Firming Up Security

A Discussion of the Requirements and Benefits of Improving Security in the Legal Industry

DOS

Development • Operations • Security

Brittany Burns
info@dos.sh
https://dos.sh

FIRMING UP SECURITY

A DISCUSSION OF THE REQUIREMENTS AND BENEFITS OF IMPROVING SECURITY IN THE LEGAL INDUSTRY

I. INTRODUCTION

In May 2017, a global cyberattack spread across more than 200,000 machines, affecting universities, hospitals, and business around the world. Known as the WannaCry attack, the attackers used the WannaCry ransomware cryptoworm to blackmail users: either pay the 300 bitcoin ransom – the equivalent of $707,700 USD – or face erasure of all the user's data. The attack is a reflection of the growing cyber risk that businesses and individuals face. In fact, it is projected that the global cybersecurity market will exceed $202 billion by 2021.[1]

Law firms are not immune to cyberattacks, and regulators, clients, and attackers are taking notice. In 2009, the FBI issued an advisory warning attorneys of highly sophisticated spear phishing attacks specifically targeting law firms.[2] By 2012, the cybersecurity firm Mandiant estimated that 80% of the top 100 U.S.-based law firms had been hacked in the previous year.[3] While the report provided little insight into which firms were hacked and the breadth of information accessed, recent attacks prove that cyber criminals are highly interested in the immense amount of data that law firms possess.

This whitepaper examines the growing risk of cyberattacks on law firms, the responsibilities of law firms to protect client information, and next steps for firms.

II. HISTORY OF LAW FIRM ATTACKS

The amount and depth of sensitive information law firms possess has resulted in an increase in cyberattacks. According to NBC news, "Law firms have tremendous concentrations of really critical private information. [Infiltrating those computer systems] is a really optimal way to obtain economic and personal security information."[4] In 2010, international law firm King & Spalding was impacted by a hacking campaign that originated in China and infiltrated the systems of Google, DuPont, and Sony.[5] While that firm was caught up in a sweeping form of industrial espionage, hackers have become more and more targeted on specific firms and the sensitive data that they hold.

- In 2010, Gipson Hoffman & Pancione was targeted in a cyberattack based out of China after filing a $2.2 billion software piracy lawsuit against the country and several computer manufacturers.[6]
- In July 2011, Wiley Rein faced cyberattacks from a Chinese hacking group specifically targeting six international trade lawyers who worked on several high profile anti-dumping and unfair trade cases against China.[7]
- In January 2015, attackers encrypted Ziprick & Cramer client data on an internal server and held it for ransom.[8]

- In March 2016, Cravath Swaine & Moore and Weil Gotshal & Manges were hacked in what was suspected to be a ploy to gain information to be used for insider trading.[9]
- Finally, in the biggest law firm hack to date, Panamanian law firm Mossack Fonesca was hacked, resulting in a data breach of 11.5 million documents and an exposure of a global network of shell companies used in tax evasion schemes.[10]

The changing tide of law firm attacks is resulting in more targeted attacks aimed at specific information that the firm holds through their representation of various clients. Law firms have incomparable access to highly sensitive information. This information includes intellectual property, market-influencing merger and acquisition information, proprietary data, court and case strategies, employee information, trademarks, pending patents, and other sensitive client information that individuals and corporations entrust to firms. With cyberattacks unlikely to slow down any time soon, attorneys need to understand their responsibilities and assess their risk matrix to effectively defend themselves — and their clients — from hackers.

> "By 2012, the cybersecurity firm Mandiant estimated that 80% of the top 100 U.S.-based law firms had been hacked in the previous year."

III. Attorney Responsibilities – Ethical, Statutory, and Legal

While the self-regulated legal industry does not require firms to implement specific cybersecurity safety measures, attorneys have a duty to safeguard their client's information. As cybersecurity threats become more and more common, industry standards are going to require higher safeguards, and firms that refuse to implement procedures to protect their systems will face greater liability.

A. Ethical Duties

Attorneys and law firms have various ethical duties under the ABA model rules of professional conduct. In addition, state bar associations implement additional ethical requirements, most of which are largely based on the ABA's guidelines. Failure to comply with the ethical duties imposed by the model rules can result in disciplinary action of the attorney and the firm. There are three duties imposed by the model rules that bear directly on cybersecurity:

- duty of confidentiality,
- duty of competence,
- and duty to supervise.

Duty of Confidentiality

Model Rule 1.6(c) requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[11] The rule protects one of the fundamental principles in a client-lawyer relationship, in that a lawyer must not reveal information relating to the representation of the client without the client's informed consent.[12]

Rule 1.6 does not prescribe exact security safeguards that have to be implemented, and instead suggests factors that should be considered in determining whether an attorney has made reasonable efforts to prevent information access or disclosure. These factors include, but are not limited to: the sensitivity of information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent the client.[13] In addition, a reasonableness inquiry is determined by industry standards and a lawyer or firm's compliance compared to those standards. For example, it is now standard for firms to encrypt emails that contain highly confidential or personally identifiable information. If a firm does not encrypt an email and sends personally identifiable information to the wrong recipient or it is intercepted by a hacker, it is likely that a disciplinary body would find the attorney's actions unreasonable.

> "Law firms have incomparable access to highly sensitive information."

Duty of Competence

Lawyers and firms owe a duty of competence to their clients, which includes "keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[14] Lawyers are not required to be experts in all technology, but to fulfill their duty of competence, they are required to understand that cyberattacks are a real and pertinent risk to their clients and firms and to implement safeguards to protect the confidential information entrusted to them.

The American Bar Association notes in their Cybersecurity Handbook, "…if a lawyer is not competent to decide whether use of a particular technology (e.g. cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer."[15]

This duty requires that attorneys do not stick their heads in the sand when it comes to cybersecurity but rather educate themselves on the risks and tools they need to safeguard their client's information.

Duty to Supervise

Lawyers have a duty to supervise junior attorneys, support staff, and third parties with access to confidential client information and ensure that "all lawyers in the firm conform to the Rules of Professional Conduct."[16] While external hacks and attacks pose a risk to firms, internal negligence, lack of training, and at times purposeful sabotage pose an equally detrimental risk. It is the responsibility of the firm to ensure that junior attorneys and staff are trained in cyber risk and that there are policies and procedures in place to appropriately handle any breach.

"While external hacks and attacks pose a risk to firms, internal negligence, lack of training, and at times purposeful sabotage pose an equally detrimental risk."

In addition, attorneys and firms must supervise third party service providers and continually reassess the protections and security that technology services provide in safeguarding client data. For example, during the National Symposium on Technology in Labor and Employment Law, Drew Simshaw and Stephen Wu examined whether the use of cloud computing services to store, share, use, and communicate client information is acceptable under the ethics rules.[17] Citing ethics opinions, Simshaw and Wu found that "cloud computing is permissible, as long as lawyers take proper steps when selecting and using services…and provide reasonable supervision of cloud vendors."[18] Attorneys may not delegate supervision to someone else and are ethically required to supervise those in the firm as well as anyone providing services to the firm who has access to client information.

B. Statutory Duties

While there are no ethical rules or legal precedent requiring specific cyber security safeguards, certain legal practice areas impose a statutory duty on firms to implement cybersecurity programs. Statutory duties placed on law firms under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and by FINRA and the SEC for the financial sector are briefly described below.

HIPAA

Attorneys handling HIPAA-related cases, such as elder law, healthcare law, insurance, medical malpractice and personal injury and who handle any work that involves protected health information (PHI) are considered Business Associates[19] and are required to comply with HIPAA's Privacy Rule and

Security Rule.[20] However, a 2016 poll conducted by Legal Workspace found that only "13% of the 240 law firms had key technology and processes in place to support HIPAA compliance and provide secure environments."[21]

HIPAA Business Associates must comply with the applicable privacy and security standards, including:

1. Entering into a Business Associate Agreement (BAA) and supervising any subcontractors who view PHI
2. Complying with the Privacy Rule[22]
    a. While Business Associates are not directly governed by the Privacy Rule, they may not use or disclose PHI in a manner contrary to the limits placed on covered entities. Thus, most Business Associates will need to implement the same policies and safeguards that the Privacy Rule mandates for covered entities, including rules governing use and disclosure of PHI and individual rights.
3. Performing a Security Rule[23] risk analysis
    a. Business Associates are required to conduct, document, periodically review and update a risk analysis of their computer and other information systems.
4. Implementing Security Rule safeguards
    a. Business Associates are required to implement specific administrative, technical, and physical safeguards required by the Security Rule, including (but not limited to):
        i. Implementing formal sanctions against employees who fail to comply with security policies and procedures;
        ii. Implementing procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking;
        iii. Implementing physical safeguards for all workstations that access PHI to restrict access to authorized users;
        iv. Assigning unique names and/or number for identifying and tracking user identity.[24]
5. Training employees and subcontractors on HIPAA rules and regulations.[25]
6. Responding immediately to violations or breach.
7. Reporting security incidents and breaches
8. Maintaining required documentation
    a. Documentation and records under the Security Rule must be maintained for six years from the document's last effective date.

The above list represents a high-level overview of the cyber security safeguards that are required of law firms who are regulated under HIPAA. However, as the Legal Workspace poll concluded, most law firms lack many of the key technologies and processes to support HIPAA compliance. While a majority of polled firms stated that they had "fundamental security processes in place with vendors to support HIPAA compliance," less than half said that they maintain and review logs of personnel who access PHI.[26] In addition, only 46 percent maintain and review logs of PHI on remote devices to ensure the devices are properly erased or destroyed when no longer needed.[27]

> "Attorneys handling HIPAA-related cases, such as elder law, healthcare law, insurance, medical malpractice and personal injury and who handle any work that involves protected health information (PHI) are considered Business Associates and are required to comply with HIPAA's Privacy Rule and Security Rule."

Financial Services

Financial Service providers' cybersecurity systems are regulated through FINRA, the SEC, and state regulators. Both FINRA and the SEC named cybersecurity as the top enforcement priority of 2017, and FINRA specifically noted that it would increase its review of financial service firms' compliance with their supervisory requirements.[28] The increase in regulation of financial service firms' cybersecurity procedures will have a direct impact on law firms as financial service clients are already beginning to demand that law firms provide them with assurance of security requirements and cybersecurity policies and procedures.

In addition, in January 2017, the first state-mandated cybersecurity law went into effect in New York. The New York Department of Financial Services ("DFS") passed a cybersecurity law outlining specific actions that New York DFS regulated companies are required to implement, as well as regulations over third party service providers to New York DFS companies.[29] The regulation became effective on March 1, 2017, and affected firms have 180 days to comply with the new regulations, which require (among other things):

1. Appointing a Chief Information Security Officer;
2. Training employees in cybersecurity;
3. Annual evaluations from a senior officer;
4. Data encryption;

5. Adopting incident response plans;
6. Adopting an approved, written cybersecurity policy and supporting policies and procedures

While many of these requirements align with FINRA and SEC requirements, the New York rule defines specific actions that regulated firms have to take before September 1, 2017. Furthermore, the rule requires that regulated firms implement rigorous third-party cybersecurity risk management policies and procedures, and require minimum cybersecurity practices from third parties in order for them to do business with the firm.

The NY DFS rule is impactful because of its express requirements to supervise and require minimum cybersecurity protocols from third party service providers. In addition, New York is the financial capital of the world and the leader of state-mandated financial regulation. It's likely that other states will begin to follow New York's lead, and law firms will have to ensure their cybersecurity programs meet the more stringent requirements.

> "Law firms are facing increased liability, loss of revenue, and reputational risk from relaxed cybersecurity policies and procedures."

C. Legal and Business Risk

Law firms are facing increased liability, loss of revenue, and reputational risk from relaxed cybersecurity policies and procedures. Recently, a class action case was brought in the Northern District of Illinois claiming breach of contract, negligence and breach of fiduciary duty.[30] The plaintiffs in the case claim that Johnson Bell, a Chicago-based law firm and one of the 500 largest firms in the country, "left its clients' confidential information unsecured and unprotected," exposing the plaintiffs to "a heightened risk of…injuries."[31] The complaint is allegedly part of a "larger effort by the plaintiff's attorneys to investigate, identify, and sue major law firms with inadequate cybersecurity."[32]

Relaxed cybersecurity protocols, policies, testing, and procedures can put a law firm at risk of an attack as well as affect potential new clients. According to the 2016 ABA *Legal Technology Survey Report*, 30.7 percent of all law firms and 62.8 percent of firms with 500 or more lawyers reported that current or potential clients provide them with security requirements.[33] Firms with outdated or inadequate cybersecurity systems in place risk losing new clients to those who have implemented more stringent procedures.

In addition, if an attack at a firm does occur, the firm faces reputational risks and a possible malpractice suit. A robust cybersecurity program can help prevent security breaches and put a firm in the best position for stopping a breach early and taking next steps to mitigate damage to the firm.

IV. Next Steps

The legal profession is notorious for being slow to adapt to technological advances, but business demands combined with growing risk is pushing the industry to adopt comprehensive cybersecurity programs. In order to implement a successful program that will please clients, regulators, and bar associations, firms must show that "(1) their security program is aligned with best practices, (2) their management is engaged, (3) they are complying with policies and procedures, and (4) they have tools deployed to detect malware and criminal behavior."[34]

The first step in establishing a firm's cybersecurity program is to build a cross-organizational team consisting of practice chairs, finance, human relations, communications, IT, and security personnel committed to understanding the cybersecurity landscape, educating employees, and implementing a comprehensive program. Once this team is established, they should meet quarterly to assess changes in technology, resources and policies within the firm.

Once a team is established, a security assessment of current policies, procedures, software, data, and systems should be done to determine gaps and deficiencies in the firm's security program and to help identify specific risks. The assessment will also help determine what information will be most valuable to hackers and drive implementation priorities. A full assessment of current systems will help lay out next steps for an organization to ensure a successful cybersecurity plan.

Following the assessment, firms should establish policies and procedures that accurately reflect the cybersecurity measures utilized. These should include policies around encrypting PHI and emails containing highly confidential information, physical safeguards around servers, electronic communications and internet use, document retention, and password security.

Regulatory Cybersecurity Requirements for New York Firms:

1. Appointing a Chief Information Security Officer
2. Training employees in cybersecurity
3. Annual evaluations from a senior officer
4. Data encryption
5. Adopting incident response plans
6. Adopting an approved, written cybersecurity policy and supporting policies and procedures

Finally, cybersecurity training should be implemented to ensure that employees understand the policies as well as the value of keeping client and firm information secure.

While establishing a comprehensive cyber security program will help mitigate risk, not all attacks can be prevented. That is

why one of the most paramount pieces of a cybersecurity program is a well-rehearsed Incident Response Plan. The plan should include the cybersecurity team and specify who is to be notified (regulators/clients/local authorities), within what time frame, what documents should be retained and who has the authority to make certain decisions about the investigation. By establishing an Incident Response Plan and rehearsing possible breaches, firms can be ready to act quickly and efficiently during an emergency.

V. CONCLUSION

Attorneys and law firms are more susceptible than ever to cyberattacks. As stewards of personal confidential information, proprietary information, and business secrets, law firms are ideal targets for those looking for highly profitable data. Lawyers have an ethical duty to protect their clients' information, and more clients are demanding that firms have sufficient cybersecurity programs in place to ensure compliance with regulations and protect important proprietary information.

DOS
Development • Operations • Security

For more information, visit https://dos.sh, or e-mail us at info@dos.sh.

DISCLAIMER: DOS provides this information to our clients, friends and peers as for educational purposes only. It should not be construed or relied upon as legal advice.

REFERENCES

[1] *Cyber Security Market by Solutions (IAM, Encryption, DLP, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery), Services, Security Type, Deployment Mode, Organization Size, Vertical & Region – Global Forecast to 2021*, MARKETS AND MARKETS (July 2016), http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html.

[2] Lolita C. Baldor, *FBI: Hackers targeting law and PR firms*, NBC NEWS (Nov 11, 2009), http://www.nbcnews.com/id/33991440/ns/technology_and_science-security/t/fbi-hackers-targeting-law-pr-firms/#.WWTKwIgrJPY.

[3] Big Law Business, *Wake Up Call: 80 of 100 Big Law Firms Have Been Hacked Since 2011*, BLOOMBERG BNA (Aug. 17, 2015), https://bol.bna.com/wake-up-call-80-of-100-big-law-firms-have-been-hacked-since-2011/.

[4] Baldor, *supra* note 4.

[5] Bloomberg News, *Hackers strike at major companies*, NJ.COM (Mar. 10, 2011), http://www.nj.com/business/index.ssf/2011/03/hackers_strike_at_major_compan.html.

[6] *A brief history of law firm cyberattacks*, LAW360 (JUNE 2, 2016), https://www.law360.com/articles/800579/a-brief-history-of-law-firm-cyberattacks.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] Model Rules of Prof'l Conduct R. 1.6(c).

[12] *See id.* cmt. 2.

[13] *See id.* cmt. 18.

[14] Model Rules of Prof'l Conduct R. 1.1 cmt. 8.

[15] Jill D. Rhodes & Vincent I Polley, The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals 66 (2013).

[16] Model Rules of Prof'l Conduct, R. 5.1 and 5.3.

[17] Drew Simshaw and Stephen Wu, *Ethics and Cybersecurity: Obligations to Protect Client Data* (March 15-17, 2015), available at https://www.americanbar.org/content/dam/aba/events/labor_law/2015/march/tech/wu_cybersecurity.authcheckdam.pdf.

[18] *Id.*

[19] 45 C.F.R. § 160.103 (Defining a Business Associate as a person who "(ii) provides, other than in the capacity of a member of the workforce of such covered entity, legal…services to or for such covered entity.")

[20] HIPAA Privacy Rule, 45 C.F.R §§ 160 and 164 (2002); HIPAA Security Rule, 45 C.F.R §§ 160 and 164 (2003).

[21] *Legal Workspace Poll Shows Law Firms Lacking in Cybersecurity and HIPAA Compliance Standards*, LEGAL IT PROFESSIONALS (Feb. 1, 2016), https://www.legalitprofessionals.com/usa-news/8320-legal-

workspace-poll-shows-law-firms-lacking-in-cybersecurity-and-hipaa-compliance-standards (hereinafter "Legal Workplace Poll").

[22] Kim Stanger, *Complying with HIPAA: A Checklist for Business Associates*, HOLLAND & HART (Oct. 26, 2015), https://www.hollandhart.com/checklist-for-business-associates.

[23] 45 C.F.R. §164.314(a)(2).

[24] *Id.*; *See also* 45 C.F.R. §§ 164.306(a), 164.308(a), 164.310, and 164.312.

[25] *Id.*; *See also* 45 C.F.R. § 164.308(a)(5).

[26] Legal Workplace Poll, *supra* 21.

[27] *Id.*

[28] *2017 Regulatory and Examination Priorities Letter*, FINRA (Jan. 4, 2017), http://www.finra.org/industry/2017-regulatory-and-examination-priorities-letter.

[29] *Cybersecurity requirements for financial service companies*, ERNST & YOUNG (Feb. 2017), *available at* http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-requirements-for-financial-services-companies/$FILE/EY-cybersecurity-requirements-for-financial-services-companies.pdf.

[30] Jason Shore and Coinabul, LLC v. Johnson & Bell, Ltd, Case No. 16-cv-4363, December 8, 2016.

[31] *Id.*

[32] Joseph Beckman, *Law Firm Cybersecurity Breach Opens Door to Lawsuit*, AMERICAN BAR ASSOCIATION (March 30, 2017), https://www.americanbar.org/publications/litigation-news/featured-articles/2017/law-firm-cybersecurity-breach-opens-door-to-lawsuit.html.

[33] Julie Sobowale, *Law Firms Must Manage Cybersecurity Risks*, ABA JOURNAL (Mar. 1, 2017), http://www.abajournal.com/magazine/article/managing_cybersecurity_risk.

[34] Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, LAW PRACTICE MAGAZINE (July 2013), *available at* https://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-law-firms.html