Everyone has seen the headlines about companies such as the retailer Target, which had the personal information, including credit-card numbers, of 70 million customers’ stolen after it was hacked in 2013. While that data could be sold for a nominal amount on the black market, hackers now realize that the information held by law and other professional services firms—details about mergers and acquisitions, pending lawsuits and new products, for instance—is far more valuable. It is fast-becoming the target of cybercriminals as a result.

In a recent program that was part of the RSM and Northern Trust’s Law Firm CFO Forum in Chicago, Andy Obuchowski, national practice leader for Digital Forensics and Incident Response Services and director of security and privacy consulting at RSM, talked about the most common threats to information security that law firms currently face. He also discussed the steps they can take to prevent data breaches or effectively respond to them should they take place.

According to the Verizon Data Breach Report, 52 percent of cybercrime committed against professional services firms is cyber espionage, 25 percent is committed through crimeware and 10 percent through miscellaneous errors. Ransomware, for example, can encrypt a firm’s data, making it inaccessible. Instead, users see a message on the screen informing them that it will be released only after the firm has paid a ransom, usually using Bitcoin, an online currency that is untraceable and can send funds to foreign countries, where hackers often reside.

Cybercrime occurs most prevalently through:

**Hacking**—Traditionally happens after a cybercriminal has figured out how to breach a firm’s system. More current methods focus on stealing data through a firm’s web applications or browser plug-ins.

**Malware**—This can include ransomware and other malware that hackers obtain easily online. It can be undetectable by anti-virus software, which provides protection 80 percent of the time at best, according to Obuchowski.

**Social engineering**—The cybercriminal gets employees to do something they normally would not do. For example, the criminal sends a staff member an email citing details about the firm obtained on LinkedIn and includes an invoice for a fictional project done overseas, which is then paid.

**Physical loss**—A laptop or other device is lost or stolen and used to commit cybercrime. If the crime is committed by an employee, the device used to execute it mysteriously goes missing. This can be a rare occurrence but can have far-reaching effects.

Firms can combat cyberattacks by instituting security controls and tools in three areas. While law firms often pursue some of these controls, they rarely have all three, which would ensure the greatest security.

**Preventative controls**—Include vulnerability, patch and configuration management; access and authentication; intrusion prevention systems and anti-virus blocking. It is valuable to note that firewalls and other systems to protect networks that are purchased at mass retailers are not as effective as those obtained from specialists or custom-developed for a firm.

**Detective controls**—Include security information and event management; managed security service providers; intrusion detection systems; monitoring of database activity, compliance and operations; anti-virus hosts and network alerts. These controls detect potential breaches and generate alarms that must be responded to in a timely fashion to be effective.
Corrective controls—Include incident response; forensics; anti-virus quarantines; system isolation; disaster recovery and business continuity plans; and administrative or legal actions. If a cybercrime occurs despite a firm’s having preventative and detective controls in place, corrective controls can still minimize or repair the situation.

Incident scoping, evidence preservation and analysis

Even with controls in place, data breaches can still occur. How a law firm responds can make all the difference in containing the damage. Ideally, someone experienced in incident response and forensics investigations is called in well before the IT department—even with its best intentions—begins to work on the issue. The specialist will systematically identify and preserve as much evidence as possible. The investigation could include network servers and applications, computer–system memory, firewalls, virtual private networks, email, building–access logs, system backups, third-party providers (such as cloud services) and video surveillance.

The specialist will want to know what is known and unknown about the event. Questions could include: How did malware get into a laptop to begin with? What has that laptop been connected to and what could the criminals have additional access to as a result?

Analyzing evidence is the next stage. The specialist will define the time period of the compromise as accurately as possible and then evaluate the risk of harm. For example, a law firm’s main server containing all of its information about current and past cases going back seven years is breached. The information is in Word documents, Excel spreadsheets, PowerPoint presentations, email and databases. The specialist will produce a comprehensive collection of that data for review by consolidating it from all file formats into a spreadsheet that is more easily analyzed.

Analysis spans many levels. Figuring out the depth and breadth of access to data that employees have based on their usernames and passwords can help identify areas affected by a breach. For example, knowing that in Windows passwords are stored as an alphanumeric string that can be cut and pasted into a password box, thus gaining someone access to a restricted area, is just one small example of considerations made during analysis. "While a firm may want to complete an investigation quickly due to numerous pressures, there are many questions that need to be asked to learn what really happened," Obuchowski said.

The process can take several weeks or months, so even when regulatory requirements stipulate that firms have 60 days to investigate an incident, they should not wait until the last moment.

Mitigating costs and risks

No law firm is too small or too large to be attacked, and more firms are being proactive now with preventative measures. Doing a risk assessment before a data breach occurs, followed by the development of a security program, is a great way to minimize risk. Have an incident response plan in place, run mock response drills and conduct security awareness training. From a technical perspective, have a program in place to classify and identify types of data. Then segregate it, dividing it among different locations—known as data pooling—to protect it. Test all backup, archiving and anti-virus solutions, noting any vulnerabilities in the firm’s network that hackers may exploit.

Finally, consider purchasing cyber-liability insurance. It provides important balance-sheet protection and is valuable for responding to events that are difficult to predict and can create big losses. Insurance often covers security and privacy liability, regulatory defense and penalties, and costs generated by breach response including computer forensics, notifications, pre-claim legal expenses and public relations. Coverage can extend to business interruption, cyber extortion and may pay for a risk assessment or allow for a reduced premium for firms that have one done. Insurance is involved in six out of 10 company data breaches now, compared to just one out of 10 breaches five years ago, according to Obuchowski. Aside from forensics and fines, law firms may find that the biggest cost they face is to their reputation if they do not take adequate preventative measures. So, investing in cyber-liability insurance and security controls could be well–spent money, time and effort to fulfill their obligation to protect their clients’ sensitive information.

Source:

The Law Firm CFO Forum

The Law Firm CFO Forum is a new program co–sponsored by RSM and the Northern Trust. It provides CFOs and other financial leaders at law firms with a continuing series of presentations on current topics of relevance to them and is an opportunity for them to network with others in their profession. The CFO Forum meets several times a year at locations in downtown Chicago. For more information, contact Barry Rosenthal or Michelle Grace.