NEWMEYER & DILLION LLP

THE "DARK OVERLORD" STRIKES THE PRACTICE OF LAW: WHAT LAW FIRMS CAN DO TO PROTECT THEMSELVES

By: Ivo G. Daniele

March 27, 2019

Ivo G. Daniele

Contact
925.988.3222
ivo.daniele@ndlf.com

Practice Areas
Privacy & Data Security
Business Litigation
Construction Litigation

Cybersecurity breaches involving law firms are on the rise with each passing year. Law firms are prime targets for cyber criminals seeking confidential and sensitive information because of the various types of legal work that law firms normally handle for their clients. Whether it be mergers and acquisitions, the use of intellectual property, purchase agreements, bankruptcy or even litigation involving divorce, law firms are a rich depository for highly confidential and sensitive information. As a result, law firms must employ comprehensive security measures to protect themselves from security breaches or risk being on the losing end of a costly malpractice claim, and suffer severe reputational harm.

Law Firms Continue To Be Targeted By Cybercriminals

According to the American Bar Association ("ABA") *2018 Legal Technology Survey Report*, 23% of the law firms who participated in the survey reported that their law firm experienced a data breach. Although this may be just a 1% increase from the 22% who reported a breach in 2017, it is important to understand that this is an increase of 8% from the stable percentages reported from 2013 through 2016.[1] The 2018 survey report also revealed that security breaches fluctuated with firm size – 14% for solo law firms, 24% for firms employing 2-9 attorneys, approximately 24% for firms with 10-49 attorneys, 42% for firms with 50-99 attorneys, and approximately 31% for those firms employing 100 or more attorneys.

Latest Law Firm Security Breaches

The notorious criminal group called "The Dark Overlord" has a history of committing data breaches of high profile companies such as Gorilla Glue, Netflix, Larson Studios, multiple healthcare companies, and Little Red Door Cancer Agency. Their goal is simple – steal sensitive information and then extort payment from the victims by threatening to release the sensitive information to the public.

On December 31, 2018, this cybercriminal group announced to the world that they had acquired 18,000 documents containing highly sensitive legal information related to insurance based litigation connected to the 9/11 tragedy. The stolen information was the attorney/client property of Lloyd's of London, Silverstein Properties, and Hiscox Syndicates, Ltd. In its announcement, The Dark Overlord boasted that they were in possession of client sensitive information, such as: "*emails; retainer agreements; non-disclosure agreements; settlements, litigation strategies; liability analysis; defense formation; collection of expert witness testimonies; communication with government officials in countries all over the world; voice mails; dealings with the FBI, USDOJ, DOD, confidential communications, and so much more.*"

---

[1] Past ABA Legal Technology Surveys reported 14% in 2016, 15% in 2015, 14% in 2014 and 15% in 2013.

Subsequent to the data breach, The Dark Overlord announced to the public that they designed a compensation plan that would allow for public crowd-funding for its organization to permit the public to view the stolen information in exchange for bitcoin payment. The more public funding it receives, the more stolen sensitive information will be unlocked and released to the public. It is estimated that this cybercriminal group already distributed information to the public on two separate occasions during the month of January 2019.

High profile cybersecurity breaches of law firms is nothing new – for example, the infamous *Panama Papers breach*, where cybercriminals leaked 11.5 million documents exposing the shadowy business of setting up offshore corporations as tax shelters for businesses, celebrities, and politicians - and the infamous *Petya Malware* attack which resulted in a digital lockdown of one of the world's largest law firms, DLA Piper. However, despite the infrequency of publicized cyber-attacks of law firms by the media, the FBI has recently announced that law firms should expect an increase in security attacks by cybercriminals because law firms are now viewed as "one-stop shops" for cybercriminals. Therefore, in order to combat the inevitable increase in cyber-attacks, law firms must get prepared.

How Law Firms Can Protect Themselves

All law firms will agree that the most serious consequence of a security breach for their firm would be the unauthorized access to sensitive client data. The American Bar Association's Model Rules of Professional Conduct, specifically Rules 1.1 and 1.6[2] and related Comments, require an attorney to take competent and reasonable measures to safeguard information relating to their clients. This duty to "safeguard' information imposes a significant challenge to firms when using technology in connection with protecting client information because most law firms are not savvy with technology and lack proper cyber security training.

In order for a law firm to protect itself from security breaches and inadvertently violate its duty of safeguarding a client's sensitive information, it is important to take the following actions:

- Start by taking an inventory and risk assessment of the firm to determine what needs to be protected – the inventory should include both technology and data;
- Develop, implement and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations;
- Ensure the cybersecurity program addresses people, policies and procedures, and technology. The cybersecurity program must designate an individual or a group to be in charge and coordinate security;
- Develop an incident response plan scaled to the size of the firm;
- Continually train staff and attorneys to identify and understand potential cybersecurity threats;
- Consider implementing a third-party assessment of firm's cybersecurity program and policies;
- Purchase cyber liability for insurance which not only covers first party losses to law firms (like lost productivity, data
- restoration, and legal expenses) but also liability protection to third parties;
- Implement authentication and access controls for network, computers and mobile devices used by the firm's staff and attorneys;
- Consider the use of full-drive encryption for computers and mobile devices;
- Have staff and attorneys avoid and/or limit the use of public WiFi when working remotely; and
- Create a disaster recovery plan to backup all data in the event of a cyber-attack or natural catastrophe.

[2]On November 1, 2018, California adopted ethics rules patterned after the ABA Model Rules of Professional Conduct.

Continually reviewing, implementing, training and updating a firm's cybersecurity program and protocols will help safeguard sensitive and confidential client information and/or data. No law firm wants to be the next data breach headline – so take the necessary steps to avoid a potential disaster.

Ivo Daniele is a seasoned associate in Newmeyer & Dillion's Walnut Creek office. His practice includes representing private and public companies with both their transactional and litigation needs. You can reach Ivo at ivo.daniele@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For almost 35 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business law, privacy & data security, employment, real estate, construction, insurance law and trial work, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by *The Best Lawyers in America©*, and *Super Lawyers* as top tier and some of the best lawyers in California, and have been given *Martindale-Hubbell Peer Review's AV Preeminent®* highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.