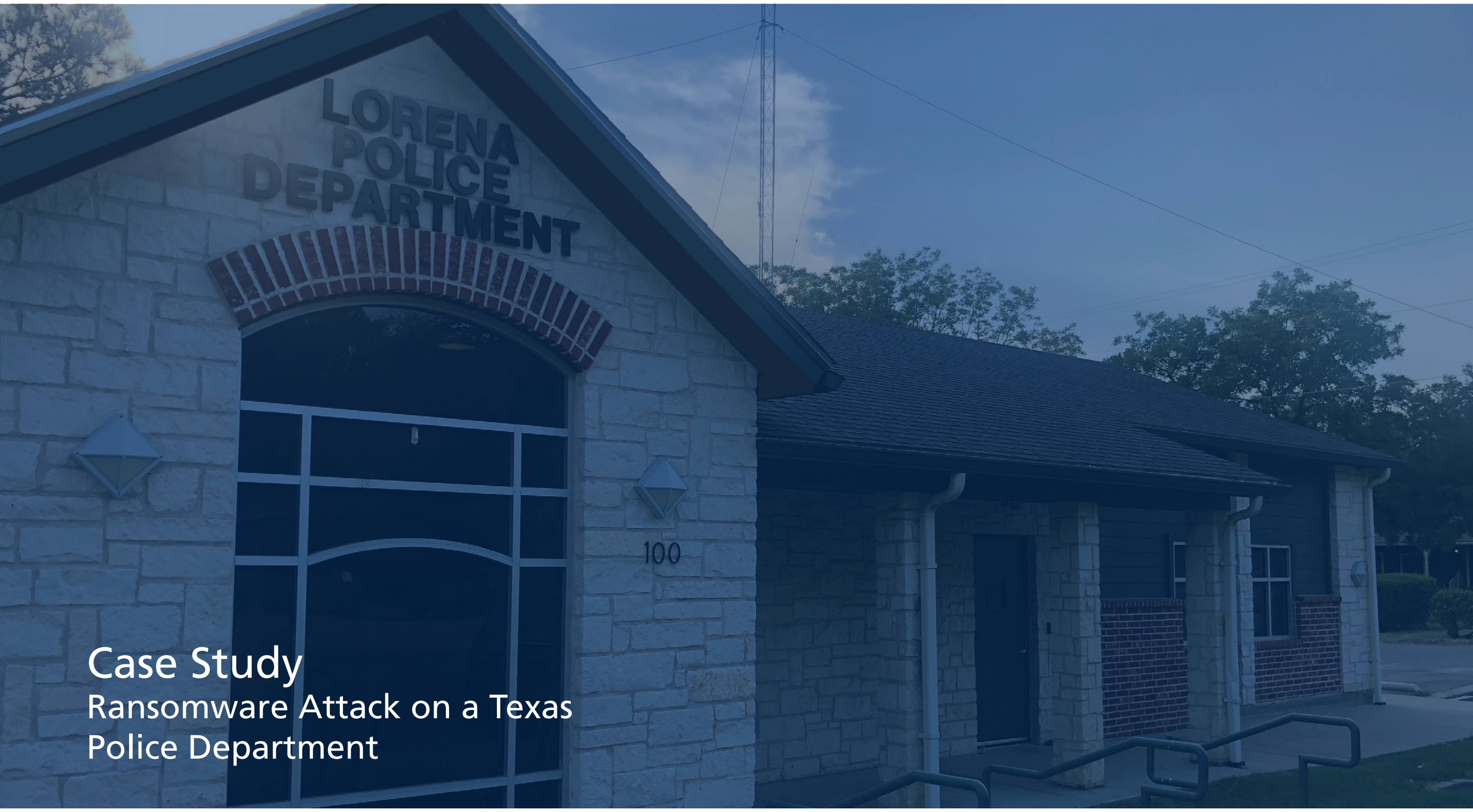
Extraco
Technology



Case Study

Ransomware Attack on a Texas Police Department

OVERVIEW

Ransomware is a serious — and growing — cybersecurity issue that police departments must be aware of. It has potential to inflict serious financial damage on an organization while damaging reputation and harming those living in the community you strive to protect.

Ransomware is malware (malicious software) that attempts to deny access to a user’s (or organization’s) data, usually by encrypting the data with a key known only to the cybercriminal who deployed the malware. After the data is encrypted, the ransomware directs the user to “pay the ransom” to the hacker (usually in a digital currency such as Bitcoin) in order to receive a decryption key. The amount of the ransom requested typically increases if the cybercriminal determines the data has substantial value.

Police Departments are prime targets for this type of attack because of the quantity and value of their data.

If a municipal service falls victim to a ransomware attack, it can be expensive to address, and a breach can create a reputation risk.

254-761-2390
www.extraco.tech

Quick Fact

According to the Federal Government, on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016.

THE CHALLENGE

The Lorena Police Department was hit by Mr. Dec, a type of ransomware virus. It rendered the department inoperable for a day and a half and crippled its technology for more than a week. The attack made its way onto one of the department's computers via an email attachment, which had an appearance of a legitimate document.

Once on the computer, the virus searched for files to encrypt. This included files on the computer itself as well as those on the department's network that were accessible via mapped network drives. Files on any drive letter or network share that could be located and accessed (through a program such as Windows Explorer) were accessed by the ransomware.

> *"Having gone to a paperless workplace, we were literally unable to function. We had no access to files, reports, and day-to-day services."*
>
> **Tom Dickson**
> *City of Lorena Police Chief*

THE SOLUTION

The Lorena Police Chief, Tom Dickson, immediately contacted Extraco Technology for help. Extraco Technology downloaded all of the Police Departments backup data and then uploaded it to its server to replace the corrupted data. The entire process took a day and a half, as the data needed to be cleaned with antivirus software. New policies were created, and antivirus software upgrades were put into place. An email filter was installed to catch, clean and filter incoming emails.

> *I'm so glad we had Extraco Technology on our side. Petar worked for two days and recovered every single file to its original state."*
>
> **Tom Dickson**
> *City of Lorena Police Chief*

Don’t Go it Alone

To become adequately protected against and prepared to respond to a ransomware attack is a daunting and a time-consuming task — and one that is never complete. Enlisting external IT resources like Extraco Technology can prove to be an efficient way to guide you through the process and maintain continuous readiness.

GUIDANCE

Police Departments of all sizes need to ensure they are regularly updating their technological administrative and physical safeguards as cybersecurity threats continue to evolve. This is particularly true when it comes to ransomware, as this type of cyberattack has the potential to paralyze a municipal service, or at least severely disrupt its daily operations and community care. Here are valuable tips to follow that will help protect your municipal service from ransomware.

- Focus on training for employees
- Create a disaster response and business continuity plan
- Monitor staff practices and habits
- Review your professional liability insurance to see if you are properly covered for cyberattacks, such as ransomware.
- Make sure your IT vendor not only specializes in IT security, but Municipalities Services as well. Failure to meet these requirements could increase the likelihood of breaches. The selection of your IT vendor is also critical as the in-house employee who handles your IT may come and go. Whereas your IT vendor is more of a constant and will be your “go-to” in the event of a cyberattack.

> *“It came as a surprise to me how quickly a cyber-attack can occur and the importance of data security. I’m glad we had Extraco Technology to guide us through this critical event and help us establish new policies to safeguard against these threats in the future.”*
>
> **Tom Dickson**
> *City of Lorena Police Chief*

ABOUT EXTRACO TECHNOLOGY

Extraco Technology is a service provider in Central Texas & DFW areas with a niche in IT support for various business offices. We understand that customers want to focus on their business and not their technical issues. Our team works directly with your software/hardware vendors to resolve problems so you don't waste time or lose focus on your customers.

Businesses see value in our monthly IT support plan because it allows the flexibility to set a fixed budget for IT services. We also provide a high level of customer service with fast response by phone, remote control and onsite. Our team believes in a proactive approach rather than a reactive one by monitoring your network, making sure all updates are done accordingly and suggesting hardware updates. With these steps complete, it allows us to prevent possible IT problems before they arise.

Extraco
Technology

254-761-2390
www.extraco.tech