HOBBY
SCHOOL OF PUBLIC AFFAIRS
UNIVERSITY of HOUSTON

White Paper Series
No. 16

“Holy Moly” – Municipal Organizations and the Cyber Ransomware Problem

Hector Ocampo and Chris Bronk

September 2021

Report:

“Holy Moly” – Municipal Organizations and the Cyber Ransomware Problem

Abstract

Cyberattacks on municipal governments are rising, often bringing significant financial damage and disruption with them. Despite their frequency, municipal governments still struggle to levy defenses against them. Shortcomings in information technology management in municipalities manifest in poor cybersecurity. Of particular interest is the problem of cryptographic ransomware, in which cybercriminal syndicates levy significant ransoms, often paid in cryptocurrencies. This paper chronicles the rise of this form of cyberattack against local government, with particular attention to a case occurring in 2019 across the State of Texas. Observations from interviews undertaken for that case are employed as the basis for a set of recommendations on how local government may adapt to confront the ransomware issue.

1
Introduction

On August 19, 2019, nearly two-dozen municipal organizations across the State of Texas were wracked by a cyberattack which shut down workstations and servers used to conduct the business of government at the local level. Many of the impacted municipalities were poorly equipped to cope with this attack, involving a form of malware (*mal*icious soft*ware*, intentionally designed to cause harm), called ransomware, which encrypted data resources until a substantial ransom was paid.[1] This ransomware incident is instructive to public policy practitioners and scholars as digital government issues advance alongside the rapid pace of technological innovation. Provided here is a chronicle of the 2019 Texas ransomware attack, as well an overview of malicious software (a.k.a *malware*) and other threats to municipal IT resources; the issues faced in constructing resilient e-government at the municipal level, including prior municipal cybersecurity cases; and consideration of policy that may aid local governments in protecting themselves and the communities they serve from cyberattack.

We commence our study with the observation that municipal governments in the United States and beyond represent some of the easiest targets for cybercriminal organizations.[2] "Cyber extortion and disruption incidents are on the rise because many governments have poor security postures."[3] This is largely attributed to a lack of funding. "Municipal governments are often poorly funded and face significant obstacles in competing with employers in industry to hire capable Information Technology (IT) staff."[4] Additionally, staff typically lack training and experience with cybersecurity issues.[5] Given that municipal governments function autonomously and do not necessarily follow state- or federal-defined cybersecurity policies, IT vulnerabilities often coalesce in municipal governments

[1] Fernandez, Manny, Mihir Zaveri, and Emily S. Rueb. "Ransomware Attack Hits 22 Texas Towns, Authorities Say." *The New York Times*, August 20, 2019.

[2] Preis, Benjamin, and Lawrence Susskind. "Municipal Cybersecurity: More Work Needs to be Done." *Urban Affairs Review* (2020).

[3] Kesan, Jay P., and Linfeng Zhang. "An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures and Cyber Losses." *IEEE Transactions on Emerging Topics in Computing* (2019).

[4] Goodyear, Marilu, Holly Goerdel, Shannon Portillo, and Linda Williams. "Cybersecurity management in the states: The emerging role of chief information security officers." *Available at SSRN 2187412* (2010).

[5] McFarland, Christiana, Brenna Rivet, Kyle Funk, Rose Kim, and Spencer Wagner. *State and Local Partnerships for Cybersecurity: A State-by-State Analysis*. National League of Cities, 2020.

that may exploited by individuals or groups in the form of cyberattacks, usually designed to purloin valuable data or exact ransoms to restore normal system operations, or both.

IT professionals in municipalities hold an important and underappreciated role in enabling the services that local governments provide, from collecting parking fees to issuing documents such as birth or death certifications. While municipalities have advanced their capabilities in delivering services via IT, "they [as well as state government] have typically lagged behind the federal government when it comes to setting and implementing security standards, hiring skilled personnel, and partnering with private industry."[6] U.S. cities and counties have become increasingly frequent targets for cyberattack in the last five years.[7] These "attacks," which are definitely damaging, but not necessarily in the same ways as an act of terrorism or international conflict, bring with them real costs in downtime, unavailable services, and remediation that ultimately fall upon municipal taxpayers. Mounting an effective set of countermeasures to these events has immediate, tangible impact. The first part of process of mounting an effective defense is to understand the threat.

[6] Wolff, Josephine, and William Lehr. "When cyber threats loom, what can state and local governments do?" *Geo. J. Int'l Aff.* 19 (2018): 67.

[7] McFarland, Christiana, Brenna Rivet, Kyle Funk, Rose Kim, and Spencer Wagner. *State and Local Partnerships for Cybersecurity: A State-by-State Analysis*.

2
Contemporary Cyberattacks and Ransomware

Cyberattacks come in myriad varieties, that typically subvert one or more core attribute of security regarding information and computing technologies: the confidentiality; integrity; or availability of information in digital form. It is easy to concoct scenarios for a failure of each of these attributes in a municipal context.[8] Evidence held by police and courts made public through a loss of confidentiality might damage a case or the broader judiciary process. A compromise of integrity in the city or county tax office's database might be detrimental to the community both in the work needed to reconstruct accurate data and the loss of trust with the municipality. Faults in availability are often especially easy to detect, for instance when the website for issuing fishing licenses or construction permits is knocked offline. These systems constitute the "attack surface" of municipal government IT; the targets of cyberattacks.[9] These systems contain vulnerabilities that may be exploited by malicious actors. These are the computers that are "hacked," and typically they are hacked by criminals, typically residing, and operating outside the United States. Cyberattacks are conducted by people who are often clever, persistent, and adaptive. They are doing what they do for a living. The best of breed are the innovators in attack tool development and modification.[10]

While there are many forms of cybercriminal behavior, ransomware is the most common form of cybercriminal action today. Ransomware is placed within a computer network environment. It then self-propagates to all connected computers.[11] Once it has gained access to a large portion of the organization's computers, ransomware proceeds to encrypt data, rendering it useless to the organization without a decrypting key. Following system compromise, users are greeted with an on-screen message detailing the dollar

[8] Sumi, Farhana Haque, Lokesh Dutta, and Farhana Sarker. "A review on cyberattacks and their preventive measures." *International Journal of Cyber Research and Education (IJCRE)* 1, no. 2 (2019): 12-29.

[9] Manadhata, Pratyusa, and Jeannette M. Wing. *Measuring a system's attack surface*. Carnegie-Mellon Univ., School of Computer Science, 2004.

[10] Wall, David. *Cybercrime: The transformation of crime in the information age*. Vol. 4. Polity, 2007.

[11] O'Gorman, Gavin, and Geoff McDonald. *Ransomware: A growing menace*. Symantec Corporation, 2012.

amount of regaining their data through provision of a key for unlocking the data.[12] The number of organizations impacted by ransomware is large and growing.[13]

Much like other organizations, municipal government offices and agencies end up becoming ransomware targets because they are relatively low risk, high reward targets with valuable information. For hackers operating outside the United States and the world's major Western democracies, there is little risk in attacking them.[14] What makes them lucrative targets is that they hold data including personally identifiable information (PII) and financial data, which can be sold easily to other criminals and used to open credit card accounts or commit other acts of fraud.[15] Ransomware syndicates now typically steal large quantities of data as well as encrypting systems of the targeted organization. Payment of the ransom is supposed to yield deletion of the stolen data and decryption of the encrypted workstations, servers, and other computing devices.

The chain of events involved that compose the anatomy of a cyberattack is well-studied.[16] Typically, attackers compromise an individual system or application, allowing them to create a foothold on the targeted network. This point of compromise is the attacker's vantage point for collecting intelligence regarding the compromised network. Such activities include: port scanning, system identification and observation, network traffic monitoring, and vulnerability scanning, and others. The information discovered in this process is then employed to tailor attacks designed to steal data, disrupt systems, or elicit ransoms.

Once systems are compromised, the most important action for the defender is to be alerted of that state, an area in which much automation and machine learning techniques have been applied.[17] Response time information is invaluable as it can help an attacker formulate a well-formed attack. For example, the water plant far from city hall could be

[12] Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. "Cutting the gordian knot: A look under the hood of ransomware attacks." In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 3-24. Springer, Cham, 2015.

[13] Adamov, Alexander, and Anders Carlsson. "The state of ransomware. Trends and mitigation techniques." In *2017 IEEE East-West Design & Test Symposium (EWDTS)*, pp. 1-8. IEEE, 2017.

[14] Dean, Alec T. "The Growth of Ransomware and its Impact on City Governments." Capstone Project, Utica College, 2019.

[15] van de Weijer, Steve GA, Rutger Leukfeldt, and Wim Bernasco. "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking." *European Journal of Criminology* 16, no. 4 (2019): 486-508.

[16] Yadav, Tarun, and Arvind Mallari Rao. "Technical aspects of cyber kill chain." In *International Symposium on Security in Computing and Communication*, pp. 438-452. Springer, Cham, 2015.

[17] Rhoades, Doug. "Machine actionable indicators of compromise." In *2014 International Carnahan Conference on Security Technology (ICCST)*, pp. 1-5. IEEE, 2014.

manipulated by cyber means and used as a decoy while the attacker focuses on other city infrastructure.[18] And while the criminal activity against a single municipality may seem mundane, it is quite possible that the activity could be leveraged by foreign nation states.[19] Disruption of one, small municipality is a minor nuisance. Disruption of dozens of them, simultaneously is another matter.

That is exactly why the 2019 Texas Ransomware case described below is interesting, as well as worrisome. While we know that the ransomware problem has grown exponentially in both public and private organizations, seeing one ransomware attack reach across a state with a population roughly equal to Venezuela's is troubling.[20] Then there is the impact of ransomware on each affected entity. Ransomware attacks have caused multiple, large municipal governments' operations to slow to a crawl, including in Atlanta, Georgia and Baltimore, Maryland, two large cities. Ransomware often forces government offices to *revert to "analog" pen and paper recording*.[21] It also forces a hard decision for municipal government: Do they pay the ransom or do try their best to restore function without doing so? Paying a ransom is not always a guarantee of decryption and may invite future ransom attacks.[22] Also, unlike large corporations or federal agencies, the resources available for cybersecurity programs in municipal governments are often far more limited. Building back from complete data loss may cost many times the ransom. As local government has widely adopted digital technologies to undertake its work, the vulnerability of those systems is worrisome. To better understand our concern, we must visit the underpinnings of e-government, or how IT helps government do business.

[18] Interview with municipal IT employee, February 12, 2021.

[19] William Hatcher, Wesley Meares, and John Heslen.

[20] Sultan, H., Khalique, A., Alam, S. I., & Tanweer, S. (2018). A Survey on Ransomware: Evolution, Growth, and Impact. *International Journal of Advanced Research in Computer Science*, 9(2).

[21] J. Comey, (2013). Confirmation Hearing of James Comey.

[22] Simoiu, Camelia, Joseph Bonneau, Christopher Gates, and Sharad Goel. "'I was told to buy a software or lose my computer. I ignored it:' A study of ransomware." In *Fifteenth Symposium on Usable Privacy and Security*. 2019.

3
E-Government and Municipal Cybersecurity

E-government refers to the computerization of government activities and transactions.[23] Applying for a driver's license, paying taxes, or requesting a birth certificate are all increasingly undertaken via Internet-connected computer resources. It is incredibly cost effective to incorporate Internet operations into municipal activity rather than employ paper records and face-to-face interactions.[24] Municipal activities once conducted in person or by moving printed documents now fit into one of three cyber-service models. These are: Government to Government (G2G) communications, across multiple levels of government, Government to Citizen (G2C) interactions between a residents and government, and Government to Business (G2B) exchanges between corporations and government entities.[25] Exchange of information with government has become more frictionless than ever before. While convenient, this new model also brings the weaknesses of reliance upon IT systems.

The Internet was originally designed for scholars and computer engineers seeking to communicate with each other. It served a community that held a high degree of trust for its membership. The Internet is now shared by billions and facilitates an ever-increasing set of government functions. Traditional mechanisms for certifying identity in government offices have been replaced by weak forms of authentication easily subverted by malicious parties.[26] The data aggregated in these transactions is valuable to criminal enterprise and is often stolen by cyber means. Over half of the cyberattacks experienced by municipal governments are data breaches. These breaches can easily be converted to widescale identity theft and fraud.[27]

Deployment of e-government is further complicated by its public nature. Communication that occurs within a police department and a city's water plant may contain large amounts of sensitive information, while the communication between the parks and recreation department may contain very little.[28] In the United States e-government efforts are

[23] 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, 2019.

[24] Ciborra, Claudio U. "Interpreting e-government and development: Efficiency, transparency or governance at a distance?." In *Bricolage, Care and Information*, pp. 90-110. Palgrave Macmillan, 2009.

[25] Conklin, A and 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.

[26] Conklin and White, "e-Government and Cyber-Security."

[27] Norris, D.F., 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.

[28] Conklin and White, "e-Government and Cyber-Security."

complicated due to the lack of a central authority for it. With 50 states and more than 3,000 counties, a variety of approaches to e-government were constructed at the lower levels of government. Securing these systems and the processes they facilitate represents an enormous undertaking for state and local agencies.[29] There is a lengthy record of cases from which we can learn in advancing that endeavor.

[29] Norris, Donald, Anupam Joshi, and Tim Finin. “Cybersecurity challenges to American state and local governments.” In *15th European Conference on eGovernment*, pp. 196-202. Academic Conferences and Publishing Int. Ltd., 2015.

4
A Brief History of Municipal Cyberattacks

In the lore of cyberattacks against municipalities, the point of origin is often considered one launched in April 2000 against the Australian city of Maroochy Shire on the country's eastern coast. Undertaken by a disgruntled software developer who had deployed pieces of Supervisory Control and Data Acquisition (SCADA) equipment onto the city's sewage management system, the Maroochy Shire, the insider cyberattack against the system caused a large release of raw sewage, including on the grounds of a major resort hotel. While this incident was mentioned as a warning for years after it happened, a spate of cyberattacks against municipalities has occurred in the last few years. Although local government was not immune to cyberattack, the problem has been largely at the margins. For instance, Aransas County, Texas was targeted by the Anonymous hacker group after it demanded that an elected family court judge be removed from office. Anonymous compromised county servers and relented after local officials explained via media that removing the judge was a state function.[30] This act of hacktivism is a far cry from the criminal extortion that has become the norm in municipal cybersecurity. Atlanta's brush with ransomware is a logical point to begin a review of this topic.

4.1 SamSam's ransoms of state and local government

In May 2018, Atlanta was compromised by the *SamSam* ransomware. SamSam relies on public facing single-factor authentication applications like RDP (remote desktop protocol) or FTP (file transfer protocol) to gain entry. The SamSam attack severely hampered the city's ability to process utility payments and manage sewer infrastructure requests. It forced the police department to file reports manually. In addition, the municipal court system was unable to hold hearings as the records need to verify warrant data were inaccessible. Even the municipally provided WiFi at Atlanta's Hartsfield International Airport, the nation's busiest, was knocked offline. A ransom for $50,000 in Bitcoin was exchanged for decryption of the encrypted data.[31] The malware employed against Atlanta deserves some attention.

SamSam was considered unique in that it purposefully offers victims with reasonably affordable ransoms. In some instances, SamSam's creators decrypted non-essential

[30] The author was part of the initial response to the Aransas County hack surrounding the 2011 release on YouTube of a video shot by the judge's daughter of an alleged act of domestic abuse against her. The Anonymous hacker group demanded his immediate dismissal, which is impossible for elected judges in Texas.

[31] Lily Hay Newman. "The SamSam Ransomware That Hit Atlanta Will Strike Again." *Wired*, March 30, 2018.

data, *sans* charge, 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.[32] SamSam has been associated with Gold Lowell, a cybercrime group alleged to be located in Iran.[33] Unlike other ransomware, it is not sold to online buyers as a service, but rather reserved for Gold Lowell and is frequently updated to circumvent antivirus detection.

Despite paying the requested ransom, Atlanta spent a total of $2.6 million on recovery efforts. Most of the expenses were in digital forensics, security advisory staff, and additional efforts to return systems to pre-attack operational states.[34] Costs added up to a figure many times the original amount of the ransom. Before it was compromised, Atlanta failed a security compliance assessment, mentioned in a January 2018 City Auditor's Report. Additionally, Atlanta did not have a formalized process to identify, assess, and mitigate risks.[35] Many of the processes put in place to secure critical data were done so in a reactive patchwork process that was not well-documented. Atlanta's failed security audit should have been a massive red flag to city leadership and SamSam was already a well-known commodity in cybersecurity circles.[36]

Before Atlanta's headline grabbing incident with SamSam, the Colorado Department of Transportation (CDOT) was also compromised by it, in February 2018. To protect itself from cyber or other disruptions, Colorado had previously established Backup Colorado, which was designed safeguard state infrastructure from disruptions. Due to confidence in backup processes, CDOT refused to pay the ransom. The attack was concentrated on CDOT functions deemed non-critical. The lack of an imminent public safety concern greatly contributed to the refusal to pay the ransom. It took roughly one week to restore the system back to working order.

While SamSam's impact on Atlanta was probably mitigated by payment of the ransom, in Colorado the attackers retained a foothold on CDOT's systems. This "reinfection" included employing additional tools on CDOT's network, in addition to the SamSam ransomware. The CDOT security team had found and removed SamSam, but only focused on the immediate areas of compromise. When CDOT's systems failed again, a state of emergency was declared by Colorado's Office of Emergency Management. After this, the Colorado National Guard deployed a team of roughly a half-dozen security professionals. The reinforced response team was able to organize a more detailed

[32] Lily Hay Newman. "The SamSam Ransomware That Hit Atlanta Will Strike Again."
[33] K. Kraszewski, "SamSam and the Silent Battle of Atlanta," *2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2019, pp. 1-16.
[34] Lily Hay Newman. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare." *Wired*. April 24, 2018.
[35] Lily Hay Newman. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare."
[36] Donald F. Norris, Laura Mateczun, Anupam Joshi & Tim Finin. "Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity."

approach to recovery. This broader effort was effective and CDOT was able to successfully recover.

4.2 RobbinHood and next-generation ransomware

Roughly a year after the SamSam attacks, a new form of ransomware began compromising systems, *RobbinHood*. While RobbinHood's mechanism for network compromise is not entirely clear, its behavior points to the entry point being a compromised domain controller, the system that performs the Internet addressing for an organization.[37] Robinhood works by searching for an RSA encryption key on a Microsoft Windows workstation or server. Then it stops Windows services for antivirus, email, and any software that can prevent further encryption. During this process, it also deletes backups of data, deletes system 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.[38]

In the wake of a public corruption scandal surrounding mayor Catherine Pugh, Baltimore, Maryland was stricken by this new variant of ransomware. City employees were welcomed with a message 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 computing infrastructure came to an abrupt halt. As in Atlanta, Baltimore's capacity to process online payments for utilities, property taxes, fines, and other city services evaporated. As a direct result, over 1,500 pending home sales were delayed.[39] Reverting to a pre-Internet mode of operation, payments could only be processed with a cashier's check or money order, along with a valid bill.

To increase pressure on the city, the attackers initiated communication with city officials via Twitter and started to leak employee information online, claiming that they would continue doing so as long as the ransom remained unpaid.[40] In addition to the removal of online payment systems and the leaking of sensitive documents, Baltimore's city email system was disabled. City employees resorted to creating Gmail accounts to restore email communication channels. Comically, Google's automated cybersecurity systems detected multiple new Gmail accounts originating from the same network and disabled all

[37] Lawrence Abrams. "A Closer Look at the RobbinHood Ransomware." *BleepingComputer*. May 28, 2019.

[38] Lawrence Abrams. "A Closer Look at the RobbinHood Ransomware."

[39] Niraj Chokish. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next." *The New York Times*. May 22, 2019.

[40] Niraj Chokish. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next."

the accounts created, producing additional downtime.[41] Fortunately, Google quickly addressed city complaints and restored the accounts.

Recovery from RobbinHood eventually cost Baltimore roughly $18.2 million. Expenditures included loss of revenue, purchase of new personal computers and servers, and additional threat mitigation. Funding came from the city's cyber insurance policy and reallocating existing city funds. Despite being able to eventually recover, Baltimore, like Atlanta, found itself in a position where its lack of strong security policy resulted in a severe lack of situational awareness during a malware incident. Once again, the remedy was underwritten by a large expenditure, however, not without city leaders losing trust and goodwill with its citizens. Allegations were made that Baltimore's systems were compromised by hackers employing the National Security Agency's *Shadow Brokers* leak, in which the agency's bespoke cyber espionage tools were discovered and repurposed by cybercriminal and foreign intelligence organizations. While this was ultimately not the case, relations between Baltimore and its federal neighbor soured. Despite the United States' premiere cyber defense agency being pulled into the ransomware issue, the problem worsened through 2019.

[41] Alina Georgiana Petcu. "The Curious Case of Baltimore."

5

Compromise Everywhere: the Texas Ransomware Attack

In August 2019, some 22 municipalities across Texas were compromised by a new variant of ransomware. The attack was likely conducted by a sole attacker working with a ransomware organization, SODIN23 and has become known as *Sodinokibi*. Sodinokibi is a successor to *GandCrab* (a ransomware variant that was responsible for 40 percent of global ransomware infections at one time) and has been seen only affecting countries outside of the former USSR.[42] The ransomware attack launched against the Texas municipalities can almost certainly be traced back to Russia or a country in Russia's orbit.[43] One of those municipalities, Borger, a city of roughly 13,000 outside of Amarillo, received the demand for $2.5 million for the cryptographic key necessary to decrypt their data. Then city commissioner and now mayor Pam Gosline's reply to the ransom figure was simply, "'Holy moly!!!!!'"[44]

As was the case in Atlanta and elsewhere, in the immediate aftermath of the attack, numerous local government offices found themselves unable 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 engaged in an uphill struggle to cope with both inadequate policy and the immediate damage of the ransomware. This ransomware attack, like many other cyberattacks, 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. The Texas Information Sharing and Analysis Organization (TxISAO) and Texas Association of Governmental Information Technology Managers (TAGITM) were drawn into the remediation phase of this ransomware attack and became hubs of information to numerous cybersecurity responders across the state. The response to the attack could be characterized as ad hoc in nature.

The Texas ransomware attack was also significant in that it laid bare a major hiccup in the communication process, that municipalities in Texas are completely autonomous and

[42] Belding, Greg. "Malware Spotlight: Sodinokibi." *Security Boulevard*, April 9, 2020.

[43] Richardson, Ronny, and Max M. North. "Ransomware: Evolution, mitigation and prevention." *International Management Review* 13, no. 1 (2017): 10.

[44] Bleiberg, Jake and Eric Tucker. "'Holy moly!: Inside Texas' fight against a ransomware hack." *AP*, July 26, 2021.

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, including cybersecurity.[45] This also explained why there were so many unique cybersecurity configurations across the Texas cities in this case.

Eventually, Texas' Department of Information Resources (DIR) initiated the process of determining how the ransomware incident occurred. DIR's investigation explained the presence of the attacker on a managed service provider's (MSP) server. The attackers gained access into a remote desktop server maintenance application, Elsinore Technologies' ScreenConnect (now ConnectWise Control). ScreenConnect is an access tool allows an authorized user to transfer files and execute code on client machines, simplifying system maintenance and upkeep. For the municipalities involved, the remote desktop service is extremely convenient as it allows the MSP to remotely manage its clients' servers and workstations. When major system patching and updating is needed, this remote access can make short work of a multiple hour or multiple day jobs. However, in compromising this service, the attacker was granted the same capability and used it to propagate ransomware. In gaining access to ScreenConnect, the attacker likely compromised administrator credentials and exploited numerous, well-known vulnerabilities in the in the ScreenConnect software.[46]

The ScreenConnect software was operated by a TSM Consulting Services, Inc, which, "provides data communications service for Texas communities, linking police agencies to a statewide law enforcement database."[47] As additional details became apparent, ScreenConnect's administrator console was found to be exposed to the Internet. Its connection to numerous endpoint computing devices, combined with its presence on the Internet, made for a highly tempting target. Additionally, the DIR 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, a tool of cyber criminals operating in the former Eastern Bloc. Once the networks of the Texas municipalities were compromised, Sodinokibi established communications with a command-and-control server (the machine used by an attacker to coordinate an attack).[48] This was likely not the first time Sodinokibi exploited the ScreenConnect platform, hinting that the program was a regular target.[49]

Fortunately, the proverbial cybersecurity wheels had already been turning prior to the completion of the attack. The recovery efforts were successful, largely in part to the Texas

[45] Interview with university IT employee, March 8, 2021.

[46] Department of Information Resources, "August 2019 Ransomware and Incident Response in Texas." 2019.

[47] Bleiberg, Jake and Eric Tucker. "'Holy moly!: Inside Texas' fight against a ransomware hack."

[48] Trend Micro Research. "Examining a Sodinokibi Attack." Trend Micro, January 26, 2021.

[49] Department of Information Resources, "August 2019 Ransomware and Incident Response in Texas."

Department of Emergency Management (TDEM) Security Operations Center's capacity to communicate with local entities and coordinate with the field teams. Months before the attack, in June 2019, Texas Senate Bill 64 was enacted giving the governor the authority to employ the Nation Guard in cyber-defense roles. Additionally, House Bill 8 was passed in 2017 and called for DIR to draft an incident response plan, which would be employed after SODIN23 was detected.[50] 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. These provisions allowed Texas's National Guard to mobilize cybersecurity professionals to aid the stricken communities. One of the senior reservists involved in the response also held down a full-time civilian position in technical operations at Dell Technologies, headquartered just outside Austin.[51]

To respond to the multiple incidents playing out across the state, other institutions at the state and federal levels became involved including: the Texas Military Department (which includes the Army and Air National Guard); Texas Division of Emergency Management; Texas A&M University System's Security Operations Center; the Department of Public Safety; the Federal Bureau of Investigation; and the U.S. Department of Homeland Security. By pooling government resources and reaching out to private sector entities, a statewide response was assembled and coordinated through the creation of multiple incident response teams. Each team was responsible for addressing a specific component of the relief efforts.[52] These ranged from field incident response, conducting a forensic analysis on the attack, and completing a criminal investigation on who coordinated the attack.

One of the major takeaways for those impacted was that multiple municipalities found themselves without effective cybersecurity policy—allowing the ransomware to burrow deeper into their networks and complicated response to the incident. It is also important to note that all the affected municipalities were not hit with the same intensity. The ones that were impacted heavily typically had little to no incident management policy in place. For instance, a small municipality, in Texas, did not have a comprehensive way of addressing machines infected with ransomware.[53] Borger, on the other hand, was fortunate enough to have a data backup regime in place that eased the recovery process.[54]

Each municipality refused to pay the ransom but ultimately faced the tedious process of recovery. For two weeks it was unable to process payments or issue official documents.

[50] Department of Information Resources, "August 2019 Ransomware and Incident Response in Texas."
[51] Bleiberg, Jake and Eric Tucker. "'Holy moly!: Inside Texas' fight against a ransomware hack."
[52] Department of Information Resources, "August 2019 Ransomware and Incident Response in Texas."
[53] Interview with municipal IT employee, February 12, 2021.
[54] Bleiberg, Jake and Eric Tucker. "'Holy moly!: Inside Texas' fight against a ransomware hack."

Moreover, there was no clear-cut incident management policy. Through collaboration with other citizens and local computer repair shops, they created an ad hoc response plan.[55] When asked about the internal shortcomings that amplified the attack impact, the IT manager 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, panicked during the ransomware attack. This town's leadership left cybersecurity on the backburner. But the shock of severe compromise by cyberattack had a positive upshot. Cyber defense capabilities have been greatly enhanced. Regular employee training is now commonplace, and formal cybersecurity policies are also more common. The ransomware attack caused a reevaluation of security policies and triggered an effective, statewide response. From this episode spring lessons for public policy that may be adopted elsewhere to prevent future ransomware attacks from producing costly damage.

[55] Interview with municipal IT employee, February 12, 2021.

6

Remedies for the Municipal Cybersecurity Problem

Through the cases identified here we assess that while cyberattacks and their ability to cause large amounts of damage are worrisome, they can be mitigated. Even the most complex of attacks can be blunted by an effective cybersecurity policy and a degree of preparation. Local government leaders and policy professionals can better prepare municipalities, both large and small, against cyberattack. Loud are calls for increased budgetary resources for cybersecurity, and while the resources would no doubt be appreciated, we should also consider how to efficiently allocate resources across communities. The SODIN attack against Texas communities was eventually mitigated, with larger players including state agencies, including the National Guard as well as federal authorities playing important roles in that process. Building on our assessment of this incident, what is needed are well-prepared strategies for mutual assistance (rather than ad hoc ones), local planning for cyberattack mitigation and response, and exercises to prepare for cyber incidents before they occur.

Rendering aid in a collective defense model at the state level centralizes resources that may then be allocated when attacks occur. Attempting to push down cyber tools and staff into the smallest of communities may be wasteful. After 9/11, counter-terrorism equipment and training including the sort designed to cope with nuclear, biological, and chemical (NBC) attacks was received by some communities but not others. Some communities received federal support while others were forced to further stretch law enforcement budgets to cope with the terrorism problem.[56] Nonetheless, every municipality should have a plan for dealing with cyberattack and drill with other communities and state authorities to be prepared.

Beyond local preparedness, there is good reason for municipalities to collaborate in the field of IT security. Collaboration can cover gaps when the capacity to go it alone on cybersecurity is unaffordable or otherwise unobtainable.[57] Municipalities have the option of joining an ISAO (Information Sharing and Analyses Organization) to better prepare

[56] Davis, Lois M., Michael Pollard, Kevin Ward, Jeremy M. Wilson, Danielle M. Varda, Lydia Hansell, and Paul Steinberg. *Long-term effects of law enforcement's post-9/11 focus on counterterrorism and homeland security*. Rand Corporation, 2010.

[57] Galinec, Darko, William Steingartner, and Vinko Zebić. “Cyber rapid response team: An option within hybrid threats.” In *2019 IEEE 15th International Scientific Conference on Informatics*, pp. 43-50. IEEE, 2019.

themselves for incoming threats.[58] In our discussions with local officials regarding SODIN, Texas's ISAO was a pivotal part of the response across the state. An ISAO is valuable in that it can combine the cybersecurity personnel from a variety of organizations who can improve measures designed to both prevent compromise and respond when attacks occur. ISAOs are largely informal organizations that just need group interest to be created.[59] Everyone is invited to be a part of the free exchange of information. Groups can consist of libraries, private firms, and universities.

In Texas, formation of the TxISAO came as a direct response to cyberattacks on municipalities.[60] It was made to help close the knowledge gaps that exist and will exist in between government 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 the state's ISAO or an increasing number of ISAOs located in large cities. The federal government can potentially reach out to all municipalities, but this has proved to be difficult as homeland security cyber resources at the local level are stretched thin.[61]

While inter-municipal collaboration is important, it can only work properly if a municipality's proverbial house is in order. In the wake of a serious cyber incident, the components of municipal government will need to work together to craft a response and coordinate with other agencies. Coordination must be tested to streamline the response process. Much like response exercises used by emergency services regarding natural or man-made disasters, cybersecurity exercises should be the norm in U.S. cities and counties. Emergency exercises 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.[62] Given that municipal government involves an entire community, exercises must focus on inclusivity to cultivate an effective response.[63] Exercises can 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. The shortcomings of these canned responses will, ideally, be revealed through successful implementations of these exercises. Walking

[58] Bakis, Bruce J., and Edward D. Wang. *Building a national cyber information-sharing ecosystem*. MITRE Corporation, 2017.

[59] Interview with university IT employee, March 8, 2021.

[60] Interview with Department of Information Resources employee, March 16, 2021.

[61] Interview with university IT employee, March 8, 2021.

[62] Weiss, Richard, Frankly Turbak, Jens Mache, Erik Nilsen, and Michael E. Locasto. "Finding the balance between guidance and independence in cybersecurity exercises." In *2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16)*. 2016.

[63] A. Conklin & G. B. White, "e-Government and Cyber Security."

through an exercise can serve as a future response plan for future intra-municipal communication and IT security.[64]

[64] Fontes, Robin L., Erik Korn, Doug Fletcher, Jason Hillman, Erica Mitchell, and Steven Whitham. “Jack Voltaic®.” *The Cyber Defense Review* 5, no. 3 (2020): 45-56.

7

Concluding Thoughts

Cybersecurity has become an important issue for almost every form of organization in the United States and much of the world. Dependence on information and computing technologies brings with it the Achilles' heel of vulnerability to cyberattack. Proliferation of ransomware activity undertaken from overseas sanctuaries has yet to be met with highly effective countermeasures by business or government. The Colonial Pipeline ransomware incident in May 2021 indicated the degree to which modern society may be disrupted by this form of cybercriminal activity. The ransomware incidents undertaken against private and public actors alike, underscore the great degree to which resiliency must be embraced and not just *efficiency*.[65] Relatively simple steps, such as maintaining a backup Domain Name System (DNS) server,[66] may considerably lessen the degree of harm that can result from a ransomware attack on local government offices. Such actions will not come without cost, however, the assumption that "It won't happen here," is false and needs to be replaced with, "It can happen here." That flip in perspective is critical for government at all levels to begin containing the ransomware problem and forcing malicious hacker groups to move on to new tactics and forms of criminal enterprise. Until then, ransomware gangs will find ample opportunity to do damage and find revenue in the easy targets found throughout local government.

[65] Linkov, Igor, and Alexander Kott. "Fundamental concepts of cyber resilience: Introduction and overview." In *Cyber resilience of systems and networks*, pp. 1-25. Springer, Cham, 2019.

[66] Lozupone, Vincent. "Disaster recovery plan for medical records company." *International Journal of Information Management* 37, no. 6 (2017): 622-626.