



## An Inside View of a Ransomware Attack Response and Recovery

---

Casey Dzimiela and Murray Jennex

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

May 7, 2023

# An Inside View of a Ransomware Attack Response and Recovery

*Casey Dzimiel*  
West Texas A&M University  
[cjdzimiel1@buffs.wtamu.edu](mailto:cjdzimiel1@buffs.wtamu.edu)

*Murray E. Jennex*  
West Texas A&M University  
[mjennex@wtamu.edu](mailto:mjennex@wtamu.edu)

## Abstract

On August 16, 2019, a ransomware attack impacted 23 organizations in north and northwest Texas. The ransomware attack was unique in that it targeted primarily small community organizations and was coordinated through a single managed service provider. Response to the attack was intense and involved several local, state, and federal organizations, with the Texas governor activating the state national guard cybersecurity unit. This paper provides a firsthand account from a member of the state national guard cybersecurity unit that responded directly to one of the affected communities. Several observations are reported, and recommendations made to help improve cybersecurity awareness and preparedness in small municipalities and small and medium organizations.

## Introduction

On August 16, 2019, 23 mostly small towns (the exception was Lubbock) in Texas, ranging from near Fort Worth up through the Panhandle, were hit in a coordinated ransomware attack that demanded a \$2.5 million payment (Bleiberg and Tucker, 2021). Response was quick and since the small towns had few incident response resources, the state and federal governments stepped in within hours with Texas declaring “Level 2 Escalated Response” crisis (Raghavan, et al., 2020) and activating the cyber resources of the Texas National Guard and placing the Texas Department of Information Resources (DIR) as lead in the investigation and response. Ultimately, no ransom was paid but it did take a week for all organizations to recover and return to full operation (Achten, 2022; Bleiberg and Tucker, 2021; DIR, 2021; Freed, 2019). Investigation found the coordinated attack originated through penetration of TSM Consulting Services, a Texas firm that provides technology services to local governments. The attack spread through screen-sharing software and remote administration to seize control of the networks of some of the company’s clients (Bleiberg and Tucker, 2021; Ocampo, 2021). The attacker was traced back to being a member of the Russian based SODIN23/REvil syndicate (Achten, 2022; Bleiberg and Tucker, 2021; Ocampo, 2021). In November, 2021, the United States Department of Justice announced an indictment against Yevgeniy Polyanin for this and other ransomware attacks and seized \$6.1 million in funds traced to payments received by Polyanin for various ransom attacks (DIR, 2021).

General facts of this attack are available in the various published accounts (many cited in this paper). This paper takes the unique approach of telling the story of one of the Texas National Guard incident responders. The lead author of this paper, Casey Dzimiel, was a member of the Texas National Guard who responded to the ransomware attack and this is his story.

## **Background**

Mr. Dzimielia has been a member of the Military since 2002, a member of the Air National Guard since 2007, and a member of the Texas Air National Guard since 2010 in a unit based out of Joint Base San Antonio-Lackland. Shortly after joining the unit, they changed missions from the 273 Information Operations Squadron (IOS) to a Cyber Operations Squadron (COS). As an IOS they worked with the Active Duty performing testing operations for new IT requirements that needed to be tested before they would be released to the Production Air Force networks. As implied in the name the unit moved into the “Cyberspace” realm with its own operational mission set instead of one of more of a supporting role. Along with this came a huge process of training everyone in the unit to be qualified to perform this mission set. Most members coming in and participating in the Operational mission are normally going to have a large baseline Information Technology background then go through anywhere from 6 months to a year of in-residence Air Force classroom training to become certified. As Cyberspace is a new “Battlefield” that the Air Force and DoD is doing its best to build structure and training around they implemented several concepts from many different areas of existing Military Operations to include even the flying world.

While the Texas Air National Guard does carry out Federal Mission Sets and does attend the same training as the active-duty military as well as the reserves there are some distinct differences which are important for the sake of this paper. The biggest difference between a “State” National Guard be it Air or Army and the Reserves or Active Duty is essentially that most of the funding is provided by the State in this case Texas, along with the fact that for Guard members their state governor is directly in their Chain of Command for a majority of aspects on the way they operate on a day-to-day basis. This all gets very messy and confusing very quickly but if you boil it down to the essentials, a state guard member is both a State and Federal representative while active duty and reserves are only Federal representative. In cases of state emergencies such as a hurricane or some sort of national disaster or emergency the state governor is able to activate state guard members quicker and with less process than the federal government might be able to depending upon the situation. There are also things that the federal government is not going to act on that the state needs to be prepared for. When activated under State Active Duty (SAD) type orders you are essentially a state employee, it does count towards your federal retirement and if you were to get injured you would not do a Federal VA claim, you would be filing Workman’s Compensation with the state. This is what happens when Texas Guardsman are activated for hurricane support. This is also the reason that the Texas governor activated the Texas National Guard to respond to the ransomware attack.

## **Response to the Attack**

Mr. Dzimielia was on his drill weekend mid-month August 2019, the one weekend each month that I am on duty for training and whatever is needed to meet my requirements as a Texas Air National Guard member. Nothing out of the ordinary happened until around lunch time on Saturday there was grumblings and discussions in the leadership circles about a large ransomware attack and there was a chance that we could be activated in support of this situation in a cyber capacity. By the end of the day Saturday, I had been assigned to a 4-man team, one of 3 teams provided to the state along with several members assigned to various other support roles and was headed home to pack with expectation to be gone a week and destination to be to one of the affected North Texas municipalities. Sunday was to be our travel day and we would arrive first thing Monday morning to begin to help in any way we were able or ordered.

Arriving Monday morning at the city municipal building unsure of what we were walking into as the only thing that we had been able to ascertain was that this was not a large city. It was by no means a one stop sign or street light town; it had its own Wal-Mart and a handful of businesses and restaurants, but it did not have a very large population, only around 10,000 people. We had an understanding of the attack and what to expect from intel provided by the Texas State Operations Center (SOC.), the Texas Military Department, Texas Department of Public Safety, Texas Division of Emergency Management, Texas A&M University System, Federal Bureau of Investigation, U.S. Department of Homeland Security, and other state, federal, and private sector partners supporting the response efforts. We knew more about what to

expect from a technology standpoint as far as the ransomware than we did about the city municipality. Initially that was more important as we were there first to support the Texas SOC in their efforts for incident response and forensics.

The team did the usual introductions and were given a tour of the facility, a brief introduction to the staff and their roles and positions as well as a location where we could set our equipment and workspace. The municipality was a very small windows domain network of less than 100 or so endpoints using private IP addresses with a handful of physical servers. There was no virtualization and all the operating systems were at least one to two full versions behind of the current standard. It was 2019 and Server 2016 was out and most of the servers were running mostly 2003/2008, there might have been one server running server 2012, but it was because it was the most recently installed application server. The “Server Room” also contained the office pet cat’s litter box amongst other odds and ends boxes and storage. There were about 25 employees in total and normally around a dozen people in the office during the main office hours, there was a 24-hour capability to this facility which normally was manned by 1-2 people.

After the tour and baseline introduction was done, we immediately began to assess the situation walking through the door there was an understanding that it was ransomware and due to the multiple other Northern Texas Municipalities, that were also reporting similarities there was a rather strong list of Indicators of Compromise (IOC) that had been built by the SOC team. We split off and logged into a few workstations as well as servers that the employees had stated they were having the issues with. It was very clear that it was ransomware, almost every directory short of system directories had all files encrypted and were unusable and in each directory was copied the same txt file that was a very simple message that if they wanted to get their data restored and unencrypted they needed to contact the listed email address or phone number (Mr. Dzimielia does not remember which) and arrange to make payment. Outside of the glaringly obvious encrypted files and “Ransom Note” sprayed across the entire network there were also other malicious processes that were running and as well as ports that were opened by the attacker for command-and-control type of actions.

In the order of operations in how this particular scenario took place and the way that it was handled from an incident response and forensics type of scenario, several days had passed since this was really first reported and the Texas SOC team that had been stood up with folks from the FBI and other Texas civilian cyber resources had already done a lot of work in compiling data from the different locations so by the time we arrived on site, they had us essentially install some remote administration tools and be their hands and eyes and send them logs and data if possible that would be pertinent to the investigation. There was an attempt to do a forensic memory capture of one of the servers or workstations in an attempt for the FBI to work through and possibly find more information on the malicious party. There were also some backups of the encrypted files that were archived so that if an encryption key was discovered at another location the files could be tested and there was a possibility critical files could be encrypted and restored.

Once a determination had been made at the Texas SOC that they were not going to pay the ransom and they were more than likely not able to apprehend the hackers/actors in time to get files restored; our military team essentially turned into a restoration effort to bring the City Municipality back online and back operational as fast as possible, but with the goal being that it would be more secure than it was before. This decision was made, and we were moving and planning in that direction before the close of business that first day, Monday. At this point we an inventory of all the assets that resided in this Municipal network. This was not accomplished in a very formal ground up and thorough format as described by most asset inventory processes. Because this City Municipality was so crippled and essentially brought to a screeching halt by the ransomware; they had generated a strong idea of what was the most important services and resources for their day-to-day operations. So, it is a terrible but demented way of clearing away the chaff and the noise down to the core important assets. If you take everything away from someone and have them function like that at a gasp for air type of situation for even a small amount of time especially when it comes to anyone wanting to accomplish a task, they will quickly be able to tell you what they once had that made their life better or what things they really and truly need to do their job.

The team worked with the city employees, their leadership, as well as receiving feedback and tasks that we were given from the Texas SOC team of services or goals that had to be accomplished before we could go

home. The list was prioritized across all parties and then we began to work to set up an order of operations as far as how this was going to need to get done to restore operations to this city. By this time, it had been discovered that all the attacked municipalities' Information Technology resources were all using the same Managed Service Provider (MSP), so the same 3rd party vendor was remotely managing all these city's resource. It was never confirmed to us (though later confirmed by the Texas SOC team) that the MSP was in fact the attack vector but the evidence in the scope of the attack and who was targeted was enough to know that was probably not a coincidence. We were given instructions to rebuild the network from the domain up, to eliminate the possibility that the hacker/actors had full domain administrative rights across several of these city networks.

We generated a priority list of services that needed to be online as soon as possible down to those "nice to have". We then wiped and reloaded this entire network. We needed to back up whatever files that employees needed, even in the off chance that a decryption capability was to appear later. The way that the attacker encrypted all the files was just a script that just ran against all the files, shares, and directories on the system and encrypted what files it was able to and then placed the ransom note and moved on. Now this was quick and dirty, and it obviously worked well enough to bring the organization to its knees enough to have to call in a state of emergency. The saving grace about quick and dirty was that if the file was in use at the time or the account did not have permissions the attacker didn't care and moved on as they just wanted to create the largest impact possible.

The office did not have any backup process, policy, or procedure to speak of, if there were backups of files they were probably related to an application that required a backup to upgrade the system, so they were not formally saved or retained in any documented or logical location. There was also not any offsite or offnet backups. Most of the database driven server applications were lucky because the database files were not encrypted because they were in use. Any flat files that were just sitting idle on the server were almost all impacted. A full inventory was generated of each server of each share as well as system inventories software, services, and applications that were running and were then deconflicted with the leadership level priority restoration list. Before any server or workstation was reloaded, the software as well as licensing was confirmed, as well as any priority applications with vendor support or needed support were contacted to ensure that if we upgraded to a newer operating system that they would still support as well as if they would need to provide us any new software and updates for time of install if they were not going to assist personally. Like most things with vendors and contracts there is going to need to be a bit of deliberation as far as what is covered under the contract and what is not.

There were only a handful of servers, but they were affected and encrypted far more thoroughly than the end user devices. We replaced the credentials that were used for the servers and a lot of the workstations and some of the end user devices because not all end user devices were affected in the same way. The impact from the script or the malicious logic that was used was hit or miss between end user device to device. The same process did need to occur with an inventory of software, services, and applications and then aligned with what was happening with the servers. The workstations did have their own priority list, it was such a small office, and each little section of people had many different roles within the organization that required different individual software to be installed or maybe even different local permissions to run. The benefit was that the employees that had special programs or circumstances seemed to have their own computers that they did not share with anyone else. This made it a bit easier as far as backing up information from workstations and ensuring what importance this computer provided to the organization.

As a team we had to balance the order of operations into what we needed to do to bring the municipality back up to a solid operational level with the priorities of the Texas SOC and the local leadership. We also had to manage expectations and translate requirements between the two. The office had a few key stakeholders that we worked with mostly and took final word from them. There was one employee that was essentially the local "Administrator". Now the remote MSP was the one that did the vast majority of managing the server-side infrastructure and the larger level tasks, but this employee was essentially their hands and feet on the ground in the office. The MSP would work through him or do updates or move things around and on the job train him how to take care of smaller repetitive tasks for users. He was who we dealt with initially for all usernames and passwords for any system or application and an explanation of anything that we did not know what it was. He was also the interface between our team and the MSP

where possible as well as knowing who to contact as far as any contracts or vendors for certain software that needed to be updated upon reinstallation of systems.

## **How the Municipality was Recovered**

The four-person military team divided up into three different efforts. Mr. Dzimielia worked on the server side, two others worked the end user devices, and a more senior member worked with the Texas SOC in a leadership role. We worked with the office administrator to get with the MSP to pull down new licenses and the software and attempted to gather all the drivers and firmware updates to reformat and reload the operating system on all the devices in the office building. All the operating system licensing was done as part of the MSP contract and since each of the twenty or so locations that had been hit as part of this ransomware attack, were trying to do the same recovery; there was normally a log jam of communication. Each site had a complete mirror setup of servers and operating systems. There was not much customization as everyone received the same cookie cutter setup. As the more repetitive questions came from each site the MSP started to at least get ahead of it and write out some documentation to be able to hand out to each site asking in a quicker format.

The big issue on the server side was the hardware, and mostly the RAID (Redundant Array of Independent Disks) setup for each server or at least the drivers needed to see all drives and set up the RAID. Mr. Dzimielia had the most server experience of anyone on the team but had been spoiled by working in a very large enterprise organization, mostly doing web based applications like SharePoint or various other Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) products where there was a team that was in charge of racking and doing most of this type of work. This team would normally hand over a blank running server with the chosen base operating system on it and he would in turn load his applications on it. Mr. Dzimielia understood the concepts and had experience doing them, but it was not something he did every day especially when it came to drivers for server RAIDS. Mr. Dzimielia had to learn by doing and trial and error. This was a stressful time as these servers needed to come back up, and most of the manufacturer drivers that were needed, were either lost, or so far out of date that they were no longer applicable to the server. The result was that new drivers had to be downloaded with the hope that they were not introducing any new form of evil into this network.

The workstation team had all the same shared issues working to get the software and keys from the MSP, and also needed to find drivers and updates for multiple versions of desktops and laptops along with having to find all the end user devices in the office. The team worked with the local leadership to determine which computers needed to be replaced first and then who worked on those devices and what files needed to be backed up and how to get that done. Because we did not bring in enough of our own personal resources there was nothing set up for us to remotely send and image to workstations, so it was a very manual workstation to workstation process with a USB drive going from one desk to another backing up users' information and attempting to find a location to keep it temporarily then putting it back when ready. There were several large USB hard Drives that needed to be purchased or commandeered to make the backup and reformat process possible. The local office administrator was able to help as he was familiar with this process and was something he had to do bringing new computers onto the network when things were refreshed.

Once the team were able to get to work with the MSP to determine what operating system would be used and then finding the binaries and drivers that made all the servers and workstations function; the next piece was to get the Windows Active Directory domain back up and running. This was critical for management and a standardized authentication and security model for all devices. This fell onto Mr. Dzimielia's shoulders to get this accomplished but again was not something that he did every day. Lots of Googling and Tech Net articles and following along with wizards and he was able to get the job done. For those that do not do it every day, it is not difficult to stand up a Windows Domain, that was not the concern, the concern was to do it in a manner that afforded this Municipality the best security posture without overcomplicating their systems and processes. Security does not work and will be circumvented if it hampers people's ability to get their job accomplished. Especially in a small-town municipality office where before this life changing event happened, they would not really and truly understand the powerful

reality if neglected. Even after this event the attention to detail and the willingness to comply to every small security will have shorter and shorter half-life as time goes by.

The main function that the Active Directory Domain did for the organization was credential management and authentication at least to the servers and end user devices. Most of the other installed applications were tied or integrated into Active Directory for authorization. Most of the time it was just certain service accounts and local rights on the machine. Most of the other applications had their own form of authentication and authorization which was username and password. The biggest change to the default settings of the domain was a separation of any local or domain administrative rights between accounts. Every user had a non-privileged user account set up and this was the account that they were to perform their daily work tasks that did not require elevated privileges. Then if they were in a work role that deemed them to have additional rights locally to their computer or across the domain these two needed to be separated. Additionally, the password policy that was in place across the office was weak. Several users had no passwords at all and were not connected to the domain. The servers to include the domain controller had passwords without really any complexity enforced, character length was 6 characters at best. Basic best practice group policies like some stronger password requirement, a timeout for inactivity to where users would need to log back in upon screensaver, account lockout on 3 incorrect password attempts were instituted. Additionally, a requirement for user and privileged accounts to change their password at 45 or 90 days was added. These were small changes that would be a change for what the users were accustomed to before but were considered relatively easy to adjust to over time and would make a big impact from a basic security stance. All these settings were discussed and vetted with the team lead as well as the local municipality leadership and they had open opportunity to ask any questions and understand the cost/benefit of the changes. Finally, a best effort was made to include the local administrator in the settings and demonstrated how to modify anything later if necessary.

Once the Domain was up and running the desktop team was able to work through the building and reformat and then add the fresh devices onto the new domain. Once this was complete, they would log into each machine as administrator and update the systems to the best of our ability with all the available Windows updates. The same was done on the server side by working to get all the server applications and updates installed and then working with the MSP or application vendors to get everything running. Many server applications that were not on the critical list of things that must be done before our orders are over, were things that the local administrator stated that he would be able to install later when things calmed down. It is an important point to bring up that with any hard time there is always going to be a lot of learning and clarity that comes from the event. This office now had a very firm understanding of what applications and resources were critical to getting up and running, what was an emergency and what could wait. Once the servers were loaded and running, best practices were applied to the Domain in the form of Group Policy. Also, documentation was prepared for the local administrator to follow and understand what had been done and what they needed to do in the future. Finally, user accounts, standard and privileged, were created and the process documented to make it repeatable.

The team also had to help get users back up and logged in; ensure that everyone's new accounts were working; and that passwords were reset and were no longer using the default password we set for everyone. All accounts upon creation were set to force users to change their password at first logon. Since all the network drives and things were gone and not a priority to be rebuilt while we were there, we essentially had to go person by person with the USB hard Drive of whatever data we were able to keep for them and then move all of it back and attempt to set that person's profile back up as close to what they remember. There was one user that had almost a gigabit of family photos that by no way were mission essential, but because of her position/importance in the organization this was something that needed to be protected. This is an example of the interpersonal politics that needed to occur at times to make things move smoothly. By the time we had gotten all the systems or at least most end user systems onto the domain we had reached the end of our orders and both the Texas SOC as well as the local municipality leadership was happy with our progress so that we could be released.

A long and detailed turn over document was prepared that included all the system documentation as far as usernames and passwords and enterprise administrator passwords that needed to be safeguarded in case there was an issue that caused the domain to require restoration. The Network did not really change as all systems retained the same IP addresses, but all the servers and workstations changed their

computer names and the logical roles of servers changed. One physical servers' location was changed to facilitate working on it. There were several things that we were not able to get taken care of but they fell under the category of "nice to have" but very much important. There were two major issues that were not addressed with local leadership. The first was their backup solution that desperately needed to involve some sort of off-network backup and just backups in general of applications and important work documents for users and the office. To safeguard against this happening again, the only way to protect against a ransomware attack is to have a very good backup solution. The second issue was a more mature patching posture to ensure both basic windows patching, which is easy if it is ensured a user has enough rights to allow them to run auto update, but also to have some additional antivirus beyond just windows firewall in place.

We were brought on as a stop gap emergency measure because of the situation, realistically this should have been something that the MSP should have resolved or helped the municipality to resolve and improve. Though due to the size and impact surrounding this event, this MSP which was a small, one-man shop was overwhelmed. This raises another issue for the municipality, what should be the characteristics of their MSP. A MSP needs to be able to handle severe events and needs to have sufficient resources to ensure this.

Mr. Dzimielia states that not only did he learn much from this experience, but it was also one of his most fulfilling missions. He has spent more time in the Texas Air National Guard doing domestic cybersecurity support than helping with hurricane support. Regardless of the type of work that is being done, there is a much different type of gratification that comes from working along side and being taken to lunch by the people you are there to help. To sit at someone's desk and look at the pictures of their family and know that this job and what they do affects more than just the person in the chair. The human element is very real and in the information technology and cybersecurity fields you spend a lot of time in your career working to get as far away from the end user as possible. This is normally just a personality thing in this career field that it's a unpopular truth that computer folks are normally not the most social of people but it is normally true that the further your name is from your desk the higher up the leadership ladder you are and normally the larger your salary. Right or wrong, it was very nice to be able to see the faces and stand beside the people and see the concern and then gratitude in their eyes as we were able to slowly repair their totaled network.

## **Discussion/Analysis**

This is a very rich case using first hand experience of responding and recovering from a ransomware attack. There is much can be learned by analyzing the events. The first lesson that jumps out is the extent of resources used to respond and recover. The attack affected 23 primarily small-town government networks in Texas (the exception was Lubbock county which was able to isolate and recover within hours of the attack). The response and recovery involved the local governments, state organizations, and the federal government. A state cyber emergency was declared and the Texas governor activated the Texas state national guard cybersecurity unit. No ransom was paid and the local governments were restored (sans much of their data) within a week of the attack. The point of interest here is that a lot of resources were committed to the response and recovery from the attack, many more resources than even large organizations can marshal. While impressive as the response and recovery was, is it realistic to expect that any small or medium sized organization could match the effort? We don't think so and the first lesson learned is that it is much better to be prepared for an attack then it is to be unprepared and have to respond and recover without any preplanning. Tuttle and Jacobson (2019) support this conclusion and discuss the very high cost of responding and recovery. It is doubtful that left on their own any small and medium organization that is not prepared would be able to respond and recover. This leaves the option of paying the ransom or potentially going out of business or failing to provide civil services. Dudley (2019) discusses how insurance companies have found it cheaper to pay the ransom than to do extensive recovery, this case supports that position. Dudley (2019) also points out that paying ransoms may only be encouraging more ransomware attacks.

Pries and Susskind (2022) point out that there is little research on cybersecurity practices in municipalities. This paper provides a glimpse into these practices in a small municipality and it is not



good. Best cybersecurity practices were not being followed. Basic practices related to passwords, firewalls, backups, etc. were way below expected and caused the municipality to be at higher risk and to lose data (note that other municipalities had better practices and so lost little to no data). Allyn (2019) worries that the coordinated ransomware attack is a trend of increasing attacks aimed at higher risk small municipalities. Pries and Susskind (2022) concur and thinks more needs to be done to prepare these municipalities. This paper again supports this conclusion. Ocampo (2021) studied municipalities and found 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. Again, this case supports this finding.

## **Recommendations**

McFarland, et al. (2020) reports that partially as a result of this attack, Texas passed House Bill (HB) 3834 that requires most state and local government employees to formalize cybersecurity trainings for their employees. The Texas Department of Information Resources, in partnership with the Texas Cybersecurity Council, have developed a vendor implemented certified cybersecurity training program to state government employees that perform at least 25 percent of their duties using a computer, local government employees with access to a municipal computer system or database, elected and appointed officials, and state government contractors. This is a good first step and should help municipality staff be more aware of cybersecurity requirements. The recommendation is for states other than Texas to consider implementing training requirements.

Raghavan, et al. (2021) propose a multi-step operations model for ransomware protection that is based on National Institute of Standards and Technology (NIST) cybersecurity standards and is motivated partially by this ransomware attack. This model addresses several of the issues observed in this case, passwords, backups, firewalls, training, etc. as well as introducing two new controls, auditing and insurance. We would recommend this model but believe that simply listing best practices that should be implemented is a more straightforward and direct way of making recommendations. We do recommend using the model to help generate the list of best practices that municipalities should implement. The practice of some concern is purchasing cybersecurity insurance. This is a good idea if the municipalities have the funds to pay the fairly high premiums. However, given the concerns raised by Dudley (2019) and Tuttle and Jacobson (2019) that encouragement by cybersecurity insurers to pay the ransom is encouraging more ransomware attacks.

Raghavan, et al. (2021) propose the use of audits. This is a recommendation we strongly encourage. At West Texas A&M University we have the Wellington State Bank cybersecurity lab founded in 2022. One of the goals of the lab is to prepare students for careers in cybersecurity with one activity being teaching students how to conduct audits of small and medium organizations by actually conducting audits on volunteer small and medium organizations. The purpose of these audits is to verify that best practices are being implemented, to make low-cost recommendations for improvement, through the audit process to educate the organization on cyber risk. The results are provided to the audited organization for free with the goal of improving cybersecurity awareness and preparedness in participating organizations. The recommendation is for other universities to begin similar programs as a form of social outreach and impact in their local community.

## **Conclusions**

This is an enlightening case that shows the inside of a ransomware response and recovery. Key findings include the large amount of resources needed to recover when an organization is not prepared, the degree to which the organization was unprepared, and the general lack of application of best practices. One conclusion is that with enough resources, any organization can recover from a ransomware attack without paying the ransom. The main conclusion is that organizations can prepare by implementing cybersecurity training, best practices, including backups, and be able to recover faster and more fully.

Key recommendations is cybersecurity training at the municipality and small organization level, implementation of best practices within municipalities and small organizations, cyber insurance if it can be afforded, and a small/medium organization/municipality audit program. We are not recommending increasing budgets because we don't think the funds are available. Nor are we recommending NIST based models that may be more detailed than needed.

## References

- Achten, N., (2022). Texas Municipality ransomware attack (2019). Cyberlaw, July 22, 2021. Retrieved on February 18, 2023 from [https://cyberlaw.ccdcoe.org/wiki/Texas\\_Municipality\\_ransomware\\_attack\\_\(2019\)](https://cyberlaw.ccdcoe.org/wiki/Texas_Municipality_ransomware_attack_(2019))
- Allyn, B., (2019). 22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault. National Public Radio, August 20, 2019. Retrieved on February 18, 2023 from <https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault>.
- Bleiberg, J. and Tucker, e., (2021). 'Holy moly!': Inside Texas' fight against a ransomware hack. AP News, July 25, 2021. Retrieved on February 18, 2023 from <https://apnews.com/article/technology-government-and-politics-business-texas-hacking-772675a2a7a095ef6e5caa72fa8ca847>.
- Dudley, R. (2019). The extortion economy: How insurance companies are fueling a rise in ransomware attacks. *Pro Publica*.
- Freed, B., (2019). More identified in Texas ransomware attack as feds urge coordinated response. Statescoop, August 22, 2019. Retrieved on February 18, 2023 from <https://statescoop.com/texas-ransomware-attack-nine-named-feds-respond/>.
- McFarland, C., Rivett, B., Funk, K., Kim, R., & Wagner, S. (2020). State and Local Partnerships for Cybersecurity: A State-by-State Analysis. National League of Cities.
- Ocampo, H. R. (2021). Municipal Governments and the Need for Cybersecurity (Doctoral dissertation).
- Preis, B., & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. *Urban Affairs Review*, 58(2), 614–629. <https://doi.org/10.1177/1078087420973760>
- Raghavan, K., Desai, M., & Rajkumar, P. V. (2020). Multi-step Operations Strategic Framework for Ransomware Protection. *SAM Advanced Management Journal*, 85(4), 16-2.
- Texas Department of Information Resources (DIR), (2021). US Justice Department Announces Indictment Against REvil Ransomware Suspect Behind 2019 Ransomware Attack on Texas Municipalities. Cybersecurity News DIR News, November 8, 2021. Retrieved on February 18, 2023 from <https://dir.texas.gov/news/us-justice-department-announces-indictment-against-revil-ransomware-suspect-behind-2019#:~:text=AUSTIN%20%E2%80%93%20The%20United%20States%20Justice,municipalitie%20hit%20in%20August%202019>
- Tuttle, H., & Jacobson, A. (2019). Enemy of the State: Ransomware Surges Against State and Local Governments in 2019. *Risk Management*, 66(11), 30-35.