PayneWest INSURANCE

Ransomware Case Study
Lessons Learned

RECOMMENDATIONS TO PREVENT AND RESPOND TO GROWING THREATS

Like so many businesses, PayneWest Insurance experienced some of the most difficult challenges in our history in 2020. As we sent employees home to work to minimize the risk of Coronavirus, another invisible threat loomed, exposing itself in October 2020 when a ransomware attack nearly crippled our operations.

Due to new security challenges caused by the COVID-19 pandemic, cyber attacks have drastically increased, and there are no signs that attacks will decrease soon. In Q3 of 2020, ransomware attacks in the U.S. numbered 145.2 million — a 139% year-over-year increase according to cyber security firm SonicWall. We share the lessons we learned in one of our most difficult weeks so that other organizations may mitigate risk of attack and respond quickly if attacked.

LESSONS LEARNED FROM OUR OWN CYBER ATTACK

Plan Now

In 2020, we deployed our disaster recovery plan for both Coronavirus responsiveness and the ransomware attack that encrypted our entire network cutting employees off from server files and email communication. (The plan was created years prior and updated annually with our risk management partners.) It would prove invaluable in both cases to proactively task appropriate company leaders, outline priority systems to be addressed first, establish alternative communication channels and lay the groundwork for quick decision making.

Lesson learned: Proactive disaster recovery planning is a must when you need to act fast in a crisis.

Use Your Cyber Policy Partners to Act Quickly and Effectively

Almost all our actions in responding to the attack were informed by our expert partners brought on by our insurance carrier. We were immediately connected to IT forensics support to detect the scope of the attack and were fortunate to learn that there was no data removed, or exfiltrated, from our network. (All of our client information was secure in our cloud-based systems.) We also were partnered with negotiation experts, who deal with cybercriminals every day and, in fact, were familiar with our threat actor and their M.O. Cyber security legal experts, also brought on by our carrier, helped ensure we were compliant with industry regulations and reporting. We also had the option through our carrier to retain a public relations firm and vendors for credit monitoring and data recovery if the attack had caused a data breach. The advice we received helped us come to resolution in days not weeks and also informed our actions to improve security systems and hinder future threats.

Lesson learned: Without a cyber insurance policy and expert cyber security partners, the road to recovery is longer and more costly in lost assets, revenue and reputation.

Ransomware Case Study
Lessons Learned

Safeguard IT Systems

With the help of our forensics partner, we immediately deployed detection software providing a direct view into our infrastructure with the ability to determine that none of our data had been removed or exfiltrated in the attack. Our agency management software, which stores client data, and our payroll system are cloud-based and, fortunately, were not affected by the attack. To help prevent future attacks, we've implemented heightened security and backup protocols.

Lesson learned: Cloud software can keep key operations working and client information uncompromised. Robust security software and protocols will help prevent future backdoor attacks.

Establish Communication Channels to Keep Employees Connected and Informed

With most employees working from home and spread across four states, we relied on our broadcast texting platform to send out communication updates. As part of our disaster recovery plan, we had previously contracted with this service provider and were able to quickly send out communications without onboarding a new vendor. With the text software offering one-way communication, we also built a password-protected chat portal on our website for employees to post questions and respond. For task force members and departments, we created Gmail accounts for email communication internally and with clients and vendors.

Lesson learned: Having backup communication channels and secondary employee contact information is key in keeping employees and clients informed when regular systems are down.

Know Your Legal Responsibilities

Working with our legal partner, we determined what information was appropriate to share without offering compromising information to the attackers. Since our clients' data was not breached, we were not legally required to share information of the ransomware attack with clients but chose to be transparent and assure them that their data had not been compromised.

Lesson learned: In a regulated industry, knowing the legal responsibilities to inform clients of a breach is necessary. Communicating beyond what is legally required goes a long way in building trust.

Train Employees As Your Front-line Defense

While we do not know exactly what caused our ransomware attack, our forensics partner determined it was likely a phishing email used as backdoor into our network. Phishing emails are a common method for cyber attackers to deliver malware or ransomware, by masquerading as a trusted entity and encouraging victims to download a document or visit a link that secretly installs malware. While we have continually provided security training and awareness for our colleagues, we have increased employee training on detecting increasingly sophisticated phishing emails across our organization.

Lesson learned: Training employees on detecting phishing emails and other scams and testing their response with tabletop exercises is one of the best lines of defense. Employees are frequently the last line of defense.