Top 5 Cybersecurity Threats Facing Title Industry – Part 5

Overview

In part 1, we examined business email compromise, which occurs when a hacker gains access to a corporate email account and assumes the identity of the corporate user in order to defraud the company, employees, customers, or partners. In part 2, we looked at some of the ways that hackers obtain and use stolen credentials in order to take over an account. In part 3, we explored the motives and methods of hackers. In part 4, we looked at today's rapidly evolving malware and ways to prevent and detect infections.

In this post, we'll be talking about having a plan in place for when people, technology, and processes fail.

Threat #5 – Being Caught Unprepared

The Problem

As we have seen from our previous posts in this series, cyber-attacks are consistently rising across all companies, but the real estate sector is particularly targeted. Every day, attackers seek to defraud title companies through business email compromise, wire fraud, phishing, account takeover, hacking, and malware. The hacking tools freely available today allow even unsophisticated actors to perpetrate
highly sophisticated and targeted hacking campaigns previously only available to nation states.

I tell all of my customers this – there is no silver bullet, or definitive way to prevent an attacker from getting into your network and getting out with your data. Effective cybersecurity requires a layered approach and must combine both prevention and detection capabilities.

In 2018, the average cost of a data breach in the US was $7.91 million, with the average cost per stolen record at $233. Once breached, the likelihood of being breached again over the next two years is 28%.

What happens when the people, processes, and technologies that are supposed to protect you from cyber-attacks fail? Do you have a plan in place for when the worst happens?

Let's take a look at some ways that you can prepare for the worst, and decrease the cost and complexity of what happens after the breach.

Early Detection Systems

There is a direct correlation between the time it takes to identify and contain a breach, and the total cost associated with that breach. According to Ponemon, the average time to detect a breach was 197 days. Companies that were able to detect a breach in less than 100 days saved more than $1 million. Similarly, companies that contained a breach in less than 30 days saved over $1 million.

Today's detection systems can alert you to malicious behavior in real-time, and some EDR systems allow security operation teams to remotely isolate any infected endpoints, preventing spread and limiting the damage. Our goal is to reduce the time to detect and contain down to minutes, not days.

Log Aggregation and Behavioral Monitoring

In 84% of all breaches, the evidence of the breach was sitting in a log file somewhere. The problem is, most companies don't aggregate or monitor these logs. After a breach, forensics are the single biggest source of first-party expense, averaging $231,457. This is the cost for a company to come in and collect and analyze all of your logs to determine how the breach happened and what data was stolen.

A Security Information & Event Management (SIEM) system, when properly configured, will continuously collect and aggregate logs from across your network into a single searchable database. Additionally, today's EDR platforms record a history of every behavior performed by a computer. This information should allow a security operation team to detect breaches in near real-time; however, in the event that the breach was not detected, these systems can also drastically reduce the cost of forensics.

Incident Response Team/Plan

According to Ponemon's 2018 Cost of Data Breach Study, having an incident response team is the #1 factor in reducing the cost of a breach, reducing the cost by $14 per record. In the middle of a breach, there is no time to decide how you're going to respond. Companies need to have a plan in place already so they can swiftly jump into action.

An incident response plan is a documented, organized, and actionable plan detailing what is to be done after a breach and who is responsible for doing it. The incident response team is the group of people who are responsible for implementing the plan.

A good incident response plan should include an actionable flow diagram that helps the team to quickly determine what information must be gathered next, and what to do afterward depending on the information discovered. It should include contact information for all third parties who will be involved, including lawyers, law enforcement, forensics, PR firms, and

identity protection services. While it is helpful to have the plan reviewed by lawyers, be careful not to let them transform the document from an easy-to-use actionable plan into a hard-to-understand document full of subsections and legalese. The whole point of the document should be to get everyone on the same page and allow your team to jump into action immediately following a breach.

The plan should be reviewed, practiced, and updated at least once per year. Tabletop exercises are designed to test your response plan through live in-person scenarios.

Drew Bradford is a TLTA member and President of Sigma InfoSec, a company that provides enterprise-class cybersecurity solutions to the title industry.