Cyber Attacks Targeting Insurers — What Are the Risks for 2017?

As most risk managers are aware, cyber incidents in the insurance sector are growing exponentially. Why? As famed bank robber (and Eastern State Penitentiary escapee) Willie Sutton is rumored to have quipped, "Because that's where the money is." Insurers, by the very nature of the business, collect and hold high-value consumer information, such as sensitive personal information, health information and payment card information. When insurers desire to increase consumer accessibility through websites and mobile apps, and when brokers, claims professionals and other support staff that increasingly work outside of an insurer's core IT systems are added to the equation, you then have many avenues in which cyber incidents can occur — avenues that may be unfamiliar to many smaller mutual insurance companies.

Recent studies also show that financial services organizations are being hit hard by the costs associated with these cyber threats, both old and new. According to the Ponemon Institute's 2016 Cost of a Data Breach report, financial services organizations — including insurance companies — are in the top three as far as the costs for remediating a data breach (mostly due to fines from regulators), and are the most likely to lose existing customers if the organization experiences a data breach.

What are the threats facing insurance companies in 2017? Your organization should be on the lookout for two major threats from expanding technologies: ransomware and distributed denial of service (DDoS) attacks. Ransomware continues to be the fastest-growing malware across all industries, up 50 percent in 2016 compared to 2015, according to new data from endpoint security provider Carbon Black. Criminal use of malicious software to encrypt files or hard drives of unsuspecting victims is so widespread that some states are enacting legislation to make recent ransomware attacks easier to prosecute.

While many companies assume that such attacks are the handiwork of sophisticated hackers that targeted larger companies, the truth is much more disturbing. Hackers have made "ransomware kits" available online for as low as $400, and little expertise is needed to launch the attack; such kits have even been advertised on YouTube.

Meanwhile, the effectiveness of DDoS attacks became apparent in October 2016. During a DDoS attack, a hacker attempts to make an online service unavailable by overwhelming it with traffic from multiple sources. The purpose of making the site unavailable is to cost the targeted company time and money. In October 2016, hackers targeted Dyn, a domain name system provider that worked with such companies as Twitter, Spotify, SoundCloud, Box, The Boston Globe, The New York Times, Airbnb and Reddit. Once Dyn was disabled, none of the other websites could be reached. Dyn later disclosed that the attack was coordinated through a large number of malware-infected, internet of things-enabled devices, including cameras, residential gateways and baby monitors.

As always, the best defense against these emerging threats is twofold: (1) a strong IT detection system, and (2) employee awareness and training. Make sure your IT system is robust and is following best practices; the NAIC's current guidelines are an excellent starting point, and you can look for additional guidance from the NAIC over the next few months. Train your employees to be on the lookout for red flags such as phishing emails, unsecured devices and websites that may contain malware; several organizations offer this service, both online and in-person. Finally, make sure that your organization has an incident response plan in place to effectively and efficiently respond to a cyber incident. The plan should identify key stakeholders, important contacts and law enforcement officials, both at the state and federal levels.

Good luck out there in 2017, and stay safe! P

RANSOMWARE continues to be the fastest-growing MALWARE across all industries, increasing

50%

in 2016 compared to 2015, according to new data from endpoint security provider Carbon Black.

As always, the best defense against these emerging threats is twofold: (1) a strong IT detection system, and (2) employee awareness and training.

Jana M. Landon is the co-chair of Stradley Ronon Stevens & Young, LLP's Data Breach Response and Cyber Insurance teams. Her practice focuses on advising organizations of all sizes in multiple industry sectors on data breach response, data security and data management issues. Jana also provides regulatory compliance services and assists clients in policy/procedure preparation, tailored by the client's specific risks and governing laws. In the area of cyber insurance, Jana assists clients in evaluating coverage, determining whether existing coverage is sufficient, and proactively protecting data before an incident occurs. In the event of a data breach, she provides post-breach counseling regarding existing insurance coverage as well as any statutory notification requirements. P