MIBA Compliance Corner

June 2016

Protect or Pay: Cybersecurity in the Age of Ransomware

By: Kevin Christensen, SHAZAM

In the realm of cybersecurity, pirates are making a comeback. Today, it's less "Captain Hook" and more "Captain Hacker," as they try to hijack your private information through a diverse arsenal of virtual weapons. And you'll never know where they'll strike.

The fastest growing style of cyberattack is the use of ransomware. Data pirates use malware to infect computers and restrict users' access to their own files, usually threatening to destroy the information unless the user pays a ransom. One common method is a pop-up screen claiming to be from the FBI or other federal agency stating you've violated some law. The message completely freezes your computer, locking it down until you pay a specified amount of money, from hundreds to thousands of dollars.

This sophisticated programming intimidates most users into paying up. Last year, according to the Internet Crime Complaint Center, U.S. businesses and consumers experienced $18 million in losses due to ransomware. After these ransoms are paid, many attackers still don't unlock the data, leaving the victim out their money and their information.

Smaller institutions may think they're not big enough to be a target, but they should think again. Cyber-attackers aren't looking for the biggest prize— they're looking for the weakest link. Data thieves also share resources and communicate vulnerable areas and successful tactics to other hackers across the globe. So the question isn't *if* your information will be targeted, but *when* and *how*.

So what can you do to protect your institution and customers from these attacks?

Traditionally, information security has been perimeter-based, with internet-facing systems secured behind firewalls. But in today's technology environment which is always on and always changing, cybersecurity is not something static that we can "set and forget." Your security must be as dynamic as the environment it protects. We know the threat is real: systems like SHAZAM's are "tested" by scammers probing for weak spots thousands of times *every day.*

One simple security step for your institution is to regularly back up your critical files. Ideally, having a well-segregated backup should be able to restore your information in the event of a ransomware attempt. This should happen before the hack occurs, since ransomware can sometimes be hidden within backup files as well.

Another safeguard is to educate yourself and your staff against the lurking

*Information for the **MIBA's Compliance Corner** is from Associate Members of the Missouri Independent Bankers Association. These services are provided with the understanding that the Missouri Independent Bankers Association is not engaged in rendering legal, accounting or other professional services. If legal advice is required, the services of a competent professional should be sought.*

danger of social engineering or “phishing” hacks. This is the most popular type of attack, accounting for over 38% of all data breaches in 2015, according to the Identity Theft Resource Center. A phishing scammer poses as a trustworthy organization (via email, social media, or other methods) to trick you into giving them personal data—which they can then use to install malware and gain a bigger foothold on your institution’s valuable information.

Your main defense is to have a partnership with a cybersecurity team that can be on constant lookout for these ever-evolving threats. The best partners will take a two-part approach. First, they’ll help you identify weaknesses in your institution’s defenses before the thieves do. Then, they’ll work with you to set up a layered security plan that best fits your needs.

There are no universal preventions for every possible threat, but your organization can put the tools in place to detect a pending attack, block likely attacks from succeeding, and protect your important data in a compromised environment. As hackers scavenge the virtual seas for your valuable information, equip your institution with dependable technology controls that have the flexibility to defend your data, whenever and however cyber-pirates try to strike.

Kevin Christensen, Vice President of Risk and Financial Services

Kevin oversees SHAZAM’s risk, compliance and merchant sponsorship programs. His risk services team works with financial institutions and merchants to provide a variety of audit, compliance, security and sponsorship services to minimize risk.

Prior to joining SHAZAM, Kevin worked for the Federal Deposit Insurance Corp. (FDIC) for 10 years. His diverse experience ranges from the community bank level to some of the largest and most complex data centers in the Midwest.

Kevin has earned the Certified Information Systems Auditor (CISA) and Certified in Risk and Information Systems Control (CRISC) designations and is a member of the Information Systems Audit and Control Association (ISACA®). In addition, he’s given presentations to regulatory examiners and bankers on topics including compliance, fraud, information security and business continuity.

About SHAZAM

The SHAZAM Network, founded in 1976, is a national member-owned and -controlled financial services and payments processing company. SHAZAM provides choice and flexibility to community financial institutions throughout the U.S. SHAZAM is a single-source provider of the following services: debit card, core, fraud, ATM, merchant, marketing, training, risk and automated clearing house (ACH). To learn more, visit shazam.net and follow @SHAZAMNetwork.