Law Firm Security Breaches: Minimizing Impact

Technology, Privacy, and eCommerce

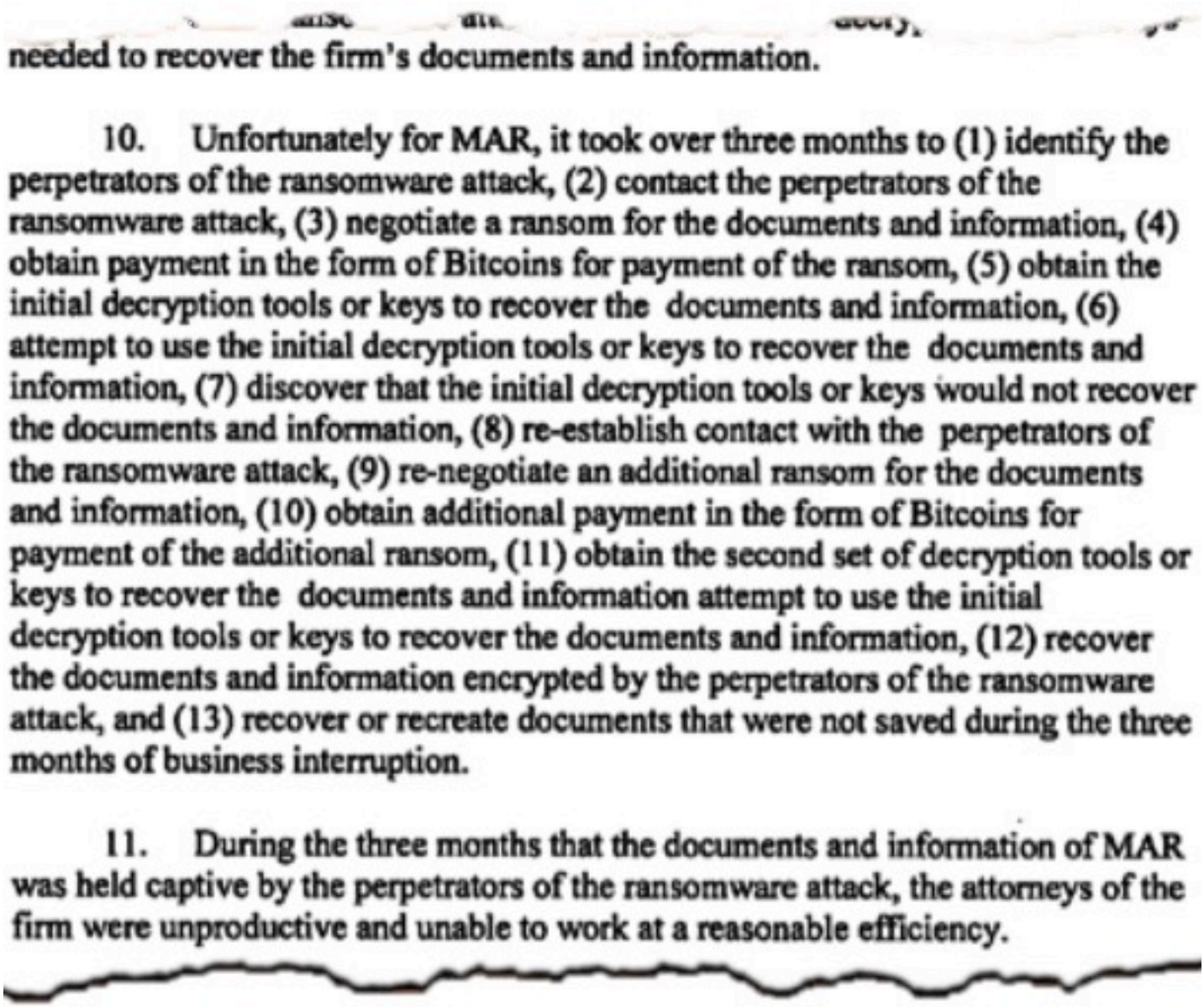
Like us, we're sure that many in-house counsel are fully engrossed in the subject matter of data security, cybersecurity, and incidence response. Hardly a day goes by when we don't hear about a massive breach (with Equifax being the latest that instantly comes to mind). At the same time, are we paying enough attention to one of the most common in-house department service providers: the law firm. In many ways, it's the perfect target, considering how much highly valuable and useful information law firms store combined with a less-than-effective security program implemented by many firms.

As entities, law firm systems contain highly-sensitive financial data, corporate strategies, trade secrets, business transaction information, and plenty of both Proprietary Information and Inventions Assignment (PIIA) and Protected Health Information (PHI). Unfortunately, many firms lack a complete, effective, privacy and security program. According to an ALM Legal Intelligence study, 22 percent of law firms did not have an organized plan in place to prepare for or respond to a data breach. Only 50 percent of law firms included in the study have cybersecurity teams in place to handle and implement the types of complex programs and initiatives necessary to deal with a data breach.

In a recent webinar put on by Logikcull, Olga Mack and Brian Focht (@NCCyberAdvocate) discussed the extensive ransomware vulnerabilities every law firm faces. Ransomware is malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. The webinar also focused on the kinds of measures in-house counsel can take to understand their exposure and risk by asking outside counsel the right questions from the outset.

The last two years have brought us a plethora of scary examples. In February 2016, a Russian

cybercriminal, under the name of “Oleras,” targeted law firms; in March, the *Wall Street Journal* reported that the nation’s biggest firms had been hacked (including names like Cravath and Weil Gotshal); in April, the “Panama Papers” were leaked, revealing confidential attorney-client information detailing tax evasion techniques; in May, a Chicago-based law firm was sued by a client for cybersecurity flaws that “systematically expos[ed] confidential client information”; in December, the DOJ charged three Chinese nationals for insider trading based on information hackers obtains from law firms.



needed to recover the firm's documents and information.

10. Unfortunately for MAR, it took over three months to (1) identify the perpetrators of the ransomware attack, (2) contact the perpetrators of the ransomware attack, (3) negotiate a ransom for the documents and information, (4) obtain payment in the form of Bitcoins for payment of the ransom, (5) obtain the initial decryption tools or keys to recover the documents and information, (6) attempt to use the initial decryption tools or keys to recover the documents and information, (7) discover that the initial decryption tools or keys would not recover the documents and information, (8) re-establish contact with the perpetrators of the ransomware attack, (9) re-negotiate an additional ransom for the documents and information, (10) obtain additional payment in the form of Bitcoins for payment of the additional ransom, (11) obtain the second set of decryption tools or keys to recover the documents and information attempt to use the initial decryption tools or keys to recover the documents and information, (12) recover the documents and information encrypted by the perpetrators of the ransomware attack, and (13) recover or recreate documents that were not saved during the three months of business interruption.

11. During the three months that the documents and information of MAR was held captive by the perpetrators of the ransomware attack, the attorneys of the firm were unproductive and unable to work at a reasonable efficiency.

We saw more these attacks in 2017. For example, in May 2017, the “WannaCry” ransomeware attack crippled over 200,000 computers across 150 countries by exploiting a flaw within Microsoft Windows that encrypts files. The attackers demanded a Bitcoin ransom payment from its victims — FedEx, the Russian Interior Ministry and Britain’s National Health Service. In June of 2017, the Petya ransomware attack exploited another Window’s vulnerability. The attacks were concentrated in Russia, Ukraine, and India and impacted Merck, Heritage Valley Hospitals, Cadbury, and essentially shut down DLA Piper. The attack on DLA Piper is worth looking into further as it sets the tone for the implications such an attack can have on an in-house legal department.

DLA Piper was first hit in Madrid, and then the attack continued throughout its global offices. It shut down email, phone, and computer systems, forcing DLA to request extensions in at least five civil

cases. It took almost a week for DLA to restore its email and other systems. Undoubtedly, this caused a great loss of productivity, billable hours, and an increase in the potential for client-driven litigation. Logikcull ran the numbers: The loss of billable hours in DLA Piper's DC office alone could cost well over US$500,000 a day.

Focht also brought up the example of Moses Afonso Ryan Ltd. v. Sentinel Insurance Co., Ltd, a firm that fell victim to a ransomware attack and sued its insurance carrier to cover US$700,000 in lost billings. What's even scarier is the tedious and lengthy process the firm had to go through to recover its data. A picture is, indeed, sometimes worth a thousand words:

In order to ensure that outside counsel are taking the necessary steps to minimize an attack's impact on sensitive data, here are the areas you should always address with your outside counsel regarding its security measures and readiness in the event of a cyberattack:

Operating system updates

While installing updates is annoying, it is strongly recommended for security reasons. Many updates involve fixing known bugs in the operating system (Windows or Mac) that create security vulnerabilities. How does your law firm make sure that every device installs those pesky OS updates as soon as they're available?

Encryption

It's simple to encrypt the entire disk of either a Mac or PC. The benefits are enormous and the costs are negligible. With encryption, the contents are unreadable unless you've logged in with your password. Devices and laptops get stolen all the time, and desktop computers are also vulnerable. Law firms need to intentionally encrypt more of their data — and be able to explain their efforts.

Two Factor Authentication (aka 2FA)

It is a good idea for law firms to sign up for 2FA for all services and/or applications housing sensitive data. 2FA puts an extra barrier for someone who wants to access email, data storage, or other systems storing confidential data. With 2FA, a password is not sufficient to gain access. Instead, you need to enter both your password, and a secondary code — typically sent to your smartphone via SMS message or via an app like Google Authenticator.

Strong passwords

The human brain can only hold so many good passwords. Weak passwords based on things like the names of our pets, our addresses, or simply the word "password" or "12345678" should be avoided. Password managers can help generate strong passwords and manage credentials for multiple accounts — requiring you to only remember one good password.

Physical security

In addition to talking about prevention, planning, and training, it's important to inquire about the physical security of the space and how the firm controls access to sensitive information.

Incidence response and disaster recovery

Similarly, it’s critical to know a law firm’s plan once something does go wrong. How does the firm plan on recovering? Do all key employees understand what role they play? It’s as important to prevent as it is to respond. Since there’s a high chance your data may be impacted, you should know what the firm will do should a cyberattack occur.

Employee training

Many security breaches result from hackers tricking users into doing things such as downloading a file infected with malware, sending sensitive data to the hacker, or sharing account credentials with the hacker. It is important to ensure that all members of the law firm — both staff and lawyers — are educated about both phishing and security. Everyone should know how to spot red flags, and how to react to a potential security threat.

Security risk assessments

While it’s great if a firm seems to be on top of security, its plans are only valuable if the firm stays current with the most up-to-date risks to its systems. Hackers get better and better every day, and your firm needs to know whether it’s systems are open to new vulnerabilities.

Insurance

All the caution in the world can’t prevent every cyberattack throughout a law firm’s entire lifetime. It’s important to make sure that law firms are insured just in case a breach does occur.

Undeniably, when we talk about cyberattacks on law firms, it is important to remember that law firms are, first and foremost, victims. While there are plenty of things law firms can do to decrease the chances of an attack, we don’t want to engage in victim blaming. As always, the goal is for in-house and outside counsel to partner strategically to make sure law firms have the most up-to-date and impactful security practices established to protect the information of all of its clients.

Olga V. Mack

Fellow

CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Katia Bloom

Commercial Lawyer and Associate General Counsel

ForgeRock

Katia Bloom is a fast-paced and strategic commercial lawyer. Currently, she is the associate general counsel at ForgeRock. Previously, she headed up legal for Avira, Inc., was a founding partner at E Squared Law Group, advising many start-up clients and was in-house counsel at Anesiva. She is actively involved in the Association of Corporate Counsel and a number of organizations promoting

women in the legal profession.