MUNICIPAL GOVERNMENTS AND THE NEED FOR CYBERSECURITY

by
Hector Rolando Ocampo

A thesis to the Department of Information and Logistics Technology,
College of Technology
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCES

in Cybersecurity

Chair of Committee: Dr. Chris Bronk

Committee Member: Dr. William Arthur Conklin

Committee Member: Dr. Jim Granato

University of Houston
April 2021

DEDICATION

I would like to dedicate this thesis to my wife and daughter, Crystal and Emma. Thank you for your unending support during this journey. Crystal, thank you for always reminding me to focus on God above all else. Emma, thank you for being my late-night study buddy and for always crashing my class meetings. I promise to help you build a robot one day.

ACKNOWLEDGEMENTS

I would like to thank Dr. Chris Bronk for his advice and guidance when writing this thesis. I started my journey in cybersecurity as his student and I am beyond grateful to be ending it as his student. I would also like to thank the individuals who provided me with valuable insight while this thesis was still forming, you know who you are.

ABSTRACT

Cyberattacks on municipal governments have been on the rise, usually causing millions of dollars in damage. Despite their frequency, municipal governments are still struggling to mount a solid front against these attacks. This is partly due to a lack of resources, a lack of managerial oversight, and a lack of collaboration. Usually, these shortcomings manifest in poor cybersecurity policy creation and implementation, causing a snowball effect that can prove to have dire consequences. Even with this knowledge, municipal governments can find themselves caught in a vicious cycle that is further exacerbated by an overall poor security posture.

This thesis seeks to put these shortcomings into perspective by providing background information into the inner workings of municipal government and the services they provide. Secondly, it will use six case studies of American cities where cyberattacks caused massive amounts of damage. Lastly, it will provide recommendations that can help a municipality still gain valuable experience and develop proper security policy in the absence of resources.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

Municipal governments provide attackers with high-yield, low-cost targets in which to focus cyberattacks. This usually stems from the fact that municipal governments are usually underfunded, understaffed, undertrained, or all three. Given that municipal governments function autonomously and do not necessarily follow a state or government defied cybersecurity baseline, gaps usually form in both the knowledge base and experience pool of different municipal governments. While cyberattacks come in all shapes and sizes, ransomware is a typical culprit today. Ransomware is a subset of malware (software intentionally designed to cause harm) that enters a computer network environment and self-propagates through all connected machines. Afterwards, it proceeds to encrypt all user data. Users are then greeted with an on-screen message detailing the dollar amount of regaining their data. Ransomware usually enters a network through a phishing email—a type of email meant to mimic a legitimate sender with the goal of compromising credentials. The user inadvertently runs malicious code that allows the ransomware to enter. Even though some ransomware enters a network environment through different means, the final outcome is the same.

This problem has grown exponentially and has caused multiple municipal governments' infrastructure to slow down to a crawl—usually causing government offices to revert back to pen and paper recording.[1] It also places municipal government in a position where they have to pick their proverbial poison—do they pay the ransom or do they do their best to restore a backup? Paying a ransom is not a full proof method as it will often let attackers know that they now have a loyal customer. Therefore, future attacks may become more complex in order to compromise the same system. There exists a palpable uneasiness in trusting a stranger that just compromised

a system, completely destroying any confidence in a clean deal taking place. There also exists the possibilities of the decryption tools not being able to decrypt the entire data.

Despite the numerous occurrences of devastating damage caused by ransomware, why are some cities still ill equipped to handle them? This thesis seeks to answer this question by analyzing the anatomy of a small city, the functions that make them desirable to attackers, the challenges they face, and providing six case studies in which these factors came together to cause serious cyber incidents. Additionally, it will look at their lasting and transformative impact on the municipalities in which they occurred. In order to provide insight into the impact of these attacks, three security professionals have been interviewed—one from a small city environment, one from a university environment, and one from a government agency environment. Using their insight, best practices and strategies will be presented at the end of the paper.

II. THE ANATOMY OF A SMALL CITY

When thinking of small city (of roughly 20,000 people or less), it might be easy to imagine a quiet atmosphere in which the community is well acquainted with each other and the fire chief, emergency response coordinator, and IT security professional are well-known faces. The reality of the situation is that these three people, with different job duties, are usually conglomerated into one person. Whether it is the fire chief, the economic developer, or the police chief, these individuals usually find themselves conducting a Dr. Seuss-like balancing act in which they must fulfill all of their duties, in addition to cybersecurity. This balancing act is usually the result of cities making due with smaller budgets and an understaffed workforce. While this is not always the case in every small city, it is worth noting that some small cities prioritize cybersecurity as the "plus one" of city infrastructure—a branch that has been tacked on to existing city infrastructure. Given the current online presence that government offices have, why is cybersecurity not held is a higher regard? Simply put, this is largely attributed to the fact that emergency responses for other kinds of emergencies have existed for decades or centuries and have evolved organically with society. For example, firefighters were once concerned citizens that would use their horse drinking buckets to stop the destruction produced by fires. Today, they employ state of the art water systems and additional tools to aid in rescue efforts. The ability to realize the practical and optimal use of this new technology evolved in conjunction to the technology itself, with each informing the next evolutionary step of the other. In essence, today's fire departments have inherited the situational awareness, procedure development, and emergency response plan capacity that have been refined and reworked by their predecessors. A byproduct of this phenomenon is quick and flexible responses to emergency events.

Cybersecurity, in contrast, is still in its infancy and society has barely started to embrace its importance in day-to-day operations—leaving a long path of trial and error ahead of it.[2] As such, it becomes difficult to understand the complexities involved in a cyber response, much less an ideal way to approach them. While the causes of fires can be adequately predicted and avoided, the point of entry for cyberattacks constantly change and adapt to the very technologies that try to prevent and detect them, leaving cybersecurity professionals in an everchanging cat and mouse game.

The optics of a burning building or a broken leg evoke a more visceral response within the human psyche. As such, it is easy to place the fire department and ambulance operation in a higher echelon of human and civic priority. This stands in stark contrast to cyberattacks, which usually occur in the quiet and often overlooked realm of cyberspace. While they have been known to, these attacks do not always bring with them explosions or the blaring sirens of ambulance. There have been instances in which industrial systems can be compromised and create such a scene, but many of these attacks are deployed in silence, with only panicked faces and clacking keyboard keys to announce their detection. When viewing emergencies from this perspective, it can almost be seen as negligent to place cybersecurity in the same level as emergency security.

Nevertheless, quietly dispatched malware can have devastating effects. For example, what would happen if a hospital's critical systems were to fall to ransomware? What could happen to the city's water processing plant if it is successfully infiltrated by a foreign adversary? What could happen to a city's residents if all of their social security numbers are stolen in a data breach? Will some of them experience massive financial loss or be charged with numerous crimes committed by a person who stole their identity? Additionally, a successfully deployed

cyberattack has the potential to generate fiscal and bodily harm. In extreme cases, even fatalities. All of these outcomes are viable and have indeed occurred in the modern day. The idea is that not only do these attacks make attackers rich, they innately steal from the citizens and can only work by weakening them—it is a purely parasitic dynamic. The tension is further stressed when determining whether or not to allocate resources to the possibility of devastation or wait until it is knocking at the door. Therein lies the main issue of cybersecurity—it is essentially a game of predictions, all of which could be right or wrong. It can be easier to predict fire hazards or areas where warning signs can be placed. How does one secure the cyberspace of a small town? Where are the main areas of impact? Should more time be spent on developing a backup policy or training employees? There is no one right answer and the answer will be different based on the current level of cybersecurity awareness of a city, coupled with their cybersecurity needs.

III. E-GOVERNMENT

E-government is at the core of modern-day municipalities. E-government refers to the moving of local government transactions to cyberspace.[3] These transactions include license applications, tax payments, and birth certificates, among many others. From a purely transactional perspective, it is more cost effective to incorporate internet operations into municipal infrastructure instead of creating city-specific methods of deploying information. The physical stacks of city records have now been adapted to fit into cyber-service model. These services include the following categories: Government to Government (G2G)—the communication that can occur across multiple levels of government, Government to Citizen (G2C)—the communication that occurs between a citizen and a government entity, and Government to Business (G2B)—the communication that occurs between corporations and the cities that house their facilities.[4] That is to say that the exchanging of information between a different entities and their government has become more accessible than ever. While convenient, this new model also adopts the shortcomings of a cyber-based system. For instance, the Internet was originally only accessible to scholars and computer scientists seeking to communicate with each other. The basic understanding of this communication was trust. Trust was implicitly assumed to be present in each thread of communication that was created. Within that specific context, it made complete sense—everyone was exploring this new frontier and wanted to test its capabilities.[5] This was further aided by the fact that the information being exchanged was of little value to anyone seeking to steal it. Today, the internet has completely evolved. It has largely been democratized and is no longer exclusively populated by scholars. The information shared online is no longer strictly academic or exploratory in nature, it comes in all shapes and size—for better or worse. Social media, business, and the occasional cat meme are now commonalities of

the Internet. Cyberspace is now shared with billions of people and has now become the home of multi-billion-dollar industries and multiple government functions. This is this new standard and it has become virtually impossible to find a business or government without an internet presence.

This new shift in function has created a cause for concern. In order to fulfill a business deal or certain government functions, sensitive information must be shared. This information, in turn, must be secure in order to prevent malicious actors from compromising it. Cybersecurity is defined in terms of CIA—Confidentiality, Integrity, and Availability.[6] Confidentiality is the concept that data should only be accessible to authorized parties. Integrity is the concept that only authorized users can modify the data and that these modifications will be reflected in all concurrent versions of the data. Availability refers to the concept that the data will always be available to authorized users.[7] Cyberspace is now filled with Social Security numbers, driver's license numbers, and bank information—all of which hold value to would-be attackers; the exponential growth of phishing attacks and identity theft serving as undeniable proof[8]. In order to combat these occurrences, an appropriate level of CIA must be maintained in municipal infrastructure.

The complexity of cyberspace can be best illustrated when comparing an in-person county office visit to an intern-based interaction. The person who is physically present at the office just needs to present their government issued identification to a county clerk and they can immediately verify the identity of the person. On the other hand, how can a clerk certify that the communication taking place over the internet has been initiated and continued by the person the user claims to be? The verification of this information falls on the hands of the software employed by the county office's online service. Additionally, that software can only function properly if it is given valid government documents. Social Security numbers, licenses, tax

identification numbers, and entitlement documents serve as the foundation for a variety of business dealings and opportunities. As such, they are held in high regard by malicious actors and must be met with a robust security policy.[9] Over 50 percent of the cyberattacks experienced by municipal governments are data breaches, most of which involved malicious intent. These breaches can easily turn into cases of stolen identity and additional fraud.[10]

The proper deployment of e-government is further complicated by the communication that occurs in its practice. Customers can range from citizens, to businesses, to other government agencies. Information is free flowing, but not all communication channels are equal. That is to say that communication that occurs between a police department and a city's water plant may consist of purely sensitive information, where the communication between a police department and citizens may contain none.[11] Many of the agencies communicating tend to operate independent of each other, but at times may need to coordinate a response together. This paradoxical nature of information sharing is further complicated by the lack of a central authority in e-government. This is largely due to the fact that there are many government bodies working on many missions with many connections already made. There is no one, unifying mission from which e-government can grab onto, further complicating the deployment of comprehensive CIA.

IV. CHALLENGES FACING SMALL CITIES: BUDGETARY CONSTRAINTS

As previously stated, e-government is one of the main functions of municipal governments. E-government can only exist when citizens trust their municipal government. Cyber incidents can completely undermine that trust and destroy government credibility. When considering the adoption and deployment of automated systems, the overall price tag of such technology is often overlooked. The reality is that these services mandate the purchasing of new software and hardware.[12] The aforementioned C-I-A Triad may be neglected in favor of adding another payment purchasing software or other system to the municipal offerings. When compared to commercial entities, which exist for the benefit of their shareholders, government entities exist to serve society. Additionally, the public perception of both of these entities differs completely. Commercial entities are seen as providers for one specific service. Government entities are seen as providers of multiple.[13] For example, supermarket owners can rightfully assume that their customers are there to buy groceries or other daily needs. In contrast, a person visiting a municipal office can be there for a birth certificate, a marriage license, a business license, or perhaps there to vote. This diversity of choices creates asymmetric risk as government offices will need to continually and securely provide them, creating multiple channels in which a mistake can prove to be costly.[14] Given their status as service providers, government offices are usually met with the expectation of perfection at low cost. That is not to say that municipal offices are completely devoid of additional help. National organizations like the National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) have provided numerous guides for deploying effective security processes.

A survey conducted by the University of South Florida, on the largest barriers facing the development of robust cybersecurity policy, found that 60 percent of respondents, all municipal

governments in Florida, listed a lack of funding as the main barrier to cybersecurity.[15] The same survey found that these departments experienced little to no investing in cybersecurity solutions in the five years leading to the survey.

An unfortunate by-product of an inadequate budget resourcing is the inability to hire more experienced professionals. Whether this is attributed to an inability or an unwillingness to act, the result is the same—more seasoned cyber professionals are not entering the city infrastructure job market.[16] Simply put, the lack of a city's capability to pay competitive salaries is a direct result of their financial limitations.[17] This, in turn, allows for private sector jobs, which can offer competitive salaries, to hire the desired personnel.

A survey conducted by the Department of Social Science in Augusta University revealed that more funding was one of the most requested aspects when considering comprehensive municipal cyber policy.[18] This is a sentiment has been present since local governments were first surveyed about the general health and effectiveness of their cyber policies and standards.[19] As previously stated, this can potentially be a by-product of the relative newness of cybersecurity as a staple in city infrastructure. Even so, failure to address this issue directly will leave municipalities at the mercy of attackers. That is to say that an attacker's actions will ultimately deem additional budget provisions as a necessity—usually in addition to the major expense of having to restore critical city infrastructure. This is not to say that a city must have state of the art equipment in order to have an effective cybersecurity. The main goal is prioritizing which aspect of IT security must come first in a city's security policy. For example, some cities may prefer to spend more time buying newer servers and another may find more success in training their employees. There is no "one size fits all" approach that can be adequately deployed to all cities. It is ultimately a decision that must be made in conjunction with city leadership.

Plainly put, no city has enough of a budget to satisfy all their needs, real or perceived. They are also sensitive to the fluctuations in the economic downtowns, as was the case with the 2008 Great Recession. Given its relative newness, cybersecurity is often placed in a position where it must compete with other city necessities. More often than not, cybersecurity development ends up losing. This lack of investing also leads to further gaps in knowledge being developed. Training is not free and can often be forgone in favor of other mission critical duties. Needless to say, this can, and usually does, have severe ramifications when faced with an active security incident.

V. CHALLENGES FACING SMALL CITIES: ATTACKERS

The main drivers of attack adaptability and ingenuity are the attackers that have modified available tools to gain access into systems or changed the paradigms associated with threat detection and prevention (i.e., using popular social engineering attacks to circumvent physical security in an office building). They are the innovators in the realm of cyber weapon development and modification. For instance, an attacker can use patch notes to determine the vulnerabilities present in previous software deployments. Given the meticulous and time-consuming nature of proper patching, an attacker can find themselves attempting to compromise an unpatched enterprise network. In some instances, patches are simply not deployed in a timely manner. In such cases, the attacker is now armed with official descriptions of the holes present in that particular system—dramatically increasing their chances of a successful attack.

Small cities fit into this equation in that they are relatively low risk, high reward targets with valuable information. Their size can often times work against them as they usually contain inadequately staffed IT departments and only severe attacks on them generate national coverage. In other words, they contain valuable information and only make a proverbial peep when attacked.[20] By nature of being a city, it is almost a guarantee that local offices contain personally identifiable information (PII) like Social Security numbers or bank information—both of which can be successfully used to steal a victim's identity. This information can be sold relatively quickly to Dark Web denizens or used to open credit cards or commit other acts of fraud.

Attackers can be motivated by numerous factors, like sabotage, blackmail, or espionage.[21] Despite their differences, these attacks are usually financially-motivated and the victims can range from city personnel trying to buy back their data after a successful ransomware attack to foreign governments seeking to gain deeper insight into local critical systems, like the

power grid or water processing plant. The entrance of nation states into this cyber arena is concerning, to say the least. As the old adage says, “where there is smoke, there is fire.” Therein lies the question--why would foreign governments want to know how the electrical grid, water plant, and other critical infrastructure works in a small city? Would these nation states not be better served by compromising Washington, D.C., or other large metropolitan areas? In short, yes, they would be served reasonably well by establishing a foothold in any of these areas. That being said, they would also run into more robust security measures that would surely complicate their capacity to launch a successful attack.

Local municipalities are the complete opposite in that they are quiet, in both a metaphorical sense and a literal sense. As mentioned before, local municipalities tend to consist of smaller, more homogenous populations. This can shape the security posture of a city by creating a false sense of security. This creates a chain reaction where city leadership may not deem any of their infrastructure as a worthwhile endeavor for would-be attackers. After all, why would the plant operations of a small town, in the middle of nowhere, matter in the grand scope of cybersecurity? Ironically, this creates a perfect opportunity for attackers as they can move into a network environment in a significantly easier fashion. If successfully able to enter critical infrastructure, attackers can create a foothold. A foothold, as the name would imply, is the initial step in deploying a cyberattack. It usually takes the form of a compromised server or machine in the enterprise network. The term refers to an attacker creating a point of entry, most likely within the network environment itself, from which port scanning (seeing what ports are open and what services are running on a machine), information gathering (at what time of day is the network most active?), traffic monitoring (what machines are communicating with each other and how often are they talking?), and overall network health (is the network using an outdated firewall?)

can be analyzed. This information is worth its weight in gold and can lead to tailor-made attacks that can completely render city infrastructure defenseless.

The application of this information can provide clear advantages to foreign adversaries. For example, an adversary can gain access into city infrastructure and see how quick city response time is to an emergency situation. Response time information is invaluable as it can help an attacker formulate a well-formed attack. For example, the water plant on the opposite side of town could be hit and used as a decoy while the attacker focuses on other city infrastructure.[22] Foreign adversaries can also see how a plant or grid is laid out and what technologies are being incorporated in their day-to-day operations. In certain instances, access to a network can grant access to intellectual property than can be copied and added to the industrial toolset of a foreign nation. Far from the realm of impossibility, this information can also be leveraged in an instance of kinetic warfare.[23] Given the vital nature of water and electricity infrastructure, a foreign adversary could potentially hold a local municipality hostage until their terms are met through compromising one or both. Additionally, an adversary could further compromise plant operation systems and create a massive explosion. Both of these scenarios would create situations where the loss of life would be a very possible outcome.

The Danger of the Dark Web

In certain instances, the main goal of a cyberattack is not the data, but the prestige associated with compromising a municipality. In the Dark Web, a proven record of successful attacks can open the door to more powerful attacks.[24] The Dark Web is a part of the internet that is mostly populated by users seeking to sell a variety of illegal services (like drugs, stolen Social Security numbers, etc.). Part of this illegal activity is the deployment of botnets. A botnet is a collection of hijacked devices (bots) that have been configured to run the commands of attackers.

The advantage of a botnet is that it can include a variety of devices that increase the reach and magnitude of a cyberattack. This can materialize into more robust phishing email campaigns or other attacks that are aimed at compromising credentials. Botnets come in all shapes, sizes, and configurations, with more complex implementations requiring a higher level of proven expertise.

A properly made botnet can take years of work to develop.[25] Therefore, their creators are usually hesitant to lend them to attackers that have an unproven record of success. If given to a novice, forensic evidence conducted after an attack can potentially unravel the botnet and undo years of hard work. Therefore, would-be attackers must resort to providing proof of a successful cyberattack. Municipalities usually provide a target that is small enough to target effectively, but also large enough to gain the attention and respect of botnet creators. After a series of proven attacks, an attacker may earn the right to man a more complex botnet. This can create a scenario where future targets find themselves at the mercy of a botnet. These attacks usually involve a high number of devices and can potentially overpower a target, generating more damage. An effective method to combat the deployment of these botnets is to prevent the initial attack from taking place, denying an attacker the prestige associated with an attack. Doing so will not necessarily remove the threat of botnets, but it can significantly curtail their use and potentially stifle the further development of an attacker's toolset.

VI. CHALLENGES FACING SMALL CITIES: MANAGEMENT AND SITUATIONAL AWARENESS

While presented as two factors, management and situational awareness are two sides of the same coin. Management, in this context, refers to the city and IT leadership. In municipalities without dedicated IT departments, this term solely encompasses city leadership. Situational awareness, in this context, refers to a security professional's perception of the security posture of their organization and the threats that that face them. Most importantly, it involves an organization's ability to use past security instances to inform and develop future incident responses. Management guides the development of situational awareness and situational awareness keeps managements abreast to the changes in the threat environment. In order for a local municipality to be successful, both of these factors must work in conjunction. On a somewhat discouraging basis, the truth is that local municipalities often find themselves experiencing the polar opposite of an ideal situation.

From a purely functional perspective, local governments tend to prefer a reactive approach, instead of a proactive approach, when implementing cyber policy—a sentiment that is usually instilled by management priorities.[26] This has created a general uneasiness as it leads to the underestimation of the damage a security breach can cause. The unpreparedness of such a response often creates an environment where IT security is seen as an alien concept that can only be navigated by IT professionals.[27] Naturally, this rests the responsibility of IT security solely on the shoulders of the IT security team. This then leads to an environment where other team members may not find a purpose or value in collaboration. On a practical level, this approach makes sense—only if cyber-attacks, like the name implies, entirely took place in cyberspace.

The reality is that cyberattacks heavily consist of social engineering components that do not require certifications or tech savvy to be discovered. For example, an employee can open a phishing email and provide their credentials. Depending on the credentials compromised, malware can be given the red-carpet treatment when infecting an enterprise network. Malware can also enter a network environment through a successful shoulder surfing attack. Shoulder surfing is when an attacker leverages the innate common courtesy of holding the door open for a person about to enter a building immediately after someone. Using this approach, an attacker can maintain an unsuspicious, but close, distance to a legitimate employee and circumvent the need for an ID tag. After consecutive uses, an attacker can find themselves physically present in a server room with critical functions. Afterwards, they can load malware into the network. Both of these scenarios did not involve overtly tactical or technical responses, just a bit of common sense and situational awareness. That being said, common sense and situational awareness, in an IT context, can only be expected when management makes their development a priority in the organizational mission.

It is a common perception, among IT professionals, that importance of management cannot be overstated.[28] Due to its functions as the tempo and priority setter, management must be able to participate and understand IT decisions because any damage sustained by that part of the organization will echo, and possibly grow, into other organizational branches.[29] As mentioned before, this can be a byproduct of cybersecurity being a relatively new concern in municipal infrastructure. Even so, the implementation of proper cybersecurity policy is severely lagging. Unsurprisingly, a survey conducted by the University of Maryland found that local governments across the United States were not adequately investing in their cybersecurity, did not provide

sufficient training, and had not applied established best practices to their cybersecurity deployments.[30]

Further complicating the role of management is the fact that municipal government exists independent of the federal government. As previously mentioned, there is no central point of authority or organization when dealing with inter-municipal communication. That is to say that municipal governments could potentially be forced to follow a federally established baseline of cybersecurity, as federal law trumps state law. One may argue that, in the absence of federal policy, a penalty system can be introduced to help curtail cybersecurity carelessness. This creates a Catch-22 where a penalty system can only work if the federal government is assured that all municipal employees receive the same quality and amount of training, which can only happen if a federal policy for training exists—completely defeating the purpose of a penalty. Furthermore, introducing a federal penalty to already struggling municipalities may lead to situations where cybersecurity is handled with fear and apprehension. While the sentiment may seem appropriate to the dangers of shoddy cybersecurity, it greatly discourages learning opportunities as inexperienced IT professionals may entirely forgo or seek alternatives to municipal job opportunities.[31] In short, cybersecurity policy creation and implementation is not adequately served by iron fist supervision—it must be introduced in an organic manner than is conducive to both managerial goals and employment training and education.

A lack of coherent training will often result in poor situational awareness. A recent survey conducted by ICMA (International City/County Management Association) surveyed numerous security professionals across the United States and found that the lack of adequately trained security personnel was listed as one of the highest barriers to comprehensive cybersecurity.[32] This same survey found that over 40 percent of local governments did not know

how often they experience data breaches—attacks that carry massive damage potential. Most importantly, over 30 percent of the professionals interviewed were not able to identify if the attacks were coming from internal or external attackers.[33] The creation of security policy is already an involved task when attack vectors and variables are mostly known. Without this information, vague policy will be inadvertently created and later applied to local infrastructure. As previously mentioned, cybersecurity does not always work with a "one size fits all" approach. Threats can still be prevented with this approach, but there exists the possibility where malicious traffic can still result in a data breach. Suppose there are two scenarios, one with a disgruntled former employee and one with an outside attack trying to gain access into a payment server. On one hand, failure to nullify a former employee's credentials will result in an internal threat, as security checks would not see their traffic as suspicious in nature. On the other hand, failure to detect suspicious internet traffic would result in an external threat, as the attacker is not authorized to interact within the network environment. Each of these threats must be handled in a different way. For example, nullifying the former employee's credentials would immediately prevent them from creating a valid employee session with the network. Inserting an IDS (intrusion detection system—a device or software that checks for malicious traffic) could foil the attempts of an external hacker. Granted, there are sure to be solutions that can address both threats simultaneously. Even so, identifying the attacks as different categories provides greater information that can solidify into thorough security policy. The ability to categorize different kinds of threats also has the added benefit of informing an organization of the threat environment they exist in. This also informs cyber policy and can lead to the identification of shortcomings in the current security operations.

An interview conducted with the IT Manager of a small Texas town put this concept in perspective. In the wake of a ransomware attack on numerous Texas municipalities (to be unpacked later in the thesis), they were faced with an uphill battle in the process of incident response. At the time, their city did not have a comprehensive way of addressing the machines that were infected with ransomware. For example, the city's backup policy was relatively nonexistent and entirely dependent on a third party. Additionally, their firewall rules had not been updated in a large span of time. They refused to pay the ransom, but were ultimately faced with the arduous process of recovery. For two weeks they were unable to process payments or issue licenses, the city was in a complete standstill. Moreover, there was no clear-cut incident management policy. Through collaboration with other citizens and local computer repair shops, they were able to jerry rig a response plan.[34] When asked about the internal shortcomings that amplified the attack impact, they mentioned that city leadership did not see an inherent risk in their cybersecurity posture. Additionally, non-IT employees were not properly trained and they, understandably, resorted to panicking in the face of the attack. All of these factors were direct products of city leadership's decision to leave cybersecurity on the backburner, a decision that had a massive negative impact. In this specific case, poor management created poor situational awareness, which later made poor decisions attractive. Fortunately, their current day capabilities have been greatly enhanced. Regular employee trainings are now commonplace, as are formal cybersecurity policies. This is largely due to the ransomware attack causing a reevaluation of their outdated security policy.

VII. RANSOMWARE AND BITCOIN

Before exploring the case studies, it is important to state the role of Bitcoin in the deployment of ransomware. The majority of the case studies to follow will deal with attackers issuing requests for Bitcoin. Bitcoin is a digital currency that exists independent from government or bank regulation. As of now, it is currently worth more than gold. Despite the volatile nature of its dollar value, attackers find this payment option attractive as it involves a heavy degree of anonymity. Bitcoin functions by using a decentralized blockchain—a process by which transaction data is linked in a chronological order and essentially synced with a globally dispersed network. This prevents one entity from having control over the record process and can help identify fraud as a fraudulent block of data will not match up with stored blocks in other computers. All an attacker needs to do is create an anonymous virtual wallet and "wash" their Bitcoin through via Dark Web (a part of the internet usually populated with users seeking to commit criminal or legally grey acts for profit). This "washing" process removes all traces of previous ownership, leaving "clean" Bitcoins that can then be exchanged for money. [35]Attackers can be traced using the blockchain, but are usually skilled in covering their tracks before any identifying information can be found.

VIII. CASE STUDIES

The following case studies serve as real world examples where municipalities, both large and small, were compromised by attackers. Despite the thesis focusing primarily on smaller municipalities, these case studies still serve as potent examples of damage cyber incidents can inflict. These attacks usually resulted from a combination of the previously mentioned struggles cities face: budget, attackers, and management (poor situational awareness). Additionally, these case studies will explore the changes that occurred after incident response to these threats was completed. At the end of this section, a summary table has been created to show how each event was impacted by or impacted each of the three aforementioned challenges—budget, attackers, and management and situational awareness.

Texas

On August 2019, 22 municipalities across the state of Texas were hit by ransomware. The attack was conducted by a sole attacker working with a ransomware organization, SODIN23. They gained access into an MSP's (Managed Service Provider) Screen Connect server. The Screen Connect service functions in a similar manner to Microsoft RDP, but it allows the user to transfer files and execute code on client machines. On a purely functional level, this service was extremely convenient as it could allow the MSP to easily manage client servers and machines. In a scenario where mass patching is needed, this service could trivialize what could potentially be a multiple hour, or even day, process. This same ability also allowed for the propagation of ransomware to work efficiently and effectively. While still serious in nature, it is important to note that only those clients who used the Screen Connect service were directly affected by the attack.

The subsequent DIR (Texas Department of Information Resources) investigation introduced two scenarios that could explain the presence of the attacker in the MSP server. The first, was that the attacker could have compromised administrator credentials prior to the first dated instance of entry. This is supported by the fact that MFA (multi-factor authorization) was not enabled. The second is that the attacker could have exploited numerous vulnerabilities in the in the Screen Connect software.[36] The evidence in this case was neither supportive or opposed to this possibility. What is clear is that the attacker gained access to the Screen Connect server and was able to execute remote commands on all clients that used the service.

In the fallout of the attack, numerous local government offices found themselves without the capacity to process utility payments, issue birth/death certificates, or even communicate through email. In addition to being blindsided by the attack, many municipalities did not have fully developed response plans and quickly found themselves fighting an uphill, two front battle against inadequate policy and the immediate damage of the ransomware. Fortunately for Texas, the proverbial cybersecurity wheels had already been turning prior to the completion of the attack. Senate Bill 64 was passed on June 2019 and gave the governor the authority to send the Nation Guard to aid in the defense of the state's cyber operations. Additionally, House Bill 8 was passed in 2017 and called for DIR to draft an incident response plan.[37] As part of its preparation, DIR conducted incident training exercises. These same exercises would later serve as the backbone for the breach response and triage process. These bills, mainly House Bill 8, allowed for the appropriate teams to be dispatched. Among the responding parties were the following:

- DIR (Texas Department of Information Resources)
- TMD (Texas Military Department)

- TDEM (Texas Division of Emergency Management)
- Texas A&M University Systems' SOC (Security Operations Center)
- Private Vendors
- DPS (Department of Public Safety)
- FBI (Federal Bureau of Investigation)
- Department of Homeland Security
- Other State Partners

Each team was responsible for addressing a specific component of the relief efforts.[38] These ranged from field incident response, conducting a forensic analysis on the attack, and completing a criminal investigation on who coordinated the attack.

When the dust settled, it was found that the Screen Connect admin console was exposed to the internet. Its connection to numerous endpoints, combined with its presence in the internet, made it a prime and obtainable target. Additionally, the investigation revealed that the attacker gained access into the system roughly 14 days before the attack was carried out. The attack used the process identifier "pid:23," an indicator that is, by and large, associated with *Sodinokibi* ransomware—hence the name SODIN23. Sodinokibi is a successor to *GandCrab* (a ransomware variant that was responsible for 40 percent of global ransomware infections) and has been seen only affecting countries outside of the former USSR. [39]Sodinokibi usually enters a system through phishing emails that compromise user credentials. These credentials are then used with RDP (remote desktop protocol) to enter a network environment and then the ransomware compromises the devices connected to the network. Once the network has been compromised,

Sodinokibi sends a message to a command-and-control server (the machine used by an attacker to coordinate an attack).[40] Findings have discovered that Sodinokibi is quite adept at evading anti-virus protocols. The findings also point to SODIN23 being familiar with the Screen Connect platform, possibly hinting to it being a regular target.[41] The recovery efforts were successful, largely in part to the TDEM SOC's capacity to communicate with local entities and coordinate with the field teams.

This ransomware attack, like many other cyber-attacks, was not just felt in the numerous client machines that were infected with ransomware and the equally numerous government processes that were halted due to its propagation. It also had a transformative quality to it that changed the way Texas viewed its own standing in cyber-security. Organizations like the TxISAO (Texas Information Sharing and Analysis Organization) and TAGITM (Texas Association of Governmental Information Technology Managers) were largely impacted by these attacks and would see themselves becoming hubs of information to numerous cyber-security professionals across the state. The attack was also significant in that it embodied a major hiccup in the communication process—the small towns themselves. Small towns in Texas are completely autonomous and do not report to a central government agency. As such, cybersecurity development, training, and deployment are entirely left to the discretion of city leadership. Unlike Texas schools, who report to TEA (Texas Education Agency), cities are left to determine what is needed for their citizens.[42] On one hand, this approach will provide the most tailor fit solutions on a city-to-city basis. On the other, it can deny small towns a state-defined baseline of best practices that can benefit all of Texas. This also explains why there are so many unique cybersecurity configurations across Texas cities. This is largely due to differences in city-specific priorities and their IT needs. It is also partly due to certain security solutions being

misunderstood or automatically being classified as too complex in nature. Naturally, this leads to a gap in knowledge forming among different cities. Without proper community or statewide involvement, this gap will continue to widen and small city IT professionals may catch themselves on the receiving end of the next incoming cyber-attack.

The ransomware attacks on Texas were not initiated by gaining direct access into municipal infrastructure, but by compromising the MSP (managed service provider) that serviced the affected cities. Even so, multiple municipalities found themselves without effective cybersecurity policy—allowing the ransomware to burrow deeper into their networks. It is also important to note that all of these municipalities were not hit with the same intensity. The ones that were impacted heavily typically had little to no incident management policy in place. [43]

Riviera Beach, Florida

On May 2019, Riviera Beach was compromised with ransomware when an employee at the police department opened an email containing ransomware. The attack was able to disable major city infrastructure like email, phones, and police records. In the absence of these services, the Office of Public Works, City Attorney's Office, and library system was unable to fulfill their day-to-day services. Riviera City had multiple factors that facilitated the spread of ransomware. First, the security system they deployed on their city infrastructure was severely outdated to the point where the manufacturer did not exist anymore. The units, purchased in 2012, only had a shelf life of 5-7 years. Secondly, the city council approved a $798,419 purchase for a new system—it was just never installed. This specific factor was the most striking as the fault was not caught until after the ransomware took hold of the network.[44] This clearly points to a completely lack of managerial accountability and situational awareness. Lastly, and the cause of the previous two issues, city council was plagued with years of management turmoil. This turmoil included a

lack of consistency in leadership roles like IT manager and city manager. Quite surprisingly, these roles were filled by numerous interim employees that were later replaced by another batch of interim employees. This shuffling of leadership lead to a scenario where the serving interim manager was not aware of the manufacturer security contract and ultimately forgot to renew it, creating new bureaucratic hurdles for an inexperienced city council to navigate. Needless to say, these factors created massive wait periods between the issuing of a purchasing request and its approval.

The root cause of these changes was the ousting of five city council members and the mayor—all due to a series of scandals involving lavish spending in council expenses for travel and car allowances. This created a scenario where the only senior member in the council had less than a year and a half of experience.[45] Understandably so, this inexperience makes it difficult to be aware of the overall issues facing the city as a whole, much less the capacity to trust department heads that were, at best, temporary workers. The senior member was essentially caught in a labyrinth with ever changing walls—where the wrong decision could also cost them their position.

All of these difficulties came to a head with the approval of a 65 Bitcoin ($600,000 value) ransomware payment. The FBI largely advised against the disbursement of payment as there is no guarantee that the provided decryption tools will work or that they will decrypt the entirety of the data. Payment also has the added effect of incentivizing future attacks. Fortunately, they received valid keys and were able to decrypt their data. Unfortunately, this case of ransomware was widely covered by national media and led to intense public scrutiny, especially considering that a $600,000 payment was authorized in a city where 22 percent of the population lived below the poverty line. In the wake of the attack, Riviera City has restructured

their security response to include training their employees to identify phishing email campaigns.[46]

The failures in this specific case were numerous. For starters, a continual shift in city leadership was essentially hollowing out the security response from the inside out. That is not to say that removing corrupt leaders was wrong. Quite the opposite, it was the correct decision. What merits further evaluation was the continual shifting of employees that followed the ousting of the council members. Keeping stability in these positions would have changed the response as department heads would have had enough time to become acquainted with the needs and capabilities of their departments. Additionally, Riviera City's employment inconsistency maintained a culture of "passing the buck on" to the next person that was going to fill a position after the current holder's brief tenure. Employees were essentially playing a chess game where each move was initiated by a new employee unaware of the move that came before their own. There was no sense of an overall mission or organizational goal. This created great losses in management's ability to maintain, much less create, a security culture—snowballing into an overall decline in situational awareness and incident response.

Colorado Department of Transportation

SamSam

Despite having a similar goal as other ransomware, SamSam relies on a more complex method of entry and is not sold as a commodity online. It is complex in that it is targeted and does not need email to enter a system. Instead, points of entry usually rely on compromising public facing single-factor authentication, like RDP (remote desktop protocol) or FTP (file transfer protocol). The delivery method is also unique in that it purposely provides victims with

reasonably affordable ransoms. This has the added effect of manipulating the psychology of victims to cave into the, often advised against, option of paying the ransom. In some instances, they decrypt non-essential data, for free, as a sign of their ability to decrypt the other data and their willingness to leak sensitive information online if the ransom is not met.[47] SamSam is a ransomware variant that has been associated with the group "Gold Lowell"—a group alleged to be located in Iran.[48] This was determined to be the case as the English used in the ransom messages were rife with grammatical errors not typically found in native English speakers. Unlike other ransomware, it is not sold to online buyers, it is proprietary to Gold Lowell and is constantly updated to circumvent antivirus detection.

On February 2018, the Colorado Department of Transportation was greeted with a message alerting them that their files have been taken hostage and the attackers were requesting a Bitcoin payment for the decryption tools. The *SamSam* ransomware was able to enter their network when CDOT was trying to implement a cloud-based business process. In order to test the process, a temporary server was created and deployed online using an administrator account. The server was discovered by attackers within the same day it was deployed. Given that this server had elevated privileges, attackers were able to brute force credentials due to the servers unlimited failed logins capability.[49] In order to prevent the spread of malware, business operations had to come to a halt. One of the operations cancelled was the payroll service. Given the threat, it had to be done. Even so, employees still have to feed their families and pay bills—creating additional tension at the management level.

Fortunately, Colorado had previously embraced a backup effort, Backup Colorado, in order to better prepare their infrastructure.[50] Due to the recent nature of their backups, CDOT refused to pay the ransom. Additionally, the attack was concentrated on CDOT functions and did

not impact critical infrastructure like traffic alerts, cameras, or traffic operations. The lack of an imminent public safety concern greatly facilitated the refusal to pay the ransom. It took roughly one week to restore the system back to working order.

Or so they thought. The next day they were greeted with new SamSam activity. The attackers had launched more attacks. This second infection came as a direct result of the attacker placing additional tools on the network, in addition to the SamSam ransomware. The CDOT security found and removed SamSam, but only focused on the tools that initially introduced it to the network. This occurrence highlights the iceberg-like character of ransomware—the fact that the true breadth of an attack is usually not evident when the ransomware is detected, but when it is further analyzed after removal. This second instance of infection led to the declaration of a state of emergency in the Office of Emergency Management. Once this declaration was created, the Colorado National Guard deployed a team of roughly a half-dozen security professionals. With reinforcements ready, the response team was able to organize a more detailed approach to recovery. Using infected machines, they were able to develop tools to detect and quarantine the ransomware. Fortunately, their tools were effective and they were able to successfully recover.[51]

Today, Colorado has invested over $17 million into their cybersecurity—more than double its original value.[52] In this scenario, SamSam proved to be an unlikely ally as it greatly sped up the legislative process necessary to increase available budgets. These budget increases were so significant that they allowed the cybersecurity team to accomplish in 48 hours the updates that would have normally taken over four weeks. A fortunate byproduct of this improved budget was that items in the security to-do list were immediately addressed before they became dire in nature. The change also spread to the way they structured policy. For instance, they reduced the number of administrative accounts from 500 to 50.

Baltimore

RobbinHood

In a similar fashion to SamSam, this ransomware is not distributed through spam. Its point of entry is not completely understood, but recent analysis of it indicates that it compromises public facing infrastructure. It also behaves differently from other ransomware—disconnecting the infected machines from network shares and targeting them individually. This divide and conquer approach points to the entry point being a compromised domain controller.[53]

Robinhood works by searching for an RSA encryption key in the C:\Windows\Temp folder. Then it stops Windows services dealing with antivirus, mail server, and any software that can prevent further encryption. During this process, it also deletes Shadow Volume Copies (a Microsoft technology that creates backups of data), deletes any logs, and disables Windows automatic repair. Afterwards, it begins the encryption process by creating an AES key for each file. This ransomware then encrypts the AES key and file with the RSA key it discovered.[54]

On May 2019, the city of Baltimore was hit with ransomware. In a similar manner to Riviera City, Baltimore's run in with ransomware coincided with the removal of key city leadership. The mayor at the time, Catherine Pugh resigned as a direct result of political scandals involving tax evasion, fraud, and conspiracy. She was later prosecuted and sentenced to three years in prison, with an additional three of probation.[55] Despite this being the correct course of action, the removal of a unifying presence, like an elected mayor, has the unavoidable impact of causing imbalance in city response as their replacement might not have had the same rapport their predecessor created with other departments. That is not to say that the job cannot be completed in a satisfactory manner, but the cohesion created by the previous position holder may

not be present—like any job, time helps create and solidify a seamless work flow. While not the direct cause of the ransomware attack, this event was quickly picked up by national media and gave Baltimore the eyes and ears of the American public—placing a proverbial magnifying glass on the impacts of the ransomware.

The ransomware itself was discovered when city computers welcomed employees with a message saying that RobbinHood had taken their files hostage and were demanding three Bitcoins (roughly $24,000 at the time) per computer or 13 Bitcoins (roughly $102,000 at the time) for the entire system to be decrypted. Following the recommendation of the FBI, city officials chose to forego paying the ransom. Like cyberattacks before, city infrastructure came to an abrupt freeze. Of particular note is that this attack was especially felt in the city's capacity, or lack thereof, to process online payments for utilities, property taxes, fines, and other city services.[56] As a direct result of this, over 1,500 pending home sales were delayed—creating a scenario where families could possibly face homelessness as they prepare for a transition into their new home.[57] The city reached a point where payments could only be processed with a cashier's check or money order, along with a valid bill. The lack of an online payment system added multiple bureaucratic hurdles to a city that was already struggling to respond to the ransomware. In order to add more pressure to the city, the attackers started to communicate with city officials through Twitter and started to leak employee information online, claiming that this would only keep on if the ransom remained unpaid.[58] In addition to the removal of online payment systems and the leaking of sensitive documents, the city was left with the inability to communicate via email. In order to combat this, city employees resorted to creating multiple Gmail accounts to restore come communication capabilities. Unfortunately, Google's security automation detected multiple accounts originating from the same network and shortly disabled

all of the accounts created—creating additional downtime.[59] Fortunately, Google quickly addressed city complaints and restored the accounts.

When analyzing the ransomware variant, it was suspected to that RobbinHood entered Baltimore's systems by using the EternalBlue exploit to bypass system security. EternalBlue was a tool originally created by the NSA (National Security Agency) to enter Windows systems. The tool was leaked and quickly became a mainstay of cyberattack efforts. As such, Baltimore was quick to shift the blame on the NSA for the release of their tools into the hands of malicious actors. The NSA was quick to respond, stating that not only was a patch for EternalBlue already available, but failure to apply it was a clear indicator of Baltimore's lack of comprehensive cybersecurity policy. To the NSA's credit, it was later revealed that RobbinHood did not, in fact, use EternalBlue, but other system vulnerabilities to enter. What is clear is that RobbinHood was most likely an opportunistic attack, as opposed to a targeted one. The language used in the ransom note was identical to the language used in other Robbinhood attacks.

When the damages were totaled, it cost Baltimore roughly $18.2 million to recover from RobbinHood. Expenditures included recovery from a loss of revenue, the additional purchase of state-of-the-art computers and servers, and additional threat mitigation. This was accomplished by using the city's cyber insurance and reallocating existing city funds. When compared to the initial ransom, the sum seems massive. Citizens were quick to condemn the additional funding of cybersecurity through the reallocation of funds from other city departments, like the city park system. Despite being able to recover successfully, Baltimore found itself in a position where its lack of strong security policy resulted in a severe lack of situational awareness that prevented critical infrastructure from getting patched. They ended up generating a large expenditure to fix

the problem—which, granted, was a step in the right direction. They also ended up paying the price of losing citizen trust and goodwill, an absolute necessity for successful city operation.

Atlanta

In May 2018, Atlanta was hit with the SamSam ransomware. A ransom for $50,000 worth of Bitcoin was issued in exchange for the encrypted data.[60] True to past deployments, this particular SamSam instance offered a reasonably affordable ransom. As mentioned before, an affordable ransom places city leadership in a dilemma as the ransom is usually cheaper to pay than the recovery efforts. That being said, it also rewards criminal activity and places future targets on city infrastructure as attackers know they are willing to pay. Simply put, buying the data today welcomes the ransomware tomorrow. The attack had the impact of severely hampering the city's ability to process utility payments, limiting sewer infrastructure requests, and leaving the police to file reports manually. The court systems were also unable to hold hearings as the records need to verify warrant data were inaccessible. Given that Atlanta's courts are considered to be the busiest court system in the South-eastern United States, the inability to hold hearings placed a massive burden on legal proceedings.

In order to better understand the reasons Atlanta was hit, it must be noted that it failed a security compliance assessment—as mentioned in a January 2018 City Auditor's Report. Additionally, Atlanta did not have a formalized process to identify, assess, and mitigate risks.[61] Many of the processes put in place to secure critical data were done so in a reactive patchwork process that was not documented. This reactive approach, which is a direct result of a lack of managerial foresight, is usually commonplace in municipal governments because it can be perceived to be more effective to repair a faulty component when it breaks. While true in other situations, the "if it ain't broke, don't fix it" mentality is not effective in cybersecurity. Quite the

opposite is true, if something is not patched in a timely manner it will only generate more risk and monetary cost. Part of this was due to a lack of city resources, but the other was a direct byproduct of clear security policy. Atlanta's failed security audit should have been a massive red flag to city leadership. Even so, cyber defense came in second place to other city priorities—a common occurrence in municipal governments.[62]

Atlanta spent a total of $2.6 million on the recovery efforts. The majority of the expenses were focused towards forensics, staffing, and additional efforts to take back their systems.[63] Like Baltimore, the end result was multiple times the original price of the ransom. Even so, Atlanta made an expensive, but necessary step in the right direction. Granted, an initial effort to patch the systems that failed the audit would have been considerably cheaper, but hindsight is always 20/20. Like Colorado, the attack and the attention it generated were key in helping to provide the security team with much needed funding. In that aspect, ransomware attack was actually beneficial. Still, a municipality should not be severely crippled before seeing the proverbial light of well-made security policy.

Oldsmar, Florida

This specific case study is unique from the other five in that it did not involve a ransom. As a matter of fact, it did not involve ransomware at all. In February 2021, an attacker gained access into a Florida water treatment plant. As previously mentioned, cyberattacks can leave municipalities in a position that can be leverage in the case of kinetic war. This attack, while unattributed to a specific state or individual, is the embodiment of this notion. The attacker attempted to increase the levels of sodium hydroxide, in the water, from 100 parts per million to 11,100 parts per million. Within the proper limits, sodium hydroxide helps regulate the PH of the water. In exaggerated quantities, it has lethal effects. Fortunately, the operator was privy to the

change and quickly changed it back to the safe levels. The plant was also equipped with PH testing equipment that would have automatically prevented the water from being released to the population. When thinking of a situation where kinetic war arises, it would not be outlandish to imagine a foreign adversary taking control of a water plant and denying water to a city's population. They could, theoretically, hold this position until demands are met—generating casualties and completely shattering the public trust in the government. While this has yet to happen in the United States, occurrences like these have been observed in other countries, like the *NotPetya* attack on Ukrainian power grid carried out by Russia. The attack was able to cripple the banking system, energy firms, and airport functions.[64] Even though the attack in Florida did not have an immediate and violent impact, the fact still stands that there was an unauthorized user playing around with critical infrastructure—a massive failure when looked at individually.

The attack was first spotted when a plant employee noticed that their computer mouse pointer was independently moving on a screen. Under normal circumstances, an observation like this would immediately spur a user to shut down their machine. This was not the case at the plant. It was fairly common as employees regularly used the TeamViewer software (software used for remote access and maintenance of other devices) to share screens and work on IT troubleshooting solutions.[65] Unfortunately, this software also served as the main entry point to an attacker. More shockingly, the question remained as to how the intruder was able to gain access to. Given the recent nature of this attack, the answers have not been completely discovered. What is certain, is that the plant had several of their industrial systems accessible from the internet.[66] This stands in direct opposition to the industry standard of not having critical equipment accessible from the internet—they should be kept away from the internet and in their own

contained network. As is usually the case with external attacks, this attack would have been eventually been thwarted by the industrial controls in place at the plant. Even so, unauthorized access into a critical network should be treated seriously and followed with a policy revision and patching process.

This attack also embodies the main concern for management in IT security—balancing function with protection. Technically speaking, a plant can be configured to prevent any and all communication with the outside world. It can be configured to be a proverbial fortress with accompanying mote. This configuration would drastically reduce the number of cyber incidents, but it would also have the added effect of reducing employee and plant flexibility. What would happen if a vital employee is not physically present at the local? How would patches be distributed in a closed environment? These are all questions that must be asked. Furthermore, the current COVID-19 pandemic has made working from home almost mandatory for certain organizations. How would a closed off organization work in a pandemic? Most likely, not to its full potential. This is why it is important to strike the balance between functionality and protection.

Even though the attack did not cause physical damage, it must be treated as an instance that could have. The main concern in this case would be the situational awareness of employees as they saw their screens being controlled. The commonality of such an occurrence played into the attacker's hand as employees did not see anything strange with this implementation. They were able to scour the network for hours before suspicion arose. While necessary for plant function, this policy would be a great candidate for renewal. For example, the plant could possibly include a communication component before initiating the remote control of machine. This approach is not immune to outside tampering, but it does create a sense of urgency

whenever an employee notices a remote takeover without preceding communication. Given the ongoing nature of the investigation and the variables involved, it would not be farfetched to potentially discover that tools were deployed or attempted to be deployed into the network for a future attack—as was the case in Colorado.

Summary Graph

	Ransom/Cost	Malware Involved	Management and Situational Awareness
Texas	Many of the affected municipalities did not have an adequate budget prior to the attack, leaving them at an equipment and personnel disadvantage.	Sodinokibi ransomware	• The Screen Connect console was found to be exposed to the internet, quickly gaining the attention of attackers. • Many cities found themselves without thorough incident management policy.
Riviera Beach, Fl	The $600,000 ransom was paid, but caused massive public backlash as 22% of the population lived below poverty.	Ransomware entered through a phishing email	• A budget proposal was approved for a new system, but it was never deployed. • City leadership was constantly shuffling, removing the sense of unified response or policy stability. • The technology in use was so severely outdated that the manufacturer did not exist anymore.
Colorado Department of Transportation	The attack sped up the legislative process and increased the cybersecurity budget to $17 million.	SamSam ransomware	• The recovery process was quick, but was initially focused on stopping the ransomware. • This caused other attacker tools to be ignored, leading to another SamSam instance and further delays.
Baltimore	• Ransom received of $24,000 for ne machine or $102,000 for the entire system. • Recovery process generated a total cost of roughly $18.2 million.	RobbinHood ransomware	• Removal of key city leadership created a sense imbalance in incident response. • City leadership shifted the blame to the NSA and were promptly proven to be wrong, decreasing their credibility. • In order to fund the recovery process, the city had to reallocate funds from other city infrastructure.
Atlanta	• Ransom of $50,00 received • Recovery process cost roughly $2.6 million.	SamSam ransomware	• The IT department failed a security compliance assessment. • There was no formalized response process. • None of the steps taken to respond to the attacks were documented.
Oldsmar, Fl	No ransomware involved.	TeamViewer software compromised	• The TeamViewer software was so commonly used that the hijacking of a user session did not seem suspicious. • Several industrial systems were accessible from the internet.

Figure 1: Summary Table of Case Studies

IX. RECOMMENDATIONS

Despite the effective nature of cyberattacks and their ability to cause large amounts of damage, they are not invincible. Surprisingly, even the most complex of attacks can be defeated by a solid security posture and some common sense. The following section will focus primarily on what can be done to better prepare municipalities, both large and small, against incoming cyberattacks.

Increasing the Budget

This first point may come off as somewhat tone deaf as it is fairly obvious. In an ideal world, this solution would be the first step in improving cybersecurity. The reality is that cities have a hard enough time with their budgets as they are. It could prove to be nearly impossible to provide IT security with additional funds. Even so, cases like Atlanta prove that municipal governments will resort to allocating the budget from other departments to IT security. When push comes to shove, local governments are not above paying millions to have their regular functions restored. This is where a proactive approach is not only better, but fiscally superior to a "wait and see" approach. Increasing the baseline budget of the IT security department will allow them to purchase upgrade equipment, security tools, and better prepare municipal staff to respond to cyber incidents. The equipment has the added benefit of being better equipped to handle new threats, having more manufacturer support, and can also serve as a deterrent for future attacks. For example, an attacker may not want to spend time on trying to compromise a network that has proven to outmaneuver their attempts at gaining a network foothold.

The alternative option would be to wait until the attack comes into fruition, presenting municipalities with the choice to pay a ransom or pay a premium (that is usually several orders of magnitude greater than the ransom itself). In this scenario, the cheapest option may prove to be the most expensive one as attackers will know that a city is willing to pay. That leaves the funneling of dollars into the recovery process as the next viable choice—which may have the unintended impact of decreasing trust in the government's capacity to address a cyber incident. Proactively allocating a greater budget to cybersecurity will have the benefits of the both of the previous options and greatly decrease their negative impact. For example, a ransom would not have to be paid if the ransomware is caught by the newer equipment. Money will not have to be reallocated if the IT budget was already enough to meet the needs of city infrastructure. Granted, some citizens or other departments may still feel uneasy with the decision, but it defeats the alternative of having citizens upset in the midst of a massive data breach. The negative correlation between IT spending and city expenditure on data breach response is a clear indicator of the effectiveness of this approach. For small municipalities that cannot invest into more equipment, it can be more cost effective to invest in cyber insurance—allowing the insurer to shoulder the majority of the financial burden brought on by the attack. [67]

The Israeli Model

The budget can also be increased in the presence of a formalize security policy. A study conducted by Deloitte found that a formalized security strategy was correlated with a higher budget.[68] When presented with a formalized incident plan, city leadership is more likely to invest in a department that is has a clear plan for how funds will be used to meet city needs. If a plan is hard to formalize, municipalities can adopt the Israeli model defense methodology. Under this model, management begins their plan development by conducting asset mapping. Asset Mapping

is essential as clearly it places major organization assets within the context of and flow of the network.[69] Money cannot be spent unless management knows what it will be spent on. This also has the added benefit of determining which systems are mission critical and which functions they perform.

The next step in the process is to plan for security to be consistent with the damage potential of the asset. That is to say that the protection of an asset must be tailored to the value of the data it contains. There should be no blanket approach when securing multiple assets. These assets should be analyzed in how they can affect the CIA (confidentiality, integrity, and availability) of the data. The scale for asset analysis ranges from 1-4 with 1 denoting a relatively small loss and 4 denoting a severe loss. This helps determine the risk intensity of a potentially compromised asset.

After the assets are categorized by their value, the current network configuration must be analyzed to see if it matches the protection requirements. In order to complete this step, the IT department must look into each component and analyze the following:

- How many users exist in the system?
- Who are the system users?
- How may interfaces exist in the system?
- Are these interfaces intra-organizational or external?
- What information is contained in these assets?
- Does the asset have remote access?
- Are permissions compartmentalized?
- Does the asset contain the latest patch?

- What is the update policy for these assets?
- What level of physical security do these assets contain?

Each of these questions is also categorized in an increasing intensity scale from 1-4. Afterwards, the average of these values is calculated—providing the risk probability. This value is then used in conjunction with maximum value of the asset's CIA analysis. The resulting formula is

$$Risk = 3i + p$$

where *i* is the maximum score of the asset in the CIA analysis and *p* is the average of the risk probability. For example, as asset with a score of 1 in confidentiality risk, 3 in integrity risk, and 4 in accessibility risk will have a max value of 4. If the average of its risk probability is 3, the formula will like so:

$$Risk = 3(4) + 3$$

This gives the asset a risk level of 15, a severe level of risk.

These values can then be used to create a graphical representation of where the asset priority lies. Each proposed solution to threats will consist of circles drawn to represent the amount of time it will take to implement a solution-with longer solutions generating larger circles. The Y-axis will consist of the asset risk level. The X-axis is the cost of implementing a solution. A finished graph will look like the one below.

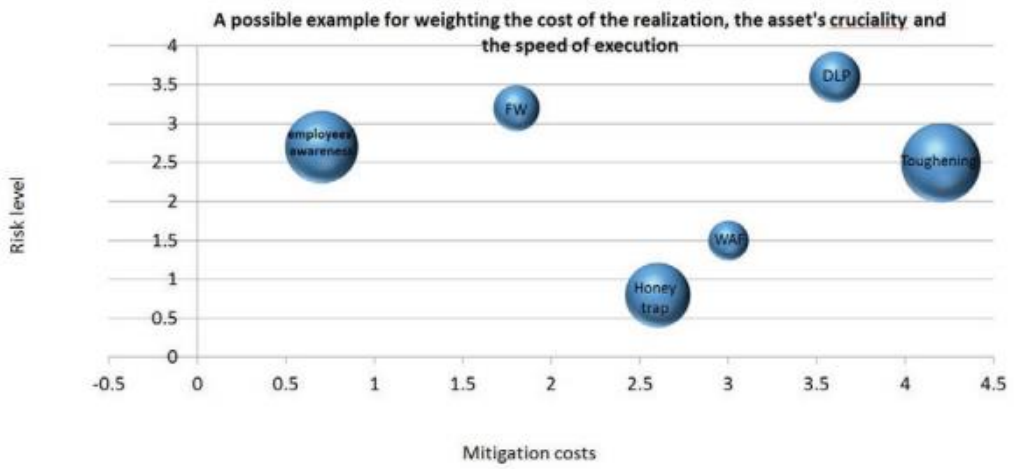

Figure 2: A Sample Work Plan[70]

This finished graph can help management determine which goals are the most pressing and cost effective. By providing expenses as a function of time and cost, managers will be placed in a better position to petition for a budget increase. This graphical representation also has the added benefit of providing management an overview of organizational needs. Even in the midst of a failed budgetary request, managers are left with a document that has been tailor made to not only map organizational needs but the money and time needed to address them. Adopting the Israeli model will provide them with the situational awareness needed to stay abreast of their current threat environment.

Collaboration

In the same vein as the popular public service announcements of the past, knowledge is power. In the field of IT security, knowing how an attacker or malware usually moves is the first step in preventing their entrance into a network—thereby avoiding massive cyberattacks altogether. Below are different types of collaboration that can greatly aid in the development of a strong security posture.

Inter-municipal Collaboration

Collaboration can cover gaps when an expanded budget is not readily available. Municipalities have the option of joining an ISAO (Information Sharing and Analyses Organization) in order to better prepare themselves for incoming threats. The power of an ISAO is that it can consists of cross-industrial organizations that organize and share their best practices for handling cybersecurity. The beauty of this arrangement is that these are largely informal organizations that just need group interest to be created.[71] Everyone is invited to be a part of the free exchange of information. Groups can consist of libraries, private firms, and universities. Most importantly, joining an ISAO is completely free. In Texas, the TxISAO came as a direct response to the aforementioned ransomware attacks on state municipalities.[72] It was made to help close the knowledge gaps that exist and will exist in multiple organizations. Given the ever-present budget struggle, joining an ISAO is an attractive method of gaining information and expertise without straining budgets. Unfortunately, many municipalities in Texas are unaware of the existence of an ISAO. ISAOs, like any other free organization, are joined voluntarily and should not be forced by the federal government—an act that would defeat the very concept of voluntary collaboration. The federal government can potentially reach out to all municipalities, but this proved to be difficult or impossible—as was the case when the federal government did not have a readily available list of municipalities in the state.[73]

One option to overcome this would be to have the federal government invest in a statewide campaign to bring additional attention to an ISAO. Signs that read “Keep Texas Clean” are generously scattered across interstate highway systems. Adopting this approach could bring further attention to cybersecurity awareness. This can be done by the state catering to its own state identity. Every state in the United States has a small descriptor associated with their

name—Texas is the Lone Star State, Florida is known as the Sunshine State, etc. These differences are also evident in their own unique flags, state anthems, and state constitutions. Within these different descriptors is a plethora of unique experiences shared within the citizens of a state. Catering to these unique, yet unifying, components of shared experience can prove to be key in closing gaps for cybersecurity and making information more accessible. In order for this approach to work, state government can design information campaigns that reflect their state identity. For example, Texas embraces the "Don't Mess with Texas" identity. In just about every souvenir shop in Texas, one can see a countless offering of merchandise that contains this phrase. Of important note, is the concept that the constant restocking of these items indicates a desire for people to purchase them.

This phrase was part of a massive 1985 campaign to keep litter off of Texas roads. For the most part it has been largely successful as it is a unifying slogan for Texans.[74] This campaign zeroed in on a shared identity of Texan state pride—making it a mainstay of the Texas experience. It quickly attracted the attention of celebrities and state figureheads alike. It is actively supported by a state agency (the Texas Department of Transportation), giving it the exposure to reach all of Texas. In the case of Texas, it could be a consideration for DIR (Texas Department of Information Resources) to embrace a campaign similar to the "Don't Mess with Texas" campaign. Given that the success of this slogan was not the result of a codified law, this can prove to be a viable alternative that seeks to unite Texas instead of policy that may be deemed intrusive to local municipalities. This has the potential to pay in dividends for TxISAO participation—gradually increasing the IT security posture of the state. State by state implementations of a similar campaign will vary, but still have the potential to be massive successes.

In the absence of a created ISAO, neighboring municipalities can coordinate with each other to create one for their region. This has the added benefit of increasing the threat knowledge pool and creating an amicable relationship among neighboring municipalities—possibly creating a united front in the face of a large scale cyberattack. Regional ISAOs can become collectors of region-specific attacks. For example, some states border other countries. Cyberattacks that impact those other nations may have the capacity to impact them as well. If an ISAO exists at the time an attack strikes, new information will quickly flood into the ISAO. This ISAO can, in turn, reach out to other ISAOs in their states. In an ideal situation, multiple ISAOs can choose to create a statewide ISAO that can serve as a unifying, central hub for state intelligence. Having a state ISAO is important as it can collect the input coming from all ISAOs within the state and work with state agencies to see the difference in threats experienced within its borders. When new trends emerge, the state can update existing information campaigns and training best practices to reflect the needs of corresponding areas.

Cross-pollination

Another option that can be used to increase collaboration is cross-pollination. As the name suggests, this method involves the enriching of state wide security posture through a process of continual idea sharing. It can also solve the problem of ISAO participation. In this method, the state government takes the first step in bridging a lack of communication with smaller municipalities. The following example will focus primarily on the state of Texas, but the concept can apply to any state government.

The first step in this process is for the state government to identify larger cities in its different regional areas. For example, DIR could potentially identify Houston, San Antonio, Lubbock, Dallas, McAllen, Brownsville, and El Paso. The next step is for DIR to send

representatives to these locations to conduct training. This training will consist of a comparison of current security policy with the DIR defined baseline. In areas that are lacking, cities would be able to revise their policies to reflect current standards. If cities are found to have a more robust policy than their state IT department counterparts, the state can update their policies. The next part of the training would consist of identifying neighboring municipalities and having the cities themselves plan a similar training exercise for their neighbors. These neighbors (smaller municipalities) will now have the opportunity to receive critical information and share some of their own. They can even host additional training or joint exercises with their neighbors. Throughout the entire process, DIR or any other state IT security department can follow up with the larger cities and the municipalities they have worked with.

The process continually repeats itself to the point where a majority of municipalities have now been exposed to a baseline measure of security and best practices to implement them. This creates a sense of managerial accountability as municipal leadership would have seen how to properly assess the current security posture and what steps are needed to correct it. Additionally, they are working in conjunction with larger cities and DIR. This has the added benefit of providing a two-way information system in which municipalities receive information, but also send some back to the state IT security branch. This can create a system where state governments are privier to the threats and changes in their constituent security needs. For example, McAllen and Brownsville are located near the Mexican border and have a heavier presence of Border Control agents. A potential threat vector could be an attacker releasing the information of Border Patrol agents and their families. Situations like these may not be common in areas like Houston, but the steps taken to protect Border Patrol in south Texas can be used to protect police databases in Houston, San Antonio, etc. Given the unique experiences that each city has, the data and

insight have the potential to be equally unique. There might even be a scenario where seemingly disconnected cyber incidents in different cities point to a larger, more sustained attack on state infrastructure.

This idea of cross-pollination can also increase ISAO participation or can lead to the creation a de facto ISAO in the absence of an established one. If collaboration is cultivated among these different cities, it will create a network of multi-industry and multi-discipline security practices across an entire state. Most importantly, there will be participants that are keeping the information alive and relevant to the ever-changing requirements of cybersecurity. There can also be instances were regional ISAOs are created in direct response to similarities in municipal needs. This further clusters information into regional variations, making it easier for state governments to get a more complete picture of the threat environment they face. This constant influx of information and continual refining of techniques can greatly help close learning gaps and create solid security policy. It also has the added benefit of making all participants part of the recovery process. In the face of a developing attack, it will prove to be much quicker to mobilize recovery forces located in neighboring cities. Cross-pollination allows municipalities to be aware of their own security posture and that of their neighbors, greatly amplifying situational awareness.

Intra-municipal Collaboration

While inter-municipal collaboration is important, it can only work properly if a municipality's proverbial house is in order. As mentioned before, municipalities contain a wide array of state and private organizations--some may include industrial complexes for private companies or institutions of higher learning. For the most part, every municipality contains a police department, an emergency response team, and a fire department. In the wake of a serious

cyber incident, all of these components of municipal government will need to work together. Needless to say, coordination must be tested in order to streamline the response process. In a similar fashion to the response exercises used by emergency services, cybersecurity exercises should be the norm. Emergency exercises, conducted in less-than-ideal condition, can help draw attention to the weaknesses and strengths of municipal response—allowing policy and practice to be seen within the context of an emergency.[75] Given that municipal government involves an entire community, exercises must focus on inclusivity in order to cultivate a refined response.[76]

The exercise is table-top based and requires representatives from a number of agencies.[77] They are then given a scenario where a simulated attack is carried on in within the municipality. Clues are gradually released to these groups and they are asked to simulate their response to the given challenge. In order to gauge their responses, they are asked a series of questions. These questions seek to focus on each group's specific decision-making process and the ways in which different department interact with each other. Given the community wide damage of a cyberattack, the response must also be community wide. By having a simulation that enters and moves through numerous municipal vectors, local governments are able to self asses their level of readiness for an emergency situation. Exercises like these are key because non-IT departments or businesses may be attacked, forcing them to work closely with local government IT security.

Joint exercises will help define the areas where municipalities must focus additional resources and attention. The practice of these exercises found that emergency responses are almost exclusively driven by pre-configured incident response plans.[78] The shortcomings of these canned responses will, ideally, be revealed through successful implementations of these exercises. The end result can serve as a future response plan for future intra-municipal communication and IT security.

The Community Cyber Security Maturity Model

The Community Cyber Security Maturity Model (CCSMM) is another tool that municipal governments have at their disposal. There exist times where local government are away of pending threats but do little to move towards implementing solutions. The CCSMM provides a framework for municipalities to improve themselves. The CCSMM incorporate three key features: a "yardstick" to measure current security posture, a "roadmap" to guide further improvement steps, and a common reference point that uses similar terminology in order to facilitate communication among different municipalities.[79]

At its core, the CCSMM uses four dimensions and five levels of proficiency to measure each of them. The four dimensions are:

- Awareness: a community understands the full potential of a threat and its impact on society.
- Information Sharing: information is reported and share across multiple organizations and municipalities.
- Policy: municipal policy has a codified system of guiding principles, laws, rules, etc. that control day to day functions. Policy should reflect cybersecurity principles in all of its implementations.
- Plans: the municipality has a plan set to address known cyberthreats and can adapt to handle future ones.

The five levels are:

- Level 1- Initial: there are some security programs in place.
- Level 2- Established: a basic program is present that addresses the four dimensions.

- Level 3- Self-Assessed: there is the existence of a minimally sustainable program.
- Level 4- Integrated: cyber security is integrated in the community, among citizens and businesses alike. At this level, the municipality is also working with the state and other municipalities.
- Level 5- Vanguard: the municipality is fully-vigilant and maintains a proper security posture.

A municipality is to initially measure their current capacity in each of the four dimensions to determine where they stand. After these baselines are created, a municipality can identify areas that are weak in security. Afterwards, they can determine the course of action needed to move to higher levels. In order for a municipality to increase in proficiency it must incorporate the following:

- Metrics: a standard of measurement for municipal security posture.
- Technology: the purchasing of new technology and the maintenance of existing technology must improve.
- Training: municipalities must increase and improve training efforts for citizens and employees.
- Process and procedures: policy must change in order to further improve security posture.
- Assessments: current infrastructure is compared with the established baseline in order to determine whether or not improvement has occurred.

The CCSMM model can prove to be an invaluable tool to not only improve with self-assessment. The fortunate by product of this process is that it leads to information sharing and a greater sense of situational awareness—increasing municipal and state security.

X. CONCLUSION

Municipalities are attractive ransomware targets for attackers. They are usually underfunded and understaffed, depriving them of valid systems and employees to aid in the incident response process. They contain sensitive information that can negatively impact the lives of their citizens and the trust they place on their municipalities. Citizens are usually oblivious to the numerous services provided to them by their local government—a fact that only becomes visible in the midst of a large scale cyberattack. Birth certificates, licenses, court hearings, and property permits are all among the necessary functions provided by local governments. These are also components that are necessary for a society to thrive and grow—it is usually not possible to obtain or begin employment or a development project without the proper documentation.

Municipalities usually provide quiet victims that only get media attention when a breach has already grown into a massive cybersecurity issue. More often than not, the lack of a clear and visible threat deprives government leadership from investing more money into their IT security programs. This leaves municipalities in a situation where they must navigate around the threat of attackers, move within the confines of already limited budgets, and overcome and educate the shortcomings of poor management culture. Even in the presence of multiple attacks in the United States, cybersecurity is not always treated with the respect and attention it deserves. As seen with the case studies, city leadership usually does not invest into their security infrastructure until a threat is already at their door and causing damage to their infrastructure.

They are also sensitive to societal change—as was the case with Riviera Beach and Atlanta. While scandals are fairly common and impactful on the national stage, they are much more destructive when felt at the municipal level. National government has checks and balances

in play that were ingrained in the American Constitution—all of which are meant to preserve balance and government function in the midst of instability. Municipalities also have checks in place, but their size and reliance on local leadership can cause scandals to create imbalance and essentially dissolve solid security incident response. This is further complicated by the fact that local governments exist in a mostly autonomous capacity where they can make decisions for themselves, without having to answer to a central power. While technically possible, efforts to coerce compliance from them can do more harm than good.

This is not to say that municipal governments are completely helpless in their security efforts. City leadership can improve their security posture by investing more into their existing infrastructure. This step is usually easier said than done, but often finds itself as a byproduct of a cyberattack. In order to combat the denial of additional funds, security teams can employ the Israeli method to refine and formalize their security policy. Under this method, management and city leadership can get a clearer view of security needs and the time and price it will cost to implement their solutions.

In the absence of money, municipalities can rely on experience to address gaps in their threat knowledge base. They can join state ISAOs or create one with neighboring municipalities. ISAOs can provide a collection of experienced threats and best practices utilized by a variety of industries and organizations. They are also free and open to any municipality that wants to join. This can help facilitate the creation of policy and the training of employees. Municipalities can also organize joint exercises among their own organizations. This allows for an emergency response to be tested and improved. Finally, municipalities can also use the CCSMM to generate their own baselines and create a plan for further improvement.

Despite the uphill battles that usually await them, municipalities are not without additional strategies to improve and strengthen themselves. If properly used, all of the suggested methods for improvement can create a solid security posture that can then be shared with neighboring municipalities. All of these factors can help create a more secure state.

NOTES

1 J. Comey, (2013) Confirmation Hearing of James Comey. https://www.fbi.gov/news/podcasts/thisweek/james-comeys-confirmation-hearing.mp3/view (April 22, 2021, date last accessed)

2 G. B. White, "The community cyber security maturity model," 2011 IEEE International Conference on Technologies for Homeland Security (HST), 2011,: 173-178

3 J. P. Kesan and L. Zhang, "An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures and Cyber Losses," in IEEE Transactions on Emerging Topics in Computing.

4 A. Conklin & G. B. White, "e-Government and Cyber Security: The Role of Cyber Security Exercises", Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS'06), Kauai, HI, USA, 2006,1

5 Ibid., 2

6 Jerome H. Saltzer, and Michael D. Schroeder. "The protection of information in computer systems." Proceedings of the IEEE 63, no. 9 (1975): 1278-1308.

7Conklin and White, "e-Government and Cyber-Security" 2

8 Ibid., 2

9 Ibid., 2

10 D.F. Norris, Mateczun, L., Joshi, A. and Finin, T. , "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity," Public Admin Rev, 79: 7

11 Conklin and White, "e-Government and Cyber-Security" 4

12 Ibid., 4

13 Ibid., 4

14 Ibid., 4

15 William Hatcher & Meares, Wesley & Heslen, John, “The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices,” Journal of Cyber Policy, 2020, no. 5: 15.

16 Ibid., 15

17 D.F Norris, L .Mateczun, A. Joshi, and T. Finin , “Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity,” Public Admin Rev, 79: 7

18 William Hatcher and Wesley Meares and John Heslen, 4.

19 D.F. Norris, L. Mateczun, A. Joshi, and T. Finin, “Cyberattacks at the Grass Roots”, 4

20 Alec T. Dean "The Growth of Ransomware and its Impact on City Governments." Order No. 22616283, Utica College, 2019. http://search.proquest.com.ezproxy.lib.uh.edu/dissertations-theses/growth-ransomware-impact-on-city-governments/docview/2303232467/se-2?accountid=7107.

21 William Hatcher, Wesley Meares, and John Heslen, 3.

22 Interview with municipal IT employee, February 12, 2021

23 William Hatcher, Wesley Meares, and John Heslen, 15.

24 David McMillen. The inside story on botnets. Somers, NY: IBM Corporation, 2016

25Avi Turiel. “Build, Buy, or Lease? The 15-Minute Botnet.” Cyren Blog, July 10, 2017. https://www.cyren.com/blog/articles/build-buy-or-lease-the-15-minute-botnet.

26 Kiki Caruson and Susan Macmanus and Brian McPhee. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. Journal of Homeland Security and Emergency Management: 3.

27 Ibid., 3.

28 Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin. “Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity”, 2020, Journal of Urban Affairs: 4

29 Ibid, 4

30 Ibid., 4

31 Interview with DIR employee, March 16, 2021.

32 Donald F. Norris, and Laura Mateczun. "LOCAL GOVERNMENT CYBERSECURITY IN THE US: Survey Tells a Cautionary Tale." LOCAL GOVERNMENT REVIEW: Putting Research Into Practice (2017): 4.

33 Ibid., 5

34 Interview with municipal IT employee, February 12, 2021.

35 Oliver Baker. "What Is Bitcoin and Why Does Ransomware Love It?" Https://www.eurostaffgroup.com. May 25, 2017. Accessed April 11, 2021. https://www.eurostaffgroup.com/media-hub/what-is-bitcoin-and-why-does-ransomware-love-it-85435/.

36 DIR, "August 2019 Ransomware and Incident Response in Texas," 2019: 9

37 Ibid., 3-4

38 Ibid., 5

39 Greg Belding. "Malware Spotlight: Sodinokibi." Security Boulevard, April 9, 2020. https://securityboulevard.com/2020/04/malware-spotlight-sodinokibi/#:~:text=This%20ransomware%2Das%2Da%2D,so%20interesting%20is%20its%20origin.

40 Trend Micro Research. "Examining a Sodinokibi Attack." Trend Micro, January 26, 2021. https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html.

41 DIR, "August 2019 Ransomware and Incident Response in Texas":18

42 Interview with university IT employee, March 8, 2021.

43 Interview with municipal IT employee, February 12, 2021.

44 Tony Doris. "IN DEPTH: How Riviera Beach Left the Door Wide Open for Hackers." The Palm Beach Post. June 23, 2019. Accessed April 11, 2021. https://www.palmbeachpost.com/news/20190621/in-depth-how-riviera-beach-left-door-wide-open-for-hackers.

45 Ibid., 2

46 Danielle Waugh. "Riviera Beach Manager: City Has Most of Its Data Back after Ransomware Attack." WPEC. August 07, 2019. Accessed April 11, 2021. https://cbs12.com/news/local/riviera-beach-manager-city-has-most-of-its-data-back-after-ransomware-attack.

47 Ibid., 4-5

48 K. Kraszewski, "SamSam and the Silent Battle of Atlanta," 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2019, pp. 1-16, doi: 10.23919/CYCON.2019.8757090.

49 Tamara Chuang. "How SamSam Ransomware Took down CDOT and How the State Fought Back -- Twice." The Colorado Sun. August 07, 2020. Accessed April 11, 2021. https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/.

50 Ibid., 2

51 Ibid., 2

52 Ibid., 3

53 Lawrence Abrams. "A Closer Look at the RobbinHood Ransomware." BleepingComputer. May 28, 2019. Accessed April 12, 2021. https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/.

54 Ibid., 2

55 Alina Georgiana Petcu. "The Curious Case of the Baltimore Ransomware Attack: What You Need to Know." Heimdal Security Blog. February 23, 2021. Accessed April 12, 2021. https://heimdalsecurity.com/blog/baltimore-ransomware/.

56 Ibid., 2

57 Niraj Chokish. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next." The New York Times. May 22, 2019. Accessed April 12, 2021. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html#:~:text=Hackers Are Holding Baltimore Hostage: How They Struck and What's Next,-After it was&text=More than two weeks ago,to the hackers' ransom demands.

58 Ibid., 2

59 Alina Georgiana Petcu. “The Curious Case of Baltimore”: 2

60 Lily Hay Newman. "The SamSam Ransomware That Hit Atlanta Will Strike Again." Wired. Accessed April 12, 2021. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/.

61 Ibid., 2

62 Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin. “Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity”, 4

63 Lily Hay Newman. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare." Wired. April 24, 2018. Accessed April 12, 2021. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

64 K. Kraszewski, "SamSam and the Silent Battle of Atlanta,"3.

65 Andy Greenberg. "A Hacker Tried to Poison a Florida City's Water Supply." Wired. Accessed April 12, 2021. https://www.wired.com/story/oldsmar-florida-water-utility-hack/.

66 Ibid., 2

67 J. P. Kesan and L. Zhang, "An Empirical Investigation,” 13.

68 D. F. Norris, L.Mateczun, , A. Joshi. and T. Finin, “Cyberattacks at the Grass Roots,” 3.

69 Israel. National Cyber Directorate. Prime Minister's Office. CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION. By National Cyber Security Authority. 1st ed. Prime Minister's Office. 24-30.

70 Ibid., 30

71 Interview with university IT employee, March 8, 2021.

72 Interview with DIR employee, March 16, 2021.

73 Interview with university IT employee, March 8, 2021.

74 "History." Dont Mess With Texas. February 02, 2021. Accessed April 13, 2021. https://www.dontmesswithtexas.org/about/history

75 A. Conklin & G. B. White, “e-Government and Cyber Security”, 5

76 Ibid., 5

77 Ibid., 6

78 Ibid., 6

79 "About the CIAS." The CCSMM. Accessed April 13, 2021. https://cias.utsa.edu/the-ccsmm.html.

REFERENCES

1. "About the CIAS." The CCSMM. Accessed April 13, 2021. https://cias.utsa.edu/the-ccsmm.html.
2. "History." Dont Mess With Texas. February 02, 2021. Accessed April 13, 2021. https://www.dontmesswithtexas.org/about/history
3. Abrams, Lawrence. "A Closer Look at the RobbinHood Ransomware." BleepingComputer. May 28, 2019. Accessed April 12, 2021. https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/.
4. Baker, Oliver. "What Is Bitcoin and Why Does Ransomware Love It?" Https://www.eurostaffgroup.com. May 25, 2017. Accessed April 11, 2021. https://www.eurostaffgroup.com/media-hub/what-is-bitcoin-and-why-does-ransomware-love-it-85435/.
5. Belding, Greg. “Malware Spotlight: Sodinokibi.” Security Boulevard, April 9, 2020. https://securityboulevard.com/2020/04/malware-spotlight-sodinokibi/#:~:text=This%20ransomware%2Das%2Da%2D,so%20interesting%20is%20its%20origin.
6. Caruson, Kiki & Macmanus, Susan & McPhee, Brian. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. Journal of Homeland Security and Emergency Management: 3.
7. Chokshi, Niraj. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next." The New York Times. May 22, 2019. Accessed April 12, 2021. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html#:~:text=Hackers Are Holding Baltimore Hostage: How They Struck and What's Next,-After it was&text=More than two weeks ago,to the hackers' ransom demands.
8. Chuang, Tamara. "How SamSam Ransomware Took down CDOT and How the State Fought Back -- Twice." The Colorado Sun. August 07, 2020. Accessed April 11, 2021. https://coloradosun.com/2020/02/03/how-samsam-ransomware-took-down-cdot-and-how-the-state-fought-back-twice/.
9. Comey, J. (2013) Confirmation Hearing of James Comey. https://www.fbi. gov/news/podcasts/thisweek/james-comeys-confirmation-hearing.mp3/view (April 22, 2021, date last accessed)

10. Dean, Alec T. "The Growth of Ransomware and its Impact on City Governments." Order No. 22616283, Utica College, 2019. http://search.proquest.com.ezproxy.lib.uh.edu/dissertations-theses/growth-ransomware-impact-on-city-governments/docview/2303232467/se-2?accountid=7107.

11. DIR, “August 2019 Ransomware and Incident Response in Texas,” 2019: 1-18

12. Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin. “Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity”, 2020, Journal of Urban Affairs: 4

13. Doris, Tony. "IN DEPTH: How Riviera Beach Left the Door Wide Open for Hackers." The Palm Beach Post. June 23, 2019. Accessed April 11, 2021. https://www.palmbeachpost.com/news/20190621/in-depth-how-riviera-beach-left-door-wide-open-for-hackers.

14. Greenberg, Andy. "A Hacker Tried to Poison a Florida City's Water Supply." Wired. Accessed April 12, 2021. https://www.wired.com/story/oldsmar-florida-water-utility-hack/.

15. Hatcher, William & Meares, Wesley & Heslen, John, “The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices,” Journal of Cyber Policy, 2020, no. 5: 15.

16. Interview with DIR employee, March 16, 2021.

17. Interview with municipal IT employee, February 12, 2021.

18. Interview with university IT employee, March 8, 2021.

19. Israel. National Cyber Directorate. Prime Minister's Office. CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION. By National Cyber Security Authority. 1st ed. Prime Minister's Office. 24-30.

20. K. Kraszewski, "SamSam and the Silent Battle of Atlanta," 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2019, pp. 1-16

21. McMillen, David. *The inside story on botnets*. Somers, NY: IBM Corporation, 2016

22. Newman, Lily Hay. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare." Wired. April 24, 2018. Accessed April 12, 2021. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

23. Newman, Lily Hay. "The SamSam Ransomware That Hit Atlanta Will Strike Again." Wired. Accessed April 12, 2021. https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/.

24. Norris, D.F., Mateczun, L., Joshi, A. and Finin, T. , “Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity,” Public Admin Rev, 79: 7

25. Norris, Donald F., and Laura Mateczun. "LOCAL GOVERNMENT CYBERSECURITY IN THE US: Survey Tells a Cautionary Tale." LOCAL GOVERNMENT REVIEW: Putting Research Into Practice (2017): 4.

26. Petcu, Alina Georgiana. "The Curious Case of the Baltimore Ransomware Attack: What You Need to Know." Heimdal Security Blog. February 23, 2021. Accessed April 12, 2021. https://heimdalsecurity.com/blog/baltimore-ransomware/.

27. Saltzer, Jerome H., and Michael D. Schroeder. "The protection of information in computer systems." *Proceedings of the IEEE* 63, no. 9 (1975): 1278-1308.

28. Turiel, Avi. “Build, Buy, or Lease? The 15-Minute Botnet.” Cyren Blog, July 10, 2017. https://www.cyren.com/blog/articles/build-buy-or-lease-the-15-minute-botnet.

29. Waugh, Danielle. "Riviera Beach Manager: City Has Most of Its Data Back after Ransomware Attack." WPEC. August 07, 2019. Accessed April 11, 2021. https://cbs12.com/news/local/riviera-beach-manager-city-has-most-of-its-data-back-after-ransomware-attack.