Lawyers Guide to I.T. Security

As data breaches become commonplace, responding to cyber-attacks is a must-have in your repertoire when practicing law in the 21st century.

Legal Industry and Cyber-Security: A 21st Century Match

Cyber-crimes and data breaches have become a grave concern for organizations of all sizes, across all industries. Law firms, however, have found themselves to be particularly vulnerable.

Cybersecurity and law firms didn’t always work together; however, recurrent cyber-attacks and the increased risk of data theft over the Internet have paired the two distant entities as virtual necessities.

Law firms are typically viewed upon as traditionalist entities that operate covertly, guarded by a layer of confidentiality. However, that notion has undergone a drastic alteration since the start of the millennia.

According to an industry survey, 80% of the largest law firms in the United States have experienced a data breach in the last few years. Lawyers have experienced a sweeping change in their traditional operations, finding themselves at the center stage of global cybersecurity threats.

From mergers to copyright lawsuits, lawyers serve a very important role in the 21st-century economy. Any threat to law firms directly and indirectly impacts every entity, organization, and person that has ever inevitably hired legal counsel in the past, or plans to do so.

Legal Data Breaches: The Trend Is On the Rise

As hackers begin to realize the goldmine potential of legal industry breaches, law firms are left with little time to barricade their practices against the threat that looms to sabotage the sanctity of their profession.

The past few years have witnessed some of the most appalling and shambolic security measures being exposed as hackers have accessed billions of dollars’ worth of data.

In light of the plausibility of such breaches, back in 2012 the Wall Street Journal reported that as the threats against law firms' pile up, "attorneys who want to protect their client's secrets are having to reboot their skills to the digital age."

Panama Papers Proved To Be A Game Changer

With an ever-growing threat of data breaches and an industry that was yet to consider safeguarding its assets seriously, it was a matter of 'when' rather than 'if' a tragedy would strike. And it did in 2016, when the law firm 'Mossack Fonseca' suffered from a calamitous data breach that made its way through the firm's email server – an event immortalized by the name of "Panama Papers."

It took 11.5 million documents and 2.6 TB worth of data for the legal industry to notice the abysmal state of I.T. security they had provided to their profession. It was followed by a warning issued to approximately 50 law firms for being blacklisted by hackers for a cyber-attack.

While the world was still making amends for Panama Papers, the globally recognized law firm DLA Piper suffered from a data breach in June 2017. Such was the impact that it had to cease global operations for three days.

It still continues to this day, as the American Bar Association's 2018 Survey reports that about 23% of law practices report that their firms had experienced a security breach at some point.

It's Not Just the Big Guns

There's an underlying tone across every cybercrime activity, be it the Panama Papers or the DLA Piper case, indicating that only the bigger firms are susceptible to such incidents.

It is obvious that links to politicians, government agencies and "high-profile" cases make the bigger law firms more susceptible to hacking attempts. However, that doesn't mean smaller firms are safe from hacking – just that they don't fetch reviews and headlines.

One good example is what happened to the 10-attorney firm located in Rhode Island, Moses Afonso Ryan. The firm was infected with Ransomware, and the hackers refused to budge unless paid $25,000 in cryptocurrency.

Even after they had paid the ransom, the hackers refused to budge, leaving the attorneys unable to bill one single hour for three months –resulting in a loss of $700,000 for the firm.

The reason why the firm gained popularity was due to their battle for due insurance payment. The point is, regardless of the size of your practice, the legal industry as a whole is battling to overcome the disastrous effects of cybercrime. Regardless of your business's size, cybercrime remains an imminent threat.

Why Do Law Firms Make An Ideal Target?

Every industry in the world is challenged by the barriers posed by cyber-crime, but none as severe as the legal industry. There are several factors as to why cyber-criminals find law firms so alluring to hack into:

Sensitive Data That Can Be Leveraged For Economic Benefit

As custodians of a wealth of confidential and valuable information, any breaches into legal industry data gives hackers access to a wide range of information on any client the law firm once engaged, or engages with.

The nature of client information that lawyers possess is sensitive, confidential, and can be easily abused. At a macro level, the financial data, corporate strategies, trade secrets, and transactional information stored with lawyers provides hackers with a goldmine of exploitable data.

Cases, such as the one where hackers made their way into the databases of seven law firms, siphoning out data that was further used to accumulate $4 million in stock trading is not a one-off incident.

Industry-Wide Ignorance towards Stricter Controls

Part of why the legal industry faces such a magnitude of hacking attempts is due to the fact that lawyers have been very laid-back when it comes to adapting to the changing global landscape. This shift in the market makes it imperative for data to be stored and communicated under stricter protocols.

Despite the very obvious threat, 22% of the law firms still have no strategy to tackle a possible data breach while only 50% have a cyber-security team.

A vast majority of law practices continue to be undertaken devoid of a proper strategic policy in place keeping a check on the growing risk to their data.

According to a study, every 2 out 3 of law firms lack devoted information security professionals. Additionally, less than a third have access to an official cybersecurity training program, and only 40% have cybersecurity policies in documented form.

In a profession where the client's confidentiality equates to livelihood, such unpreparedness can only be justified as unprofessionalism.

What Are the Cyber Threats Faced by the Legal Industry?

Hackers require access into information-heavy databases, and look to deploy deceiving ways to gain access, which although may come off as negligible but have the potential to gulp down your entire data.

Phishing

One of the most common methods to deceive unknowing law firm employees is by sending them seemingly official links that lead to viruses. Such links are predominantly sent through email, but can also be sent using text messages or social media.

One study reported that 59% of all emails law firms receive can be attributed to phishing or spam. Hackers send a colossal volume of phishing emails to increase the probability of somebody clicking on them.

Ransomware

Ransomware is a type of malware that – once admitted in your database – will prevent the user from accessing files or data of any form. This type of hacking is usually done to extract a payment out of the user.

However, there have been cases where the files are not returned even after the payment of the ransom – leaving law practices with no alternative other than to beef up their security systems and ensure maximum cautiousness.

This type of malware is usually installed in a device using spam email, which constitutes 90% of Ransomware cases. Ransomware is a more advanced form of cyber-attack involving the demand for large sums of cash in return for data, leaving large law firms as the specified target.

Data Breaches

Arguably the most devastating forms of cyber-crime, data thefts aim to illegally retrieve confidential information (owing to which law firms are so lucrative), and use it for multiple unethical and illegal purposes.

The loss of confidentiality due to data breaches tarnished the reputation of a law firm, which is why experts unanimously agree that cybersecurity is a necessity for the legal industry.

The list is by no means exhaustive, and is a summary of the biggest cyber threats faced by the legal industry. There are plenty of variations of threats, such as Friday Afternoon Crime, but the core idea remains the same.

Hackers look to enter the system disguised as clients, superiors, and other stakeholders. The legal industry as a whole needs to implement a stable policy to counter the danger that lurks around corners. Regardless of size, every lawyer hosts a plethora of confidential information that can be leveraged in return of ransom or any other incentive, to illegally and unethically benefit the hacker.

Ethical Bindings on The Lawyers

Beyond the threat posed by data breaches and the loss of billable hours, lawyers are ethically bound to safeguard and preserve confidential attorney-client information. For American lawyers, the ABA's (American Bar Association) Rules of Professional Conduct has overlapping clauses where rules remain applicable to a lawyer's behavior regarding the protection of their client's confidentiality.

Competence

As per the Model Rule #1.1: ***"A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, thoroughness, preparation, and skill necessary for the representation."***

While the case for cybersecurity can be argued for in this rule, it is the comment to the rule which makes it clear.

Comment 8 to the same rule states: ***"To maintain the required knowledge and skill, a lawyer should keep abreast of the changes in 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."***

The crux of this comment instructs lawyers to keep an eye out for any development in their profession which can alter or modify their practice – such as the vitality of cybersecurity.

Confidentiality

According to Model Rule 1.6 (c): ***"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."***

The rule expands further, with comment 18 stating: ***"Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information***

relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

The interpretation of this would be that if a law practice has implemented a strong safety system in addition to acting in a competent manner to safeguard confidential client data from unintentional disclosure, it can be evicted from any violation of ethics guideline charge.

However, in no certain way does the Model Rule state a definitive guide as to whether the attorney is to tell the clients about a breach. Experts unanimously agree that if the lawyer's conduct of the matter has been substandard, giving rise to a potential malpractice claim, it is best that the lawyer discloses the breach to the client.

Staff Supervision

As hackers hone in on how to foil the latest security measures, it is only logical that lawyers learn to update their practice to counter such attempts. One crucial aspect of this is to train the staff employed to be cautious when dealing with the hacker's mode of gaining access such as spam emails.

As security standards are updated every year, it is binding on every lawyer to not only integrate such knowledge in their practice but also ensure that the staff remains trained.

In this regard, ABA's Model Rule #5.3 states: ***"With respect to a nonlawyer employed or retained by or associated with a lawyer: (a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer; (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer.***

What Steps Can The Law Firms Take?

The duty of a lawyer to safeguard the information of the client is sacrosanct, and modern cybercrime trends extend this responsibility to avert any unauthorized access of that data.

Here are some of the steps law firms can take to provide a comprehensive and competent security infrastructure against cybercrime:

Upgrade Your I.T. Infrastructure

After law firms have ascertained the type of information they store and the protocol that matches, it's time to upgrade their I.T structure. Akin to a physical vault, the sturdier and rugged the walls of your I.T. structure, the difficulty it is for any data thief to break in.

Your infrastructure is the key to streamlining your business processes and aiding in providing a competent barrier against unauthorized users. In the modern business landscape, everything from interoffice communication and attorney communication, to client interaction and billing is based on I.T.

The moment your I.T. infrastructure is sabotaged, you can't access information, you can't communicate, and you sure can't bill. With the help of a robust infrastructure that accounts for the threats faced by your industry, not only do you shield your practice from the evil of cyber-attacks, but also do your due diligence to preserve your client's trust.

Opt For Reliable Network Solutions

The advent of modern network providers has facilitated the use of advanced, enterprise-level networking solutions for all sizes of organizations, and law firms shouldn't trail behind.

In a time where technology has become as vital for a small firm as it once was to a bigger one, compromising on the level of service equates to compromising on the level of commitment you're willing to put in.

A stable network that provides smooth access around the clock, alongside a strict watch on the firewalls, and network stability is key in protecting your core system from intruders.

Don't Compromise On Security Protocols

The walls that keep your law firm safe are typed in binary and made in code. As hackers continue to come up with sophisticated ways to attack your database, there is no time for the legal industry to rest.

When drafting up your security protocols, there are no cutting corners. It is more than just an investment into your practice; it is a necessity to preserve the sacredness of the privacy that drives the industry.

From email detection systems that actively pursue any intrusion and detection to protect against viruses and malware – there is a whole industry dedicated to providing you the high-grade security you need.

In order to up the ante against cybercrime, law firms are repeatedly advised to hardwire their firewalls and detail their authorization process through encryption and 2-factor authentication systems. That's not all – a comprehensive and relatively safe security system ensures there is a security incident and event management system in place, along with a documented policy to guide future security upgrades.

Migrate To the Cloud

The beauty of the cloud lies in its increased feasibility that elevates it far beyond a simple remote storage solution. Local servers are fitted with poor controls, devoid of a proper security infrastructure capable of catering to the increasingly sophisticated cybercrime tactics.

The increased collaboration is further complemented by the added security afforded by the cloud. By adding remote access in the mix you're looking at a safe and secure environment that allows you the liberty to store and access data from virtually anywhere.

Business Backup and Disaster Recovery

In this digitalized world, there is no "foolproof" security, just false claims. While it is necessary for the lawyers to act prudently to protect their data, it is equally important to allocate resources for the backing up of data, and have a contingency plan in case a tragedy does befall the practice.

If faced with a hacking attempt, there are clients that need to be catered to, a pathway that needs to be ascertained, and precious data that needs to be retrieved. A comprehensive backup and disaster recovery plan answers all of such queries.

From ensuring there is an on-site and off-site data repository, to ensuring there is minimal downtime with instant local virtualization, and a hybrid cloud backup – a solid backup and disaster recovery plan can prove to be the difference between a successful counter to a hacking attempt, or the irrefutable damage sustained from one.

The Answer Lies In Informed Use of Technology

It's 2019: it’s practically impossible to establish authority in your niche without integrating technology into your practice. However, such integration presents a double-edged sword: while you shift your operations from manual to digital for added feasibility, you’re also opening up your data and making it susceptible to possible breaches.

Herein lies the problem that continues to haunt the legal industry. Should an industry that prides itself on tradition be accepting of the change that technology brings, and open itself up to possible breaches? Or should it continue to shun the progress technology provides and risk lagging behind to more tech-savvy alternatives?

The essential problem with this narrative is that it sheds light at the two extremes, completely neglecting the road down the middle that leads to success. Technology doesn’t have to be chaotic or extreme – it is simply a means to be more effective and efficient.

While many lawyers still struggle to decipher cyber security requirements – overwhelmed by the task; they choose to ignore this as simply not sustainable. Twenty-six now **require** that lawyers stay informed about the changes in the legal industry and clients are increasingly demanding of an effective cyber security infrastructure.

Law practices will take some time to shake off the firmness and stagnancy that has defined their profession, but they must adapt to the radical changes disruptive technology has caused around the globe if they are to protect the confidentiality that forms the core of their profession.

About JMARK

JMARK is proudly leading the technological integration across the legal industry. As an esteemed MSP (managed service provider), JMARK prides itself on its continuous success, formed on the pillars of expertise and a stellar track record.

With years of providing I.T. Solutions to the legal industry come from our deep insight into the problems faced by law firms, regardless of size, as they face the modern threats posed by the rapid increase in cybercrime.

As one of the leading I.T. security providers in the world, JMARK provides law firms with an I.T. plan that has been meticulously cultivated to adapt to their needs. Most importantly, JMARK assists them in keeping the unwavering commitment to their profession and those who lay their trust in them, to safeguard client confidentiality.

A data breach is inevitable as cybercrime becomes more intricate and more targeted by the day; the question begs to be asked: is your law firm protected against a cyber-attack?

If you wish to learn more about the types of breaches that you could be facing based on your current security system, contact JMARK. Call us at 844-44-JMARK or type us an email!