the standard industry frameworks like NIST and MITRE. This provides users with the option of pivoting to larger frameworks for assistance with concepts not included in the scope of my framework.

Supporting Pages

While creating my layout for the website, I decided that I wanted to include more content than just the framework and its associated documents. I felt that I needed to include more information to help viewers get a better grasp on cybersecurity and its application in modern small businesses. I decided to break down some of the sections included in this capstone paper and implement them on the website.

I started by including a page entitled *Threats* which is dedicated to explaining some of the common cyber threats encountered by businesses today. Many people are not familiar with the nuances of different types of threats and their characteristics and only know them by terms like "virus" and "hacking". The Threats page provides descriptions and illustrations of some of the relevant threats I took note of while investigating cyberattacks on businesses. Included among these are phishing, ransomware, and password attacks.

The second supporting page I added was *Common Mistakes* to mirror the chapter of this paper dedicated to breaking down vulnerabilities and misconfiguration prevalent in small business networks. I kept the mistakes listed on the website short and too the point so that viewers can quickly identify security mistakes and assess whether or not they are prevalent in their network. The write-ups for the mistakes also include a short recommendation on how the mistake can be fixed so the viewer can get a general idea of where to look into the framework body.

The final page I included for pretext was *Notable Incidents*. This page is a brief collection of data breaches, ransomware attacks, and other cybersecurity incidents against small businesses that I found interesting. They were compiled during my research for this project, and some of

them made it into this paper as references. For the website, I kept descriptions of the incidents short and sweet. I made sure to emphasize that each incident was enabled by a security configuration that would be addressed in the framework.

Stage 1: Identify & Document

We are now moving into the structure of the framework itself. Each stage of the framework has its own dedicated page where the recommendations and guidelines are nested under the stage title. Stage 1: Identify & Document provides a checklist of inquiries and data collections a business owner must make in their network environment before chasing security controls. The goal is to gather as much information as possible on the current state of the cybersecurity posture.

One of my goals in creating this framework was emphasizing the point that good cybersecurity is a team effort. Therefore, I came right out of the gate with a guide on creating a cybersecurity team within an organization. Knowing that the target audience is small businesses with low number of employees, I made the guideline flexible. It focuses on instructing the business owner to gather a diverse team of individuals that will have different perspectives on the state of workplace cybersecurity. Financial advisors, Subject Matter Experts, and employees who utilize company devices are all mentioned as good candidates for membership in a cybersecurity team.

After the business owner assembles a team to advise developments in workplace cybersecurity, they are provided with detailed guidelines on inventorying digital assets in the workplace as they currently stand. In particular, the framework provides guides for creating hardware and software asset inventories, network topology maps, physical security site surveys,

data classifications, identity inventories, and third-party access inventories. In keeping with the goal of simplifying as much of the work as possible, the framework provides users with basic templates for creating these documents.

Stage 1 closes out by directing users to use the collected data to create a risk assessment and a gap analysis. Risk assessments are a core part of cybersecurity, as they essentially dictate the direction a cybersecurity program will take. Business owners are instructed to weed out the top threats to their business and use their personal knowledge of their finances to determine which weaknesses would cause the greatest damage to the business if exploited. This ends up creating a roadmap that ranks necessary cybersecurity fixes by urgency.

The gap analysis plays off the risk assessment by using the same data to determine how far the business needs to reach to achieve a certain standard of security. I created a checklist of general cybersecurity end goals that business owners can compare to their current state. The list is not an exhaustive benchmark of cybersecurity controls, but it does provide the business owner with some sort of land to swim towards moving forward.

Stage 2: Plan

Once the business leadership has a general idea of where their security posture stands, they can begin creating plans for implementing new controls and technologies. The first essential task highlighted by the framework is defining Maintenance Windows. Based on my experience as a work study in a campus IT department, one of the biggest ills in any organization is miscommunication between IT and other departments. Employees come into work everyday expecting the business technology to work. Any sort of downtime or intrusion by IT, no matter how critical, creates an environment of irritability and even panic. Therefore, the framework

provides a general guide on how to schedule non-intrusive maintenance windows and clearly communicate them to the workplace.

The bulk of Stage 2 is focused on drafting cybersecurity policies for the workplace. A lot of the difficulties regarding workplace cybersecurity can be mitigated by having clearly defined policies in place ahead of time. Employees have no real guidance on what should and should not be done with technology if it isn't in writing from the very beginning. To avoid these confusions, the framework directs the creation of Acceptable Use, Disaster Recovery/Business Continuity, Password, Bring Your Own Device, Remote Access, and Master Data Handling policies.

Additional sections of Stage 2 are dedicated to considering certain technologies that may improve the overall security of the business. Active Directory and cloud Identity & Access Management are recommended as options for creating a centralized plane of identities and devices, as well as having a way to easily push out security policies. Linux and various cloud Infrastructure as a Service platforms are recommended for more secure hosting of any required servers. The framework also provides a guideline for defining clear data disposal and destruction methods to protect sensitive company information, as well as a list of well-known hotlines and sources for aid in the event of a severe cyber incident.

Stage 3: Implement

Stage 3 is the real bulk of the framework and is realistically where most users are going to find the most help. Stage 3 contains a list of controls, configurations, and concepts to improve overall cybersecurity posture. Documentation for Stage 3 varies in detail. Some of the more complex topics contain walkthroughs for implementing a control or concept. On the other hand, smaller topics like Secure Boot and Job Rotation receive short descriptions with a general idea

on where to look for tutorials. This provides a balance between keeping the framework vendor agnostic and also providing detailed help with certain technologies.

One of the key features of Stage 3 is the inclusion of an exported Local Group Policy for Windows hosts. Windows has the operating system market dominated and is the OS most likely to be found in any given organization. Exploits for Windows are a dime a dozen, and as a result, security recommendations for locking down Windows can get quite granular. Many business owners are unaware of the workings of Group Policy. On top of that, few individuals want to take the time to set hundreds of individual security settings in the Group Policy console. Using the Center For Internet Security Windows 11 Benchmark and the Microsoft Security Compliance Toolkit as references, I configured recommended security settings on a Windows 11 Local Group Policy and then exported them using the LGPO utility. The exported Local Group Policy is available for download within Stage 3, along with instructions on how to import it into another Windows machine. This provides users with the opportunity to provision their Windows hosts with industry standard security settings with only a minimal amount of work.

The Local Group Policy provided doesn't stop at the Windows operating system either. Group Policy allows you to import templates to configure granular security settings on a number of different software programs. The templates are downloaded in .ADMX format from the software vendor's website. The Group Policy I configured contains settings for Google Chrome, Mozilla Firefox, Microsoft Edge, and Microsoft Office desktop. Each one was configured with the industry benchmarked settings specified by the Center for Internet Security. Essentially, this downloadable LGPO allows small business owners to harden an entire Windows deployment with just a few commands in the terminal. Each specific program I configured has a PDF displayed in Stage 3 outlining exactly what settings are configured.

Stage 3 also includes several guidelines for hardening authentication. Building off the Password Policy specified in Stage 2, the framework recommends universal adaptation of Multifactor Authentication in the workplace. Readers are presented with some of the pros and cons of various authentication methods. A document on Passwordless Authentication is also provided, encouraging business owners to look towards the future when implementing technological changes.

I mentioned earlier that I wanted to keep the focus on small business needs as much as possible. This meant that some very specific, niche technologies were included in the framework. Stage 3 includes documentation on securing Point of Sale (POS) systems, online Content Management Systems and website builders, social media pages, and video conferencing tools. All of these technologies have a broad presence in small organizations, thus earning them inclusion in the framework.

Stage 3 encompasses a broad range of technologies and sub-categories of cybersecurity. Everything from applying cable locks to desktops to setting up password managers is discussed in this stage. I have no expectation that users of this framework will implement every control and technology mentioned in Stage 3 in one go. This stage is meant to be continuously re-assessed by both me and the end users. Different recommendations and technologies will come and go and be built upon as the tech industry continues to change.

Stage 4: Educate & Test

The task of improving cybersecurity posture is not a one and done deal. Even after the appropriate controls and configurations are implemented to get an organization closer to industry standards, testing needs to happen to ensure continuing functionality. Testing cybersecurity

controls can take various forms. The most thorough option is performing penetration tests. These are scans that attempt to exploit digital infrastructure to give the owners insight into the performance of security controls and ideas for improvements. This option is a tough one, since the target audience of this framework likely lacks the skills needed to perform such tests. In larger, more metropolitan areas, there may be third party firms that perform penetration tests as a service.

Basic testing of cybersecurity controls can be done with the use of simple scans and tools. Nmap is a tool mentioned multiple times in the framework. It performs detailed port scans of networks and outputs any open ports and services found during the scan. Using Nmap and other such open-source tools is a great way for business leadership to get a basic understanding of the effects of their security controls.

Implementing security controls is only half of the battle. Oftentimes, the deciding factor between exploitation and security is the people in an organization. Human errors and insider threats regularly make the news for their roles in serious cyberattacks. Stage 1 started the entire framework off by providing a blueprint for building a workplace cybersecurity team. Much of Stage 4 is dedicated to keeping the workplace up to date with cybersecurity strategies and objectives. The upside of small businesses in this regard is that it can be much easier to create a holistic understanding of cybersecurity since there are fewer employees.

Stage 4 recommends the integration of various sources of Threat Intelligence throughout the workplace. Keeping everyone well versed in the latest news about new cyber threats and events can facilitate sharing of intelligence by casual word of mouth. As a result, the workplace can become more cybersecurity aware. Some employees may even become interested in

proactively defending the organization against threats. Again, considering the target audience, the framework recommends basic sources of threat intelligence, such as popular cybersecurity news websites and social media pages. Options are provided for integrating more comprehensive threat intelligence, such as the open-source platform OpenCTI.

All of the guidelines provided in Stage 4 are centered around the objective of creating a "Culture of Cybersecurity". With regular attention and fine tuning, the cybersecurity program in a small business can become one smooth system, with all four stages of this framework blending together, regularly building off of and improving one another. Keeping digital assets safe should not be a burden that produces endless anxiety, but a collaborative effort that every employee contributes to.

Conclusion

Digital transformation is going to take the global economy to places never before imagined. The accessibility of new technologies to broad audiences helps grow its potential. With the rapid growth of technologies such as cloud computing and artificial intelligence, we can expect markets to become more automated with increased online presences. E-commerce and online shopping/ordering have exploded since the COVID-19 pandemic and has brought industries like hospitality to the digital sphere. If you told somebody just twenty years ago that they would be able to rent a room and order delivery from their phones two decades later, they probably would not believe you.

No matter how bright the future gets for digital entrepreneurship, there is always going to be one huge dark cloud looming overhead ready to downpour. Cyber threat actors are always ready to pounce, sinking their teeth into the hottest new online trend and extracting as much useful data as possible. Exciting new apps and online services are being released monthly but so are exploits targeting vulnerabilities in their infrastructure. It has become very apparent that cybercriminals are getting better, stealthier, and are growing in quantity to match the expansion of the Internet.

The people who end up feeling the most helpless in this new world are not the federal agency directors or the Fortune 500 CEOs, but the gas station owners and barbers. The engineering firms and restaurants. Community churches and museums. Small businesses and organizations are stuck in a grey area where nobody considers them high value enough to waste time on, yet at the same time they are vulnerable to the same types of attacks as any other organization. These small organizations are also processing and digitally storing larger amounts

of data thanks to the accessibility of new technology. Small businesses cannot continue to function in a world where they collect important data targeted by threat actors, and at the same time receive no mainstream support from major cybersecurity initiatives.

From the genesis of this capstone project, I had the small businesses and community organizations in my hometown in mind. The charm of having a populated local economy and being able to trust somebody you know to provide goods and services is invaluable. But tragically, this trust can feel uneasy with careful observations of common cybersecurity mistakes. The Wi-Fi signals broadcasting into busy open streets, the Windows 7 systems connected to the Internet and resting on the same network segment as the Point-of-Sale devices, the passwords written on yellow sticky notes in plain view of anybody who walks in. These mistakes are everywhere.

The mission of this project was to offer a free opportunity for small organizations to correct these mistakes. I know many people who run these small organizations, and I understand the roadblocks they face. Many of them don't understand cybersecurity and frankly do not care to. They know it's something they are supposed to care about, and subconsciously they are well aware of the devastation a cyberattack will bring. They just don't have any idea where to look for basic help.

I sought to give these business owners a way to improve their cybersecurity from the ground up, rather than immediately hitting them over the head with recommendations for ten new high end security appliances right off the bat. Many of the basic systems and devices present in small businesses have hardening features already available. Basic SOHO routers and the

Windows operating system have very granular, zero trust style controls built right in. They just need somebody to know enough to configure them.

This framework is not meant to be a static collection of documents with a bunch of technical jargon. It is meant to improve and adapt to new requirements and trends over time. As my IT experience and the experiences of the UMPI Cybersecurity program grow, new content will be added, allowing our local business owners to learn with us. Technology is going to take our world to strange places in the coming decades, and malicious actors will be ready to pounce at every opportunity. Regardless, small organizations will always have a place to go for help navigating the challenges of a changing digital world with this framework.

References

APT32, SeaLotus, OceanLotus, APT-C-00, Group G0050 | MITRE ATT&CK®. (2024, April 17). Attack.mitre.org. https://attack.mitre.org/groups/G0050/

Baker, E., & Cartier, M. (2024). Phishing Trends Report (Updated for 2024). Hoxhunt.com. https://hoxhunt.com/guide/phishing-trends-report

Berr, J. (2017, May 16). "WannaCry" ransomware attack losses could reach $4 billion. Cbsnews.com. virus-losses/

CERTEU. (2019, August 2). Massive breach at Capital One, purportedly due to a cloud misconfiguration (Threat Memo 1908021). CERTEU. Retrieved from https://cert.europa.eu/publications/threat-intelligence/threatmemo1908021/pdf

Chandramouli, R. (2022). Guide to Secure Enterprise Network Landscape. Guide to a Secure Enterprise Network Landscape, 800-215, 5–28. https://doi.org/10.6028/nist.sp.800-215

CLOUDFLARE. (2017). What was the WannaCry ransomware attack? Cloudflare.com.

Collier, Kevin, and Angela Yang. "Tea App Hacked: 13,000 Photos Leaked after 4chan Call to Action." NBC News, 25 July 2025, www.nbcnews.com/tech/social-media/tea-app hacked-13000-photos-leaked-4chan-call-action-rcna221139.

Cybersecurity Insiders. (2024). 2024 cloud security report (p. 14). In collaboration with Check Point Software Technologies Ltd. https://www.cybersecurity-insiders.com/

Fier, J. (2019, August 4). Lessons from the Capital One Breach on Cloud Security. Darktrace.com; Darktrace. https://www.darktrace.com/blog/back-to-square-one-the capital-one-breach-proved-we-must-rethink-cloud-security

Framework Security. (2024, October 2). The Target Breach: A Historic Cyberattack with Lasting Consequences - Oct 01, 2024. Frameworksec.com. https://www.frameworksec.com/post/the-target-breach-a-historic-cyberattack-with lasting-consequences

IBM. (2024). Cost of a data breach report 2024. IBM. https://www.ibm.com/reports/data-breach

IBM. (2025). IBM X-Force 2025 Threat Intelligence Index. IBM. leadership/institute-business value/report/2025-threat-intelligence-index

Johnson, R. (2019, January 2). 60 Percent of Small Companies Close Within 6 Months of Being Hacked. Cybercrime Magazine.

Kapko, Matt. "LastPass Breach Timeline: How a Monthslong Cyberattack Unraveled." Cybersecurity Dive, 2 Mar. 2023, www.cybersecuritydive.com/news/lastpass cyberattack-timeline/643958/.

Key Cyber Security Statistics for 2025. (2025, March 28). SentinelOne. statistics/#top cybersecurity-threats-figures

Lampariello, D. (2024, November 14). Rising cyber threats put water systems at risk; Maine utilities not immune but preparing. WGME. threats-put-water-systems-at-risk-maine utilities-not-immune-but-preparing

Lampariello, D. (2025, January 28). More than 33,000 Mainers affected by PowerSchool data breach, new filing shows. WGME. https://wgme.com/news/i-team/more-than-33000 mainers-affected-by-powerschool-data-breach-new-filing-shows-maine-school-districts powerschool-student-information-system-cyberattack

Microsoft. “Windows 11 System Requirements.” Support.microsoft.com, Aug. 2021, support.microsoft.com/en-us/windows/windows-11-system-requirements-86c11283 ea52-4782-9efd-7674389a7ba3.

MITRE. (2017, May 31). APT28. Attack.mitre.org. https://attack.mitre.org/groups/G0007/

Morgan, S. (2023, July 7). Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. Cybercrime Magazine. damage-costs-predicted-to-reach-250-billion-usd by-2031/

NIST. (2024). defense-in-depth - Glossary | CSRC. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/defense_in_depth

NIST. “NIST Special Publication 800-63B.” Pages.nist.gov, 28 Aug. 2024, pages.nist.gov/800 63-4/sp800-63b.html.

NSBA. (2025, June 12). NEWS | NSBA Highlights New Data on AI Adoption, Trends in Small Businesses. NSBA | since 1937. https://www.nsbaadvocate.org/post/news-nsba highlights-new-data-on-ai-adoption-trends-in-small-businesses

One, C. (2020). CYBERSECURITY GUIDE FOR SMALL BUSINESSES. Business.sparklight.com; Sparklight Business. https://business.sparklight.com/sites/default/files/documents/Cybersecurity_ebook_0.pdf

OWASP. “OWASP Top Ten.” Owasp.org, OWASP, 2021, owasp.org/www-project-top-ten/.

Pepitone, J. (2019, July 30). What we know about Paige Thompson, the alleged Capital One hacker. CNN. https://www.cnn.com/2019/07/30/business/paige-thompson-capital-one

PowerSchool Breach Affected 33,000 Maine Residents. (2025, January 29). GovTech. https://www.govtech.com/education/k-12/powerschool-breach-affected-33-000-maine residents

Presque Isle Police Department - Distributed Denial of Secrets. (2024). Ddosecrets.com.

QuickBooks. (2025, January 16). Download the Intuit QuickBooks Small Business Annual Report 2025. Intuit.com. https://quickbooks.intuit.com/r/small-business-data/index annual-report-2025-download/

Reed, R. (2025, January 28). More than 33,000 Maine residents affected by PowerSchool data breach, filing states. WMTW. https://www.wmtw.com/article/powerschool-data-breach maine-residents-affected/63590250

Rosenbaum, E. (2021, August 10). Main Street overconfidence: America's small businesses aren't worried about hacking. CNBC. overconfidence-small-businesses-don't worry-about-hacking.html

Small Business, U. (2024). The Impact of Technology on. https://www.uschamber.com/assets/documents/Report-The-Impact-of-Tech-on-US-Small Business.pdf

Sobers, R. (2023, September 6). 86 Ransomware Statistics, Data, Trends, and Facts [updated 2022]. Www.varonis.com. https://www.varonis.com/blog/ransomware-statistics

StatCounter. (2025). Desktop Operating System Market Share Worldwide | StatCounter Global Stats. StatCounter Global Stats. share/desktop/worldwide

Steinberg, S., Stepan, A., & Neary, K. (2021). Target cyber attack: A Columbia University case study (SIPA-21-0021.1, pp. 2–3). Columbia University, School of International and Public Affairs. The Trustees of Columbia University in the City of New York.

Tomaselli, K. P. (2021, April 27). Hackers threaten to dump Presque Isle police files on dark web. Bangor Daily News. https://www.bangordailynews.com/2021/04/27/aroostook/presque-isle-police-server hacked-by-ransomware/

Tomaselli, K. P. (2021b, April 29). Presque Isle police await hackers' next move with stolen data after ransom deadline passes. Bangor Daily News. https://www.bangordailynews.com/2021/04/29/aroostook/presque-isle-police-await hackers-next-move-with-stolen-data-after-ransom-deadline-passes/

Tyson, M. (2025, July 22). 158-year-old company forced to close after ransomware attack precipitated by a single guessed password — 700 jobs lost after hackers demand unpayable sum. Tom's Hardware.

United States Attorney's Office. (2022, October 4). Former hacker sentenced for stealing computer power to mine cryptocurrency and stealing the personal information of more than 100 million people. Www.justice.gov.

Verizon. (2025). 2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot. Verizon. https://www.verizon.com/dbir

Volz, D. (2017, December 19). U.S. blames North Korea for "WannaCry" cyber attack. Reuters. idUSKBN1ED00Q/

Ward, M. (2014, August 6). Cryptolocker victims to get files back for free. BBC News.

Wood, C. (2021, August 16). Ransomware hit two Maine water facilities earlier this year. StateScoop.

Yu, Yi-Jin, and Katie Kindelan. “Tea Dating Advice App Confirms Hack, Says 72K Images, Including Selfies, Accessed.” ABC News, 25 July 2025, abcnews.go.com/living/story/new-dating-advice-app-tea-rockets-1-app/?id=124067965. Accessed 21 Aug. 2025.