"CYBER ARMAGEDDON: TEN WAYS TO PROTECT YOUR LAW FIRM FROM ANNIHILATION"

By: Theodore M. Schaer of Zarwin Baum, Elizabeth S. Fitch of Righi Fitch and Kelly Geary of Integro

Law firms are low hanging fruit in the cybercriminal world. Patrick Fallon Jr., Assistant Special Agent in charge of the FBI's Pittsburgh field office explains, "Law firms are a rich target. They don't have the capabilities and the resources to protect themselves. Within their systems are a lot of the sensitive information […] [T]herefore, it's a vulnerability that the bad guys are trying to exploit, and are exploiting."[1] Furthermore, following the recent flood of law firm data breaches including Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, "Plaintiffs law firms are already planning to bring class action legal malpractice litigation against legal industry players over the exposure of clients' information."[2] Cybercriminals are no longer only going after large corporations and national governments; they are also hitting small- to mid-sized firms. Law firms must be proactive by protecting their information, raising internal awareness and implementing a cyber-breach protocol.

Data breaches have a greater impact on law firms because they hit at the core of what makes the attorney-client relationship so important. The sacrosanct duty of confidentiality holds law firms to a higher standard of cybersecurity best practices. This duty is reflected in hundreds of American Bar Association publications, states' rules of professional conduct and state and federal statutes. For all other types of businesses, many data breach statutes require the information breached to have been disseminated, but for law firms, the duty of confidentiality significantly lowers the bar so that mere infiltration of information without dissemination would be considered a breach of confidentiality.

---

[1] Conte, Andrew. "Unprepared Law Firms Vulnerable to Hackers." *TribLIVE.com*. Trib Total Media, 13 Sept. 2014.
[2] Coe, Aebra. "BigLaw In Crosshairs As Firm Plans Data Breach Litigation." *Law360.com*. Law 360, 31 Mar. 2016.

The idioms -the emperor has no clothes and the cobbler's children having no shoes - could not ring more true for law firms and cybersecurity. The recent deluge of law firm data breaches[3], has demonstrated that even firms that advise large corporations and handle transactions that involve gigabytes of sensitive information do not implement their own cybersecurity advice. They talk about encryption and social engineering without planning for an attack or implementing their cyber-breach protocols. This is what fuels plaintiff firms, such as Edelson PC to prepare class action litigation against law firms over client data breaches.[4]

Overall it is the lawyers' need for, and increasing reliance upon, mobility that makes law firms such juicy targets for cybercriminals. The myriad of ways that attorneys interact with technology through different servers, cloud storage, laptops, smartphones and tablets provides for an abundance of cybersecurity vulnerabilities as well potential breaches of client confidentiality. The threat of a data breaches against law firms of all sizes is increasing by the day. Law firms can no longer turn a blind eye and avoid the growing problem – to do so would be irresponsible. Managing partners and firm leaders must first admit there is a problem and commit to making the changes necessary to protect themselves and their clients. They must invest the time and money in data and network security. Because each firm is different, so too will be their approach to cybersecurity. However, there are still universal strategies with respect to both data security and network security that every law firm can and should employ to safeguard the sensitive information they own. Although there is certainly overlap between what might is considered "data" security and that which is considered "network" security, we will discuss each separately along with the key associated strategies.

---

[3] HONG, NICOLE, and ROBIN SIDEL. "Hackers Breach Law Firms, Including Cravath and Weil Gotshal." *WSJ.com*. The Wall Street Journal, 29 Mar. 2016.

[4] Coe, Aebra. "BigLaw In Crosshairs As Firm Plans Data Breach Litigation." *Law360.com*. Law 360, 31 Mar. 2016.

DATA SECURITY

For our purposes, when we use the term "data security" we are referring to the confidentiality, integrity, availability and appropriate use of data. Although there are a number of different data security strategies, we will focus on the key strategy – Encryption.

ENCRYPTION

No matter the size, law firms must encrypt their data. "46 States require businesses to notify a person if their personal information was the subject of an unauthorized disclosure."[5] But all but one have exceptions for encrypted data. Encryption is a law firm's first line of defense - external communications and internal storage of confidential information must be encrypted as a baseline protection for confidentiality and privacy.

Within firms, intranet systems should be set up and data passing between computers on the firm's intranet should be encrypted. This prevents information from being leaked even if it is mistakenly removed from the firm's internal server or sent to the wrong person via email attachment. Each firm's intranet will vary based on volume and format of data being stored but even small firms with fewer than 100 attorneys can have gigabytes of clients' information stored on their servers and their attorney's smartphones on any given day. Therefore all, devices attorneys use must also have encryption capabilities.

Today more than ever, the attorney's need for mobility puts clients' information at a higher risk for breach. Transferring data from a remote laptop to a firm's server or sending an email from an attorney's smart phone to client or vendor's account has the potential for a cyber-

[5] Panneton, Raymond L. "Encryption Is the Key to Securing Sensitive Law Firm Information." *The Legal Intelligencer* 30 Mar. 2016, P. ed., sec. 2015: 5+. Print.

breach. Client's sensitive information regardless of which device it is sent from is a potential treasure-trove for cybercriminals. However, even if a firm's server is encrypted, there are added layers of protection to ensure confidentiality within emails. For example, Proton Technologies AG created ProtonMail which uses encrypted email servers and built in end-to-end security that complies with Switzerland's strict privacy laws. ProtonMail is just one example of a best practice to secure client communications.

Encryption does not have to be expensive. Microsoft Outlook provides an encryption option for email software. Technology security companies such as Silent Circle have created smart phone apps that use encryption technologies so whether it's sending email or storing information in the phone itself, encrypted information is much more difficult for hackers to access. For added protection, firms could choose to use custom built smartphone operating systems that contain embedded encryption technologies. These operating systems come armed with firewalls and encryption protocols to safeguard against cyberattacks. Although encryption is only half of the battle, all law firms must encrypt their data as part of a baseline standard of practice to ensure that confidential information remains confidential.

Again, encryption is only one data security strategy firms should be employing. Others include: (1) Securing the firms Physical Premises: Many firms experience a breach following an office break-in where laptops or other devices have been stolen; (2) Be a Data Minimalist: Evaluate your data. Know how much PII, PHI and Confidential Corporate information you hold and use – know how much you ***need*** to hold and use. Limit what information you collect and how long your store it for; (3) Know Where you Data is: Do you have a local server or do you rely on the cloud? If your data is in the "cloud" do you know where the cloud provider keeps your data? and, (4) Limit Access to Information: Evaluate and limit access to PII, PHI and

Confidential Corporate information. Only those that ***need*** access to such information should ***have*** access. Recognize and appreciate that this may require changes to workflow.

NETWORK SECURITY

Now we move on to "network security". For our purposes, when we use the term "network security" we are referring to policies and procedures that a firm adopts in an effort to prevent against and monitor unauthorized use or access to all its computer systems on which data is stored, managed or processed. Below we will discuss some of the key elements that should be considered and incorporated when preparing network security policies.

NETWORK SECURITY POLICIES

Even state-of-the-art security will not prevent human error. Social engineering accounts for many of today's costliest cyberattacks which means every law firm is at risk.[6] Scams and attacks have come from all angles. Whether it is phishing emails, phone calls or social media deceit (where the criminal pretends to be a friend who already knows so much about potential target/employee in order to steal a company information) an employee can be the weakest link in a law firm's cybersecurity.

Implementing cybersecurity policies and making sure to train employees on those policies is critical to securing clients' information and maintaining confidentiality. A clear cybersecurity policy should detail the law firm's breach protocol and educate all employees, on all levels (from the receptionist to the Managing Partner), on user responsibility for all firm devices including – employees' personal devices used for work. Training with regard to

---

[6] *Verizon 2015 Data Breach Investigations Report*, issued in April 2015. http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/

suspicious emails, hyperlinks or phone calls will prevent many of the potential breaches from the outset. The key in any employee training is raising awareness for every employee's user responsibility especially when it comes to client's information on employee's personal devices and use of specific cybersecurity programs on firm's servers.

The second aspect of training comes from having a solid plan in place when a breach inevitably does occur. With data breach notification statutes in 47 states and a piecemeal of federal data breach notification statutes in place, having a data breach plan is a necessity for any law firm. Every plan should involve a core group within the firm to lead when a breach occurs and having everyone else in the firm know exactly what to do if a breach is suspected. Time is of the essence, not only because breaches can occur in an instant but many notification statutes have a deadline to notify clients of the potential breach of personal information. Everyone on the team must be fully cognizant of all the steps the firm must take to stop the breach and make sure everyone who needs to be is properly notified. The plan should encompass not just the cyber liability and data breach notification lawyers but also IT security specialists, cyber forensic experts and a PR professional. All of these different experts will help law firms navigate the turbulent storm that is a data breach. Even with a written policy, the firm must ensure preparedness by running cyber breach drills. These drills are the best way to ensure everything – from stopping and analyzing the breach to making sure all clients are properly notified – is done in order to minimize a law firm's liability.

The amount of data breaches is only growing and the potential damages are tremendous. As lawyers, it is unacceptable and irresponsible for law firms not to take appropriate action and protect their client's information. Without cybersecurity policies in place, law firms risk breaking their legal and ethical duties to their clients. Law firms must begin to use serious encryption

software on all their devices, train their employees and implement individualized cyber-breach plans. Unfortunately, most cyber security experts believe that even the best data and network security plans cannot fully protect any firm from a determined hacker or a careless employee. Accordingly, firms should consider the various methods of risk transfer that might be available to them in the event of, what may be, the inevitable.

RISK TRANSFER

There are two primary methods of risk transfer that are potentially available to a firm in the event of a cyber incident: (1) non-insurance: contractual indemnification and hold harmless provisions in a business contract – perhaps with a cloud service provider or a data management vendor, and (2) insurance: the purchase of insurance products targeted at specific risks.

NON-INSURANCE

Most firms rely, to some extent, on outside vendors for various products and services. In most situations, these relationships are contract based and likely contain some sort of indemnification and hold-harmless provisions. In light of the highly interconnected nature of the business world today, it is likely that these vendors have some level of access to your firm's network and data. Or, in the event the firm relies on a cloud service provider or outside data manager, they are actually holding your data. Here are a few things to keep in mind when evaluating these relationships: (1) The strength of an indemnity agreement is dependent upon the financial strength and viability of the other - remembering that losses in the cyber space could be catastrophic and frequent; (2) Conduct regular audits of any vendor that is managing or processing data for which you are the owner; and, (3) Understand and re-evaluate the promises

you have made to your business partners about security and understand the limitations surrounding the insurability of contractual indemnity obligations you may assume.

INSURANCE

All firms have a portfolio of traditional business insurance products, such as Commercial General Liability, Error & Omissions, Employment Practices, Director & Officer Liability, and Commercial Crime. Cyber risk presents a unique challenge in that the risk itself does not fit squarely within any of the traditional products.

A cyber security event has the potential to impact multiple traditional insurance policies. However, most traditional products are not intended to, nor designed to, fully respond. This has lead to tremendous growth in the stand-alone cyber insurance market in recent years. The growth of the cyber market, in turn, has caused underwriters of traditional insurance products to revise the policy forms so as to affirmatively address cyber-related exposures by either providing some limited coverage by endorsement or by excluding the exposure entirely. The market is, in essence, shifting coverage in order to make way for the new product - cyber. But, this transformation is far from complete – we are just at the beginning. Managing Partners and firm leaders must carefully review all insurance policies, including any stand-alone cyber coverage, to determine the extent of coverage they have, as well as any gaps that may exist.