RANSOMWARE READINESS FOR SMALL AND MEDIUM-SIZED BUSINESSES

Colin Choquette

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Department of Information Systems and Operations Management

University of North Carolina Wilmington

2024

Approved by

Advisory Committee

_____	_____	_____
Ulku Clark	Geoffrey Stoker	Hosam Alamleh

_____
Bilge Karabacak, Chair

Accepted By

_____
Dean, Graduate School

TABLE OF CONTENTS

ABSTRACT

Ransomware Readiness for Small and Medium-Sized Businesses. Choquette, Colin, 2024. Capstone Paper, University of North Carolina Wilmington.

Cybersecurity readiness against ransomware attacks is critically under-prioritized among small to medium-sized businesses (SMBs), posing severe risks to their financials, data, and integrity. This project aims to enhance ransomware readiness within this vulnerable sector by implementing a comprehensive Cybersecurity Ransomware Readiness Toolkit and Vulnerability review. The study begins with an initial survey to assess current cybersecurity practices and awareness levels regarding ransomware within participating SMBs. Subsequently, a detailed Nessus scan diagnoses the existing network vulnerabilities from those SMBs. The core of this project revolves around developing and deploying a toolkit that includes preventative measures, educational resources, and practical cybersecurity tools designed to fortify SMBs against ransomware threats, with a Vulnerability review that gives a description, remediation steps, and resources to mitigate the vulnerabilities found in the Nessus scan. Post-implementation, a second survey, and Nessus scan evaluate the toolkit and review the effectiveness and the changes in the cybersecurity posture of the SMB participating. This project collaborates with the University of North Carolina Wilmington Cyber Clinic and the Carolina Cyber Center of Montreat College to raise awareness and significantly improve the cybersecurity readiness of SMBs against ransomware.

CHAPTER 1: INTRODUCTION

Regarding small and medium-sized businesses, cybersecurity is one of the most overlooked aspects, specifically with regards to ransomware attacks. This type of oversight can significantly damage financials, reputation, and legal/regulator consequences. The main problem examined within this paper is that small-to-medium-sized businesses consider cybersecurity complicated, expensive, or not thought about, especially in the case of ransomware. Ransomware is becoming a more prevalent attack by people known as threat actors who are people that intentionally attack IT systems. These sorts of businesses should understand that threat actors typically go for the easy victory or the low-hanging fruit, which makes them more vulnerable than bigger businesses. Having that understanding, these businesses must have access to tools and resources that provide effective but easy and cheap ways to mitigate ransomware. With this project, the hope is to provide information by using the training received from the Carolina Cyber Center and the University of North Carolina Wilmington Cyber Clinic by providing a vulnerability scan for the participating companies as well as a comprehensive ransomware toolkit and vulnerability review to help mitigate this attack for these companies.

According to Veeam's 2023 data protection Trends report, about 85% of ransomware attacks targeted small businesses (Hanks, 2024). Since small to medium sizes typically do not have a very fleshed-out infrastructure, cyber criminals use that to their advantage to easily exploit these businesses. With a lack of availability for recovering their data, criminals find it very easy to get a quick payday from these businesses. Within that 85% of ransomware attacks, a high percentage of those businesses did not have an incident response plan (Hanks, 2024). Those that did, nearly a third of them did not test their plans, so these businesses do not have an adequate understanding of how to deal with this sort of attack. This resulted in a high percentage of these businesses having to pay a ransom to gain access back to their data as they could not operate without it. As mentioned earlier, the effects these attacks have on small and medium-sized businesses are devastating as there are extreme financial implications. These businesses can

suffer the cost of recovery and the high cost of paying the ransom if they choose to go that route. There is also the cost of removing the ransomware, strengthening their security, and hiring professionals to help consult and possibly implement mitigations to prevent another attack. In addition, there is a penalty for having the affected data not able to be used again as it was corrupted and lost. The 2023 Trends report stated that about 15% of companies had complete data loss due to a ransomware attack (Hanks, 2024).

Additionally, there is the effect of reputational damage when a company suffers from a ransomware attack. Customers and suppliers could quickly lose confidence in this company and keep their data secure and safe. With a reputational impact, these customers would typically take their business elsewhere as customers would feel that their data and information would not be properly protected.

Lastly, the effect of regulatory and legal consequences after a ransomware attack should be considered. This consequence depends on where the company is located. There could be legal action taken upon them such as fines, individual lawsuits or class action lawsuits, investigations into the extent of the breach, and remediation costs that take place when trying to recover from the attack. The need to perform corrective actions towards the vulnerability that was exploited as well as search for any other vulnerabilities that could be exploited in the future are additional needs.

It should be noted within the 2023 ransomware Trends report that cybercriminals initially used common tactics to infect the victim's computer with ransomware. These tactics are called phishing, where the threat actor sends an email or a text message to trick the user into giving them personal information such as passwords and login credentials. There are also malicious email attachments where the threat actor sends an email to the victim and tricks them into downloading the attachment within the email. Drive-by attacks are another method where a user visits a website and unknowingly downloads ransomware to their machine. It should be known that software vulnerabilities can be exploited to gain access to servers or machines on the network

and then drop the ransomware (Hanks, 2024). An example of this tactic is the Eternal Blue exploit used by the WannaCry ransomware, which exploited a vulnerability within a server message block to infect the machines.

There are several different types of ransomwares, ranging from malware that encrypts your files to malware that completely wipes the device it affects. According to an article by Esteban Boards at Recorded Future, there are seven types of ransomwares: crypto-ransomware, locker ransomware, scareware, doxware, ransomware as a service, and wiper malware.

Crypto ransomware is one of the most common types of ransomwares that cybercriminals use. This malware uses encryption to entirely encrypt all critical files and data on the machine, which locks everything until a ransom is paid and a decryption key is given (Veeam, 2023).

Locker ransomware, unlike crypto ransomware, does not encrypt the files on the system but locks the entire computer system, making it unusable until a ransom is paid to access the system. The locker ransomware may not encrypt the data on the machine but is still very disruptive as you cannot access any data stored on the machine (Veeam, 2023).

Scareware is malware that can lead to a ransomware attack. This malware is used to trick users into downloading ransomware by displaying a scary message that looks legitimate. Some examples of this message could be that malware has infected your computer, and you need to download this fake antivirus software to remove it (Veeam, 2023).

Doxware, or extortionware, is a type of ransomware that gains access to the victim's device in order to gather private information and data and threaten to release it or expose it to the public if the ransom is not paid. This sort of threat is devastating to a victim, especially to small and medium-sized businesses, as data is one of the most critical assets for a company. Having that data released to the public could cause extreme repercussions such as legal/regulatory consequences and reputational impacts (Veeam, 2023).

Ransomware as a service (RaaS) is where ransomware tools are rented or sold to cyber criminals without any sort of coding experience. This sort of model allows for even more

cybercriminals to gain access to ransomware, meaning more attacks are possible (Veeam, 2023).

Wiper malware is a sort of malware that is used to delete all files that it infects. This malware runs similarly to ransomware in the sense of infecting files and causing changes to the file system. This malware does not aim for financial gain; it only seeks to infect systems and delete the data contained in the systems (Veeam, 2023).

It is important to understand the most common types of ransomwares and the most notable ransomware to date. CryptoLocker was first seen in September 2013 and is known for encrypting files using the Rivest-Shamir-Adleman (RSA) public key cryptography. It mainly targeted Windows systems and caused an estimated damage of 3 million in just 9 months. The most infamous ransomware, known today as WannaCry, was conducted back in 2017. It caused mass panic as it took advantage of Microsoft's exploit called Eternal Blue, which attacked the vulnerability in the SMB protocol. This attack caused around 4 billion dollars in damages worldwide.

CHAPTER 2: LITERATURE REVIEW AND ANALYSIS

Literature Review

Ransomware is a crucial topic for small to medium-sized businesses (SMBs) because of their threat against them. “Small business owners are often tasked with many roles, including IT manager. In fact, a McAfee survey of business owners found that the majority (80%) self-managed their business protections. With limited time and resources to devote to this critical task, 60% spent less than an hour each week managing those protections, despite the risk of cyber-crime with 43% of all cyber-attacks targeted at SMBs” (McAfee Deploys Online Protection Solution, 2023). Small to medium sized businesses typically do not have the resources or time to be able to put into their cyber protections. With that, these businesses are often the main target for cyber criminals. Current trends of ransomware showed that this attack avenue had an even less barrier of entry and a high return on investment where “According to estimates by cybersecurity company Recorded Future, ransomware groups executed 65,000 targeted ransomware attacks in 2020” (Sakellariadis, 2022). There is also the use of Ransomware as a Service (RaaS) where a group of criminals were able to outsource the development of ransomware. These trends showed that cybercriminals were able to gain access and execute ransomware attacks on a mass scale and with the limited resources, time, and expertise of SMBs, these attacks were often conducted on them. With synthesizing existing research on the effects of ransomware on SMBs and the characteristics and strategies of ransomware attacks of both detection and mitigation techniques, these businesses are able to gain a better understanding on how ransomware attacks can cause major financial, operational, and reputational damages which can result in chaos and ultimate failure of that business. There is also the hope of allowing these businesses to gain a greater understanding of the different types of ransomwares and the different attack vectors that can be exploited as well as the understanding of detection and mitigation techniques such as an incident response plan and antivirus/antimalware.

Some of the main ways that SMBs were affected by ransomware are financial,

reputational, and operational impacts. With most cyber criminals' motive being financial gain, it was not a shock that when a company was attacked, these criminals asked for an absorbent amount of money typically in the form of cryptocurrency. When it comes to financial impact "ransomware attacks present victims with a post-attack choice (and, in some cases, opportunity to negotiate): pay ransom (and hopefully retrieve access to the locked resource) or incur the full losses associated with giving up on that digital asset" (August et al., 2019). This showed that when a business was attacked by ransomware there are not many options and usually a business is going to lose money or assets with either choice they picked. With the impact of the ransomware payment itself, there is the remediation cost that is needed. These costs are for removing the ransomware, restoring systems, and ensuring the malware is completely eradicated. An example of the financial impacts of ransomware is the SamSam ransomware attack. This was estimated to earn $6 million in payments. Another example is the CryptoLocker ransomware that was speculated to have generated over $30 million in payment within just 100 days (August et al., 2019). There were additional financial impacts from legal and regulatory fines that specifically targeted businesses that held sensitive information such as health information (August et al., 2019).

Further impacts included the operational impacts these impacted normal business operations such as disabling emails or not allowing employees to access data they needed to perform their daily work. From an article called "Ransomware Threat and its impact on SCADA" it spoke about how ransomware can freeze the Supervisory Control Acquisition and Data Acquisition (SCADA) configuration and management abilities, damage Human Machine Interface (HMI) ability to controllers, and paralyze historian dependent operations which can lead into a major halt in business operations (Javed Butt et al., 2019). This halt in operation can lead to system downtime which can be catastrophic for a business and lead to major financial loss as well as to switch to paper workflow which can be extremely time consuming and labor intensive. An example to explain this would be if a business' main product was a webserver and a ransomware

attack were to cause the server to go down, then that business would suffer major loss every hour from that website being down. There was also the operational impact of data being lost from a ransomware attack. "…victims are threatened to pay the ransom, otherwise the hacker or cyber actor owning the access, intends to corrupt or delete the encrypted files" (Javed Butt et al., 2019). If a ransomware attack were to occur on a business, there was the chance of that attacker corrupting all the data in the machines that were infected. This would ultimately destroy them, causing major operational impact because employees would not be able to access the information they need or the server would not be able to process the data, resulting in all services going down. Long term reconciliation was another impact to consider with a ransomware attack. This is when all systems are restored, but there is the need for manual reconciliation of data collected during the down time which could be extremely labor-intensive (Chen et al., 2021).

An SMBs reputation was also affected by an attack. When a business is attacked by ransomware there is a result on how current and future customers or clients would view them. There is a loss of client and customer trust with them perceiving the business as not able to protect sensitive data. Though "Customers and clients can be forgiven, potentially indicating a wider societal acceptance is cyber security breaches cannot always be prevented. However, poor communication practices, both internally and externally, may have significant reputational consequences, as May the risk of data exfiltration" (MacColl et al., 2024). This shows that reputational damage from the customers can be forgiven on the attack itself, yet they are not so forgiving when it comes to poor communication about the attack. Reputational harm could also come from the media's negative publicity from their coverage such as news outlets and social media which damage a company's image (Corbet & Goodell, 2022). A business' reputation could also be affected internally with poor internal communication during and after the attack. This could lead to a loss of trust among the employees. Finally, there is the long-term reputation harm explained in the article "The Scourge of Ransomware." It states, "One employee at the manufacturing company recollected that customers would repeatedly ask about the ransomware

incident Eden months after the attack, and that rumor about customers leaked personal data added to the reputational harm done" (MacColl et al., 2024). This showed how even months after a ransomware attack, clients and customers still bring it up, proving that there was a long-term reputation harm when it comes to being a victim of a ransomware attack.

When it comes to protecting a business from ransomware it is important to understand the different types of ransomwares, the different attack vectors used, and the evolution of ransomware. There are multiple different families such as CryptoWall and CryptoLocker which both appeared in 2013 and deployed via compromised websites and email attachments with a command and control (CC) on the Tor Network. Reveton appeared in 2012 and was deployed via drive-by downloads with a command and control on MoneyPak (Aurangzeb et al., 2017). Ransomware families include crypto-ransomware which once executed the malware by silently searching for and encrypting files on the victim's machine. Once that step is completed, a message is displayed that asks the user for a ransom in return for their files. After the ransom is paid, the victim would be given either a key or an executable file that was used to decrypt their files (Anghel & Racautanu, 2019). There is also locker ransomware that locks access to the victims machines by demanding a ransom to regain access to the machine. Doxware is a type that collects sensitive information from the victims machines and then threatens to release that information unless a ransom is paid (Anghel & Racautanu, 2019).

The final ransomware type is known as mobile ransomware. This is malware that targets mobile devices such as tablets and phones and is encrypted while blocking access to the device and asking a ransom payment to gain access back. With these types of ransomwares, they were able to exploit multiple different attack vectors within a business. Malicious emails and spam campaigns are an example of an attack vector. This is where attackers send emails that look to be legitimate to trick a user into clicking a malicious link or downloading a malicious attachment (Aurangzeb et al., 2017). The use of SMS messaging and third-party apps was typically seen on mobile devices where the malware can be spread by the user downloading a malicious third-party

app or clicking on a malicious link in a text message. Brute forcing passwords is an attack vector where attackers brute forces login credentials for services such as Remote Desktop Protocol (RDP) or Secure Shell (SSH). Once broken in, the attacker was able to deploy the ransomware where it would travel through the network encrypting files (Aurangzeb et al., 2017). Lastly, there is the attack vector of drive by downloads; this is where legitimate websites were compromised with malicious code. When users visit the website, the ransomware is automatically downloaded on the victim's computer without them knowing (Aurangzeb et al., 2017).

The evolution of ransomware can be broken up into three generations starting with the first generation, or locker ransomware, where it did not include any encryption of data. "Basically, they were a form of lockerware which would only lock most parts of the system leaving only essential devices such as the keyboard to enable the victim to pay the ransom." (Zimba & Chishimba, 2019). This ransomware is able to lock the screen, modify the boot menu, lock other system devices, and go after random targets unlike modern ransomware that can go after specified targets. There was not much complexity in the first generation but the second generation, or crypto ransomware encryption, was introduced and victim data was being encrypted. These encryption techniques were poor, and the keys were able to be recovered (Zimba & Chishimba, 2019). This is because the ransomware payload had the recovery key within the payload. This generation was also where the more known version of ransomware started to show up, but still had some major flaws. The recovery key being in the payload is an example of this. The third generation, or hybrid crypto ransomware, is the modern ransomware and is capable of robust encryption techniques and communications with a command-and-control server (C2 server). "Ransomware has evolved to include C2 communications for various purposes. The C2 infrastructure usually houses the malware and the associated encryption and decryption keys." (Zimba & Chishimba, 2019). This generation of ransomware is able to use asymmetric encryption where the public key is embedded into the payload and is used to encrypt the victims data while the private key was with the attacker or on a C2 server. This generation

also has a way to prevent recovery unlike the previous generation with data deletion. Compared to the previous generations, the third generation is the most dangerous and robust ransomware to date, and it is the current generation of ransomware that is in the field today.

When trying to protect a business, understanding different detection techniques is important and includes traditional and advanced techniques. It is also important to understand the challenges with detecting ransomware. Traditional detection techniques include signature-based detection; this is a detection technique that uses known patterns or signatures. It took the program and compares the code with a database of known ransomware signatures. If it is flagged then the program is ransomware (Bijitha et al., 2020).

"Signature based detection methods are good in detecting the known malwares, but they are unable to detect unknown malware and polymorphic malware because they can change their signatures. (Tahit, 2018)" This is a big flaw with signature-based detection where if the program had obfuscation then it could easily be bypassed. Anomaly based detection is a method that has two phases. The first phase is a learning phase where the model tries to understand what the normal baseline of the machine is. The second detection phase monitored the system for unusual behavior that strayed from the normal baseline of the machine (Bijitha et al., 2020). It solved the problem of signature-based detection because anomaly-based detection could detect unknown ransomware by identifying abnormal behavior and unusual file encryption patterns and unexpected file access. "...the high false positive rate commonly associated with anomaly-based detection techniques." (Bijitha et al., 2020). This was because after the learning phase if there is any activity that was outside that baseline, it was flagged as suspicious even if it was not.

Specification based detection "...leverages some specification or rule set of what is valid behavior in order to decide the maliciousness of a program under inspection" (Bijitha et al., 2020). This detection technique used rules in order to detect ransomware. It is an upgrade from anomaly detection as it addresses the high false positivity rate. It did this by using well defined rules for detection.

Lastly, honey pots are a detection technique that used a decoy machine for attackers to attack. If an attacker were to drop ransomware on this it could be detected and analyzed for other detection methods (Tahit, 2018). This does not only divert the attacker from other systems but can provide insight on the attack technique to better enhance other detection methods for suture attacks.

Traditional techniques are great but have some pitfalls. Fortunately, in combination with advanced techniques, the holes in a business can get even smaller. Advanced techniques are machine learning based detection where it can undergo supervised learning or unsupervised learning by analyzing a large set of features from static and dynamic analysis. It can then use the information it learned to detect ransomware and is able to detect ransomware via the application programming interface (API) calls, file system operations, and network traffic (Burrueta et al., 2019).

Network traffic analysis is a detection technique that looks for ammonolysis patterns such as frequent DNS queries and dynamically generated domain names or connections to known C2 servers. This did this by detecting malicious or known domains for C2 servers before the encryption started (Burrueta et al., 2019). The flaw with this is that if the ransomware encrypts everything before it starts communicating with the C2 server then it is relatively difficult to detect before anything could happen.

Canary Files are files placed in users directory and are heavily monitored. If the files are accessed or modified then it could indicate ransomware activity (Burrueta et al., 2019). With this you leverage by making these files look sensitive and make them an early warning system to detect unauthorized access of malicious activity quickly. This can be done by setting up alerts for any interaction with these files.

With ransomware being a constantly changing malware there are some great challenges that come when trying to detect it. These challenges are polymorphism and obfuscation "...malware creators can quickly generate thousands of binary variants of functionally identical

samples, effectively circumventing signature-based approaches." (De Gaspari et al., 2022). With criminals adding polymorphism and obfuscation it caused the code and the signature to change constantly which helped bypass any sort of signature-based detection. Process splitting is another challenge where malware distributes the operations across multiple different processes. This sort of evasion could be used to bypass anomalous based detection by doing processes that are not too significant to disguise themselves as normal activity. Functional splitting is a challenge because ransomware operations are split into different functional groups that do a specific task. This is very similar to process splitting, evading any anomaly detection while making it look legitimate. A final challenge is Mimicry; this is an evasion technique that has the processes of the ransomware mimic the behavior of a benign process.

In combination with detection and prevention, having awareness and recovery plans are extremely important to stay up to date and be prepared if an attack were to occur. Having great awareness of ransomware within a business is extremely important as it could help with an employee's understanding of the threat posed to the business and the potential damage it could cause (Luo & Liao, 2007). By understanding the tactics used by attackers, employees could be more vigilant and cautious on emails sent to them and the websites they visit. This will help with preventing ransomware from infiltrating their systems and network.

Recovery from a ransomware attack can be split into a five-phase plan. Phase one, called hyperacute, is the immediate response within the first 48 hours of the incidence. In this phase there is an assessment of the initial damage, and a report made on the capabilities that are still running as well as a switch to manual workflows, such as pen and paper, if need be. Communication with shareholders and other stakeholders should also occur during this phase (Chen et al., 2021). Phase two, called acute, happens in the first three weeks and deals with operations continuity. This consisted of the continuation of using manual operation if need be such as fax and paper, set up of temporary offline solutions if possible, such as DVDs, and to ensure data consistency and analog archiving for eventual reconciliation (Chen et al., 2021).

Phase three, which is infrastructure recovery, deals with rebuilding the IT infrastructure. This phase consisted of assessing the state of critical systems such as the databases and determining if they are recoverable or lost. The IT infrastructure is rebuilt with clean assets to ensure that it is a malware free environment and to restore access to digital systems gradually to ensure that they are secure and functional (Chen et al., 2021). The reconciliation is phase four and deals with data reconciliation. It consisted of reconciling critical data such as client and customer information and digitizing any paper operations that are done before the recovery of the IT infrastructure (Chen et al., 2021). The final phase or could be considered the first phase or phase 0, involved continuous readiness planning that dealt with ongoing preparation. This consisted of forming a cyberattack response task force that can plan and update procedures, establish an incident command system to coordinate response during an attack, develop a continuity of operations playbook that detailed recovery steps, and perform regular practice of these recovery and response plans with tabletop simulations (Chen et al., 2021).

Ransomware had an extreme impact on small to medium sized businesses, where it can affect their financial stability, operational continuity, and reputation. These attacks caused massive financial burdens through direct costs such as ransomware payments and indirect costs such as downtime and loss of customers. This attack also causes operational disruption such as system downtime and data corruption. These disruptions paralyze critical functions which result in productivity loss and financial loss. Additionally, SMBs face long term reputational damage as customers lose trust in the business' ability to protect sensitive information. To respond to these threats there are many detection and mitigation strategies available ranging from traditional techniques such as signature-based erection, to more advanced techniques such as machine learning. Implementing awareness programs and structured recovery plans enhanced readiness for ransomware attacks. Further research would be needed to create cost effective cybersecurity solutions tailored specifically for SMBs which often operate on limited resources. Some current detection and mitigation techniques included machine learning models or anomaly detection.

There is limited research on how these businesses can use federal resources to assist in implementing effective defenses. In the future, studies on scalable AMB specific solutions that have a balance of effectiveness, affordability, and simplicity should be done. Though SMBs lack the resources of larger companies, using the insights from this research helped strengthen their security posture. Investing in cost effective detection tools such as signature-based monitoring and protection, mitigated potential attacks. Having a recovery and incident response plan implemented allowed for SMBs to react swiftly, and minimize the damage during an attack. Having a proactive approach with regular backups, employee training and awareness, and extensive monitoring allowed for SMBs to improve their resilience to these attacks.

Review of Training

There were multiple types of training provided during the duration of this project. The Carolina Cyber Center (C3) training entailed internship training and participation in a cybersecurity workshop. In addition, there was training at the UNCW Cyber Clinic during the summer of 2024. This training included NICE challenges, immersive lab training, and hands-on work with the Nessus Vulnerability Scanner. A review of all training with shared opinions on its importance and recommendations on what training students should pursue for the UNCW Cyber Clinic in the future is included.

Carolina Cyber Center

The training with C3 began with a focus on the cybersecurity workshop, where there was a presentation on basic cybersecurity implementations that small and medium-sized businesses can adopt to gain a competitive edge. This training then moved into an internship with the Carolina Cyber Center, with a total of 200 hours, with a maximum of 20 hours per week, to go over worksheets and training—learning the basics of a Security Operations Center (SOC) and key concepts within a SOC environment. Additionally, there was Range Force training, which provided hands-on experience with various ideas and tools.

The workshop training began with developing a Python web scraper for the Wilmington

Chamber of Commerce. This script utilized the regex (regular expression) library, Beautiful Soup 4, and the requests library. The function was to scrape the Wilmington Chamber of Commerce website to gather information on approximately 500 businesses. The information consisted of company names, addresses, phone numbers, and websites, which were then added to a CSV file. Additionally, multiple tools were used to find company owners' names and email addresses. An example included Hunter.io, which searched for contact information when provided with a domain name. Another example was Clay.com that was employed to take the CSV file created from the web scraper and find specific data, like an email or name, by searching multiple websites using resources like Hunter.io. The gathered information was then imported into a tool called Edison Marks, which performed a passive scan of each company's domain and provided a score similar to a credit score reflecting the security posture of the domain. After completing all passive scans, outreach was initiated with two emails. The first email introduced the workshop, providing the date, discussion topics, and an overview of what would be covered. The second email was a follow-up, reiterating the information and including an Edison Marks report to show the company's current score.

A presentation was then created to be delivered during the workshop. This practical presentation focused on basic cybersecurity practices that small and medium-sized businesses (SMBs) could implement to improve their security posture. The first concept discussed was the analogy of being the slowest gazelle, illustrating that just as a gazelle must be faster than the slowest to avoid being caught by a lion, companies must ensure their security is stronger than that of their peers to avoid being targeted by cyber attackers, who often go for the easiest targets. The presentation outlined at least five key practices for companies to implement, stressing the practicality and applicability of these practices: training employees on security principles, keeping software up to date and maintaining backups, encrypting data, running antivirus software, considering the use of VPNs for remote work, enabling multi-factor authentication, enforcing strong passwords, and protecting their website and domain.

Rapid-fire assessments were conducted for participating organizations using an online resource called Velocity. This tool allowed for survey assessments on various topics, such as NIST Ransomware assessments, CMMC assessments, and basic cybersecurity assessments, which was the focus of this workshop. The evaluation asked questions such as “What information does the organization have access to?” and “Does the organization perform external or internal application penetration tests or vulnerability assessments?” Upon completion of the assessment, a score similar to a school’s grading system (A to F) was provided, along with suggestions for improving the company’s score. The experience received from the workshop was positive, making it a valuable and enriching experience. Engaging with people of varying technical abilities in cybersecurity and providing basic information to these organizations to enhance their security posture was particularly rewarding. The training provided by the Carolina Cyber Center was highly beneficial and could serve as a model for future workshops aimed at small and medium-sized businesses, inspiring and motivating the audience about the potential benefits of the training.

In addition to the workshop experience there was a comprehensive internship training program at the Carolina Cyber Center. This entailed a wide range of online training modules. These modules covered not only the fundamentals of cybersecurity but also the essential knowledge required for operating in a Security Operations Center (SOC). The program began in a Google Classroom, where the research delved into topics such as a basic SOC lab, operational security, and DevOps videos. The curriculum also included practical security measures that can be implemented on workstations, such as password protection, VPNs, malware or antivirus software, and password managers. Moreover, the internship explored various compliance standards, including PCI DSS, SOX, and GLBA, and delved into different frameworks like the MITRE ATT&CK framework, along with tools such as Metasploit, Nmap, Nessus, and Cisco Packet Tracer. The program also addressed attacks and vulnerabilities, including WordPress vulnerabilities and social engineering, and provided labs related to these topics. Furthermore, it

examined IoT devices and the associated vulnerabilities, ensuring a comprehensive understanding of the cybersecurity landscape.

Upon completing the Google Classroom modules, RangeForce Labs were then assigned. This resource provided virtualized cybersecurity training through labs and hands-on experience with multiple tools. This hands-on experience was a key component of the training, as it allows the gaining of practical skills with tools such as Splunk, YARA, Wireshark, basic shell scripting, Windows processes, Windows Active Directory, Ceramic firewalls, malware sandboxing, and malware analysis using open-source intelligence. The training also involved challenges such as malware cleanup, SSH backdoor, spoofing, cookie security, persistence, SOC detection, and static and dynamic analysis challenges. Additionally, the course covered the Elastic Stack SIEM solution, ensuring a well-rounded and practical training experience.

Throughout this internship, the information was highly valuable, and the experience was both unique and beneficial. While the content in the Google Classroom was primarily conceptual, consisting of videos and readings on SOC-related topics, it provided a solid foundation in SOC basics. The modules on security tools like Nessus, Nmap, and Metasploit were particularly excellent, offering hands-on experience with these tools. The Cisco Packet Tracer module was also an effective tool for learning and deepening networking knowledge. However, the most significant and valuable training provided by the internship was through RangeForce's online training platform. This platform offered extensive hands-on training with various tools and concepts in cybersecurity. It was found that RangeForce is an exceptional resource for virtualized training and should be recommended as the primary training method for students in the UNCW Cyber Clinic, focusing on tools and cybersecurity concepts.

UNCW Cyber Clinic

The UNCW Cyber Clinic training primarily utilized the online platform NICE, where multiple NICE challenges were completed. Additionally, the clinic used Immersive Labs' online training platform, which offered numerous virtual training modules. The Cyber Clinic also

provided training on the Nessus vulnerability scanner.

The NICE challenges are online, real-world simulated environments where participants complete specific tasks to ensure that all systems are in a desirable state. These tasks started with essential server maintenance and cleaning. This involved providing documentation on the process, performing cleaning, boot partition management, disk checks, scheduling reboots, and conducting physical maintenance for a server. The next challenge involved searching for network anomalies by analyzing different packet capture files to identify the source and nature of attacks on each server. After determining the cause, a ticket was submitted using the simulation virtual ticket system.

In a subsequent challenge, the focus was on password management, where brute force attacks were performed on multiple accounts to identify any with vulnerable passwords. Upon finding such accounts, it was required to go into Active Directory and set the option for password change at the next login. Another challenge involved assisting with help desk login failures; in this scenario, a user could not log into the workstation's domain, so the task was to remove the device from the domain and then rejoin it, allowing the user to log in successfully.

The following challenge addressed unauthorized activities, requiring the activation of firewalls on different workstations and servers, restricting remote desktop access for domain controllers and workstations, removing unauthorized users from the servers, and eliminating any persistence mechanisms they may have established. The next task was vulnerability management and scanning. In this room, which required a review of a Nessus vulnerability scan output file to identify vulnerabilities within each server and then addressed these issues. The vulnerabilities included SSH problems that required updating or reconfiguring the SSHD configuration files and outdated shell, FTP, Samba, and PHP versions, all of which needed to be updated to the most recent versions to mitigate vulnerabilities.

The final challenge was an in-depth layer defense, where the task was to implement correct firewall rules on multiple Linux systems and ensure proper firewall configurations on

Windows Domain Controllers and Windows workstations. After completing these challenges, valuable hands-on experience and knowledge was gained in network maintenance, network analysis, firewall maintenance, and vulnerability management. NICE challenges and RangeForce training are recommended to be used as primary tools for training new students in the Cyber Clinic.

The next phase of training received at the Cyber Clinic was through the Launchpad Immersive Labs online platform. This training covered the NIST Cybersecurity Framework, the MITRE ATT&CK Framework, and the OWASP Top 10. It also included topics such as hashing and encoding and an introduction to networking. The training further covered the Linux command line and Windows concepts, reviewing the basics of interacting with the Linux command line and the Windows operating system. There were simulations for different types of incident response, such as data exfiltration, parsing person storage table (PST) files, and addressing phishing vulnerabilities in Office 365. The labs focused on packet analysis using Wireshark, where the researcher learned the basics of Wireshark and practiced applying these skills. The training then progressed to log analysis, explaining server logs, their formats, and the different types of logs, such as access and error logs. It also covered analyzing logs using the Linux command line in a Linux system. Additionally, the Immersive Labs training introduced Splunk, covering its interfaces, the types of data sources it handles, how to perform searches in Splunk, and how to create dashboards and visualizations.

CHAPTER 3: METHODOLOGY

This project is conducted on a single SMB in the Wilmington, NC area and the process starts with a comprehensive survey and an in-depth Nessus scan of the SMB's network. The initial survey in Appendix A addresses multiple topics, starting with the Nessus scan. It covers the IP addresses, devices, and subnet ranges of the SMB. The survey then addresses ransomware awareness; within this section, the survey asked questions allowing for a greater understanding of how familiar the SMB is with ransomware and if there is anything in place to keep the organization up to date and be prepared for any possible attack. There are then questions concerning policies and procedures, allowing for a more generous understanding of any policies or procedures that could help prevent ransomware. This section also inquired whether the SMB has incident response plans or requirements for reporting phishing emails. Finally, the survey covered technical controls that provide insight into the presence of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). There are also questions that ask if the SMB practices restricting privileged accounts and ensuring scheduled updates for applications and operating systems were also examined.

After the initial survey, a Nessus scan was conducted, covering all the devices the organization wanted to scan. The scan was a fundamental network scan that identified vulnerabilities and gathered information about each scanned device; the IP addresses, subnet ranges, and devices outlined in the initial survey were utilized to direct this scan.

After completing the initial scan and survey, a Ransomware Readiness Toolkit was developed, and a vulnerability review was performed. The ransomware readiness toolkit, as Appendix B outlines, consists of three main sections. The first section features a checklist designed for SMBs, providing a comprehensive list of security measures to help them prepare for and respond to a ransomware attack. The topics covered were identifying assets, security controls, access controls, network segmentation, monitoring and logging, incident response plans, awareness training, backup and recovery testing, vulnerability and patch management, email

security, and endpoint detection and response. Each topic briefly describes what it was, best practices, and learning resources. Next is a section on helpful websites and resources; this has websites from the National Institute of Standards and Technology (NIST), the Cyber Infrastructure Security Agency (CISA), the Cyber Readiness Institute, and the Federal Trades Commission (FTC). There were also open-source intelligence websites such as AbuseIPDB, VirusTotal, and Hybrid Analysis. Under each website is a short description of what it is, along with a link to the websites and essential notes. Lastly, there is a section on tools; the tools listed are cheap or free and easy to use, these tools are backup solutions, endpoint protection, network security, email security, monitoring and response, vulnerability scanning, security awareness training, and multifactor authentication. Under each tool, there is a description of what the tool is, with a link to pricing and an installation guide. This toolkit is vendor-neutral and is created for all types of SMBs regardless of the industry.

The vulnerability review is vendor-specific and covers the vulnerabilities found from the initial Nessus scan. The review looks at all critical, high, and exploitable vulnerabilities. The review describes each vulnerability with remediation recommendations, steps on how to remediate, and links to resources on how to remediate or more information on the vulnerability. Once these steps are completed, they are handed off to the SMB for review. The SMB can then utilize information from the toolkit, the vulnerability review, or both. When the SMB has adequate time to review both resources, an exit Nessus scan do the exact scan that the initial scan conducted.

An outro survey shown in Appendix C discusses what the SMB thought about the Ransomware Readiness Toolkit and the vulnerability review. This survey asks questions such as "How clear and understandable was the content of the Ransomware Readiness Toolkit?" and "How adequately do you find the remediation steps provided for the vulnerabilities identified?" These questions help identify what went well and what did not and allow the SMB to provide feedback on the resources provided to them.

CHAPTER 4: TOOLS AND RESOURCES

There were many vital tools and resources used and developed to perform every task needed for this project. The ransomware readiness survey was used to gain a greater understanding of the SMBs security posture to ransomware as well as gather information for the Nessus scan. The Nessus scan, both initial and outro, used the Nessus Vulnerability Manager to perform the scan and to help analyze the output. The Ransomware Readiness Toolkit and vulnerability review were made to help the SMB to bolster their security posture towards ransomware. Lastly, the Ransomware readiness outro survey which was used to gain an understanding on how the SMB perceived the resource that where provided to them.

The Ransomware readiness survey shown in Appendix A, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), was used greatly when figuring out questions to ask. The survey went over the information of the Nessus scan such as the different subnets on the network asking if the IT infrastructure is in the cloud, on premise, or hybrid. Additionally, it asked the Internet Protocol (IP) numbers, subnets, and other devices if they would have liked to be scanned. Then the survey transitioned into a section of ransomware awareness that had the categories, identify (ID), protect (PR), and respond (RS), used to help with the questions. The questions asked were how familiar the organization was with different types of ransomwares and the impacts they can have and how often the organization updated its training sessions to include ransomware threats. The questions in this section stemmed from the subsections of the NIST CSF ID.RA risk assessment, PR.AT awareness training, RS.RP response planning (National Institute of Standards and Technology, 2022). The next section of the survey asked questions in regard to policies and procedures. This section used the categories of PR, ID, respond (RS), and recover (RC) to help with the creation of these questions. Some of the questions asked were how the organization maintained an up-to-date inventory of all IT assets and was there a mandatory policy for employees to report suspected phishing attempts. The subsections used in this section were PR.IP information protection and procedures, ID.AM asset

management, PR.AT workforce training, PR.DS security monitoring, PR.DS data security, RC.CO communication, RC.RP recovery planning, RS.IM improvements (National Institute of Standards and Technology, 2022). The last section went over questions on technical controls, the categories used during this section are PR, detect (DE). Some of the questions asked in this section list the type of solutions deployed at the organization and how they were integrated to protect from ransomware and explain the network segmentation strategy used to protect critical systems against ransomware spread. The subcategories used in this section are DE.CM monitoring, PR.PT protective technology, PR.MA maintenance, DE.AE event detection, PR.AC access control, PR.AC least privilege, PR.IP patch management, and PR.DS third party security (National Institute of Standards and Technology, 2022).

For both the Initial vulnerability scan and the outro vulnerability scan, the Nessus Vulnerability Management system was used. With this tool it was able to perform a basic vulnerability scan that looked for all information and all types of vulnerabilities on a network. This was outside of authentication, so all information and vulnerabilities were grabbed from outside any system authentication. This tool also provided a detailed output from each scan allowing for a filtering of vulnerabilities by asset which helped with visualizing which assets had the most vulnerabilities. Lastly, these tools allowed me to export the results to a PDF for the SMB to have in case they wanted to see results beyond what was provided from the vulnerability review.

The Ransomware Readiness Toolkit shown in Appendix B was made to give resources and a checklist for SMBs to better prepare and mitigate a ransomware attack. This was broken into 3 main sections which covered a checklist, websites and resources, and recommended tools. With the checklist section it was broken into 11 different subsections that went over different aspects to look at in a business to properly secure from ransomware. Within each subsection there was a description of the point that was being talked about with points of best practices and some resources to learn more about this point or to learn more about implementation. Some examples

in this section were access controls which was the step that made sure there were controls in place that reduced access to sensitive information, minimizing the risk of ransomware gaining access to these assets. The best practices would be Multi-factor authentication, least privilege, and account monitoring and auditing. The resources provided were CIS Control 5 of account management and CIS control 6 of access control management. Each topic related to minimizing the risk of ransomware. The next section dove into important websites such as NIST, CISA, Cyber Readiness Institute, and FTC. Each website provided information or mitigation strategies on ransomware. Additional websites, such as AbuseIPDB, VirusTotal, and Hybrid Analysis were highlighted. These websites gave a SMB a free way of analyzing any domains or files that they believed to be suspicious by inserting the domain or the file hash into these websites to see if it had been reported before. The tool section of the toolkit describes that each of the tools were relatively cheap or free to allow for, if a SMB would like to use them, they could have the resources to do so. Also, this section was broken into eight subsections with each section being a vital way of mitigating ransomware attacks. A highlighted example would be backup solutions because if a ransomware attack were to happen, it is important that the SMB have their data backed up, so they were able to quickly and effectively recover their critical systems. A few more of the tools highlighted were Microsoft Azure Backup and AWS Backup, giving a description of each tool with a link to a pricing calculator or pricing website depending on the tool. It also included a point on how the tool would best be used as well as a link to a resource to learn more about the tool and documentation. In total there were 33 tools highlighted within this toolkit providing a decent amount of variety to the SMB.

The Vulnerability Review was the resources created for the SMB to provide detailed information on several different severity vulnerabilities in the initial Nessus scan. The severity of vulnerabilities that were reviewed were described as critical, high, and mediums if Nessus Vulnerability Manager labeled it as exploitable. The layout of this review provided a review of each vulnerability by asset. With each vulnerability there was a description of the vulnerability

and recommended remediations. Additionally, there were steps on how to perform the remediations if available. Lastly, there were links to resources that provided more information on the vulnerability and a guide on remediation with more information on the recommended remediations. The review was made to help the SMB with an easy to follow and non-overwhelming resource on the high-level severity vulnerabilities on their network. With this review it was able to help with identifying each vulnerability on the network and see if the SMB has any vulnerabilities that were related to ransomware or could be exploited by ransomware.

The Ransomware Readiness Outro Survey shown in Appendix C, was a survey that was created to get a review from the SMB on the resources that were provided to them. The survey was split into two sections and asked a total of 17 questions. Within the first section were questions on the Ransomware ReadinessToolkit. Some of the questions asked were "How clear and understandable was the content of the Ransomware Readiness Toolkit?" and "Please provide any suggestions or comments on how the toolkit can be improved." These questions were asked to gain a greater understanding of the impact this resource had on the SMB from the employee's perspective. The next section was on the Vulnerability Review and questions asked here were "How adequate do you find the remediation steps provided for the vulnerabilities identified?" and "Were the resources provided for further learning and remediations helpful?." The questions in this section were made to gain an understanding if the vulnerability review was helpful to the SMB and if what was provided was useful to the employee.

CHAPTER 5: FINDINGS

For the findings of this report, it is going to look at the Ransomware Readiness Survey conducted on an SMB with this survey it presents an examination of existing security posture, with an emphasis of ransomware awareness, policies and procedure, and technical controls. These findings also provide an analysis of Nessus vulnerability scan results on the SMBs network which include a wide range of IP addresses and a look at critical, high, and medium vulnerabilities. Furthermore, there is an analysis on the finding of an outro survey which examines the feedback from the SMB that participated in this project. These findings set a stage for deeper understanding of the SMBs cybersecurity readiness and highlight the areas requiring urgent attention and improvement.

For the initial Ransomware Readiness survey starting with the section on the Nessus scan, it was found that the SMB wanted 22 different IP addresses scanned with an additional range of 50 IP addresses once on site. In total the survey found that the SMB had 72 unique IP addresses scanned by Nessus. These ip addresses include assets such as a lead switch, WAPs, Servers, virtual servers, and workstations. Moving on to the next section on ransomware awareness the survey found that the SMB was familiar with the concept of ransomware but did not know really how it worked. Additionally, the SMB does not have any updated training to keep employees up to date on the latest security trends of tactics related to ransomware. There is just an emphasis to not opening suspicious emails or clicking on emails they are not expecting, Also, There is no system of addressing vulnerabilities or threats related to ransomware the SMB is more reactionary to anything that comes up. Lastly, it was asked to see if the SMB would be able to effectively respond to a ransomware attack, they said not completely that they do have backup procedures but if there were to be an attack they do not have an expertise in containing and eradicating it to be able to restore their data.

Looking at the policies and procedures section it was found that the SMB has backup procedures in place with three backup servers off site and two onsite behind closed ports with

those ports opening during backup times. It was also found the SMB does not have any employees that have received any training related to responding and recognizing ransomware threats or indicators of compromise (IOC) as well as the tracking IT assets is conducted by excel spreadsheet that is updated throughout the year and during a yearly audit. There is also a requirement for reporting suspicious emails but there was nothing on how that is enforced. Additionally, there is no data classification by sensitivity, which means there are no additional security measures for more sensitive data. All data is given the same level of protection. Lastly, in relation to incident response and recovery the survey found that the SMB does not conduct any testing of their incident response plan but they do attempt to update it with additional safeguard, also it was found that the in a scenario of recovery the mean time to restore (MTTR) for data backups and snapshots of work machines it about a couple days. But, for the entire network it was found that it would take a more significant amount of time.

Lastly, for technical controls it was found that there is no centralized network or log monitoring system to minotaur and analyze any security events. But they do have EDR solutions on all work machines as well as on premise firewalls. It was also found that the SMB does not have data at rest encrypted even though their servers have the capability to. Additionally, with their EDR solutions they also have Microsoft Defender enabled on each workstation with MFA for all Office 365 users. For backups, the SMB does snapshot backups of every word machine during the weekends with a full backup once a week. Additionally, work machines and applications are updated on an unscheduled basis. Lastly, found in the survey network segmentation is only applied to backup servers through closed ports and there are two admin with access to servers that have MFA enabled, with users having access to all files on the file server with local administrator privileges to their machines, except they do not have access to some restricted share folders. The only measures taken for third parties is the use of reputable software and VPN rights, other than that it is trust between the vendor and the SMB.

From the findings of this survey, it is noticed that the SMB does have the most basic

security practices in place such as backups and updates, with some authorization in applications and segmentation for backup servers. But it is noted that the SMB does lack access control as all users have access to all files on the file server and users have admin rights on their work machines as well as third party vendors not being restricted to what they need on the network. Lastly, there are also the problems of lack of encryption for data at rest on servers and lack of employee training and awareness of security threats and tactics and lack of enforcement of reporting suspicious emails.

Two Nessus scans were conducted: an initial scan to identify vulnerabilities before using the Ransomware Readiness toolkit and Vulnerability Review, and a follow-up scan to confirm if any vulnerabilities were successfully patched. These scans are also used to see if there are ransomware related vulnerabilities on the network. Starting with the initial scan it was able to grab vulnerabilities from 43 assets from the 72 IP address scanned. From this scan it resulted in 4 critical, 14 high, and 35 medium vulnerabilities. Looking at the critical vulnerabilities three out of the four were related to VMware version Vulnerabilities and one was related to a buffer overflow vulnerability. With these vulnerabilities there are multiple CVEs related that are able to be exploited by ransomware. Such as the buffer overflow attack having CVE-2020-5344 where an attacker is able to run arbitrary code on the affected systems which can allow them to initiate a ransomware attack (National Institute of Standards and Technology, 2020), as well as for the VMware vulnerabilities there could be multiple different ways of attack as the version found is not supported and my additional unpatched vulnerabilities. Next looking at the high vulnerabilities these vulnerabilities where related to Microsoft guest accounts, more VMware version vulnerabilities, SNMP agent, OpenSSH version remote code execution (RCE), VMware reflected denial of service, and Internet Small Computer Systems Interface (ISCSI) unauthenticated target. From these vulnerabilities there where only a few that could possibly be exploited and these are OpenSSH version has multiple vulnerabilities such as CVE-2023-48795 (National Institute of Standards and Technology, 2023), CVE-2023-51384 (National Institute of

Standards and Technology, 2023), and CVE-2023-51385 (National Institute of Standards and Technology, 2023) these vulnerabilities can allow for unauthorized to gain access of execute arbitrary commands remotely which could lead to a ransomware attack. There were also VMware multiple vulnerabilities such as CVE-2020-4004 (National Institute of Standards and Technology, 2020) and CVE-2020-4005 (National Institute of Standards and Technology, 2020) these vulnerabilities can allow attackers to execute code remotely and perform unauthorized actions when they may have affected a system vulnerable to ransomware deployment. Lastly, looking at the medium vulnerabilities these were related to SMB signing not required, OpenSSH vulnerabilities, SSH Terrapin, VMware RCE, and Dell EMC version vulnerability. From these vulnerabilities the ones that could possibly be exploited by ransomware is OpenSSH multiple vulnerabilities which includes the same CVEs from the high vulnerability, VMware RCE which is referenced as VMSA-2021-0002 (VMware, 2021) and can allow attacker to have RCE which can be used in deploying ransomware. Lastly, the SSH Terrapin identified as CVE-2023-48795 (National Institute of Standards and Technology, 2023) can be used by an attacker to gain access via a SSH session to then deploy a ransomware attack. With the vulnerabilities found in the initial scan Looking at the results of the outro scan it was found that from the resource provided the SMB was able to remediate 50% of the critical from 3 to 2, a 57% remediates in the highs from 14 to 8, lastly a 40% remediation of mediums from 35 to 14. This comes out to a total of 45% of total vulnerabilities remediated from 53 to 24. From these stats it shows that there was a slight effectiveness of the vulnerability review. But with this project the SMB said that they were unable to remediate the vulnerability on their virtual servers as they would not have the expertise at the moment to do so as they would want to break something. Using the stats from the Nessus scan and the understanding of their limited expertise on some of their servers the results of the vulnerability review and Ransomware Readiness Toolkit were successful. Most of the remediated vulnerabilities were from the medium SMB signing vulnerability. Additionally, all remaining critical and highs are from the virtual servers that were not remediated.

The outro survey was conducted to see if the Ransomware Readiness Toolkit and vulnerability review were useful from the SMBs opinion. The survey starts off with questions about the Ransomware Readiness Toolkit. With those questions it found that the SMB thought the toolkit was clear and tools and resources provided were somewhat easy to implement and were effective in helping the SMB prepare to handle an incident. It was also noted the SMB did not have Email Security, vulnerability assessment, awareness training from the checklist. With this toolkit it allowed them to understand ways of getting these points implemented. Next looking at the vulnerability review from those questions it found that the SBM thought the review was very satisfied with the thoroughness of the review, and felt that the remediations were very easy to implement with the resource on those remediations very helpful. It was also noted that the SMB was well done and having a step-by-step guide is extremely helpful when it is not known what to do. It was also noted that in-person review would be a great improvement as the SMB does not have an in-person IT staff. Having an in-person review would allow for quick information as to not having to wait for emails.

The findings from the Rasnowmare Readiness survey showed a concerning but not uncommon scenario among SMBs, with a lack of awareness of ransomware and a significant gap in proactive security practices and employee training. Despite some basic security measures like backups and patch updates, the SMB overall ability to respond to and mitigate the risk of a ransomware attack was insufficient, mainly from the lack of knowledge and understanding of some security practices. The vulnerabilities identified from the Nessus scans with remediation efforts reveal both progress and persistent challenges, specifically in addressing critical and high-level security vulnerabilities. These findings not only highlight the importance for enhancing security training and infrastructure but also serve as a call for other SMBs to adopt a more rigorous and informed approach to cybersecurity, ensuring that they are not only prepared but resilient to these threats.

CHAPTER 6: OUTLINE OF COMPLETED WORK

The paper started with an introduction covering the problem being addressed and the motivation behind this project. The paper also discussed a review of literature and analysis with subsections covering the literature review, Carolina Cyber Center training, and the University of North Carolina Wilmington Cyber Clinic training. Following this, there is a chapter covering methodology with a following chapter on tools and resources. Next, the paper discusses findings with subsections, covering the survey, Nessus scan, and overall project outcomes. Finally, the paper would conclude with information on future works.

The introduction is a vital part to the paper, offering a comprehensive overview of the project's problem by giving statistics on how impactful a ransomware attack can be on the SMB. This chapter gave a brief, yet comprehensive background on ransomware and the different types.

The review of literature and analysis was extremely important as it meticulously examined papers and articles on four key topics: effect of ransomware on SMBs, ransomware characteristics and attack strategies, ransomware detection techniques, and response and recovery from ransomware. This comprehensive review ensured that the reader was well-informed and knowledgeable about the key aspects of the research. The review of training covered training from the Carolina Cyber Center and the second detailing training from the UNCW Cyber Clinic. The methodologies chapter provided a detailed explanation of how the research was conducted, along with the tools and processes to be used.

Next, the paper reviewed the tools and resources created and used. This section discussed both the initial and outro surveys, the toolkit, and vulnerability review. The discussion overviewed what the tool was as well as underlined the reasoning for what was included.

The findings chapter provided subsections on the survey results, scan results, and the overall project outcomes. These results highlighted the differences observed between the beginning and end of the project and whether the Cyber Readiness Toolkit and Vulnerability review had a positive or negative impact on the businesses. Lastly, the paper concluded with a

chapter that included future works.

CHAPTER 7: CONCLUSION

With ransomware becoming a significant threat for small to medium-sized businesses (SMBs), this project aims to heighten the awareness of the increasing risk. The aim is to equip SMBs with essential tools and resources by examining their practical application within an SMB. This approach seeks to inform and empower SMBs to effectively counteract ransomware threats with proactive and informed strategies. This starts with an introduction that explains why this topic is important, as SMBs are the main target of cybercriminals, with them being low-hanging fruit. These attacks can have financial, operational, and reputational impacts on these businesses. There is also an analysis of the different types of ransomware families and ransomware types, with crypto-ransomware being an example. The report moves into the literature review by analyzing the effects of ransomware on SMBs, ransomware characteristics and attack strategies, detection techniques, and awareness and recovery.

Additionally, the training received from the Carolina Cyber Center and UNCW Cyber Clinic was analyzed. There is then a look at the methodology where this project follows the process of having an initial survey that focuses on the topics of a Nessus scan, ransomware awareness, policies and procedures, and technical controls. The project then moves into the initial Nessus scan, followed by developing and sharing a Ransomware Readiness Toolkit and Vulnerability review. The project then ends with an Outro scan and survey to see the impacts of the two resources provided. Next, an analysis of the tools used and made during this project covers the Ransomware Readiness Survey, the Nessus Vulnerability Management system used to perform the initial and outro Nessus scans, and the outro Ransomware Readiness survey. This led to the findings of this project, where the Ransomware Readiness survey found that the SMB had very basic security practices in place but needed more technical controls and security awareness from employees. Additionally, there was an analysis of the results for the Nessus scan where it was found that the resources provided caused 40% of vulnerabilities that were analyzed to be remediated. Lastly, the Ransomware Readiness survey showed that from the SMB's perspective,

the resources provided were beneficial and allowed their business to strengthen its security posture. Having resources such as the Ransomware Readiness toolkit and the vulnerability review provided to the SMB, they saw a slight improvement in their vulnerabilities and a significant improvement in their security posture. The information provided that they did not know before allows this business to be one step ahead of the rest and minimize the risk of the ransomware attack. The hope is that more SMBs will follow in their path and put more thought into their security to prevent any possible attacks in the future.

Future Works

From This project, many things could be improved, starting with performing this process on multiple SMBs to understand better how practical the toolkit and review can be. A tool can also be created for the toolkit that can scan Windows machines and give a score on how vulnerable they are to typical ransomware vulnerabilities. Additionally, a recommendation by the SMB is to perform most of the review and analysis in person with the SMB so that if they have questions, they are able to get answers in real time instead of waiting for an email. There can also be a more tailored scan focusing on ransomware instead of a full basic scan and sifting through the results to see if there are any vulnerabilities related to ransomware. Lastly, from the scan, the output goes to a ransomware ecosystem dashboard that will provide graphics and tables that would be earlier for an SMB to understand. Small to medium businesses are always going to be a main target for cybercriminals, especially when the understanding of cyber security is complete and expensive. By providing resources like the ones in this project, the hope is to start a culture shift where SMBs will notice that cyber security can be easy and cheap with the right knowledge and resources.

REFERENCES

Anghel, M., & Racautanu, A. (2019, June 2). *A note on different types of ransomware attacks*. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2019/605

August, T., Dao, D., & Niculescu, M. F. (2019, May). Econinfosec. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_60.pdf

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017, June). *(PDF) ransomware: A survey and trends*. ResearchGate. https://www.researchgate.net/publication/317380115_Ransomware_A_Survey_and_Trends

Berrueta, E., Morato, D., Magana, E., & Izal, M. (2019). A survey on detection techniques for cryptographic ransomware. *IEEE Access*, *7*, 144925–144944. https://doi.org/10.1109/access.2019.2945839

Bijitha, C. V., Sukumaran, R., & Nath, H. V. (2020). *A survey on ransomware detection techniques*. SpringerLink. https://link.springer.com/chapter/10.1007/978-981-15-3817-9_4

Chen, P.-H., Bodak, R., & Gandhi, N. S. (2021a, June 22). *Ransomware recovery and imaging operations: Lessons learned and planning considerations - journal of imaging informatics in medicine*. SpringerLink. https://link.springer.com/article/10.1007/s10278-021-00466-x

Corbet, S., & Goodell, J. W. (2022, February 12). *The reputational contagion effects of ransomware attacks*. Finance Research Letters. https://www.sciencedirect.com/science/article/abs/pii/S1544612322000411

De Gaspari, F., Hitaj, D., Pagnotta, G., De Carli, L., & Mancini, L. V. (2022). Evading behavioral classifiers: A comprehensive analysis on evading ransomware detection techniques. *Neural Computing and Applications*, *34*(14), 12077–12096. https://doi.org/10.1007/s00521-022-07096-6

Hanks, C. (2024, August 2). *Small business ransomware: What you need to know: VEEAM*. Veeam Software Official Blog. https://www.veeam.com/blog/small-business-ransomware.html

Javed Butt, U., Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019). Ransomware threat and its impact on SCADA. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 205–212. https://doi.org/10.1109/icgs3.2019.8688327

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security*, *16*(4), 195–202. https://doi.org/10.1080/10658980701576412

MacColl, J., Hüsch, P., Mott, G., Sullivan, J., Nurse, J. R. C., Turner, S., & Pattnaik, N. (2024, January 16). *The scourge of Ransomware: Victim insights on harms to individuals, organizations and Society*. Kent Academic Repository. https://kar.kent.ac.uk/104628/

MCAFEE DEPLOYS ONLINE PROTECTION SOLUTION. (2023). *Computer Security Update*, *24*(7), 6–8. https://www.jstor.org/stable/48733724

National Institute of Standards and Technology. (2020). CVE-2020-4004, VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG), Workstation (15.x before 15.5.7), Fusion (11.x before 11.5.7) contain a use-after-free vulnerability in the XHCI USB controller. Retrieved 2024, from https://nvd.nist.gov/vuln/detail/CVE-2020-4004

National Institute of Standards and Technology. (2020). CVE-2020-4005, VMware ESXi (7.0 before ESXi70U1b-17168206, 6.7 before ESXi670-202011101-SG, 6.5 before ESXi650-202011301-SG) contains a privilege-escalation vulnerability that exists in the way certain system calls are being managed. Retrieved 2024, from https://nvd.nist.gov/vuln/detail/CVE-2020-4005

National Institute of Standards and Technology. (2020). CVE-2020-5344, Dell EMC iDRAC7, iDRAC8 and iDRAC9 versions prior to 2.65.65.65, 2.70.70.70, 4.00.00.00 contain a stack-based buffer overflow vulnerability. Retrieved 2024, from https://nvd.nist.gov/vuln/detail/CVE-2020-5344

National Institute of Standard and Technology. (2022, March 4). *Cybersecurity Framework v1.1 - CSF Tools*. CSF Tools - The Cybersecurity Framework for Humans. https://csf.tools/reference/nist-cybersecurity-framework/v1-1/

National Institute of Standards and Technology. (2023). CVE-2023-48795, The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. Retrieved 2024, from https://nvd.nist.gov/vuln/detail/CVE-2023-48795

National Institute of Standards and Technology. (2023). CVE-2023-51384, In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. Retrieved 2024, from https://nvd.nist.gov/vuln/detail/CVE-2023-51384

National Institute of Standards and Technology. (2023). CVE-2023-51385, In ssh in OpenSSH before 9.6, OS command injection might occur if a username or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. Retrieved 2024, from https://nvd.nist.gov/vuln/detail/CVE-2023-51385

SAKELLARIADIS, J. (2022). *Behind the Rise of Ransomware*. Atlantic Council. http://www.jstor.org/stable/resrep42765

Tahir, R. (2018, March). *A study on malware and malware detection techniques*. MECS Press. https://www.mecs-press.org/ijeme/ijeme-v8-n2/IJEME-V8-N2-3.pdf

Veeam. (2023). *What is ransomware?: VEEAM*. Veeam Software. https://www.veeam.com/glossary/what-is-ransomware.html

VMware. (2021). VMware Security Advisory VMSA-2021-0002, VMware ESXi and vCenter Server updates address multiple security vulnerabilities (CVE-2021-21972, CVE-2021-21973, CVE-2021-21974). Retrieved 2024, from https://www.vmware.com/security/advisories/VMSA-2021-0002.html

Zimba, A., & Chishimba, M. (2019, January). *(PDF) understanding the evolution of ransomware: Paradigm shifts in attack structures*. ResearchGate. https://www.researchgate.net/publication/330734778_Understanding_the_Evolution_of_Ransomware_Paradigm_Shifts_in_Attack_Structures

APPENDIX A
Ransomware Readiness Survey

Nessus Scan:

- How many different subnets do you have in your company?
- Is your IT infrastructure on premises, in the cloud, or hybrid?
- Which Subnets, servers or on premise/ BYOD devices would you like to be scanned by Nessus? Note: If you have BYOD policies in effect, please consider connecting personal devices to the company network during the scan
    1. Servers (provided Number of servers and Ip addresses):
    2. Subnets (provided Subnet ranges):
    3. On premise/BYOD devices (provided number of devices and Ip addresses):

Ransomware Awareness:

- How familiar are you with the types and impacts of ransomware affecting similar-sized organizations in your industry?
- How often does your organization update its cybersecurity training session to include the latest ransomware threats and tactics?
- Describe how your organization identifies and addresses emerging security vulnerabilities and threats related to ransomware.
- Evaluate your organization's readiness to respond to a ransomware attack, including personal, technology, and procedural perspectives.

Policies and Procedures:

- List specific policies and technical controls in place that directly mitigate the risk of ransomware attacks?
- How does your organization maintain an up-to-date inventory of all IT assets, and how often is it reviewed?
- Describe the ransomware recognition and response training provided to employees, including frequency and content.
- Is there a mandatory policy for employees to report suspected phishing attempts or suspicious behavior? How is it enforced?
- How does your organization classify data sensitivity, and what protections are in place for each classification level?
- How does your organization classify data sensitivity and what protections are in place for each classification level
- Describe how your organization's incident response plan is tested, including the types of drills conducted in the past year.

- What is your organization's defined Recovery time objective (RTO) for critical systems in the event of a ransomware attack?
- Detail the process and frequency of updating and testing your organization's response plans, including coordination with external third parties.

Technical Controls:

- How does your organization continue monitoring program function to detect signs of compromise, including ransomware indicators?
- List the types of security solutions deployed at your organization and ow they are integrated to protect against ransomware?
- Provide details on the currency and scope of security software on all organizational devices.
- How is your centralized logging system utilized to identify potential ransomware threats?
- Explain the ransomware segmentation strategy used to protect critical systems against ransomware spread.
- How does your organization manage and monitor the use of privileged accounts to reduce the risk of ransomware exploitation?
- Detail the patch management policy for operating systems, including timeframes for critical patches related to ransomware threats.
- Describe your schedule for application updates and patches particularly focusing on security updates.
- How does your organization manage cybersecurity risks associated with third party vendors, especially those with network access privileges?

SMB Ransomware Readiness Toolkit

This vendor-neutral toolkit provides a comprehensive Ransomware Security Checklist designed for you to ensure that each listed item is implemented in some manner within your business. The ransomware resources I have included are extensive, comprising websites for learning more about ransomware, frameworks to aid in prevention, and online tools offering open-source intelligence on suspicious IP addresses, files, or domains. Additionally, there is an extensive list of tools that can assist in preventing ransomware. While you do not need to use all these tools, having at least one from each category—or a similar tool, as it is impossible to list every available option—will significantly enhance your security against a ransomware attack.

Adhering to this toolkit will significantly assist in mitigating and preparing for a ransomware attack.

Checklist:

- **Identifying assets**
  - This step is great about identifying all hardware, software, data, and digital assets critical to your business, which could be targeted by a ransomware attack
  - Best practice:
    - Inventory all digital assets (Documents, Software, all assets that are in digital form)
    - Inventory all hardware assets (server, workstations, laptops, mobile devices)
    - Identify all assets that are critical (financial record, customer databases, all assets that are critical to business operation)
    - Possibly using an asset management software which can track, mange, and optimize your assets an example of that tool is Freshservice
  - Resources:

        - This a link to the NIST cybersecurity framework Identify category
        - This is a link to the CIS Controls v8 – Control 1: Inventory and Control Enterprise Assets
- **Security Controls**
    - This step is to make sure that there are controls in place to create a layer defense within the organization to reduce the risk of a ransomware attack.
    - Best Practices (Below are some of the most important controls when trying to mitigate ransomware, there a lot more controls provided within the resources):
        - Endpoint Protection – using antivirus and anti-malware software to prevent malicious malware from infecting your endpoints.
        - Backup and Recovery – regularly back up your critical data to be stored offline or in the cloud and test those backups to make sure they can be recovered
        - Patch Management – regularly update your software and operating systems to protect against vulnerabilities that are exploited by ransomware attackers
        - Data encryption – encrypt all sensitive data that is at rest and in transit to prevent data exfiltration for a ransomware attack
    - Resources:
        - This is a controls implementation guide SMBs from CIS that provides more controls: Link
        - This is a list of the top 20 controls by SANS: Link
- **Access Controls**
    - This step is to make sure there are controls in place that reduce access to sensitive information on systems to minimize the risk of ransomware gaining access to these assets.
    - Best Practices:
        - Multi-Factor Authentication (MFA) - make MFA a requirement for access to critical application and systems
        - Least Privilege Access – use this principle to limit user access rights to only what they need for their roles
        - Account Monitoring and Auditing – make sure to track user activity will allow for you to detect early signs of ransomware attacks
    - Resources:
        - CIS Control 5: Account Management: Link
        - CIS Control 6: Access Control Management: Link

- **Network Segmentation**
  - This is the process of isolating different network segments to contain a ransomware attack by preventing the spread of the attack.
  - Best Practices:
    - Use Firewalls or VLANs to restrict communication between segments
    - Divide the network into subnetworks such as networks for servers, workstation, guest Wi-Fi
    - Keep backups isolated from production networks to prevent ransomware spread
  - Resources:
    - DIY Guide to Network Segmentation: Link
    - CISCO resource on Network Segmentation: Link
    - CIS Control 12: Network Infrastructure Management: Link

- **Monitoring and Logging**
  - This step is for ensuring effective monitoring and logging to help detect suspicious activity early, allowing quick response to any ransomware attempts.
  - Best Practices:
    - Use SIEM tools such as Splunk or the ones provided below
    - Regularly review logs for unusual login patterns, large data transfers, and other anomalies
    - Use alerts for indicators of compromise that relate to ransomware
  - Resources:
    - CIS Control 13: Network Monitoring and Defense: Link

- **Incident Response Plan**
  - Having an incident response plan ready and in place can allow for your team to be prepared to swiftly and structurally respond to any incident including a ransomware attack.
  - Best Practices:
    - Have clear defines roles and responsibilities in case of a ransomware attack
    - Create an action checklist which includes isolating affected system and notifying relevant parties
    - Make sure to practice this plan regularly with tabletop exercise, simulations, or paper reviews
  - Resources:
    - NIST 800-61 Revision 2 specifically Chapter 3: Link

- SANS Incident Handlers Handbook: Link

- **Awareness Training**
  - Having regular training and activity to educate employees on identifying phishing email, ransomware tactics, and security best practices can reduce the risk of an incident happening. Employees are the weakest link for a business, so having them be aware is beneficial
  - Best Practices:
    - Run monthly or quarterly phishing simulation exercises
    - Train employees to report suspicious emails and links
    - Have an easy-to-understand guides and refresher courses on safe data handling
    - Conduct annual cybersecurity awareness training
  - Resources:
    - KnowBe4 guide to security awareness Training: Link
    - CISA Security Awareness Training: Link

- **Backup and recovery testing**
  - Having secure and regular backups is a critical defense against ransomware as if you were to be attacked you can easily recover from a backup. But testing these backups is just as important to make sure they are functional and can be restored quickly.
  - Best Practices
    - Schedule automated backups for critical data and store that backup either offline or in the cloud
    - Perform quarterly backup restoration test to confirm that the data can be recovered swiftly
    - A good back practice is a full and incremental backup to ensure both latest and long-term records are secured
  - Resources:
    - CIS Control 11: Data Recovery: Link

- **Vulnerability Assessments and Patch Management**
  - Having regular vulnerability assessments and patches can help reduce risk by identifying any unpatched software or misconfiguration that ransomware attackers often exploit.
  - Best Practices:
    - Perform scheduled automated vulnerability scans using tools like Nessus or Qualys

        - Create a patch management schedule and prioritize critical patches, especially for operating systems, web servers, and applications
        - Perform weekly vulnerability scans and monthly patch updates for high-risk assets
    - Resources:
        - CISA Recommended Practice for Patch Management of Control Systems: Link
        - CIS Control 18: Penetration Testing: Link

- **Email Security**
    - Email being one of the primary entry points of ransomware, having robust email security and anti-phishing systems in place are essential for reducing risk of an incident.
    - Best Practices:
        - Have spam filtering, antivirus, and link scanning tools on email platforms a valuable tool is Microsoft Defender for Office 365
        - Have Domain based Message Authentication, reporting, and conformance (DMARC) to prevent email spoofing
        - Have spam filter in place to block suspicious emails and prevent phishing attempts
    - Resources:
        - Here is a DMARC Guide by the Global Cyber Alliance: Link
        - CIS Control 9: Email and Web Browser Protections: Link

- **Endpoint detection and response**
    - Having endpoint detection and response systems in place on endpoint can monitor for suspicious behavior and enable rapid response to stop a ransomware attack before it spreads
    - Best Practices:
        - Have a EDR solution such as the tool listed below to monitor end points and detect anomalies
        - Configure alerts for unusual behavior, such as rapid file encryption or disabling of security tools.
        - Use a EDR solution to isolate infected devices when ransomware is detected
    - Resources:
        - EDR Deployment: the complete Hot-to-guide: Link
        - CIS Control10: Malware Defenses: Link

Important Websites:

Here are multiple resources for multiple different organizations that can help you with getting more informed on ransomware and how to better protect, mitigate, and respond to this sort of attack. There are also websites that can be used to identify any malicious files, IP addresses, and domains.

- **NIST**

From the National Institute of Science and Technology there are five resources that I want to highlight. Here I will give a brief overview of each resource from NIST:

- Tips and Tactics: Preparing Your Organization for Ransomware Attacks

For this resource it provides tips to protect your organization from ransomware and tips on how to recover from a ransomware attack. This is great for gaining a basic understanding of the basics of protecting and responding to ransomware. Below are the tips mentioned the document will have more detail for each point:

Protecting you Organization:

- Use of antivirus always
- Keep all computer and applications patched
- Use security products to block access to know ransomware sites
- Configure operating systems or other applications to only allow authorized applications
- Restrict or prohibit use of personal devices on the network

Tips for users:

- Use only standard account not admin accounts
- Avoid personal applications and websites
- Avoid opening files and clicking links from unknown sources

Recovering from Ransomware

- Develop and implement and incident recovery plan
- Plan, implement, and test your data backups and restorations strategies
- Maintain an up-to-date list of internal and external contacts

- NIST Cybersecurity Framework Quick Start Guide

This resource is a quick start guide for implementing the NIST cybersecurity framework. It goes over all five domains and gives a few pointers for each. Below is each point and a couple pointer for each the document will have a more detailed description for each point:

  - Identify
    - ID critical processes and assets
    - Maintain hardware and software inventory
    - Etc.
  - Protect
    - Train Users
    - Conduct regular backups
    - Manage access to assets and information
    - Etc.
  - Detect
    - Maintain and Monitor logs
    - Test and update detection processes
    - Etc.
  - Respond
    - Ensure response plans are tested
    - Ensure response plans are updated
    - Etc.
  - Recover
    - Ensure recovery plans are updated
    - Communicate with internal and external stakeholders
    - Etc.

- Getting Started with Cybersecurity Risk Management: Ransomware QuickStart Guide

This resource is very similar to the above resource as it goes through the five domains of the NIST cybersecurity framework. But the difference of this resource is it goes into more detail of each point and adds points to a few domains. Below are the added points there being a detailed description for each point within the document:

  - Respond
    - Develop a response plan
  - Recover
    - Test and update recovery plans

NISTIR 8374: “Ransomware Risk Management: A Cybersecurity Framework Profile”

For this resource it is a report that defines a ransomware profile which identifies security objectives from the NIST framework that help with preventing, responding, and recovering from ransomware. This profile can be used as a guide to manage the risk of ransomware attacks. Below is a link to the PDF of the report and goes into detail on the profile and provides additional resource:

NIST Ransomware Framework PDF

- Protecting your Data from Ransomware and Other Data Loss Events

This resource talks about a few recommendations on what a business should do to protect your data from either ransomware of other data loss events. Below is the recommendation that provided the resource will have a more detailed description of each point the resource also provides a website that provides detailed info on how to implement backup solutions:

  - Identify files and process for backups
  - Determine frequency of backups
  - Test backups and recovery plan
  - Website: www.nccoe.nist.gov/msp

- **CISA**

The Cybersecurity and Infrastructure Security Agency has two sites that I would like to highlight and here I will provide a summary of those resources:

- Stop Ransomware Website

This website provides three great resources starting with the Ransomhub which covers some information on ransomware such as technical details where it talks about how ransomware attack operates with going over the vulnerability’s actor typical exploit, how discovery happens as well as going over some indicators of compromise. Below is a link to this resource it will provide more detail:

RansomHub

The second resource provided is a guide of simple practices that an organization can do to help prevent a ransomware attack. Below is a link to this resource look and see what you link would be best to follow:

Stop Ransomware Guide

The last resource is a guide on what to do if your organization were to be hit by a ransomware attack. It goes through the domain of an incident response plan so detection and analysis, reporting and notification, containment, and eradication, lastly, recovery and post incident analysis. Below is a link to this resource for more detail:

I've Been Hit by Ransomware

- Ransomware Executive One pager

This resource is a quick information one pager that covers different preventative measures an organization can implement. It also goes over the different types of ransomwares. Below I list out the different ransomware as that is something that I have yet to touch on. I would recommend looking at this resource to learn more about these infamous ransomwares:

  - Cryptowall
  - CTB-Locker
  - TeclaCrypt
  - SAMSAM
  - Locky

- **Cyber Readiness Institute**

The CRI has a downloadable ransomware playbook that goes over some great points on how to protect, respond, and recover from a ransomware attack. It also has an interesting information guide that you can use to map out what to do depending on what has happened. Below is a link to download the PDF:

Ransomware Playbook

- **FTC**

The Federal Trade Commission has a resource that goes over the general information of what ransomware is. It talks about how ransomware could happen such as the use of phishing emails, exploits from server vulnerabilities, infected websites, and malicious online ads. This resource then goes over 4 of the best ways to protect your business from ransomware attacks. Lastly, this goes over what to do if your business is attacked. Below is a link to this resource:

Ransomware Guide

- **AbuseIPDB**

This website is a great resource for identifying if an IP address or domain name is malicious. To use this site, you take any IP or domain that you know more about and add it to the input box and search. It will show the amount of time it has been reported, the domain, ISP, location (country and city), and the percentage of how malicious.

abuseipdb.com

- Important notes:
  - If the IP shows <10% malicious it is not malicious as sometimes there are automated systems that make reports, and they can be wrong.
  - You should be worried about IPs that show >50%.

- **VirusTotal**

This tool is great for determining if either a file hash, IP address, or Domain is malicious. Inputting one of those pieces of data will provide a list of vendors and if those vendors marked what it inputted as malicious. This website will also give other detailed information on what you entered such as the company that owns the IP/domain or if you input a hash it will say with the program is. This website is great for figuring out if any IPs, Domains, or file hash you come across are malicious.

VirusTotal.com

Important Notes:

- If you find that something you imputed has about 3-5 flags typically it does not mean anything as each vendor sets their detection differently and some vendors make their product super sensitive.

- **Hybrid Analysis**

This website is used to drop suspected files in and have them tested within a sandbox environment. This is great for determining if any files you deem suspicious are. This website also provides detailed information on what to file does such as software change it may perform or network call outs it may make.

HybridAnalysis.com

Important Notes:

- This website does require you to make an account it is free

Tools:

- **Backup Solutions**
  - Veeam Backup
    - This is a data protection solution that offers backup and recovery for virtual, physical, Network attached Storage (NAS), and cloud environments
    - Cost for this solution varies but for a 1 year 5 instance license it will run for about $428. They do provide a pricing calculator at this link. Price Calculator
    - This tool is great for businesses that need data protection across different infrastructures such as on premise and cloud
    - Veeam Product Guides
  - IDrive
    - A backup solution that protects data through online backups so that your data is available when needed and stored off site.
    - The pricing for this solution allows for multiple devices for a single device. Pricing Plans
    - This is a great easy to use cost effective cloud backup.
    - Machine Backup instructions for a single machine, IDrive 360 Videos for cloud backups
  - Microsoft Azure Backup
    - Backup solution provided by Microsoft It is a great reliable solution for backing up and recovering data from azure instances as well as on premises.
    - Here is a pricing website that provides a pricing calculator. Azure Backup Pricing
    - This tool is great for businesses that utilize Microsoft products, especially within a hybrid environment.
    - Azure Backup Doc
  - AWS Backup
    - Solution provided by Amazon that gives centralized backups for AWS instances as well as on premise resources.
    - AWS Backup Pricing
    - Best for businesses that heavily use AWS instances.
    - AWS Backup Doc
  - Google Cloud Backup
    - Secure and scalable backup options to google cloud
    - Google Backup Pricing

        - This is great for businesses to utilize google workspaces or google cloud
        - Google Backup Doc
    - Acronis
        - This is a backup solution that provides active protection to prevent ransomware
        - There is a pricing calculator, but it requires an account creation
        - This solution is great to provide backup and ransomware protection
        - Installation Guide

- Endpoint Protection
    - Malwarebytes
        - This is an antivirus software that can provide real-time protection for malware and ransomware.
        - This software has a free version but if you want to have automatic scanning and more features there is a premium version. Malwarebytes Teams Price
        - This is an affordable and easy to use software
        - Video for Malwarebytes installation
    - Microsoft defender
        - This is a built-in anti-virus and anti-malware for windows with threat detection and incident response.
        - Windows defender comes with windows, so it is free
        - This software is great for businesses that heavily use Windows systems.
    - Sophos intercept X
        - This is an advanced endpoint protection that provides ransomware prevention. It also provides protection for mobile devices.
        - Pricing goes by per user here is some estimates on pricing for this tool
        - This is a great tool that provided comprehensive endpoint protection
        - This is an installation guide for windows

    - CrowdStrike Falcon Go

        - This is a cloud-based endpoint protection that provides AI based threat detection to prevent ransomware and data breaches
        - This software is about $60 per device. Here is the purchasing option
        - This is great for businesses that seek lightweight, cloud based, security with quick implementation
        - Since the Falcon GO software is new there is no installation guide for it

- Network Security
    - PfSense
        - This is a firewall and router with VPN, NAT, and intrusion detection capabilities.
        - This software is free as PfSense is open source
        - This a great cost-effective tool but does need some expertise in the tool to full utilize it
        - Here is the download page and a page for getting started
    - Cisco Umbrella
        - This is a cloud-based DNS security and web filtering solution provided by Cisco
        - Pricing depends on the number of uses here shows the pricing
        - This tool is great for businesses that want to provide DNS layer security against malware and phishing sites which could have ransomware
        - This is a quick start guide
    - Quad9
        - This is a DNS security tool that uses privacy and security in blocking domains and filtering internet traffic.
        - This is a free and public DNS service
        - This is great for businesses that want a free and easy to implement DNS security solution
        - This is a Windows 10 installation guide
    - OpenVPN
        - This is a VPN solution that provides secure remote access and encrypted connections
        - This is open-source software, so it is free
        - This is great cheap solution that businesses can use for secure connections for remote users
        - This is an installation guide for Windows

- NordLayer
    - This is a business focused VPN solution provided by NordVPN
    - The pricing for this tool varies here is the pricing options
    - This is a great tool that is easy to use
    - This is a getting started guide
- Snort
    - An intrusion detection and intrusion prevention system for network monitoring and real time threat detection
    - This is an open-source tool, so it is free
    - This tool does require some expertise so if a business does have someone that understands this tool it can be a great asset
    - This is some deployment guides
- Suricata
    - This is an advanced intrusion detection and intrusion prevention system that has deep packet inspection, protocol detection, and network monitoring.
    - This is an open-source tool, so it is free
    - This is also a tool that requires some expertise but is great for businesses that need a robust network monitoring system
    - This is a quick start guide

- Email Security
    - PhishTitan
        - This is an email security solution that provides anti-phishing, and malware protection features
        - This is a link to get a price
        - This is great for businesses that need an email security tool that is easy to use
        - This a links for startup guides for Customer admin and MSP admin
    - Barracuda Essentials
        - This is an email security solution with advanced threat protection, archiving, and data loss prevention
        - This is a link that can help you get pricing information
        - This is great for businesses that need email continuity and advanced threat protection
        - This is some quick startup guides
    - Mimecast

        - This is an email security platform with phishing protection, archiving and email continuity
        - This link shows that different plans offered
        - This is great for businesses that need email threat protection and continuity
        - This is a connect guide
    - Sophos Email
        - This is an email security tool that is provided by Sophos
        - This link can get pricing, but you need to fill somethings out
        - This is great for businesses that want great email security from a known vender

- Monitoring and Response
    - Wazuh
        - This is a security monitoring and incident response platform that can provide intrusion detection and vulnerability scanning
        - This is an open-source tool, so it is free
        - This is great for businesses that need a customizable security monitoring solution
        - This is a startup guide
    - Graylog
        - This is a centralized log management and SIEM solution for monitoring, analyzing, and visualizing security data
        - This is pricing
        - This is great for a business that needs a scalable log management solution for threat detection
        - This is a great startup guide
    - Zabbix
        - This is a network and infrastructure monitoring with real time tracking and alerts
        - This is a free tool
        - This is great for businesses that need real time monitoring for servers and networks.
        - This is a quick start guide
    - SureLog
        - This is a log management and SIEM solution for security analysis and reporting
        - This solution can cost a one-time fee of 2,000

        - This is great for businesses that need log management for compliance and threat detection
        - This is a user guide
- Vulnerability Scanning
    - OpenVAS
        - This is a vulnerability scanner to assess network security and identify vulnerability
        - This is open source, so it is free
        - This is great for businesses that need a free tool for vulnerability scanning
        - This is a setup guide
    - Qualys
        - This is a cloud-based vulnerability management tool that provides automated scanning and reporting
        - This tool has a free version and subscription here is a link to see subscription plans
        - This is great for businesses that need a cloud based scalable vulnerability management tool
        - This is a great getting started guide
    - Nessus Essentials
        - This is a version of Nessus that provides scanning for up to 16 Ip addresses
        - This is the free version of Nessus
        - This is great for businesses that need to scan high risk assets
        - This is an installation guide

- Security Awareness training
    - KnowBe4 Free Phishing Test
        - This is a phishing simulation tool to test employee awareness and enhance email security practices
        - This is a link to pricing
        - This is great for businesses that what to improve employee phishing identification skills
    - Cofense PhishMe Free Edition
        - This is a too, for phishing email simulation and education for employees
        - This is a free tool
        - This is great for businesses that want to strengthen employee's ability to detect phishing emails

- Multi Factor Authentication
    - Microsoft Authenticator
        - This is an MFA app for one-time passwords and push notification, designed to integrate with Microsoft products
        - This is a free app
        - This is great for businesses that use Microsoft products or azure
    - Google Authenticator
        - This is MFA app providing time-based, one-time passwords for a range of applications
        - This is a free app
        - Great for businesses that need a simple cost-free solution for MFA
    - Duo Security
        - This is a scalable MFA solution that offers various authentication methods including push notification and codes.
        - It can be free or for payment depending, this link shows the pricing
        - This is great for businesses that have a diverse amount of application that need flexible MFA options

APPENDIX C

Ransomware Readiness Outro Survey

Thank you for allowing me to assist in enhancing your ransomware defense and security posture. I strived to provide comprehensive and practical resources and solutions. Your feedback will be crucial in letting me know what I did correctly and what I should improve in the future to ensure that I can meet future expectations. Please take a few minutes to complete this survey.

Ransomware Readiness Toolkit:

1. How satisfied are you with the Ransomware Toolkit provided? What aspects specifically?

- Very Satisfied
- Satisfied
- Neutral
- Dissatisfied
- Very dissatisfied

Explain:

2. How clear and understandable was the content of the Ransomware Readiness Toolkit?
    - Very Clear
    - Clear
    - Average
    - Unclear
    - Very Unclear
3. Where are the tools and resources provided in the toolkit easy to use or implement?
    - Very Easy
    - Somewhat Easy
    - Neutral
    - Somewhat Difficult
    - Very Difficult
4. Which of the toolkit recommendations were you able to implement? (Please list the tools below)
5. Were there any tools or resources provided that you did not use or would not recommend using? (Please list them below and provide a reason)
6. If any tools or resources were used, how effective were they for your business? (If so, please provide an explanation on how)
    - Very Effective

- Effective
- Moderately Effective
- Slightly Effective
- Not Effective

Explain:

7. In case of a ransomware threat, do you feel better prepared to handle the incident because of the toolkit?
   - Yes
   - Somewhat
   - No
   - Not Sure
8. Please provide any suggestions or comments on how I can improve the toolkit.
9. Would you be interested in further assistance or additional resources related to cybersecurity? (Provided by either Me {Colin Choquette} or UNCW)
   - Yes
   - No

Vulnerability Review:

10. How well did the vulnerability review help you understand the current security posture of your systems?
    - Very Well
    - Somewhat Well
    - Neutral
    - Somewhat Not
    - Very Not
11. Were the descriptions of the vulnerabilities clear and easy to understand?
    - Very Clear
    - Clear
    - Average
    - Unclear
    - Very Unclear
12. How adequate do you find the remediation steps provided for the vulnerabilities identified?
    - Very adequate
    - Somewhat adequate
    - Neutral
    - Somewhat Not
    - Very Not

13. Were the resources provided for further Learning and Remediation Helpful? (Please explain how)
    - Very Helpful
    - Somewhat Helpful
    - Neutral
    - Somewhat Not
    - Very Not

Explain:

14. How easy was it to implement the recommended remediations for the vulnerability review?
    - Very Easy
    - Somewhat Easy
    - Neutral
    - Somewhat Difficult
    - Very Difficult
15. How satisfied are you with the thoroughness of the vulnerability review?
    - Very Satisfied
    - Satisfied
    - Neutral
    - Dissatisfied
    - Very dissatisfied
16. What improvements, if any, would you suggest for future vulnerability reviews? (Please provide some recommendations below)
17. From an SMB perspective, do you have any additional comments or insights you would like to share about your experience with this project? (Please provide them below)