Ohio Law Firms Suffer Cyber Breaches – LESSONS LEARNED

By Steve Couch
President and CEO, OBLIC

oblic
Ohio Bar Liability Insurance Co.

Yes, it's true.

Ohio law firms of all sizes can and do suffer all sorts of cyber breaches. OBLIC began providing complimentary cyber breach protection in 2014 and almost immediately began assisting Ohio law firms with responding to and recovering from cyber breaches. Since OBLIC began providing cyber breach insurance protection, it has helped respond to 23 cyber breach claims against Ohio law firms, with the two largest claims incurring notification costs exceeding $23,000 each. In all, OBLIC has helped Ohio law firms save out of pocket costs (not covered by a typical insurance policy) exceeding $117,500 in dealing with these nasty claims. Unfortunately, these claims are just the tip of the proverbial iceberg.

How Did This Happen?

The practice of law traditionally poses plenty of challenges—knowing and keeping abreast of the latest case law and statutory developments, honing your craft and improving your skills, complying with procedural and professional rules, finding and selecting desirable clients, collecting a reasonable fee and many, many others. Until just a few short years ago, protecting attorneys and their firms—whether as an owner, manager or insurer—was largely focused on helping them avoid, manage, repair and respond to the occasional mistake committed while navigating these traditional challenges.

Enter computers, digital storage, the internet, emails, the "cloud" and ever-increasing innumerable ways to conduct business faster and easier, and then add the widely unexpected, or at least under-appreciated, cyber criminal. Most law firms were not, and many still are not, truly prepared to defend themselves against the intentional actions of these unseen criminals. Unfortunately, customary loss prevention programs practiced by even the most sophisticated law firms were not designed to address this new risk.

Cryptomining. Ransomware. Business email compromise. Spear phishing. This is the new language of business risk. The highly publicized cyber breaches at Marriot (500 million records), Equifax (143 million records), Target (110 million records), JP Morgan Chase (76 million records), eBay (145 million records) and Yahoo (two breaches, 500 million and then one billion records) get a lot of publicity, but law firms are seen as treasure troves of low-hanging fruit by hackers.

LAW FIRMS AS TARGETS

Hitting closer to home, do the breaches of the Cravath, Swaine & Moore and Weil, Gotshal & Manges law firms sound familiar? According to Fortune, these law firms were allegedly targeted by China because of the clientele of these firms and the potential gold mine of confidential information they maintained. The office of the U.S. Attorney for the Southern District of New York is apparently investigating.

And then there was the attack against Mossack Fonseca, a Panamanian law firm, widely referred to in the press as the "Panama Papers." More than 2.6 terabytes of data were stolen before the law firm realized there was a breach, and a crucial 11.5 million sensitive records were lost, leaving the law firm with difficult conversations to be had with some very unhappy clients.

Cyber attacks against law firms were first widely reported beginning in 2008, and the frequency of publicly known law firm breaches has steadily been growing. In fact, Cisco, in its 2015 Annual Security Report named law firms as the seventh highest target for cyber criminals in 2014. In its report on law firm cyber security, LogicForce revealed over 200 U.S. law firms faced hacking attempts between 2016 and 2017, and 40 percent of the firms didn't even know the attack had occurred. The ABA recently reported that 25% of all U.S. law firms have experienced at least one data breach.

SPEARPHISHING

The most common cyberattack reported by law firms is "spearphishing," an email that appears to be from a trusted individual or business that is known or familiar, but instead is from a criminal hacker who wants to gain access to a law firm's computer system or obtain information to enable the theft of financial, credit card or other confidential, valuable data. The email typically requests the addressee to click on an executable link that then "opens the door" to the hacker, launching spyware, malware or a Trojan Horse. Many times, the addressee opens this door without ever realizing anything untoward has occurred.

PHISHING

The kissing cousin of the "spearphishing" attack is the rather simple "phishing" attack. This email usually appears to come from a large, well-known company or website with a broad membership base, and like its cousin, asks the addressee to click on an executable link. Any law firm, no matter its size or sophistication, can fall victim to these types of attacks without proper loss prevention preparation and education.

RANSOMWARE

In this scenario, the hacker gets someone within the firm (anyone with computer access) to click on a link which then launces a program that takes over the computer system, disabling it and holding the law firm's data and files hostage until a "ransom" of some sort is paid, often with bitcoin.

PERSONALLY IDENTIFIABLE INFORMATION

Cyber criminals are looking for all sorts of valuable information, from client confidential information to personally identifiable information (PII). PII can be used, directly or indirectly, or in combination with other information, to identify a particular individual. It includes:

- A name, identifying number, symbol or other identifier assigned to a person;
- Any information that describes anything about a person; and
- Any information that indicates actions done by or to a person, and any information that indicates that a person possesses certain personal characteristics.

Some examples of personally identifiable information, as defined by Ohio Revised Code (ORC) 1347.01, are names, Social Security numbers, resumes, correspondence, addresses, phone numbers, driver's license numbers, state identification numbers, professional license numbers, financial account information, medical and health information, physical characteristics and other biometric information, tax information, education information, individuals' job classifications and salary information, performance evaluations, employment applications and timesheets. Does your law firm possess any of this type of data?

LAW FIRMS CAN BE A PERFECT TARGET

As law firms act as warehouses of client and employee data, they should recognize they are not immune to cyberattacks. Not only are they not immune, in many ways law firms are the perfect targets. Most, if not all, law firms possess some amount of the above-described personally identifiable information and, in many instances, vast amounts of such information, whether that of their clients, employees, or parties and witnesses in litigation.

THEFT

In addition to the phishing attacks previously described, law firms also commonly experience cyber breaches due to the loss or theft of a laptop, thumb drive, smart phone, tablet or other mobile device. If the information on the device was not encrypted and contained or had access to files containing any of the personally identifiable information described above, a breach has likely occurred. With access to office email and other law office networks, such theft can be an open door for cyber criminals to gain access to and steal confidential information.

Employee theft is also a significant risk within the law firm environment. Whether it is the theft of a laptop as described above, theft of the actual data itself, or theft of user identifications and passwords, such can occur and often go undetected for a lengthy period of time. Such conduct can originate with an employee or can originate through outside parties who "influence" an employee in a compromised position (for various reasons), i.e., social engineering. Often, by the time such conduct is discovered, the stolen data has made its way to third parties for various nefarious purposes, usually including identity theft.

25%

of U.S. LAW FIRMS have

EXPERIENCED AT LEAST ONE

DATA BREACH

Attorneys' Responsibilities

Besides the common law duty owed by attorneys to protect the confidential information entrusted to them by clients, two additional sources of duties require attorneys to protect data: the Rules of Professional Conduct and federal and state law. Rule 1.6 of the Ohio Rules of Professional Conduct requires an attorney to maintain the confidentiality of information relating to representation of a client and Rule 1.9 requires the same for information of former clients. Rule 1.15 of the Rules of Professional Conduct requires that an attorney safeguard property of a client in his or her possession—a fiduciary obligation.

Most states and U.S. territories also have enacted data security breach notification laws. Ohio's notification law, ORC 1349.19, applies to personally identifiable information of Ohio residents. It defines a "breach" as unauthorized access to and acquisition of unencrypted computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that results in, or is reasonably believed to cause a material risk of, identity theft or fraud to the person or property of an Ohio resident.

Pursuant to this law, a breach of security of the person's or business's data system must be disclosed to any resident of Ohio whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person, if the access and acquisition by the unauthorized person causes, or reasonably is believed will cause, a material risk of identity theft or other fraud to the resident. Disclosure is required to be made in the most expedient time possible, but no later than 45 days following its discovery or notification of the breach of the system, subject to the legitimate needs of law enforcement activities. Failure to comply with this notice requirement is subject to investigation and a potential civil action brought by the Attorney General.

Costs Involved

The types of costs associated with a data breach can be many, beginning with the expenses associated with hiring a computer forensics expert to determine how much information was compromised, and most importantly, whose information was disclosed. This cost can range from a few thousand dollars to tens or even hundreds of thousands of dollars, depending on the breadth of the breach. Another typical cost is that associated with compliance with the notice requirements of the state(s) of residence for those persons whose information was disclosed, and depends largely on the number of records disclosed. This cost will also vary based on whether the notice can be sent electronically, whether it must be mailed, whether additional costs need be incurred to locate the persons whose information has been disclosed, and whether alternative notice or publication is necessary.

Once a breach is discovered, additional costs are often needed to repair any damage to the systems themselves, replace or restore software or data records that might be damaged or corrupted and block further access to the criminal(s) who obtained the personal information. These out-of-pocket costs do not include the potential damage to reputation caused by a breach, often occurring as a loss of trust of clients who entrusted their confidential information to the law firm. Most law firms will also experience some form of business interruption as a result of a data breach, as many hours will be devoted to investigating, responding to and repairing the breach. Finally, if clients sustain damage as a result of the data breach, such as damage to their credit resulting from identity theft or loss of funds from financial accounts, they may articulate a claim for negligence or malpractice.

40% ***of the*** **FIRMS**

DIDN'T EVEN KNOW THEY WERE ATTACKED

9 ways to limit the risk of cyber breach

1 Develop a comprehensive information security plan designed to prevent data breaches. A great resource is the ABA Cybersecurity Handbook.

2 Conduct a risk assessment, which often can be aided by the services of knowledgeable, objective, independent IT vendors.

3 Use appropriate encryption technology on servers, desktops, laptops and all mobile devices.

4 Limit access to computer systems, email, and directories to known and trusted users only, and implement and follow appropriate password policies.

5 Develop and follow a data retention and destruction policy, so personal data is not at risk. It is important to sanitize and eliminate personal information that is no longer needed, and frankly, to avoid collecting personal data that is not essential. Law firms should carefully analyze where such data is kept, and limit the number of places where such data is retained.

6 Keep anti-virus and security software up to date, regularly applying recommended patches.

7 Educate employees about appropriate handling and protection of sensitive data, proper use of email, and use and protection of passwords.

8 Implement and follow a written internet security protocol (WISP) to explain in detail how internet access and usage should be conducted on firm computers, and specifically, the limits on such usage. Not only is this employee education process important, but management of this exposure should continue through employee exit strategies, realizing that unhappy former employees pose a significant risk for a potential data breach.

9 Develop a comprehensive breach preparedness plan, to enable decisive action and avoid operational paralysis when a data breach occurs. This will allow a firm to timely respond to a breach incident, perhaps limiting the scope of the breach and potential damages to those whose information has already been compromised, as well as limiting the amount of lost productivity and negative publicity that might result from a data breach. With careful thought and planning, law firms can significantly lower their exposure to a potential data breach and have a road map in place when and if such event occurs.

oblic

OBLIC Can Help

Although a client's claim for cyber breach-related damages based on negligence or malpractice may be covered under some legal professional liability insurance policies, most often "first party-related costs/damages" are not. Such first party costs/damages can include most of those mentioned above: business interruption, privacy breach response costs, notification expenses, breach support and credit monitoring expenses, damage to data and computer programs, cyber extortion expenses, computer forensic and investigation fees, public relations expenses, legal expenses, etc.

It is with these risks in mind, and in recognition that the costs of a cyber breach to a law firm can be significant, that the Ohio Bar Liability Insurance Company (OBLIC) includes cyber breach insurance coverage, FREE OF CHARGE, in all of its legal professional liability insurance policies protecting Ohio law firms. This coverage provides protection for the first party type damages described above, which are not ordinarily covered by a professional liability policy, with additional protection for defense costs and penalties incurred as a result of a regulatory investigation.

Such coverage provides limits of liability of $50,000 per claim and in the aggregate for firms of ten attorneys and fewer, and $50,000 per claim and $125,000 in the aggregate for firms of eleven or more. Moreover, OBLIC encourages its policyholders to purchase additional cyber breach coverage, with higher limits and broader coverage terms (at very affordable rates), via its subsidiary the OSBA Insurance Agency. Finally, OBLIC policyholders also receive complete complimentary access to an extensive treasure trove of cyber security loss prevention tools and resources.

We have cyber breach coverage for your firm, no matter the size, type of practice or scope of cyber security protection needed.

If you are not an OBLIC policyholder, or you are a policyholder but don't have adequate cyber security coverage, call or email an OSBAIA Agent:

RICK CREEL
Vice President, Sales and Business Development
(614) 344-4157
rcreel@osbaia.com

TAMMY J. THORNTON
Senior Sales Executive
(614) 572-0616
tthornton@osbaia.com

DANNA BLACKBURN
Sales Executive
(614) 572-0616
dblackburn@osbaia.com