INDUSTRY INSIGHT / HARRISON E. TROPP

Cybercrimes pose an existential threat to all companies, including financial services law firms. But knowing what to do in the event of a loss can help mitigate it.

Foreclosure law firms have played an important role in the implementation of technology and have, in many ways, led the charge. Whereas traditional firms transmit an aura of forced conformity, the default sector has been seemingly receptive to technological progress. From the development of proprietary case management systems to installing paperless file and barcoding classifications, many firms have been receptive to exploring new efficiencies. Unfortunately, technological advancements do not always yield positive results. In the not too distant past, the thought of a law firm being infiltrated remotely by a third party seemed far-fetched, if not completely absurd. In an era of illicit creativity though, cyber-related crimes have continued to rise in recent years and now pose an existential threat to all companies, including law firms.

THE FIVE FOLLIES

Cybercrimes unfortunately do not fit a standard mold. According to Travelers Insurance, there are five specific types of threats, and understanding each type can better prepare a firm for a potential loss.

1. **General Hacking:** While it can be argued that all versions of cybercrimes involve some sort of hacking, this is perhaps the most basic one. Hacking occurs when a person gains access to information by way of weak or default passwords. Moreover, hackers can install malware to capture keystrokes, thus increasing the potential of a password being compromised.

WOLVES IN SHEEP'S CLOTHING

The ABA estimates that, of the firms infiltrated by a cyber threat, "notification is typically the largest single direct cost, with an estimated cost of $200,000. This includes requisite activities such as creating contact databases, retaining outside experts, postal expenditures, and determining regulatory requirements."

2. **Social Engineering:** Perhaps one of the more common crimes in the legal sector involves a hacker taking the identity of someone within a firm in order to force an action. For example, a hacker will infiltrate the email box of Law Firm A's Managing Partner. The hacker then composes and sends an email to Law Firm A's accounting department requesting a wire transfer of $100,000. Believing that the request is legitimate, the accounting manager sends the requested funds. Although the transmitted funds are often unrecoverable, most cyber-insurance policies have a specific sub-limit for social engineering.

3. **Spear Phishing:** Spear Phishing begins when an unsuspecting person receives an email from what they believe to be a legitimate source. Usually, this email will contain a hyperlink, and once the recipient clicks on that link, a hacker immediately gains access to professional and personal information. The hacker can now view anything that the employee has access to on the firm's servers. In the default space, such an action could potentially expose thousands of records of confidential borrower information, including social security numbers.
4. **Rogue Employee:** According to Travelers, inside threats account for 15% of all data breaches. This type of threat is especially concerning due to the level of access some employees have to confidential or sensitive information. Not only can rouge employees access information, but they can also install malware or other malicious programs if they are technologically competent.
5. **Ransomware:** Citing the Verizon Data Breach Incident Report, Travelers acknowledges that Ransomware is the fifth most common form of malware. Ransomware occurs when an individual penetrates a firm's network and essentially holds their private information "ransom" until some form of monetary compensation is received. Upon receipt of payment, the individual hopefully then releases the information back to the firm. The most recent and crippling example of this came in 2017 with a Ransomware attack on DLA Piper. The attack resulted in the complete shutdown of the firm's entire U.S. IT operations for several days.

NUMBERS DON'T LIE

In her 2018 Gallup article "Cybercrimes Remain Most Worrisome to Americans," Megan Brenan found that Americans are more concerned about cybercrimes than violent crimes. Perhaps just as alarming, 71% of those polled indicated that they frequently fear a computer hacker will access their personal financial information. Brenan further noted, "The frequency with which Americans worry about becoming victim to a variety of different crimes is similar to last year, as they remain much more likely to fear being victimized by cybercrimes than traditional crimes."

The impending fear of victimization has continued to grow over the years, in part due to Americans' increased reliance on digital information. Millions of Americans have been affected by a data breach in one form or another, whether due to an isolated incident such as identity theft or by way of a larger data breach. Continued dependency on digital platforms has increased potential exposure, whether in the form of online banking or through social media.

According to the American Bar Association (ABA), 25% of all law firms in the United States have experienced at least one data breach. While firms certainly maintain a looming fear of an imminent breach, a core driver for such fears pertains to the hard and soft costs relating to an actual cyber loss. The ABA estimates that, of the firms infiltrated by a cyber threat, "notification is typically the largest single direct cost, with an estimated cost of $200,000. This includes requisite activities such as creating contact databases, retaining outside experts, postal expenditures, and determining regulatory requirements."

In terms of a direct loss, the same article references a 2016 report by insurer QBE. A study by the insurer confirms that more than $120 million was stolen across the legal profession within an 18-month period as the result of data breaches. If that number was not staggering in and of itself, there are also the resulting soft costs of cyber loss, including employee and network downtime, loss of billable hours, unrecoverable date, and reputational damage. In addition, law firms could be susceptible to lawsuits from their clients.

MITIGATING THE THREAT

The ABA has produced a treasure trove of valuable information to help firms not

only recognize cyber risks, but also to assist in providing the appropriate measures law firms need to take to help mitigate a cyber loss. According to the ABA, the first line of defense includes controlling access by way of authentication measures. These include basic processes such as the routine updating of passwords, as well as more complex systems such as fingerprint readers and facial recognition.

The universal consensus acknowledges that, no matter if the device is a smartphone or laptop, all devices used by attorneys should incorporate some form of basic authentication. In addition to strong passwords, the ABA further recommends that firms also maintain a level of encryption. In basic terms, encryption allows data to be protected until it is decrypted by using a specified password or other measure. This form of access control protects data in storage and transmitted data. Data can include information housed on devices or servers and information exchanged through email or another messaging form. There is an additional concern with the popularity of remote access as web-based applications, as well as virtual private networks (VPNs). Thankfully, most platforms already utilize some level of basic encryption.

Finally, there are other types of security measures the ABA recommends, including anti-spyware, firewalls, antivirus programs for devices, and intrusion detection. Firms that believe they could be especially prone to a cyberattack can hire third-party companies to perform a network penetration test, and then remediate any findings accordingly.

While the ABA's suggestions are valuable to all firms, foreclosure firms have an extra layer of responsibility both in terms of protecting their clients' information but also in terms of shielding confidential borrower information. If there is a "fortunate" component to compliance requirements, it comes in the form of the technology audit.

While client mandates pose a staggering cost to default firms, both in terms of physical security and cybersecurity, they do outline requirements that make default firms more protected than most. In fact, the ABA's recommendations and most servicer requirements share many similarities. Both include multi-factor authentication measures, disaster-recovery and business continuity plans, as well as the need for encrypted remote access.

ALL IS NOT LOST

The increased creativity employed by cybercriminals makes it difficult to thwart every potential threat. While recognizing the risk is the obvious key to prevention, knowing what to do in the event of a loss can help mitigate further damage. A data breach involves myriad complexities, making cybercrimes much more difficult to track than any traditional form of theft. Often, a hacker can spend an indefinite amount of time monitoring a firm's network before he or she decides to cause damage. Once a cyberattack occurs, the first step is to identify the problem and understand the root of the issue. This next step may not be as apparent, but there is a crisis-management component firms will need to employ to prevent reputational discreditation.

Vivian Hood, the CEO of Jaffee Partners, outlines a step-by-step guide in her 2018 piece for *The National Law Review*, entitled "Law Firms and Cyber Attacks—What's a Law Firm to Do?" In her article, Hood argues that perhaps the single most important response was for firms to alert relevant parties before a breach became public. Hood notes, "Now more than ever, transparency is necessary—even though it may seem like the least desirable approach to take."

Hood makes the argument that sharing the news of a data breach before its leaked by someone else allows a firm to prevent further reputational damage. This decision is a small component of a firm's overall crisis communications plan, which should be shared with clients, staff, attorneys, and even vendors. A standard plan should have an outlined process for what information is to be communicated (and by whom), as well as a timeline identifying the breach, including information pertaining to what the firm is doing to lessen the damage.

ENSURING YOUR TECH FUTURE

While controlling the narrative is important to maintaining reputational integrity, there is undoubtedly a monetary component to consider as well. Cyber-insurance is a relatively new coverage type that came into existence approximately 15 years ago as a standalone policy with individual limits and sub-limits. In its basic form, cyber-insurance protects firms in the event they have a data breach and a resulting loss. Types of covered losses could be direct, such as an intercepted wire transfer, or indirect, such as the loss of revenue during network downtime.

Once a cyberattack occurs, the first step is to identify the problem and understand the root of the issue. This next step may not be as apparent, but there is a crisis-management component firms will need to employ to prevent reputational discreditation.

Other coverage provisions include limits for computer and legal experts, betterment, data restoration, and public relations. For law firms of all sizes and practice demographics, cyber-insurance is a relatively inexpensive layer of protection considering the exorbitant expense associated with a cyber-incident. For the foreseeable future, cyberthreats will remain a global danger to all companies. While lawyers and IT specialists alike have improved the network security of their respective firms, the ongoing creativity of hackers makes it difficult to outstep this ever-changing peril. It is important that all employees remain cognizant of cyber-fraud and continuously monitor any potential danger. While cybercrime certainly won't be eliminated, it can be appropriately managed so law firms can lessen their risk of a loss. DS