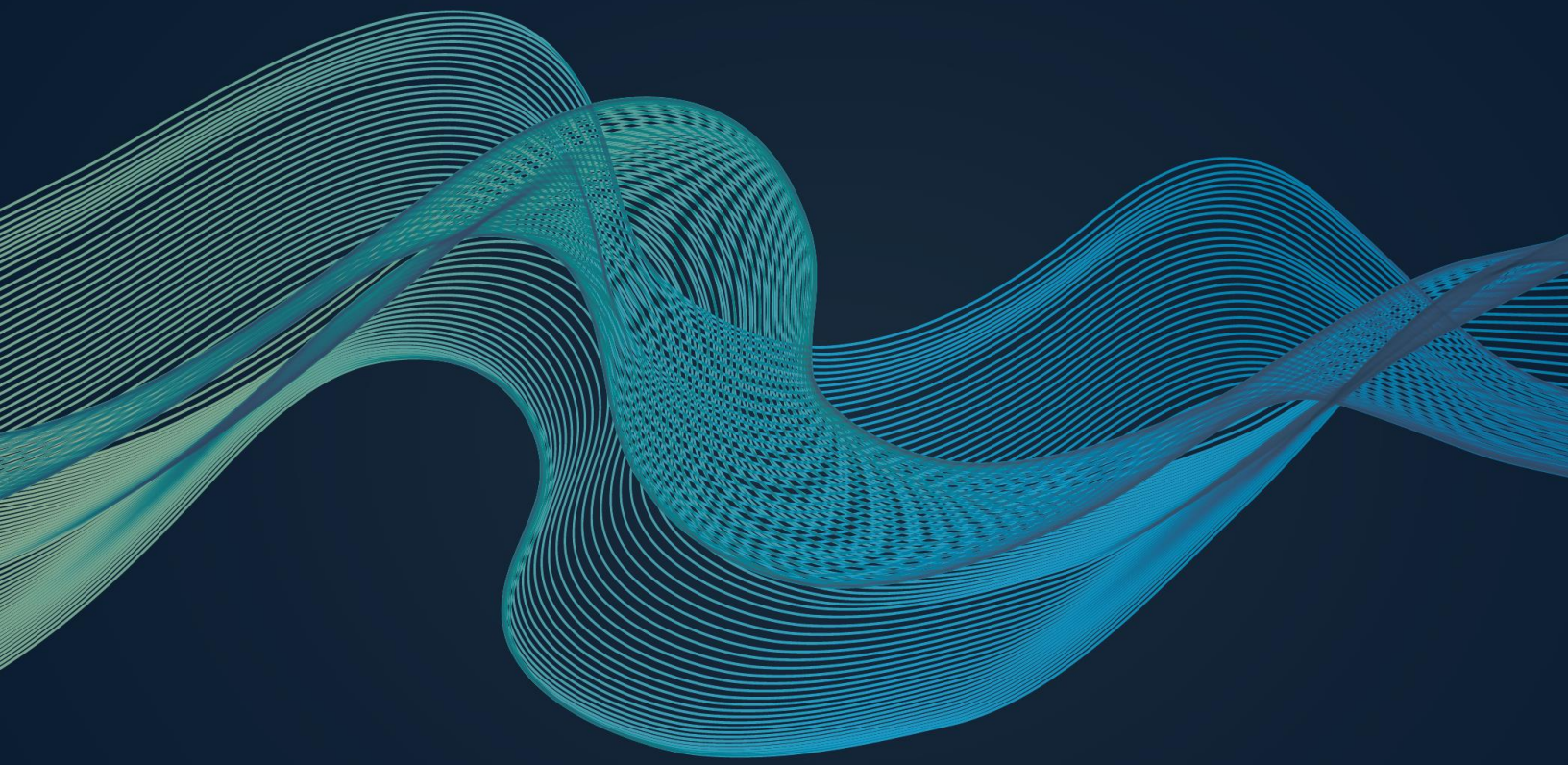
Flipping the Script:

Law Firms Hunted by Cybercriminals



SURFWATCH
CYBER IN SIGHT

Introduction

As businesses put more resources into defending against cyber threats, cybercriminals have shifted tactics to focus on easier-to-exploit organizations in the supply chain – including law firms. In fact, one FBI agent recently stated that nearly all of the top law firms have faced some sort of data breach. This risk is heightened for firms involved in mergers and acquisitions, intellectual property and other types of information targeted by nation-states and cybercriminals.

The American Bar Association (ABA) agrees that law firms are prime targets, writing that lawyers are both "attractive" and "soft" cyber targets:

- ***Attractive targets*** - Law firms handle a variety of high-value information including intellectual property such as patents and trade secrets, insider information on corporate deals and mergers, details on accounts and executives, sensitive information regarding lawsuits, and personal information and other corporate data.

- ***Soft targets*** - While corporate clients may have sophisticated security in place to manage cyber risk, law firms' defenses are often weaker; with less resources dedicated to cybersecurity and lacking awareness of the latest cybercrime trends.

These warnings to law firms are not new:

- 2009 – The FBI warned of "noticeable increases" in efforts to hack into the computer systems of law firms and public relations companies.
- 2011 – 80 percent of top law firms reported a breach, and the FBI began meeting with firms in major U.S. cities in an attempt to shine a light on cyber problems.
- 2012 – The ABA created a Cybersecurity Legal Task Force to raise awareness of cyber issues and provide a platform for involvement across the legal and technical communities.
- 2014 – The ABA survey found "that [law firms] are not employing basic security measures used frequently in other businesses and professions."

Cybercriminals have developed an infrastructure around various ways to exploit and monetize stolen data – from more basic personal data and correspondence to highly sensitive, highly valuable information like financial information, intellectual property, and corporate deals. Not only is there a legal and ethical obligation to keep up with the cyber threat landscape and protect client data, but it is now quite often a client-driven demand. Firms with stronger cybersecurity practices are better positioned while those that lag behind may find their clients seeking out counsel that can provide more assurance.

Gaining situational awareness of the threat landscape is a simple way to put clients at ease and better protect the information being targeted. Cyber risk insights can also be attained immediately without the need for expensive tools or a search for hard-to-find cyber talent.

It is crucial that both law firms and in-house legal counsel understand the types of data being targeted by cybercriminals, the legal and ethical responsibility around protecting that data, and the cyber risk they face. This paper examines those areas as well as some basic security steps that can be employed in order to gain awareness and better protect client data with limited resources available.

Cyber Threat Trends Facing Law Firms

In 2015 Harvey Rishikof, co-chair of the American Bar Association's Cybersecurity Legal Task Force, described law firms as a "treasure trove" of attractive information, saying the information from clients on deal negotiations provides a keen interest for criminals, foreign governments, adversaries and intelligence entities.

A recent Citigroup internal report warned bank employees that digital security at many law firms remains subpar and that those firms were "high risk" and would "continue to be targeted by malicious actors looking to steal information on highly sensitive matters such as mergers and acquisitions and patent applications."

Data from SurfWatch Labs confirms that law firms are being targeted, particularly when it comes to personal information and sensitive data such as corporate documents, trade secrets, and correspondence that can be sold, traded, or used to gain a business advantage.

Date	Score	Polarity	Industry Targets	Actors	Targets	Effects	Practices
2015-08-15	47		Murphy Pearson Bradley & Feeney	unidentified hacker	laptop computer	leaked personally identifiable information 1494 patient records exposed	Unauthorized Access/Disclosure
2015-07-29	**74**		Permanent Court of Arbitration (PCA)	unidentified Chinese hacker	Peace Palace Permanent Court of Arbitration website	compromised website stolen sensitive data	Advanced Persistent Threat strategic web compromise (SWC) Adobe Flash Player vulnerability CVE-2015-5119
2015-07-26	56		Atkinson, Andelson, Loya, Ruud & Romo	unknown	individual data	stolen mailing addresses stolen financial information data breach stolen names stolen phone numbers stolen social security numbers stolen medical records	

Source: SurfWatch Labs' C-Suite application makes cybercrime easy to understand across all stakeholders with a variety of easy-to-comprehend dashboards related to cyber risk, cyber-attacks, and other trends.

Some of the top cyber threats targeting law firms include:

- **Spear phishing emails**, which are malicious messages tailored to individuals in order to appear legitimate, are often used to infect a specific target such as when attorneys with high-profile clients in the oil and gas industry were targeted with an Adobe PDF attachment masquerading as an analyst report – each of the lawyers that clicked on the message were then infected with malware. Spear phishing emails were also used to steal, among other information, privileged attorney-client communications related to SolarWorld's trade litigation with China, according to the Justice Department's indictment of five members of the Chinese military in May 2014.

- **Ransomware**, which encrypts a victim's files and then attempts to sell the victim the key to unlock their own data, has affected various law firms. A small office in North Carolina had every single file encrypted after a lawyer clicked what was believed to be a voice mail attachment sent via email, and a California-based law firm had ransomware infect one workstation before traveling to the in-house server and encrypting all the data on shared folders. In many cases victims either pay the extortion or lose access to the files if they are not backed up.

- **Hacktivist** groups like Anonymous target law firms involved in controversial cases such as when Puckett & Faraj, which represented a staff sergeant that was accused of leading a group of Marines responsible for the deaths of 24 unarmed Iraqi civilians, had its email accounts hacked and more than two gigabytes of correspondence stolen and leaked. They later admitted to using weak passwords on the firm's gmail accounts.

- **Employee information** is also often targeted as McKenna Long & Aldridge discovered when they announced in 2014 that current and former employees had their personal information accessed by an unauthorized party including tax information, Social Security numbers, and passport information.

Law Firms Face a Legal & Ethical Obligation to Ensure Cybersecurity

In August 2014, the ABA adopted a resolution encouraging the following:

> *"… all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected."*

As they noted at the time, the resolution includes law firms.

Data kept by lawyers and law firms is often protected by attorney-client privilege or the work product doctrine; therefore, there is an obligation to protect that information, as the ABA Model Rules of Professional Conduct highlights (emphasis added):

- *Rule 1.1, Comment 8* - To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

- *Rule 1.6* - A lawyer shall make **reasonable efforts** to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

There is an ethical obligation related to competent representation that legal counsel stay current on the risks posed by technology and take reasonable action in order to protect against those risks. Additionally, recent data breaches have spurred some clients to demand counsel pay increased attention to issues regarding the cybersecurity of their data. However, "reasonable", especially when it involves complex technological issues around potential risk, is not always clear-cut (see the comments on Rule 1.6).

Having a high-level awareness of cyber risks related to a firm's IT infrastructure, supply chain, and clients – as well as what cybercrime issues other law firms are facing – is an easy and efficient way to gain more

understanding any potential cyber issues and what "reasonable efforts" can be enacted in order to lower cyber risk.

It is also important to highlight the often-heard misconception, particularly among smaller offices, that cybercriminals would not bother targeting this firm or that counsel. Cybercrime has largely evolved into an organized and profit-driven business that thrives on casting a wide net and exploiting the weakest members of the supply chain in order to obtain valuable information. As various agencies have noted, legal offices fit this model as they are both attractive targets and have "softer" defenses than many organizations.

Cyber Risk Intelligence – First Step to Understanding Your Threat Landscape

With increased client and ethical expectations regarding data security, it is essential that law firms have at least a general understanding of the threat landscape. Cyber risk intelligence provides a key aspect that is often missing when it comes to an organization's cybersecurity: situational awareness.

This means examining the outward, high-level view of cybercrime that is impacting the sector and similar businesses and then applying that knowledge inward to the specifics of an organization to gain a clear picture of important risk areas.

- ***Outward cybercrime landscape*** - Everything that is impacting similar organizations including all of the cyber-attacks, data breaches, advisories, vulnerabilities, legal actions, and security research as well as the actors, targets, effects, and practices behind each of those.

- ***Internal organizational landscape*** - Everything related to an organization's technology including IT infrastructure (e.g. software, devices, methods of communication), vendors and others in the supply chain including banks and health insurers, and other potential avenues of compromise including human resources and social media.

This situational awareness helps provide visibility into the most relevant risk areas facing an organization so that better, more cost-effective decisions can be made that address the most important threats.

Understanding and Addressing Cyber Risk

As SurfWatch Labs' noted in the 2015 Mid-Year Cyber Risk Report, supply chain cybercrime continues to pose a risk for many organizations. With connections into many organizations, law firms must:

- Continuously monitor the types of information being exchanged
- Understand any potential risks should that data be compromised
- Take appropriate action to address critical cyber risks

Unfortunately, it appears that many law firms are unaware of potential risks and do not have policies in place to address those cyber concerns.

According to a 2014 ABA survey:

- While improved from 2013, nearly a third of respondents said they either do not have or do not know if their firm has technology-related policies in place (e.g. records management, email and computer use); this was more prevalent at smaller firms

- Overall, 25 percent did not know if their firm had experienced a data breach; however, over half of respondents at larger firms (50+) did not know, and firms of more than 500 reported 67 percent uncertainty

- 45 percent reported malware infections and an additional 28 percent did not know if their firm had been infected

Lawyers do not need to be cybersecurity experts, but they should be informed enough to know if they are meeting their ethical obligation of "reasonable efforts" to protect client data.

SURFWATCH CYBER IN SIGHT

Some examples of the types of questions that law firms can answer through effective use of cyber risk intelligence include:

- What type of data is most sought after by cybercriminals?
- Have these malicious actors shifted their tactics lately?
- How are other firms and lawyers being impacted by breaches and other cyber-attacks?
- What vulnerabilities are being actively exploited related to software used by our organization?
- Have there been cyber-incidents at vendors or others in our supply chain?
- What are the top active threats involving employee-owned devices?
- Where can resources be directed to achieve the largest and most "reasonable" results?

3 Additional/Next Steps to Mitigate Cyber Risk

While situational awareness is an important first step to determining potential cyber risk, implementing the basic security measures that the ABA, government agencies, and banks have all have said tend to be lacking among the legal profession can make a significant impact on mitigating that risk. Once an organization understand the threats that are actively targeting law firms, it can take a more preventative cyber defense stance and implement the following measures.

1. Protecting Access to Data

Data is the most sought after commodity when it comes to law firms, and account credentials are often the only "key" needed to access that data. An attacker may get this by tricking the victim with social engineering, getting lucky because so many people use default or easy-to-guess passwords, or trying credentials that were stolen in another data breach in the hopes a person may have re-used a password across multiple sites and applications. That is why it is crucial that accounts are protected with strong passwords and multi-factor authentication:

- ***Strong passwords*** - It is important to have a strong and unique password on each account; otherwise if one account gets compromised, multiple accounts become vulnerable. The easiest way to manage the multitude of complex passwords is to use a password manager.

- ***Multi-factor authentication*** - Another common method of security is to have a second factor of authentication in addition to a password. Many email providers, financial institutions, and others use a text code sent to a cell phone as a second form of authentication.

In addition to secure account credentials, other commonly deployed methods and tools can be used to ensure that clients' data is kept safe.

- ***Encryption*** - There are many ways to encrypt ranging from individual files and emails to entire devices. While this is a common best practice recommended for all organizations that deal with sensitive data, it is not a cure for everything. At some point the files must be decrypted; therefore, an attacker using legitimate credentials could still potentially gain access.

- ***Physical security*** - Preventing stolen devices or stopping intruders from gaining access to a building to socially engineer or otherwise get information they should not be able to access is often overlooked when it comes to cybersecurity.

- ***Device-related issues*** - Features like remote wiping and encryption can help should someone lose a device, and clear policies around appropriate methods of accessing data and keeping devices secure can help ensure employees are not engaging in risky behavior.

2. Protecting Data in the Cloud

In recent years the practice of storing data in the cloud has gained widespread popularity. The Alaska Bar Association Ethics Committee weighed in on this topic, writing the following in 2014:

We concur with the consensus among states' ethics committees that a lawyer may use cloud computing in a manner consistent with his or her ethical duties by taking reasonable steps to protect client data. While a lawyer need not become an expert in data storage, a lawyer must remain aware of how and where data are stored and what the service agreement says. Duties of confidentiality and competence are ongoing and not delegable. A lawyer must therefore take reasonable steps to protect client information when storing data in the cloud. The requirement of competence means that even when storing data in the cloud, a lawyer must take reasonable steps to protect client information and cannot allow the storage and retrieval of data to become nebulous.

"Reasonable" steps must be taken, and the onus is on the lawyer to understand the technology.

3. Importance of Risk Awareness and Training

Perhaps the most important takeaway regarding managing cyber risk is that it is not a "set it and forget it" process. People are often the biggest weakness when it comes to cybersecurity, and training is often a cost-effective way to reduce the risk facing organizations.

It is crucial that law firms have clear technology-related policies in place that define how data will be handled securely, a method of maintaining an ongoing situational awareness of cyber risk, and a training program that informs all those in the organization of the relevant risks. Cyber risk awareness and risk mitigation can become part of the larger business discussion alongside a variety of other key business areas that are also measured, tracked and evaluated.

Conclusion

The warning bells continue to sound from government agencies and legal organizations that lawyers and law firms are increasingly being targeted due to a combination of the valuable corporate data they handle and the fact that they are often an easier point of compromise than the businesses they represent – which are likely to spend more time, money and resources combatting cybercrime.

Facing that increased risk, it is imperative that legal counsel begin to employ at least the basic security protections that many firms are lacking as well as develop an understanding of the cyber risks facing them and the potential pitfalls that may come as a result of a cyber-attack.

A cyber risk intelligence program, which translates the sometimes confusing threat landscape into information and metrics that are easy to understand and act on, can provide an immediate guide to the relevant cyber risks facing law firms. With this information, the limited cyber resources available can be used in a smart and effective way to help combat the increasing risk those firms face from nation states, cybercriminals, and other malicious actors.

About SurfWatch Labs

SurfWatch Labs delivers powerful cyber risk intelligence analytics and applications through a business intelligence approach that helps organizations improve their long-term cyber resilience.

Created in 2013 by former US Government intelligence analysts, SurfWatch Labs solutions go beyond the low-level threat data and security tactics that organizations can drown in, by providing insights into cyber risks and their impact on key business operations. SurfWatch empowers customers to:

- Easily visualize and comprehend how cybercrime affects all aspects of the business
- Continuously monitor personalized cyber risk Key Performance Indicators (KPI's)
- Include cybersecurity as a strategic, foundational component of the business operation

SurfWatch Labs: Cyber In Sight. For more information, visit www.surfwatchlabs.com.

Contact us at:

info@surfwatchlabs.com

(866) 855-5444

Follow us at:

SURFWATCH
CYBER IN SIGHT