LORICCA
HIPAA COMPLIANCE SPECIALISTS

CASE STUDY

THE UNNATURAL DISASTER OF MAT-SU BOROUGH

Cyberattacks continue to rise and it's clear that they hold the potential to create a malicious trail of short- and long-term troubles for the organizations that suffer them. Underestimating their power to pull down systems and cause millions of dollars in damages, loss and wasted energy is one of the greatest IT mistakes companies—and government bodies—can make in the twenty-first century.

 COPYRIGHT © 2019 LORICCA, INC.

THE CYBERATTACK

A good example of the long-term effects of cyberattacks is the attack on Matanuska-Susitna Borough in Alaska. The borough declared a disaster on Tuesday, July 31, 2018, and nearly six months later, is still finding ways to foot its bill of $2.3 million in costs associated with the event.[1]

Borough IT Director Eric Wyatt said a state of emergency was declared largely due to the sheer damage in dollars that they foresaw the incident producing, which at the time was estimated to be near $750,000.[2] When 650 servers and computers went offline, borough officials decided to bring other devices, such as office phones and computer systems, offline as well to avoid further risk.[3]

The borough also quickly discovered that they were simply next in line in a long series of cyberattacks—210th to be exact, a number uncovered in the lone file left behind.

THE ATTACK METHOD >>

THE ATTACK METHOD

This cyberattack is considered a "multi-pronged, multi-vectored attack" by borough officials because it was developed and executed through several different strains of malware, including Trojan horse software, that opened up additional venues of attack and opportunities to push past passwords and target connected machines.[4] It's believed to have spread through emails containing links to a malicious website that likely targeted people with local administrative permissions who opened suspicious-looking emails and attachments that appeared to have come from coworkers and familiar peers.[5]

THE LESSONS LEARNED >>

THE LESSONS LEARNED

Natural disasters aren't the only disasters that can cripple a city. Cyberattacks can come in many shapes and forms and they take both brainpower and advanced security measures to tackle. What the Matanuska-Susitna Borough's experience with cyberattacks should teach organizations today is that cyber threat intelligence and security awareness training are two vital components of a successful data protection plan.

» **Cyber Threat Intelligence (CTI):** More companies are relying on the integration of cyber threat intelligence and security information and event management (SIEM) to prevent future cyberattacks. This means gathering data on malicious bodies and analyzing that data to produce helpful reports, keeping companies informed of existing and possible threats.

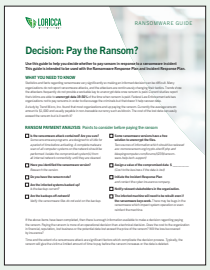
» **Security Awareness Training:** Security awareness training should be a part of every cybersecurity program, regardless of company size. This includes anti-phishing training and other need-to-knows on corporate policy and best practices for navigating everyday IT tasks. In Mat-Su's case, security awareness training that educates employees on how to identify and handle suspicious emails might have prevented the cyberattack or at least reduced its overall impact.

PROTECT AGAINST RANSOMWARE >>

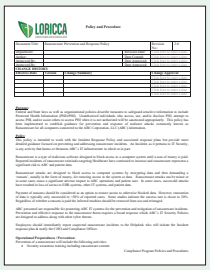
HOW TO PROTECT AGAINST RANSOMWARE

1. Make sure you're regularly backing up: do three backups on two storage types with at least one offsite backup.
2. Keep your systems updated and don't delay in applying patches.
3. Use reliable anti-malware programs. While these applications are not full-proof they do add necessary protection to your systems.[4]
4. Educate your employees so they can identify social engineering and spear-phishing attacks. Many ransomware attacks are initiated by someone "clicking" on a link they should not.
5. Implement controlled folder access. It can stop ransomware from encrypting files and holding the files for ransom.

RANSOMWARE RESOURCES



Ransomware Decision Guide



Ransomware Policy

FOR HELP PROTECTING YOUR INFRASTRUCTURE AND COMPANY, CONTACT US. www.loricca.com | 855-447-2210

ABOUT LORICCA

Loricca is an IT security compliance provider that specializes in security risk assessments for healthcare organizations and commercial, retail, finance and device manufacturing companies, among others. Our goal is to keep these organizations and their vendors compliant and protected from the cybersecurity risks of today and tomorrow by delivering streamlined risk assessments, credible letters of attestation, fast and responsive service and an experienced team.

Sources

1. Mat-Su Borough Eying $1.3 Million Balance after Insurance Payout for 2018 Cyber Attack, KTUU
2. Massive Cyberattack Prompts Mat-Su Disaster Declaration, KTUU
4. Mat-Su Scrambling in Wake of Malware Attack Hidden in System for Weeks, Anchorage Daily News
5. Advanced Persistent Threat: Mat-Su Borough, Valdez Fighting Highly Sophisticated Cyber Attack, KTUU