Q1 • 2017

LOGICFORCE

Law Firm Cybersecurity Scorecard

Background

The* Law Firm Cybersecurity Scorecard *is compiled by LOGICFORCE for the purpose of educating the industry on the current state of law firms' IT systems and data management.
The FBI[1] continues to issue warnings that law firm cyber terrorism is on the rise with petabytes of client information being stored on local systems, in the cloud, and with third party vendors at risk. We need to look no further than recent breaches at Cravath Swaine & Moore, Weil Gotshal & Manges[2], and the 11.5 million documents leaked detailing financial and attorney/client information – from the Panamanian firm Mossack Fonseca – to realize the gravity of the situation.

The *Law Firm Cybersecurity Scorecard* will be issued quarterly and is part of our commitment to thoroughly study, understand, and report on the imminent amount and magnitude of threats faced by law firms today as well as the steps they are taking to mitigate the threat.

To that point, per a recent Law 360[3] report, law firm Managing Partners list cybersecurity as their number three priority, behind financial profits and generating revenue. Even though cybersecurity seems to be an area of particular focus, this scorecard will illustrate that law firms continue to struggle with making operational investments and instituting practices that do not provide a quantifiable financial return. Thus, they jeopardize their reputations, client relationships, and in some cases, financial well-being.

It is important to note that we believe law firms are fundamentally consistent with their corporate clients when it comes to countering unwanted intrusions and protecting data. With a major distinction being the ethical rules outlined by the American Bar Association, requiring confidentiality of attorney/client work product and reasonable protection of information.

In highlighting the current landscape, our hope is to provoke meaningful dialogue and action by law firms and their corporate legal clients, to better prepare for cyberattacks that, as you will see, are happening every day.

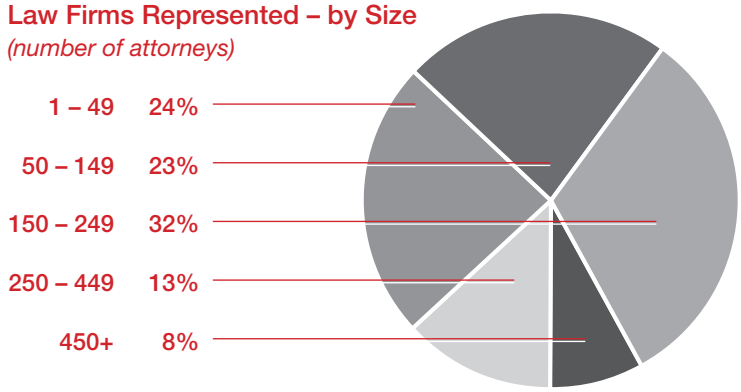
---

(1) Federal Bureau of Investigation, Cyber Division-160304-001 at 2 (2016). Print. "Criminal-Seeking-Hacker" Requests Network Breach for Insider Trading Operation
(2) Hong, Nicole, and Robin Sidel. "Hackers Breach Law Firms, Including Cravath and Weil Gotshal." Hackers Breach Law Firms, Including Cravath and Weil Gotshal. The Wall Street Journal, 29 Mar. 2016. Web.
(3) Hays, Kali. "Data Security Not Top Concern For Firm Leaders, Report Finds - Law360." Law360 - The Newswire for Business Lawyers. N.p., 2 Dec. 2016. Web.

Methodology

The data represented in this study is a compilation of critical data points determined by LOGICFORCE and gathered through internal collection of anonymized LOGICFORCE system monitoring data, responses to client surveys, our proprietary SYNTHESIS E-IT SECURE™ assessments, and published industry information. The data points were specifically selected to accurately reflect both the cybersecurity threats and current efforts by law firms to limit risk of cyber exposure to breach. For this study, LOGICFORCE surveyed and assessed over 200 law firms, ranging in size from 1 to 450+ total attorneys, located throughout the United States, working in a full complement of practice areas.

Law Firms Represented – by Size
(number of attorneys)



Key Findings

Every law firm assessed was unwantedly targeted for confidential client data in 2016-2017 (49% of total study group)

- Approximately 40% did not know they were breached

4.2 billion records were compromised across 4,169 publicly confirmed breaches in 2016.[1]

We see consistent evidence that cyberattacks on law firms are non-discriminatory. Size and revenues don't seem to matter.

- M&A, IP, and General Business Information does seem of primary interest for insider trading purposes according to the FBI[2]

Firms without a dedicated Information Security Executive typically budget cybersecurity expenditures as part of the technology budget

---

LOGICFORCE – Synthesis E-IT Secure™ is a trademarked IT systems and data management assessment tool developed specifically for the legal industry by LOGICFORCE

80%

of firms are not vetting their third-party service provider's data security practices. Nearly 63% of breaches are linked to third-parties.

95%

of assessments done by LOGICFORCE show firms are not compliant with their data governance and cybersecurity policies. 100% of those firms are not compliant with their client's policy standards.

1 firm lost an entire practice group due to a failed audit.

18 law firms said they lost a client for failing an IT audit in 2016.

53%

of firms have NO data breach incident response plan developed.

60%

of firms do not have a specifically appointed Security & Compliance Manager and have no plans to appoint one.

88%

of AMLAW firms have cyber security practices.[3]

34%

of firms reported getting a client data security and systems audit in 2016. Based on industry data and survey responses, LOGICFORCE expects this to reach 50% in 2017 and 65% in 2018.

77%

of firms do not maintain any cyber insurance coverage.

LOGICFORCE

(1) SRB. "2016 Reported Data Breaches Expose Over 4 Billion Records." 2016 Reported Data Breaches Expose Over 4 Billion Records. Risk Based Security, 25 Jan. 2017. Web.
(2) Doc. No. Federal Bureau of Investigation, Cyber Division-160304-001 at 2 (2016). Print. "Criminal-Seeking-Hacker" Requests Network Breach for Insider Trading Operation
(3) Dipshan, Ricci. "Most Firms Feel Assured in Cybersecurity Abilities, But Is That False Confidence?" Law Journal Newsletters, 01 Jan. 2017. Web.

Threats

Network Intrusion Attempts: 10,000/day

There are over 10,000 intrusion attempts per network every day. This number is consistent across our entire sample set. A large percentage of these attempts are likely carried out by automated scripts, which do not discriminate based on firm size, and do not target specific businesses, or people. A sole practitioner's Internet threat is at equal risk to an AMLAW 100 firm the moment they connect their system to the Internet. A firewall is the first line of defense, but without a comprehensive monitoring solution, intrusion attempts will mostly continue to go unnoticed.

Phishing/SPAM Emails: 59%

59% of all email attempting to be delivered are classified as phishing/SPAM emails. The threat level of these emails can range from benign marketing annoyances to ones much more malicious and costly. Some examples of more malicious emails are messages designed to bait the end user to login to a fraudulent system for credential theft, or emails containing some form of ransomware that when clicked will lock all the files in the firm, and, at the extreme end, the so-called "CEO fraud" spear phishing emails that have led to estimated corporate losses of billions of dollars. Like the usage of a firewall, noted above, a continuously learning SPAM filtering solution is a necessary line of defense, but crafty spammers, as well as new and emerging threats, will beat a simple system. Additionally, pressures from firms to ease filtering rules – to eliminate the potential for false positives – continue to increase the opportunity for a well-crafted phishing email to reach a user's inbox.

Invalid Login Attempts: 1,000/day/user

This statistic represents invalid login attempts to services exposed to the Internet through webmail, cloud based DMS, terminal servers, custom web portals, or practice management systems. While the ability to access these services from any device, anywhere, has revolutionized the way firms operate, it has also created an opportunity for a compromised password to cause a tremendous amount of loss and exposure. An easily guessed password, which is unfortunately quite common in the absence of an enforced password policy, is an open door for malicious attackers to easily steal data.

Assessed Financial Risk: $221/record

The average financial risk per compromised record is approximately $221[1]. While this may not seem like much, consider the possible number of records available with sensitive personally identifiable information (PII), including social security numbers, driver's license numbers, credit card information, protected health information (PHI), and more that may be dispersed through the infrastructure on persistent storage, in the cloud, or on personal devices. A data breach would, in almost every scenario, not lead to the loss of one record, but most likely thousands, and possibly millions. In 2016, the average cost per breach was $4 million.

Corporate Client Data Security Audits: 34% of firms surveyed had their cybersecurity practices audited by at least one client in 2016

The most common industries requiring data management and cybersecurity compliance in-line with their own internal standards are retail, healthcare, finance, and utilities. It is important to note that these audits are becoming more frequent and increasingly complex in the amount and types of questions being asked per audit. Average questionnaires range from 50 to 135 questions, with many requiring on-site access.

66% of law firms have reported a breach of some type, with varying levels of compromise.

(1) 2016 Cost of Data Breach Study: Global Analysis. Ponemon Institute© Research Report. Print.

Security Incidents

Our numbers show about 66% of law firms have had a breach of some variety, with varying levels of compromise. While many firms will anonymously provide the fact that they have been breached, few will admit to the scope, cause, or events of the breach.

Mediation

Cybersecurity Policies:
Only 34% of law firms surveyed have document policies and procedures.

Penetration and Vulnerability Testing:
Only 18% of law firms surveyed conduct some type of penetration and vulnerability testing. As a result, 50% report that they have made investments in systems remediations.

Type of Testing:
It is encouraging that 100% of the law firms that did conduct systems penetration and vulnerability testing did so through an independent third-party.

Full Disk Encryption:
Our findings show that only 25% of the law firms analyzed have implemented full disk encryption across their entire organization.

Multifactor Authentication:
We see the implementation of MFA as mission critical but current levels are very low at 21%. This may be the single easiest and most impactful way to help secure firm data without significant investment.

Data Loss Prevention Services:
Data loss prevention, or DLP, is technology that scans documents, emails, and other types of data leaving the firm for things like Social Security Numbers, PII, PHI, and blocks the transmission of data if these types of patterns are found. DLP can also scan data going onto removable media for physical transport. Our study found that currently 27% have instituted DLP.

Training:

22% of law firms in this study have a documented cybersecurity training program for their employees. Typically, these trainings are for software usage, such as Microsoft Office Suite, or potential email phishing exercises. Only 29% of the firms with training programs did them at regularly scheduled intervals and only 42% made them mandatory for their attorneys. It is important to note that the most recent Verizon DBIR report[1] shows that over 80% of breaches occur via social engineering tactics on end users.

Insurance:

Only 23% of firms have cybersecurity insurance policies. Cybersecurity coverage amounts varied from $1 million to $25 million. In some instances, firms assume that, since they have cybersecurity insurance, there is no need to take other steps toward being secure. In reality, this insurance will not protect the firm's reputation or ongoing ability to generate revenue, which will surely be decreased in the event of a breach.

Investment:

Surveys of AMLAW 200 firms from Chase Cost Management (CCM)[2] show spending on cybersecurity averages 1.92% of revenue. LOGICFORCE, in its findings, show spending on cybersecurity is approximately 10% of the AMLAW firm average, or 0.2% of revenue.

Records Management Policy:

A properly constructed and followed records management policy is not only a crucial step to reducing risk and limiting liability, but is also a great way to tame IT costs for the firm. 80% of firms have a records management policy in place, but only 30% mention electronically stored information (ESI) in those policies. 100% of firms LOGICFORCE has assessed have been out of compliance from electronic records management policies.

Security Executive:

Only 30% of law firms analyzed have a credentialed Chief Information Security Officer, Information Security Manager, or another similar position. Most firms leave the responsibility of cybersecurity to whoever is responsible for their IT ecosystem, which in most cases is an IT Director or Manager.

Third-Party Risk Assessments:

20% of firms are vetting the cybersecurity and data management policies of their third-party service providers. LOGICFORCE is seeing increasingly more corporate client data security audits that include a section concerning third-party service providers.

---

(1) Verizon. 2017 Data Breach Investigations Report. Rep. 10th ed. Print.
(2) Chase Cost Management. "AMLAW 200 Firms Spending as Much as $7M Per Year on Information Security." PR Newswire, 27 Aug. 2015. Web.

Scorecard

The LOGICFORCE *Law Firm Cybersecurity Scorecard* was created to give an 'Industry Score' in regards to the health of cybersecurity practices in the legal industry. The scoring system is designed to show how well firms are implementing the most critical mediation methods. The 12 categories listed, represent various mediation techniques for the described threats highlighted in this document.

SCORING: The values found in the 'Implementation Score' column reflects the percentage of implementation for each category across the legal industry. The values found in the 'Weighted Value' column is based on LOGICFORCE's assigned level of importance for each mediation technique. The 'Weighted Average' for each category is calculated by multiplying the 'Implementation Score' for each category by the respective categories' 'Weighted Average'. The 'Industry Score' is then calculated by summing the 'Weighted Average' for each category.

Categories	*Implementation Score*	*Weighted Value*	*Weighted Average*
Cybersecurity Policies	**34%**	**10%**	**3.40%**
Penetration and Vulnerability Testing	**18%**	**10%**	**1.80%**
Type of Testing	**100%**	**1%**	**1.00%**
Full Disk Encryption	**25%**	**5%**	**1.25%**
Multifactor Authentication	**21%**	**10%**	**2.1%**
Data Loss Prevention Services	**27%**	**5%**	**1.35%**
Training	**22%**	**10%**	**2.20%**
Insurance	**23%**	**10%**	**2.30%**
Investment	**10%**	**5%**	**0.50%**
Records Management Policy	**80%**	**9%**	**7.20%**
Security Executive	**30%**	**15%**	**4.50%**
Third Party Risk Assessments	**20%**	**10%**	**2.00%**
Industry Score			**29.60%**

Summary

While there are some law firms that implement most, or even all, of these mediation techniques, the fact is, many aren't doing enough when it comes to protecting themselves. In turn, they are not protecting their clients' data. Corporations are auditing the firms they work with much more frequently to ensure these measures are in place and to check that the firms are taking their responsibility seriously. They want to know that their information is being kept secure and will only work with firms that are doing what is required to keep it that way. It is important to note that an incident response plan and ability to detect when a breach occurs is the single most important thing a firm can do to ensure the protection of client data and the maintenance of industry credibility. While limiting opportunities for breach is of the utmost importance, decreasing the discovery time and the overall damage caused by an incident are also critical factors from the firm's perspective. It is truly not a question of if, but when, an incident will occur.

To combat the threat of cyber breaches we recommend the following actions be taken:

- Organize a cross functional team consisting of firm management, practice chairs, IT, procurement, administration, and human resources
- Set the tone for cybersecurity from the top and appoint a CISO/CIO to be the person in charge
- Inventory all software systems and data and evaluate risk. Not all client information is created equal. Some client data may need to be segregated on a special highly secured server depending on its value.
  - A data remediation plan with specific deletion policies is critical
- Establish a critical points contact, Internet service providers, law enforcement, and data forensic experts.
- Leverage third-parties with experience and education in data security.
- Develop regularly scheduled training programs for all staff.
- Implement multifactor authentication for any application that can be accessed directly from the Internet.

(continued, next page)

(Summary, continued)

- Utilize cyber insurance if your law firm is connected to the Internet, receives email, or maintains any sort of electronic records.
- Develop third-party assessments.
  – Firms need to evaluate all parties whom have access to any data entrusted to its' care.
- Conduct a gap analysis of the firm's current cybersecurity position and identify where the firm should be.
  – The roadmap needs to encompass the next 3 years.
- Create security policies that are in line with where the firm is today, and update as the security posture of the firm changes.
- Undergo a yearly penetration test by an independent third-party. Penetration testing can show gaps in current technical controls or weaknesses in training programs.
- Schedule vulnerability testing at least once a month, to ensure systems are protected from the latest known threats.
- Enable encryption on all devices. This includes laptops, desktops, phones, tablets, and anything else that can potentially store sensitive information.
- Put Data Loss Protection systems in place. These systems are critical for identifying sensitive data leaving the firm.

For more information about the LOGICFORCE Law Firm Cybersecurity Scorecard*, or how LOGICFORCE can assist your firm in raising your score and improving the security of your clients' data, please contact us. LOGICFORCE welcomes your questions and looks forward to serving your firm.*

1201 Demonbreun St., Suite 930
Nashville, TN 37203

800-866-1635

www.logicforce.com

LOGICFORCE