JTECH

JUDSON INDEPENDENT SCHOOL DISTRICT

DR. LACEY GOSCH, ASSISTANT SUPERINTENDENT

September 27, 2023

TO: The Subcommittee on Cybersecurity, Information Technology, and Government Innovation and the Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs

RE: Ransomware

FROM: Lacey Gosch, Ed.D, Assistant Superintendent of Technology, Judson Independent School District, Live Oak, Texas

My name is Lacey Gosch, and I represent the Judson Independent School District in Live Oak, Texas, as the Assistant Superintendent of Technology. My goal is to share through testimony the effects of a cybersecurity incident, specifically Ransomware, on public schools. Although my primary role and the events related to this testimony are from my experience as the leader of the technology department serving over 24,000 students and 4500 employees across seven municipalities in the San Antonio, Texas area, I also serve in the capacity of an elected School Board Member for another smaller school district in Texas. Therefore, my passion for seeking school support in combating cybercrime runs deep.

Texas alone has over 1,200 public school districts of various sizes and budgets. Judson ISD was fortunate to have obtained internal financial, personnel, and technological resources to combat the threat. Our status as the 56th largest and the 12th fastest-growing district in the state aided our recovery efforts. Many other school systems across Texas and the nation do not have those types of internal resources available, resulting in difficult decisions that are not only costly in monetary terms but costly to the individuals these institutions serve. The costs are not limited to data loss or data breach, but they extend to monetary loss in recovery and replacement efforts, security efforts, and mental and physical health effects that are rarely discussed or considered because of these events.

As my testimony will demonstrate, support comes from within only. The topic of Ransomware is rarely shared among organizations and is viewed as a scarlet letter or badge of dishonor to technology and security teams. The topic is considered to be one that should only be discussed in closed rooms and behind locked doors. However, I am here to testify that this issue must be discussed openly and provide support to adequately protect, prevent, and mitigate cybersecurity breaches. The mentality that any organization is too small or insignificant to be affected by a cybersecurity breach is living under a false sense of security. The truth is that cybersecurity events in organizations need to be viewed not as improbable but as absolute. The question is not if it will happen but when it will happen.

Brief Summary

Judson ISD received notification of a ransomware attack on our data and network systems on June 17, 2021. The threat actors were identified as PYSA (Protect Your System Amigo), a variant of the Mespinoza strain of malware. The attack initiated from a single vector with two pivot points. The entry vector was a technology employee's device, which was also one of the pivot points. The second pivot point was a video streaming server that was designed to have no outside connectivity and was used for internal video streaming only. From these points, the threat actors were able to penetrate the backup systems, data stores, and all devices connected to the network at the time of the attack. From the full investigation, a total of 428,761 individuals were affected by the breach, with 221,000 of those individuals residing outside the state of Texas.

The district paid a total of $547,000 in ransom not to obtain our data but to ensure the deletion of data captured by the threat actors. The recovery efforts of the district were aided by attorney consultation, third-party support for data mining, insurance payouts, and district financial resources above and beyond insurance coverage. However, the actual work of recovery was only possible through the efforts of the district technology department's dedication to supporting the students and employees, key vendor partners who provided services free of charge until the district could later negotiate a purchase, and some local school district friends that assisted us in communications and business operations functions, when others were too scared to even to take our calls. Some of the roadblocks included some vendors withholding information that could have assisted in the hunt for the threat actors and other roadblocks that almost prevented the payroll process for many of our employees. Thankfully, there are other companies and other school districts who saw the need as an opportunity to learn with us and how we must rely on each other because a calvary does not exist to come to the rescue. The total recovery from the event took longer than one year to complete, and the district continues to make improvements. These improvements do not come without costs, and the further the event flies from the minds of leadership, the less critical the continued funding is viewed. Insurance coverage is helpful, but the coverage goes to attorney fees, communications and public relations fees, threat actor hunts, data mining, and notification expenses. Insurance does not cover ransom payments or costs for upgrades to mitigate damage or repairs. The costs for recovery and repair far exceed the limits of a policy, forcing a district to make difficult decisions about replacement, repair, prevention, and mitigation. In the paragraphs below, I provide a detailed account of our processes and the mental, emotional, physical, and financial impacts of a ransomware event.

Our Story

On June 17, 2021, I received a call at approximately 5:00 a.m. from Matthew Fields stating that our system had been affected by Ransomware. This phone call came only 34 days after I had arrived at Judson ISD in my capacity as Assistant Superintendent of Technology. Upon arriving in Judson only a month prior, I visited with many on my technology team and was astonished by the outdated, out-of-support, and antiquated practices, systems, and hardware used by the district in the management of systems, data storage, and communication. Data storage and email systems were maintained on the premises, and the support provided to staff to combat potential threats was limited in scope. The repeated mantra from everyone was that solutions such as End Point

Protection, Cloud Storage, Immutable backup systems, Multi-factor Authentication, Email Security Monitoring, and other safeguards known to help maintain the integrity of a system were denied due to funding issues. In addition to these needs, other deficits existed, such as failed wireless controllers, backup battery systems in disarray, system cores out of life and out of support, and switching technologies that no longer provided proper support for district operations. Due to COVID-19, many of the end-user products had been updated, but not the infrastructure needed to support the load. The district did not have any means to manage off-site end-user devices. On-site, the district did not have port security for devices directly connecting to the network. Across the district, external hard drives, thumb drives, and network drives were the primary norms for storage. Judson ISD is similar to many K12 institutions in the management of technology. Schools are often faced with balancing the need for student curriculum, personnel resources, facility needs, and other operational costs on limited budgets.

In most cases, the choice to fund a technology resource unseen by community constituents gets placed on the back burner. These factors among outdated technologies within the district attributed to the breach occurring only a month later. However, regardless of the knowledge my team or I possessed, the time for Judson ISD to prepare, prevent, mitigate, and control a cyber event ran out.

The first indication that we might have a problem came to Matthew Fields around 1:30 a.m., and by 3:30 a.m., he was no longer able to connect to any internal system from his location. Mr. Fields arrived at the office at about 4:30 a.m. and began checking systems. He discovered that all desktop operating systems and server interfaces were inaccessible, and the only visible connection to any system was a ransom note visible on the screens, which stated that all data on all devices was encrypted, including backup systems. The ransom note also included contact information for the threat actors and the names of the perpetrators. Mr. Fields briefly investigated the depth of the attack to verify the information provided in the notes and discovered that every system was, in fact, compromised. He immediately contacted local law enforcement, county law enforcement, and the Federal Bureau of Investigations to report the breach.

With each contact of a law enforcement agency, we received the same response: collect your case number from your local agency, review the white papers on prior crimes, and keep us updated as you gather information. No other supports were offered, and no law enforcement ever set foot on the property. As we reviewed the ransom note and other information, it became clear that the threat actors were the famed group PYSA (Protect Your System Amigo), a variant of the Mespinoza strain of malware commonly leveraged in high-paying assaults and victim selection based on their ability to pay. In 2021, PYSA was the third most prevalent ransomware strain, with primary targets of higher education and K12 institutions. The group was most notably known for double extortion involving publicizing stolen information should the victim refuse to comply with ransom demands.

With no direct support from outside agencies, the district was left to our expertise in addressing the event. The technology team deployed staff in the first hours of the attack on June 17th to campuses and began the process of unplugging every endpoint device, including phone systems across the district. WIFI passcodes were changed and taken offline, and all network systems were secured. Hot spots were located for students and campuses to continue to utilize Chrome devices to support summer school. The district's singular cloud-based system for students, through the use of Google and ContentKeeper's cloud-based content filter, had been unaffected, and therefore, with the support of hot spots, our students could continue to operate with minimal interruption. The ability to continue normal operations with the same access as students was not possible for employees and district operations. Due to the depth of the breach, the district was without email, document access, data access, payroll access, purchasing power, access control to buildings, security cameras, or any other networked device to support district operations. The operations of the district were at a standstill, and our only recourse of support was our own ingenuity and hard work.

Judson ISD had purchased a cyber insurance policy for a sizable amount. Within the first 24 hours, the district held an emergency board meeting to discuss the event with School Leaders and activate the authority needed to invoke the insurance policy to address the next steps for the school district. The School Board awarded the Superintendent the authority to proceed with purchases and agreements to support the district based on information and resources provided through the district's cyber insurance policy. The insurance policy provided legal support, communications support, and third-party support to manage communications with the threat actors and conduct the hunt for the entry points and some answers as to the depth of the attack.

Through the attorney and the insurance company, Judson ISD contracted with Blue Voyant to assist in the hunt for the threat actors and conduct data mining to assist the district in contacting those affected by the breach. This process required that the district create forensic images of all servers, data centers, and endpoint devices for review by the Blue Voyant Team. These images were created by Matthew Fields and were shipped to Blue Voyant for review. Judson ISD is unique in that we had an individual familiar with forensic imaging and security measures to retain evidence in an investigation. Many school districts do not have employees with these capabilities, and this can create an additional layer of expense in terms of collecting evidence, protecting evidence, and ensuring the integrity of the findings.

Additionally, the district needed to locate all district PC devices, collect them, and install VMWare Carbon Black Endpoint Detection and Recovery (EDR) software so that all systems could be monitored as part of the hunt and recovery efforts. This process required that the district hire additional contractors to assist our teams in touching each district device individually. The total number of devices exceeded 4500. Some of the devices were housed at the campuses, but many devices were in the hands of employees who had taken them home over the summer vacation. Therefore, the district hired additional temporary employees to walk every campus and collect each device for inspection. District employees who were off-site for the summer were instructed to come to the district office to have the EDR software installed at one of our district locations.

Due to the need for monitoring and review of district devices and server data, the district was asked not to move toward any recovery efforts until Blue Voyant completed the hunt and review of all information. This request was mainly due to the district's financial interest in maintaining insurance coverage and reimbursement for expenses. This process began on June 19, 2021, and the full completion of the work with Blue Voyant did not end until June 13, 2022. This did not conclude the work needed to contact all individuals affected by the breach nor full operations of all aspects of our network, so our work was not done even a year later. However, the work associated with the hunt for information and the data mining necessary to identify all those affected ended almost one year after the initial incident. The district did not wait the entire year before bringing systems back online or repairing the network for operations. As a team, we were forced to make some of our own internal decisions to begin the process of repair. We waited approximately two weeks prior to beginning the repair of our systems in hopes of some answers from the contractors and attorneys on what to do next. However, those answers did not come in a timeline that was effective or efficient for preparing for the start of school in less than 30 days.

During the first week of recovery and research efforts, Blue Voyant remained in contact with the threat actors. The threat actors provided a complete file list of every file name, drive, and system owned by the district. The district was able to review the complete listing of the files to determine the amount of data collected by the threat actors. The district requested proof beyond the listing by asking for five distinct files from our system. One file requested was recent, one file from a former Chief Technology Officer, and other files spanning a 10-year period. In each case, the threat actors provided the exact files requested. It was at this point that the district needed guidance on the next steps to protect our employees and students. Based on the reputation of the threat actors, it was known that payments resulted in data being returned via decryption keys and prevented the release of the data. As PYSA was known in prior attacks, ours was no different. If we were to pay their ransom, we would receive the decryption keys, but they would also agree to destroy data that they had collected rather than release it. Blue Voyant advised that they had success with this group in the past as being reputable to their word on the destruction of the data, but they were also reputable to release the data if demands were not met. This required that the district carefully consider options. Paying the ransom meant that student and employee personally identifiable information could be protected, but the cost would be solely the responsibility of the district to cover in addition to any additional costs for repair and mitigation.

Therefore, the priority for the systems team was to assess our backup situation. Based on the time of the attack, our team had pulled removable drive back-ups of all data on the day prior to the attack, and those backup drives were stored at an off-site location. Our virtual servers also reported that data had been backed up, and we had some level of confidence that we could restore our system without assistance from the threat actors.

We quickly discovered that our drive back-ups were intact and could be used to restore critical district data once the servers were cleaned and systems restored. Therefore, we knew we could recover necessary district data prior to June 15, 2021. However, the backup drives did not account for all district data. Many of our systems were stored on virtual servers. Sadly, the Systems Engineer discovered the virtual backups were being generated, and all notifications of successful backups were being reported. However, to his astonishment, as soon as the back-ups were made and reported, the Ransomware was immediately encrypting and deleting the records. This told us that we would be able to recover almost all systems without the need for any support from the threat actors. It would be more time-consuming, and we would not be able to restore all data for all users. However, the critical financial and student data needed to maintain operations would be available. At this point, we were able to advise the district that, from a technological aspect, we would be able to restore the network and commence operations without the need for a ransom payment. We had the capabilities to replace hard drives, restore servers, and rebuild in the cloud, as was the original plan for the district without any decryption keys or support.

The problem for the district was not in our inability to utilize backup systems to restore the system or in our lack of ability to get the district operational. The concern was the secondary threat of the release of data. Consequently, the district made the difficult decision to pay the negotiated amount of ransom to prevent the student and employee data from being released on the dark web. The ransom payment was made in Bitcoin and equated to an amount of $547,000. The payment occurred on June 29, 2021.

The payment was made, and the district received the decryption keys. We did try to utilize them to see if they might speed up some processes. However, the discovery was additional worms and viruses built into the keys, and we ceased our curiosity towards their use. Our disaster recovery process began seven days after it began. Our advice from the third-party investigators was to wait until all of their processes were completed before we commenced rebuilding the network. However, we knew that we had less than 30 days before our first school opened. Our team sat down and wrote out a plan. Yes, we had all the official documentation required by statute for emergency operations and business continuity plans, but none of these documents are helpful in this type of situation. They were as useless as the paper that they were printed upon. We needed a real plan, and our first actionable step was to restore communications.

The district closed for the week of the July 4th holiday, which provided our team the ability to begin the process of building back our communications. We began with phones and were able to fully rebuild and deploy the new Microsoft 365 platform on July 12, 2021, with email. The restoration of email and communications was not accomplished by the efforts of any third-party contractor, outside funding, or governmental intervention. This process was completed by the efforts of the JISD team members Matthew Fields and Marvin Morrow and district partners, such as Barracuda Networks and VMWare Carbon Black that provided us resources, discounted pricing, and access to their platforms to assist us in speed of operations while putting into place the safeguards necessary to prevent, mitigate or detect any future attacks. These partners continued to provide us with solutions and support over the coming months as the district expanded to immutable backup systems, cloud-based redundancy, firewalls, and multi-factor authentication measures.

Due to these events, Judson ISD is in an optimal position technologically to prevent and mitigate future attacks. However, licensing renewals and software upgrades will continue to be costly for maintenance. In a way, Judson was fortunate. We were able to restore our systems. We were able to protect our students and staff. The unfortunate part of our story is that the state of technology and the funding and support for Judson prior to the event are no different from thousands of K12 schools needing support. One of the lessons learned through our experience was not only about the tangible hardships of an attack, but we also discovered the non-tangible hardships. During the event's initial hours, our team observed the stress and potentially harmful ramifications of an attack on the physical and mental health of those involved. As data disappeared from our servers and backups were destroyed, a team member who had dedicated his career to the building of the network witnessed his life's work being destroyed. This resulted in the need for EMS, as his body's response was a potential cardiac arrest episode. Thankfully, he was able to recover. However, this was just one example of the mental and emotional stress caused by an event that did not have to unfold in such a drastic measure. With the proper training, funding, and support, K12 institutions have the desire and the ability to assist in the fight against cybercrime.

Our experiences, as outlined in this testimony, have highlighted areas that we believe would truly change the landscape of cybersecurity protections for K12 educational institutions. Our recommendations include assistance in funding, training, and appropriate implementation of the following items.

- Hardware Supports
    - Immutable Back-up Systems – Typically cost prohibitive to school districts, but a current requirement for insurance.
    - IPS/IDS Firewalls or Next Generation Firewalls – Current minimum requirements set for school districts are strictly related to student protection from explicit content. IPS/IDS or Next Generation are recommended but not considered the standard. To effectively isolate a malicious event, these installations are required.
- Software Supports
    - Endpoint Protection with Endpoint Detection and Remediation – This is a costly endeavor for school districts. Education is needed about this functionality as many try to protect only from the data center/server locations. Most breaches are internal and come from end users. Without EDR/EDP for users, the funding allocated by districts to this solution may be wasted. Support for acquiring affordable EDR/EDP for all users is needed.
    - Lateral Movement Detection – This is software to detect when logins are used to gain privileges on other machines to gain access to logins with higher privileges eventually.
    - Centralized Logging and Management – This is software that is used to ingest all data from security devices and manage them. The amount of data that is ingested is far beyond what one person can do on their own. In most cases, technology teams are limited to one person on staff to monitor.
    - Data Leak Protection – This software looks for data in files, such as social security numbers, PII, and Credit card data. The software prevents files from being leaked or shared with outside entities. This is a necessity for cloud-based storage.
- Other
    - Basic Support for Disaster Recovery and Business Continuity Planning to include Cyber Events. This is cumbersome, and updates are limited or non-existent and is not a typical requirement in most states.
    - Assistance with Social and Emotional Support for Staff Involved.
    - In-place or at-rest encryption of Social Security numbers in databases. This is often excused by encryption in motion. However, Ransomware is not looking at data in motion.

- Support for affordable multi-factor authentication that is hardware-based rather than the free support provided by software companies related to email recovery and text messaging. This has also become a requirement to obtain insurance coverage.

The above-listed items are the foundational needs for schools to proactively address the growing concerns of cybersecurity. In programs like telecommunications, schools have been afforded discount programs or grant programs such as e-Rate that allow for discounted pricing and tiered supports to address needs. Providing this type of avenue for schools to help in the fight against cybercrime can open doors for districts to be able to see the possibilities of purchasing, maintaining, and expanding their capabilities in protecting the data and integrity of our school systems.

I want to thank the Committee on Oversight and Accountability for providing the structure to hear the issues related to the issue of Ransomware in our public schools. I am honored to have been able to present our story and our recommendations to the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, led by Chairwoman Nancy Mace, and the Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs, led by Chairman Pat Fallon. I am thankful to the Subcommittees for seeking our input and being offered the opportunity to take part in recommendations for solutions to a growing problem. I have been honored and privileged to serve in these proceedings, and I extend my gratitude to all parties involved.

Thank you,

Lacey Gosch, Ed.D
Assistant Superintendent of Technology
Judson Independent School District