Case Study

mimecast

City of Seguin, Texas

Leading in Rural Cybersecurity Evolution

A Small Town with a Big Security Footprint

The City of Seguin is a South Texas community with a growing population of 30,000 plus residents. As the city has grown, its cybersecurity needs have also expanded. Citizen, vendor, employee and operational data needs to be protected, and the city's technology enterprise must be kept secure. Shane McDaniel, Director of IT for the City of Seguin, is tasked with optimizing cybersecurity defenses and ensuring the community's technology needs are met, including overseeing some 450 employees, 30 facilities and multiple data centers.

While smaller, more rural communities often believe they are too small for cybercriminals to target, the City of Seguin is clearly an exception. IT staff understands the risk that all government agencies face and are taking a proactive approach to keeping city assets and data safe.

At a Glance

The City of Seguin is a South Texas community with a growing population of 30,000 plus residents.

The IT department looks after 450 employees, 30 facilities and multiple data centers.

Problem

Citizen, vendor, employee and operational data needs to be protected, and the city's technology enterprise must be kept secure under increased ransomware attacks against state and local government.

Solution

Email Security, Targeted Threat Protection, Impersonation Protect, & Awareness Training

Benefits

- IT Departments more aware of the threats that are out there. Solicited and unsolicited spam is kept out of user's inboxes.
- Mimecast reporting pulls key performance indicates and shares with city management to highlight concerns being addressed.
- Thanks to behind the scenes information provided by MImecast after implementing the tool, the City of Seguin put additional security procedures in place to further reduce the chance of mistake.

> **“Mimecast changed the game for us, making us more aware of the threats that are out there and keeping solicited and unsolicited spam out of the users’ inboxes.”**
>
> *Shane McDaniel*
> *Director of IT, City of Seguin*

Public Sector is Getting Hit Hard

Ransomware has become a significant problem with cybercriminals aggressively targeting state and local governments. There were 966 identified public sector ransomware attacks in 2019, with a total impact in excess of $7.5 billion. Last year the average ransom demand was $338,700 for government organizations, and it has been increasing at a progressively sharper rate in recent years.

Those with malicious intent know smaller entities often do not have the resources or funding to defend themselves, with many not having the security protocols in place to prevent incidents. Hackers capitalize by demanding high ransoms that the entities may have no choice but to pay if they want to keep government services running and avoid major reputational and financial damage.

As the City of Seguin’s IT Director McDaniel said, “Whether it’s a private business or government, IT departments need to get it right 100% of the time when it comes to protecting against security threats. It’s a tough ask.”

All it takes is one click internally to unleash a cyberattack. IT teams need to address the problem proactively by having a multi-layered approach to security, and that’s exactly what Seguin IT has done.

Taking a Proactive Approach

City of Seguin’s employees have a lot of email traffic to contend with. With an average of 55-60k incoming emails a month, potentially malicious engagements were frequently making their way into end users’ inboxes. After implementing Mimecast’s security solution superfluous emails came to a “screeching halt,” even resulting in some users reaching out to the IT Team to thank them for cleaning out junk email.

McDaniel commented, “Mimecast changed the game for us, making us more aware of the threats that are out there and keeping solicited and unsolicited spam out of the users’ inboxes.”

Mimecast’s reporting functionality gave the City of Seguin more insight into what was happening behind the scenes. McDaniel uses the tool to generate monthly reports from which he pulls key performance indicators. He shares them with city management to highlight security concerns being addressed. The performance indicators show email volume, number of blocks, number of unsafe URL clicks, and impersonation attempts, among other KPIs. “In 2019 alone, Mimecast identified and blocked 32% of our overall email traffic with security issues – including spam and phishing attempts,” said McDaniel. His team is also leveraging the tool to identify users who repeatedly click on questionable links, and address the issue proactively before something adverse happens.

The city was experiencing, on average, 30 impersonation attempts a month. Most of the attempts directly targeted employees in the HR and Finance departments, with attackers imitating vendors, the city manager, department heads and even the city’s mayor trying to initiate financial related change requests. These emails were often so well crafted that they could easily be mistaken for legitimate communications.

Mimecast blocked these attempts, making the IT Department and subsequently all employees more aware of the types of threats that were coming in via email. “Less than 1% of random phishing attempts make it to the end user’s inbox,” said McDaniel, “It’s rare when we have to actively pull something out of our domain these days.”

Mimecast enhanced the IT Department’s visibility into internal business processes that needed to evolve. In part thanks to behind-the-scenes information provided after implementing the tool, the City of Seguin put additional security procedures in place to further reduce the chance of mistake. For instance, whenever a direct deposit change request comes in, the process must be completed in person rather than relying on email and phone requests alone like in years past.

> **“This tool is invaluable because it protects us from so many potentially costly and/or bad situations that could negatively impact city services or force us to revert to legacy processes.”**
>
> *Shane McDaniel*
> *Director of IT, City of Seguin*

McDaniel takes this a step further when speaking to employees at new hire orientation by showing examples of attempts to reroute staff direct deposit information. "I point out that HR never received these requests, but attempts occur more often than most probably realize. I've had a few new employees come up to me after presentations and tell me about a similar incident that happened in their previous environments. It's unfortunate but it's another one of those things we have to stay on top of."

The Value of Implementing Layers of Security

Organizations often don't realize how significant the impact of a cybersecurity event can be until it happens. McDaniel commented, "This tool is invaluable because it protects us from so many potentially costly and/or bad situations that could negatively impact city services or force us to revert to legacy processes." He's seen other organizations around the country get hit hard in recent months. It's difficult to fully comprehend just how much reputational damage and financial loss one cyber incident can cause until an agency experiences it themselves.

McDaniel's advice to other orgs? "Push the security narrative as far as you can with your leadership team. Enlist them to be cyber advocates and help spread the awareness message. Fight the good fight and protect your environment to the best of your ability."

The threat landscape is continuously evolving, and cyber criminals have become crafty and more aggressive. The public sector can no longer afford to let its guard down and implicitly trust whatever is before them. To stay safe, agencies need to question things and stay vigilant.

McDaniel commented, "We understand no tool can 100% prevent a ransomware attack from getting through, but we feel much better having email security in line. Having layers of security in place reduces the attack vector and subsequently the chances of such an attack from happening."

When asked if he would recommend Mimecast to peers, McDaniel's response was resounding, "I would, and I have. I wouldn't vouch for something I didn't believe in."