ALM LEGAL INTELLIGENCE

Cybersecurity and Law Firms: Ignorance Is Risk

Brought to you by Infinite Spada

infinite·spada

EXECUTIVE SUMMARY

Confronted with an uptick in cyber attacks and the increasing demands of their clients, law firms are scrambling to come to terms with an evolving cybersecurity landscape that not only poses an unprecedented, existential threat to the confidentiality and trust inherent in the attorney-client relationship but also presents new revenue opportunities for the practice of law around issues related to data, privacy and information security.

Drawing from the results of the inaugural ALM Legal Intelligence Law Firm Cybersecurity Survey, this report consists of three sections:

- Law Firms and the Cyberthreat Environment: An Overview
- Fulfilling Due Care and Pursuing Best Practices
- Cyber Opportunity? Data, Privacy and Information Security as a Practice Area

In addition to the content outlined above, the report contains a set of tools that introduces cybersecurity best practices, overviews the current regulatory environment, and lists cybersecurity trends to monitor.

Notable findings include:

- Nearly 10% of firms have not performed a formal information, security and privacy assessment.
- Approximately one-third of firms do not hold cyber liability insurance policies.
- More than 55% of firms have either already established a cybersecurity practice or have plans to form one.

Overall, the report presents a picture of an industry trying to play catch-up in understanding both the risks and opportunities presented by corporate cybersecurity imperatives. As the report also details, law firms that invest in building credible expertise in cybersecurity have an opportunity to gain competitive advantage — but the window for capitalizing on this burgeoning new area of the law is closing quickly.

ABOUT THE AUTHORS

Lead Author – Steven Kovalan
Senior Analyst, ALM Legal Intelligence
Phone: *202-731-4595;* ***Email:*** *skovalan@alm.com*

Steve is a Senior Analyst at ALM Legal Intelligence. He has more than seven years of experience as a research analyst focusing on topics ranging from intellectual property to government contracting. Prior to joining ALM Legal Intelligence, Steve was a Senior Advanced Research Analyst at Deltek, where he supported federal public sector contractors in their business development, market analysis and competitive intelligence efforts by providing custom research reports analyzing the federal government contracting market. A member of the District of Columbia Bar, Steve holds a Juris Doctor from the West Virginia University College of Law and a Bachelor of Arts (summa cum laude) in history and political science from West Virginia University.

Daniella Isaacson
Senior Analyst, ALM Legal Intelligence
Phone: *212-457-7977;* ***Email:*** *disaacson@alm.com*

Daniella is a Senior Analyst at ALM Legal Intelligence. Her experience includes advising law departments in relation to strategy, technology, market intelligence and operations. Prior to joining ALM Legal Intelligence, Daniella was an analyst with Huron Consulting Group's Law Department Management practice in the firm's New York office and a secondee in London. Before attending law school, Daniella spent three years in Beijing, China, where she worked in market entry consulting. A member of the New York Bar Association, Daniella holds a Juris Doctor from the Benjamin N. Cardozo School of Law and a Bachelor of Arts in international affairs (magna cum laude) from The George Washington University's Elliott School of International Affairs.

Nicholas Bruch
Senior Analyst, ALM Legal Intelligence
Phone: *617-866-0229;* ***Email:*** *nbruch@alm.com*

Nick is a Senior Analyst at ALM Legal Intelligence. His experience includes advising law firms in developing and developed markets on issues related to strategy, business development, market intelligence and operations. Prior to joining ALM Legal Intelligence, Nick was an Associate with Huron Consulting's Law Firm Strategy Practice in the firm's New York and London offices. Nick holds a Master of International Business from the Fletcher School at Tufts University and a Bachelor of Arts in economics and philosophy from DePaul University. In addition to consulting to law firms, Nick has written extensively on the legal market on topics ranging from market segmentation and market entry to future industry trends.

RESEARCH METHODOLOGY

This report relied on a number of research avenues, including results of the inaugural ALM Legal Intelligence Law Firm Cybersecurity Survey; results of the 2015 ALM Legal Intelligence Am Law Tech Survey; four weeks of one-on-one interviews with corporate counsel, law firm attorneys and information security officers, consultants, and industry experts; ALM Legal Intelligence's proprietary data sources, including RivalEdge; and the authors' analysis of the body of research conducted by others on the topic of cybersecurity. For purposes of this report, cybersecurity is defined as "whether and how electronic data and systems are protected from attack, loss or other compromise."[1]

ALM Legal Intelligence had five cybersecurity surveys in the field representing five verticals: law firms, corporate counsel, insurance, real estate and financial services. This paper focuses only on the law firm survey. In total, ALM surveyed 369 business organizations on their cybersecurity practices.

In connection with the inaugural *Law Firm Cybersecurity Survey,* ALM Legal Intelligence collected results from 69 law firm respondents, who identified as CIO (28%), COO (14%), IT Director (14%), Information Security Director (9%), CFO (7%) and Executive Director (7%), among a few others. The annual gross revenue of the respondent law firms was predominantly greater than $50 million (86%). Interviews typically lasted 60 minutes and covered a range of topics related to cybersecurity preparedness, breach management, and the role that corporate counsel and law firms play in helping manage these threats.

Please note, due to rounding, graphs may not total 100%.

1 Hogan Lovells, "Cybersecurity: The Corporate Counsel's Agenda," Bloomberg BNA, November 15, 2012.

LAW FIRMS AND THE CYBERTHREAT ENVIRONMENT: AN OVERVIEW

Meeting the Challenge: Fulfilling Due Care and Benchmarking Best Practices

Target settles for $39 million.[2] Home Depot customers are projected to confront $3 billion in fraudulent charges.[3] Sony's hackers claim to have lifted 100 terabytes of data, with multiple lawsuits and seismic damage to the corporation's reputation as a result.[4]

"On a scale of one to 10, the risks law firms are facing are an 11."

– Daniel Solove, professor at the George Washington University Law School and organizer of the Privacy + Security Forum

The list of corporate cyber attack victims seems to grow every day, but are the nation's largest law firms being confronted by similar threats? The answer is a resounding yes. Big Law is big business, and as a result of the nature of their relationship with those they represent, firms are often privy to the inner most confidences of their clients. Law firms hold vast amounts of sensitive and valuable client data, from trade secrets and other intellectual property to employee information and internal financials. All of these factors make them prime targets for cyber intrusion.

"A lot of firms have been hacked, and like most entities that are hacked, they don't know that for some period of time. Sometimes, it may not be discovered for a minute or months and even years."

– Vincent I. Polley, a lawyer and co-author of a recent book on cybersecurity for the ABA

For those in the legal community who believe, "It cannot happen to me," recent studies have shown that the threat of an attack to law firms is no longer abstract or theoretical; rather, it is now a harsh reality. Daniel Solove, professor at the George Washington University Law School and organizer of the Privacy + Security Forum, believes, "On a scale of one to 10, the risks law firms are facing are an 11."[5] Bloomberg News previously reported that cybersecurity firm Mandiant, a division of FireEye, estimated that 80 major US law firms were hacked [in 2011].[6] In September 2015, Law360 reported that the 2015 ABA Legal Technology Survey found that 25% of law firms with at least 100 attorneys have experienced a breach due to a hacker, website attack, break-in, or lost or stolen computer or smartphone.[7]

Furthermore, there is even some indication that those numbers could be conservative estimates due to firms either failing to discover a breach or not publicly disclosing incidents. Vincent I. Polley, a lawyer and co-author of a recent book on cybersecurity for the American Bar Association, argues, "A lot of firms have been hacked, and like most entities that are hacked, they don't know that for some period of time. Sometimes, it may not be discovered for a minute or months and even years."[8] And, earlier this year, *The New York Times* reported on an internal Citigroup memo, which asserted law firms were "high risk for cyberintrusions" and complained, "Due to the reluctance of most law firms to publicly discuss cyberintrusions and the lack of data breach reporting requirements in general in the legal industry, it is not possible to determine whether cyber attacks against law firms are on the rise."

2 Bronstad, Amanda, "Target Pays $39M to Resolve Data-Breach Litigation," Law.com, ALM Media, December 2, 2015.
3 Lipka, Mitch, "Home Depot hack could lead to $ 3 billion in fake charges," Moneywatch, CBS News, September 16, 2014.
4 Zetter, Kim, "Sony Got Hacked Hard: What We Know and Don't Know So Far," *Wired*, December 3, 2014.
5 Harrison, Erin E., "Heightened Risk of Cyberattacks Puts Pressure on Law Firms to Bolster Defenses," *Legaltech News*, ALM Media, August 14, 2015.
6 Pearson, Sophia and Michael A. Riley, "China-based Hackers Target Law Firms to Get Secret Deal Data," Bloomberg News, Bloomberg L.P., January 31, 2012.
7 Maleske, Melissa, "1 In 4 Law Firms Are Victims Of A Data Breach," Law360 (www.law360.com), Portfolio Media, September 22, 2015
8 Goldstein, Matthew, "Law Firms Are Pressed on Security for Data," *The New York Times*, The New York Times Company, March 26, 2014.

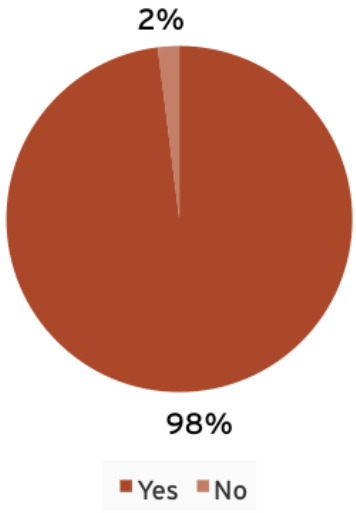
LAW FIRMS AND THE CYBERTHREAT ENVIRONMENT: AN OVERVIEW

Meeting the Challenge: Fulfilling Due Care and Benchmarking Best Practices

Though official figures tracking trends in law firm data breaches may be difficult to uncover, within the legal industry itself there is the belief that attacks are on the rise. For example, a whopping 98% of law firm respondents to the ALM Legal Intelligence Law Firm Cybersecurity Survey believe that the legal industry is increasingly a target for cyber-attacks.

Even with threats apparently on the rise, perhaps the most important factor that should drive the law firms out of their relative complacency on the issue of data security is the changing behavior of their largest and most important clients. General counsel and their law departments are increasingly recognizing that their law firms should be treated like any other vendor in the corporate supply chain. As such, general counsel are including provisions related to cybersecurity in their law firm retention agreements and are considering firms' data security practices when determining which firms to retain.

Do You Believe Cyber Attacks Are Increasing in Frequency Within the Legal Industry?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

These requirements are arising particularly from the financial and healthcare industries, as they tend to be highly regulated. As a result, they generally have more sophisticated data security protocols. For example, in December 2014, Benjamin M. Lawsky, New York Superintendent of Financial Services, issued a memorandum to all chartered or licensed banking institutions in New York State, alerting them that its regular information technology examination procedures would henceforward require that covered organizations "describe [their] due diligence process regarding information security practices that is used in vetting, selecting and monitoring third-party service providers."[9]

The ALM Legal Intelligence Law Firm Cybersecurity Survey provides some insight into this phenomenon. Though the numbers are relatively modest at the moment, with 71% of law firm respondents indicating that less than one-fourth of their clients currently demand details of their data security practices and policies, expect these numbers to rise — and steeply — in the near future. Jeffrey Norris, CISSP, senior director of information security at LexisNexis, said, "If you look at the analysis of data breaches, such as Target and Home Depot, and the resultant communications by the FFIEC [Federal Financial Institutions Council] on management of third-party service providers, the spotlight has swung towards law firms due to security concerns on how they handle the

9 Lawsky, Benjamin M., "New Cyber Security Examination Process," New York Department of Financial Services, December 10, 2014.

LAW FIRMS AND THE CYBERTHREAT ENVIRONMENT: AN OVERVIEW

Meeting the Challenge: Fulfilling Due Care and Benchmarking Best Practices

data they're entrusted with."[10] This sentiment was echoed in many informal conversations with general counsel on the topic. In almost each instance and regardless of industry, general counsel indicated that they were turning their attention to the data security practices of their outside counsel. So the question remains: Are law firms ready to have their data security practices put under the spotlight? Those that get out in front of this issue have an opportunity to distinguish themselves from their competition and gain a competitive advantage over their peers.

Cybersecurity Threats and Consequences

Having established that cybersecurity should be a primary area of concern for law firms, next we turn to the nature of the risk. The following figure provides some examples.

Examples of Cybersecurity Threats

Threat/ Consequence	Description
Data Volume and Location	Companies often keep confidential information on online or internal databases for convenience, which also makes it easy for outside attackers or malicious employees to access.[11]
Employee Errors	Employees have been found to be a source of cyber risk due to errors or malicious intent.
Third-Party Vendors	Third-party vendors, including outside counsel, often pose an enormous risk to companies, both due to weak controls within their organizations as well as an entry portal to the company's systems.
Technology Glitches	Technology can be a help or a hindrance in managing cybersecurity. In some instances, it can be a source of a leak or allow for new and improved ways for hackers to gain access to internal systems.
Hackers, Phishers, DDoS and Other Stealthy Lurkers	Hacking is the single most frequent type of data breach, but all malicious threats should be protected against.[12]
External Access	In the digital age of working from different devices and locations, including mobile phones, accessing the system remotely from a variety of platforms creates cybersecurity concerns.[13]
Financial, Reputational and IP Concerns	A wide range of consequences for a data breach should be planned for and managed, including reputational risk, financial liability and loss of IP.[14]
Lack of Resources	Lack of resources makes it more difficult for companies to adequately prepare against cyberthreats, particularly for smaller organizations.[15]

Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

10 Harrison, Erin E., "Heightened Risk of Cyberattacks Puts Pressure on Law Firms to Bolster Defenses," *Legaltech News*, ALM Media, August 14, 2015.
11 Fitch, Elizabeth S., and Theodore M. Schaer, "The Year of the Cyber Breach," IADC Committee Newsletter, IADC Law, March 2015.
12 Hackers were found to be the most frequent cause of loss (31%). "NetDiligence 2015 Cyber Claims Study," NetDiligence (netdiligence.com), September 2015.
13 "2015 Data Breach Investigations Report," Verizon Enterprise Solutions, (www.verizonenterprise.com).
14 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
15 "NetDiligence 2014 Cyber Claims Study," NetDiligence (www.netdiligence.com), December 2014.

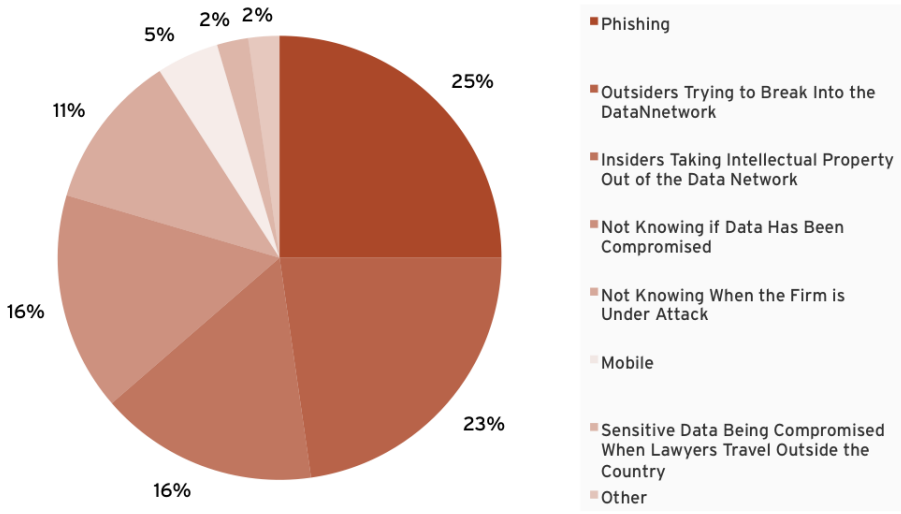
LAW FIRMS AND THE CYBERTHREAT ENVIRONMENT: AN OVERVIEW

Cybersecurity Threats and Consequences

What makes cybersecurity such a difficult topic to get a handle on is that these threats are ever evolving, and as a result, all enterprises, including law firms, must be vigilant and agile in responding to changing circumstances.

The chart at right, containing data from the 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey, a survey of law firm CIOs and IT directors, reflects how those at the top of law firm technology departments view the current threat landscape.

What Do You Perceive as the Biggest Security Threat to Your Law Firm?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

According to the survey respondents, phishing (25%), hackers (23%), insider threats (16%), and not knowing if data has been compromised (16%) are the current top security concerns. A reflection of the changing nature of these threats, according to Scott Angelo, CIO at K&L Gates, is that, "Phishing is significantly different now than even 18 months ago. It is much more sophisticated, [the emails] look much more real. This is a business for these people, and you have to take the view that you are up against a business. It just happens to be a criminal business."[16]

> "Phishing is significantly different now than even 18 months ago. It is much more sophisticated, [the emails] look much more real. This is a business for these people, and you have to take the view that you are up against a business. It just happens to be a criminal business."
>
> — Scott Angelo, CIO at K&L Gates

While the threats themselves are varied and changing, the ultimate consequence of a breach almost always hurts the firm's bottom line. This could be from business interruption resulting from a ransomware attack (holding access to the victim's system hostage to an online payment); even more likely, it might arise from the damage to the firm's reputation subsequent to the public disclosure of any type of intrusion. Confidentiality, underscored by requirements in codes of professional responsibility, is at the heart of the legal profession, and once clients believe a firm can no longer be trusted, the damage may be irreparable.

16 Cohen, Alan, "Phishing, Attacks Top Data Concerns of Law Firm CIOs," *The American Lawyer*, ALM Media, November 22, 2015.

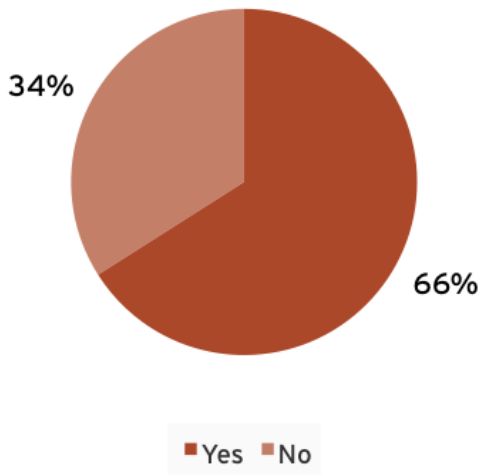
LAW FIRMS AND THE CYBERTHREAT ENVIRONMENT: AN OVERVIEW

Legal Industry Response to Cybersecurity

Faced with an increasing number of attacks and a myriad of security threats that could have incalculable consequences, the legal industry is starting to take notice. According to the 2015 ALM Legal Intelligence Am Law Tech Survey, 77% of law firm CIOs and IT directors are more concerned about security threats than they were two years ago.

However, that concern might not be translating to increased investment. Sixty-three percent of respondents to the ALM Legal Intelligence Cybersecurity Law Firm Survey indicated that their firm used less than one-half of 1% of the firm's gross revenue for data breach detection and prevention, and 85% reported that their firm used less than one-half of 1% of the firm's gross revenue for response and remediation efforts.

Are You Comfortable With Your Law Firm's Ability to Withstand a Cyber Breach?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

While there is no magic number when it comes to law firm data security spending, these steps are likely insufficient. Half of the respondents to a Chase Cost Management (CCM) survey, drawn primarily from large law firm CIOs and IT directors, indicated they felt their total capital and operating budget for information security is not enough.[17] This could help explain why slightly more than a third of the respondents to the ALM Legal Intelligence Law Firm Survey revealed that they are not comfortable with their law firm's ability to withstand a cyber breach. Moreover, for the approximately two-thirds of respondents who are comfortable with their firm's position, the results of the law firm survey measuring industry adoption of data security best practices might belie that confidence.

17 Don, Brett C., "What Price Peace? Key Expense Management Strategies for Law Firm Data Security," Chase Cost Management, June 3, 2015.

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

Using Best Practices and Navigating an Unclear Regulatory Environment

With regard to law firms in particular, individuals seeking to implement a comprehensive data security regime may encounter significant cultural barriers along the way. When asked to assess the difficulty of creating a cultural change on the issue of cybersecurity within law firms, Curtis Collette of MetLife's e-discovery strategy and global technology and operations litigation support, remarked, "I do think it is not hopeless but it is not going to be easy."[18] According to Joe Abrenio, Vice President of Advisory Services and General Counsel at DeltaRisk, a Washington, D.C.-based firm that provides security and risk management services to government agencies and commercial organizations, "Law firms are relatively new targets. For this reason alone, law firm management is struggling to understand their specific threat profiles and finding and hiring cybersecurity talent. More fundamental, law firms are hesitant to spend time, money and resources on cybersecurity concerns, which management, attorneys, and staff may not fully understand or appreciate. Finally, the pressure on lawyers to meet client needs and litigation deadlines makes them less focused on security and more concerned with immediate productivity."[19]

"Law firms are hesitant to spend time, money and resources on cybersecurity concerns, which management, attorneys and staff may not fully understand or appreciate."

– Joe Abrenio, Vice President of Advisory Services and General Counsel at DeltaRisk

Given cybersecurity's ambiguous requirements under state and federal law (See Appendix 1), fulfilling the requirements of due care can often require more common sense than prescription. At the same time, there are certain best practices that should be followed and others that are based on business-judgment decisions related to risk and cost (See Appendix 2).[20]

Further, the foundation of an effective cybersecurity program that meets the standard of due care is the existence of a cybersecurity plan and support team. While there are many best practices and regulations to address within that structure (particularly for more highly regulated industries), the bottom line is that it is necessary to embed an understanding of cybersecurity – the risk, response, and action plan – within the business organization.[21] Appendices 1 and 2 detail some best practices and cybersecurity regulations to keep in mind when structuring a cybersecurity policy.

In pursuit of best practices to combat the cyberthreat, some of the more sophisticated firms are looking to other industries for answers. For example, sharing of cyberthreat information is often considered a key best practice. In the financial industry, the Financial Services Information Sharing and Analysis Center (FS-ISAC), billed as "[t]he only industry forum for collaboration on critical security threats facing the global financial services sector," serves to facilitate the exchange of threat information.[22] At the behest of the financial industry, FS-ISAC has

18 Harrison, Erin E., "'Fundamental Shift' in Law Firms' Cybersecurity Efforts," *Law Technology News (Online)*, ALM Media, February 5, 2015.
19 Harrison, Erin E., "Banking Industry Demands Firms Harden Cybersecurity Profiles," *Law Technology News (Online)*, ALM Media, February 26, 2015.
20 On one end of the spectrum, Bank of America puts no cost constraint on their cyber program. Nash, Kim S., "Bank of America Tech Chief Says Metrics Are Key to Security," The CIO Report, *Wall Street Journal*, July 28, 2015.
21 Hogan Lovells, "Cybersecurity: The Corporate Counsel's Agenda," Bloomberg BNA, November 15, 2012.
22 Financial Services Information Sharing and Analysis Center (www.fsisac.com).

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

Using Best Practices and Navigating an Unclear Regulatory Environment

served to advise the legal industry in the creation of its own information-sharing platform. To do so, the FS-ISAC worked in conjunction with law firm members within the International Legal Technology Association (ILTA) and its cybersecurity-focused component, LegalSec — along with a group of law firms including Sullivan & Cromwell; Debevoise & Plimpton; Paul, Weiss, Rifkind, Wharton & Garrison; Allen & Overy; and Linklaters — to form the Legal Services Information Sharing and Analysis Organization (LS-ISAO). Launched in August 2015, open to law firms of any size, and requiring an $8,000 membership fee, the LS-ISAO provides a forum for member law firms to anonymously share threat data. While most legal industry insiders expect law firms to embrace the new organization, some expressed reservations about joining, citing the concern that even when sharing information anonymously within the framework of the members-only forum, the firm might risk having itself publicly identified as the victim of a breach.[23]

"More and more of our clients are auditing the security posture of law firms and most are basing their requirements upon ISO certification."

— David Fleming, CIO at Goodwin Procter

A second best practice borrowed from other industries that gaining traction with law firms is the pursuit of certifications such as the International Organization for Standardization's ISO 27001, which recognizes information security management. Goodwin Procter pursued and achieved ISO 27001 certification in October 2015. CIO David Fleming told Legaltech News, "Given the almost weekly news reports of data breaches, certifications are a clear and structured way to ensure the proper safeguards are implemented to meet our ethical confidentiality obligations to clients .... More and more of our clients are auditing the security posture of law firms and most are basing their requirements upon ISO certification .... It helps to reassure our clients in regulated industries that their legal data is properly guarded."[24] In early 2015, citing data from ILTA, *The American Lawyer* reported that as of December 2014, 18 large law firms were certified and 21 were seeking certification.[25]

23 Simmons, Christine, "Cybersecurity Data Sharing Is Now Available to Law Firms," *New York Law Journal*, ALM Media, August 19, 2015.
24 Silverstein, Ed, "Goodwin Procter Latest Am Law 100 Firm to Earn ISO Security Certification," *Legaltech News*, ALM Media, October 28, 2015.
25 Ibid.

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

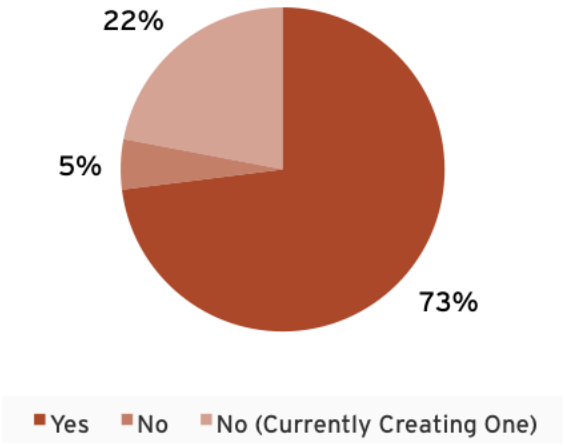
Benchmarking Best Practices

The following are some best practices that survey respondents do well, and some that could be improved upon:

1. Data breach plan in place

Seventy-three percent of respondents currently have a data breach plan in place, 22% are in the process of creating one, and only 5% do not have one and are not planning on creating one.

Does Your Law Firm Have a Data Breach Plan in Place?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

According to Jason Straight, senior vice president and chief privacy officer at UnitedLex, a legal outsourcing services provider with a practice dedicated to cybersecurity risk management, a data breach plan is a key strategic imperative. "Rather than focus all efforts on preventing an attack, law firm partners should develop an information security program based on the premise that the firm's network is already compromised," argues Straight. As a result, firms will be made to confront the following questions that he believes are vital to an effective data breach response:

- How would the firm know whether it was compromised?
- Who is responsible for managing the firm's response to a security breach that affects client data?
- What information would investigators need to determine the scope and scale of an incident, and is the firm equipped to collect and preserve such information?[26]

To determine whether a breach has occurred, or once a breach has been uncovered, and to assess the scope and scale of the incident, firms should use the services of computer forensics experts. Having a crisis panel in place allows for faster mobilization in case of an emergency, which can serve to lower management costs.[27] Slightly more than 20% of survey respondents indicated that they do not have preexisting relationships with computer forensics experts who can respond immediately to a data breach. Further, only 50% of respondents reported that their plan identifies specific outside firms to contact in case of breach. The cybersecurity plan and team should always identify roles and responsibilities, including outside counsel, for managing the firm's response to a breach. Because cyber-attacks move quickly, not having this foresight in place can waste time when it is most precious.

26 Straight, Jason, "Law Firms Aren't Immune to Cybersecurity Risks," *The National Law Journal* (Online), ALM Media, January 26, 2015.
27 Implementing an incident response team can decrease the average per capita cost of data breach from $217 to $193.2. "2015 Cost of Data Breach Study: Global Analysis," IBM, Ponemon Institute, May 27, 2015.

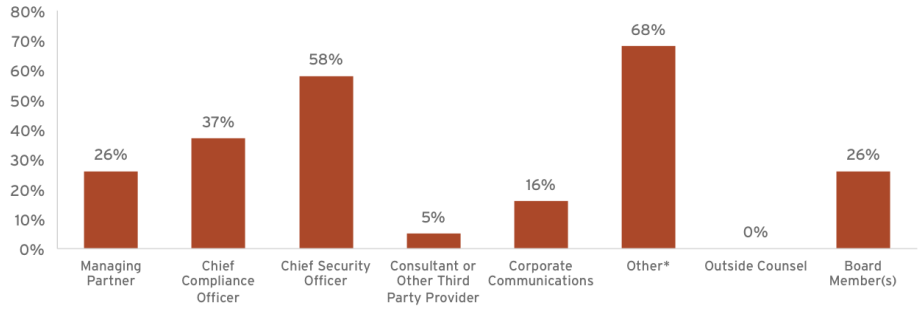
FULFILLING DUE CARE AND PURSUING BEST PRACTICES

Benchmarking Best Practices

2. Cybersecurity team in place

Only half of law firm respondents have a data protection team or committee in place, suggesting that the legal industry is behind with regard to creating the proper infrastructure to support effective prevention and response measures. Among other industry experts, Jason Straight of UnitedLex believes that cybersecurity is not just an information technology issue.[28] Rather, it is a problem that is best countered by a holistic approach that crosses disciplines by integrating stakeholders from information technology, legal, human resources, risk management and firm leadership.[29] The variability in the survey results suggests that firms are bringing multiple parties to the table, but that there is no overriding consensus as to who should be the primary players.

If Your Law Firm Has a Data Protection Team, Who Is Represented (Select All That Apply)?



*Other includes CIO, CFO, COO, CPO; information security; IT security; insurance; general counsel; executive director; admin management; directors of conflicts and records.
Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

Dr. Larry Ponemon, founder of the Ponemon Institute — a research center dedicated to issues such as privacy, data protection and information security — advocates that any law firm with 500 lawyers or more should have the following staff to serve at the core of their data security program:

- **Chief Information Security Officer** – Should oversee cybersecurity at the firm, but should not report to the CIO. Should report to an executive body.
- **Regulatory Policy Wonk** – Responsible for understanding the applicable privacy and data security laws and regulatory environment.
- **Security Architect** – Makes sure the law firm's technology is effective and functioning properly.
- **Forensics Expert** – Mitigates damages post breach and might also serve to train firm staff on data protection best practices.[30]

Additionally, some firms are even going so far as to create the role of law firm chief privacy officer to serve as a central player in creating, implementing and administering data security practices and procedures. One such firm is Fox Rothschild, whose partner Mark G. McCreary was recently bestowed the title of CPO. In his role as CPO, McCreary is overseeing the firm's efforts to achieve ISO 27001 certification, reviewing client data and privacy-related requirements, reviewing and revising firm security policies, and taking an active role in training firm staff on best practices.[31]

28 Straight, Jason, "Law Firms Aren't Immune to Cybersecurity Risks," *The National Law Journal* (Online). ALM Media, January 26, 2015.
29 Ibid.
30 Gluckman, Nell, "How Much Should Firms Pay to Protect Themselves From Hackers?" *The Am Law Daily,* ALM Media, September 2, 2015.
31 Passarella, Gina, "Client Data Concerns Drive Creation of Law Firm Chief Privacy Role," *Legaltech News*, ALM Media, September 25, 2015

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

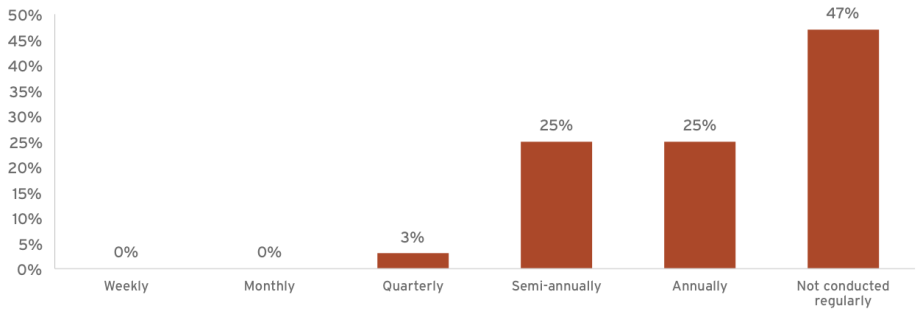
Benchmarking Best Practices

While the most sophisticated law firms have a dedicated data security team that comprises individuals with the skills necessary to confront the multidisciplinary nature of the problems presented by cyber-attacks, at the very least all firms should have some designated internal legal professionals to be engaged if a breach occurs. Twenty-three percent of law firm respondents, however, have not taken this step. The irony (and potential threat to business) here is that as corporate legal departments are embracing a greater role in connection with cybersecurity, the law firms themselves lag behind in recognizing that internal data security is a concern that stretches beyond the IT department.

3. Training

Eighty-seven percent of law firm respondents indicated that they train employees on processes and polices to prevent data breaches. Training employees on topics such as the effective use of passwords or the recognition of phishing schemes can be low-cost investments that have a substantial return by preventing breaches from occurring at all.[32]

How Often Does Your Law Firm Conduct Fire Drills on Data Breaches?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

However, the current practice of conducting "fire drills," – training lawyers and staff on what to do in case of an actual breach – leaves room for improvement. The majority of respondents (47%) stated they do not regularly conduct drills, followed by those that conduct them annually (25%) and those that conduct them semi-annually (25%). Law firms should strive to implement fire drills more regularly: at least semi-annually, if not more frequently.

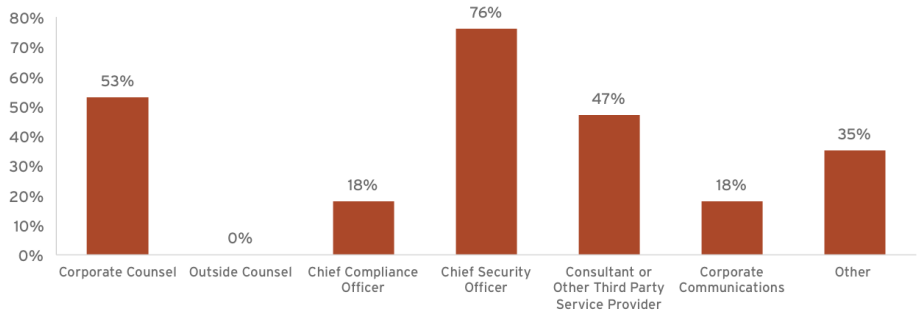
32 Gluckman, Nell, "How Much Should Firms Pay to Protect Themselves From Hackers?" *The Am Law Daily*, ALM Media, September 2, 2015.

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

Benchmarking Best Practices

Moreover, the team members involved in fire drills should be much more robust, reflecting the holistic approach previously discussed. Additionally, because cybersecurity as a whole should be an initiative that ultimately rests with firm management, the responses in the figure at right suggest that the fire drill training is lacking partnership buy-in.

When Fire Drills Are Conducted, Who Is Involved?

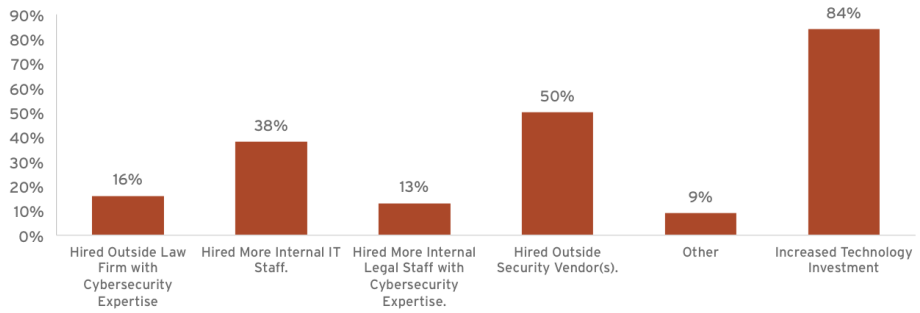


Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

4. Using Experts

Should a law firm feel that it is lacking in cybersecurity expertise, it may look to fill its cyber knowledge and skills gaps by increasing internal staff or by consulting with external experts. For instance, if the firm hasn't established a formal training procedure, third parties can conduct the training.[33]

How Has Your Law Firm Increased Its Readiness in Handling Potential Security Breaches?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

The survey responses shown in the bottom figure, which indicate that firms are increasing their readiness through investment in technology (84%) and IT staff (38%), further reinforce the notion that law firms primarily view cybersecurity as a technology issue. While technology is a vital component of any data security regime, law firms would be well served by also investing in resources that serve to address the legal, risk management, human resources, communication and strategic business consequences of data security planning, implementation, remediation and response.

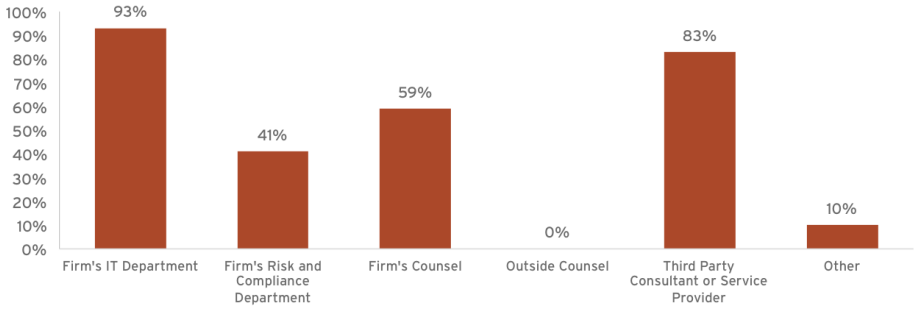
33 "The Battle Continues: Bridging the Data Security Chasm: Assessing the Results of Protiviti's 2015 IT Security and Privacy Survey," Protiviti, 2015.

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

Benchmarking Best Practices

5. Audits

If Your Firm Performed a Formal Information, Privacy and Security Risk Assessment, Who Was Involved?



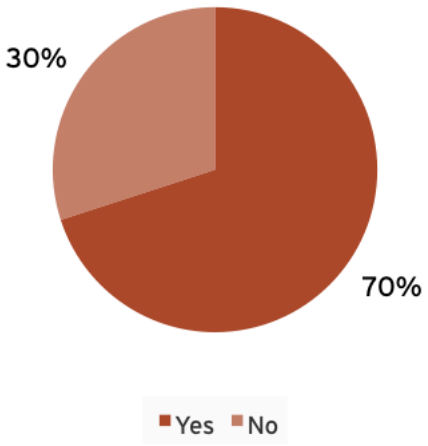
Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

Only 71% of law firm respondents have performed a formal information, privacy and security assessment, which is almost always the first step in creating and implementing a data security plan. Consequently, nearly 30% of firms have not taken formal steps to identify their "crown jewels" (i.e., their most sensitive and valuable data), and, as such, are at a distinct disadvantage when instituting security protocols. If the firm fails to identify vital data assets, it cannot properly assess risk or institute controls. This problem is further compounded by the fact that only half of respondents indicated that they have trained auditors with the ability to conduct data protection audits.

However, those firms that have performed a formal information, privacy and security risk assessment are moving in the right direction by including multiple parties and disciplines in the process. The assessments still skew heavily toward IT (93%), but it is heartening to see that many firms (83%) also rely on outside consultants (Figure 10). That said, there is still room for improvement. The process would benefit from the perspectives and expertise of other parties, including corporate counsel, risk management executives, firm leadership and human resources.

6. Cyber Liability Insurance

Has Your Law Firm Purchased Cyber Liability Insurance?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

Only 70% of respondents have purchased cyber liability insurance. This area calls for some improvement. Law firms should buy stand-alone policies from a cyber insurance provider and ensure that the provider meets the firm's coverage requirements. Because this field is rapidly changing, it is important to shop around and consult different providers before purchasing.[34]

Organizations that have sensitive data should purchase cyber-specific insurance and ensure that third party vendors add them as a beneficiary to their cyber insurance. Eighty-seven percent of law firm respondents indicated that they require third parties to carry cyber liability insurance, which suggests firms are taking seriously the role of supply chain management in privacy and data

34 Privacy & Data Security Law Resource Center, "Views on Corporate Cybersecurity Insurance Options From Thomas H. Bentz Jr. of Holland & Knight LLP," Big Law Business, Bloomberg BNA, August 18, 2015; Interviews with industry experts.

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

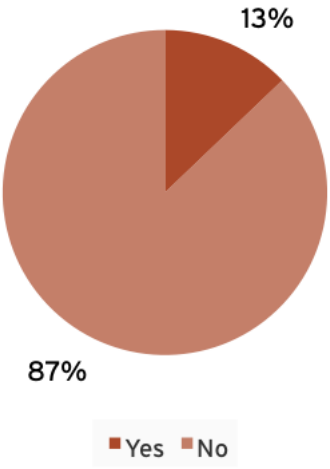
Benchmarking Best Practices

protection. In addition to requiring that third-party vendors carry cyber-specific policies, law firms should also conduct thorough due diligence in connection with any supplier's data security practices and procedures. Business organizations should be cognizant of the fact that internal security protocols are only as strong as the weakest link in their supply chain, and, as previously discussed, regulators are beginning to put industry on notice that vetting of third-party vendors is required to meet standards of reasonable care.

7. The Cloud

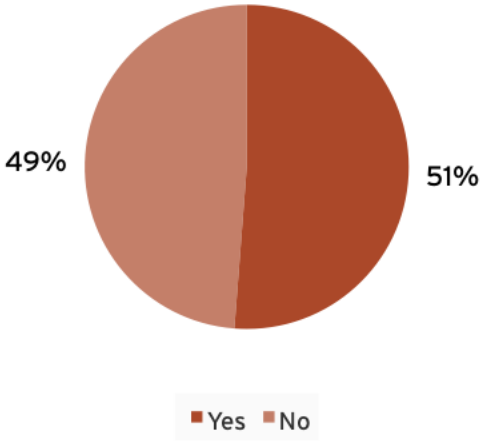
Respondents to the 2015 ALM Legal Intelligence Am Law Tech Survey of law firm CIOs and IT directors are nearly split down the middle on the use of the cloud – 51% embrace it and 49% do not.

Does Your Law Firm Require Third Parties to Carry Cyber Liability/Data Breach Insurance Coverage?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

Does Your Law Firm Embrace Cloud Computing?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

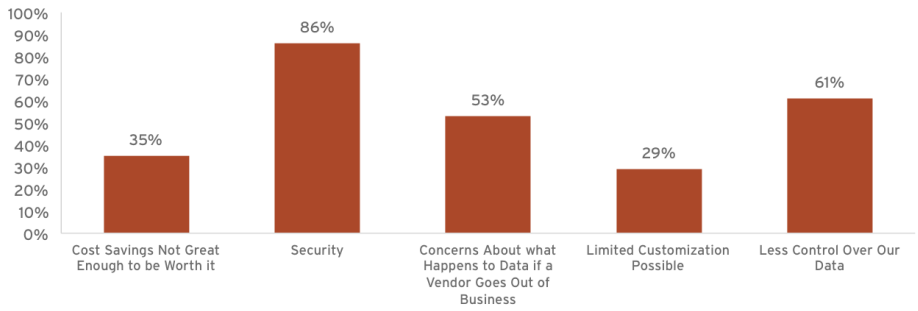
35 Cohen, Alan, "Phishing, Attacks Top Data Concerns of Law Firm CIOs," *The American Lawyer*, ALM Media, November 22, 2015.

FULFILLING DUE CARE AND PURSUING BEST PRACTICES

Benchmarking Best Practices

When asked in the same survey to identify their biggest challenges or worries regarding software-as-a-service (SaaS) cloud computing, those same CIOs and IT directors overwhelmingly identify security (86%) as the primary concern, followed by diminished control over data (61%) and fears about the data if the cloud vendor goes under (53%). While the cloud debate won't be settled here, it might be beneficial to consider some of the pros and cons. Those who are wary of the cloud cite the aforementioned security risks and also raise concerns about navigating international privacy regulations, especially in Europe, when data is housed in a cloud environment that facilitates easy transfer across borders. On the other hand, in addition to appreciating its benefits in supporting business continuity, those who favor the cloud identify the time and cost savings achieved by outsourcing the maintenance and management of data storage to vendors.[35] Further, there are also some cloud supporters who claim that the security concerns of cloud detractors are misguided. They assert that the real security risk is in the use of physical systems that are more susceptible to being lost, stolen or damaged – risks that are not applicable to information stored in the cloud.[36]

What Are, or Have Been the Biggest Challenges or Worries Regarding Saas Cloud Computing?



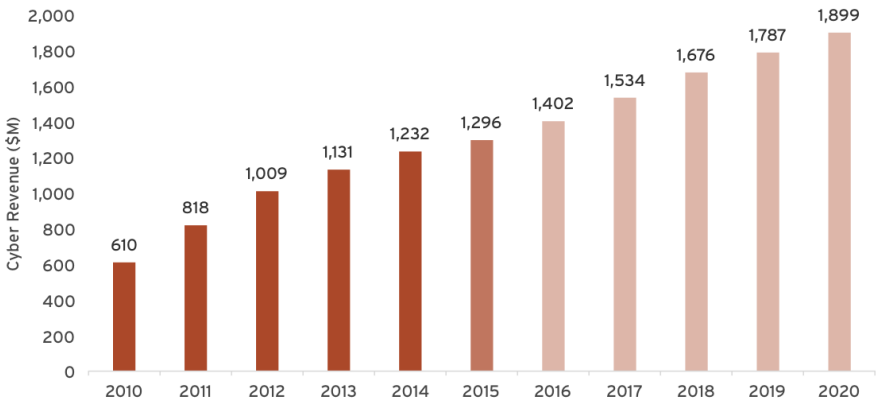
Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

36 Herbst, T. Christopher, "The Cloud is More Secure Than Physical Alternatives – Period," *Legaltech News*, ALM Media, October 16, 2015.

CYBER OPPORTUNITY? DATA, PRIVACY AND INFORMATION SECURITY AS A LEGAL PRACTICE AREA

With all the discussion in the preceding sections about security threats, it would seem that the emergence of information age technology has brought only doom and gloom to the legal industry; however, that is not the case. Besides increased efficiency and analytical capabilities (a topic for another time), the data revolution has spawned the creation of a discrete practice area around issues of data, information security and privacy. As discussed in the previous sections, data security is a multidisciplinary issue where legal has a central role to play.

Am Law 200 Cybersecurity Legal Services Market ($M)

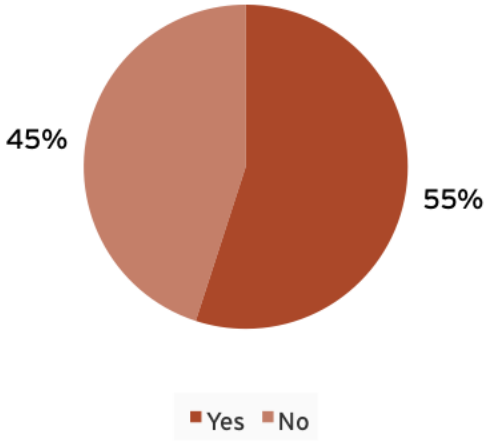


Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

An analysis of ALM RivalEdge data reveals that, from 2010 to 2015, the market for cybersecurity legal services among Am Law 200 firms increased more than 100%, growing from $610 million to $1,296 million. While the rate of growth is expected to slow, ALM Legal Intelligence projects that the market will increase another 46.5% over the next five years, reaching $1,899 million in 2020.

Given this projected growth, it's no surprise that law firms are looking to take advantage of this emerging market. Sixty-seven percent of the respondents to the ALM Legal Intelligence Law Firm Cybersecurity Survey indicated that they have a cybersecurity practice group or plan on starting one.

Does Your Law Firm Currently Have a Cybersecurity Practice Group?

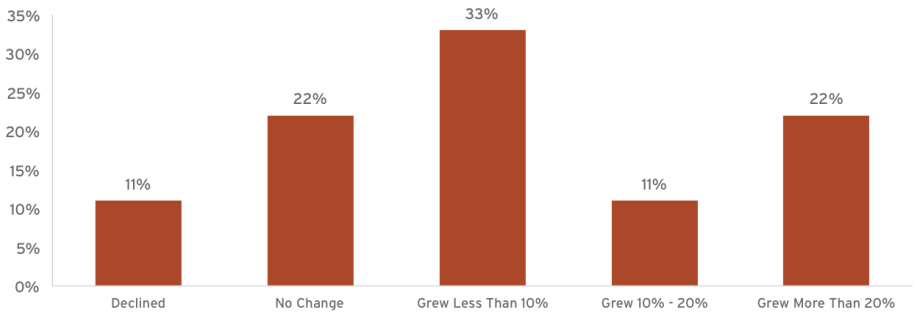


Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

CYBER OPPORTUNITY? DATA, PRIVACY AND INFORMATION SECURITY AS A LEGAL PRACTICE AREA

Sixty-six percent of survey respondents reported that their firm's cybersecurity practice group billings increased over the previous year, providing further evidence of a growing market. Note that there are also signs that some firms are beginning to separate themselves, while others are starting to lag behind – 22% of respondents experienced more than 20% growth while on the other end of the spectrum, 11% of firms saw declining growth.

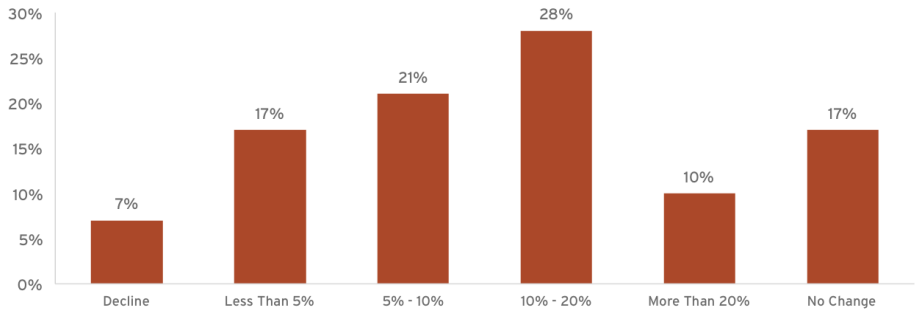
How Much Did Your Firm's Cybersecurity Practice Group Billings Change Last Year Versus the Previous Year?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

Additionally, firms are generally optimistic about the future of the market as well. Seventy-six percent of survey respondents with a cybersecurity practice group expect their group headcount to grow over the next five years. Though again, there is some divergence among the market players. On the one side, there are the 10% of firms that expect their cybersecurity practice group headcounts to grow by more than 20% over the next five years, while on the other, there are the 24% of firms that expect no change or declining headcounts over the same time period.

In the Next Five Years, How Much Do You Expect Your Law Firm's Cybersecurity Practice Group's Headcount to Grow?



Source: 2015 ALM Legal Intelligence Law Firm Cybersecurity Survey

With increased competition and a growing market, how are firms differentiating themselves? Some attorneys are looking to establish their bona fides by earning industry certifications as a Certified Information Systems Security Professional (CISSP) or Certified Information Privacy Professional (CIPP).

CYBER OPPORTUNITY? DATA, PRIVACY AND INFORMATION SECURITY AS A LEGAL PRACTICE AREA

For example, an analysis of RivalEdge data reveals that there are at least nine attorneys at Am Law 200 firms with a CISSP certification.

Am Law 200 Attorneys with a CISSP Certification

Firm	Attorney	Title	Practice(s)
Alston & Bird	Peretti, Kimberly K.	Partner	Telecom & Tech; Litigation; Gov. & Regulatory
BakerHostetler	Gainer, Randal L.	Partner	Telecom & Tech; Litigation
BakerHostetler	Koller, M. Scott	Other Counsel/ Attorney	Telecom & Tech; Entertainment/Media
Cooley	Sabett, Randy	Other Counsel/ Attorney	Telecom & Tech; Aerospace & Defense
Foley & Lardner	Overly, Michael R.	Partner	Int'l/Cross-Border; IP; Telecom & Tech
Ice Miller	Merker, Nicholas	Associate	Energy, Natural Resources & Environment; IP; Telecom & Tech; Entertainment/Media; Litigation
Jones Day	Silberman, Gregory P.	Partner	IP; Telecom & Tech; Int'l/Cross-Border
King & Spalding	Johnson, Glenn	Other Counsel/ Attorney	White Collar; Gov. & Regulatory; Int'l & Cross-Border; Arbitration/Dispute Resolution; Litigation; Telecom & Tech
Latham & Watkins	Boyle, Kevin C	Partner	Telecom & Tech; M&A; Corporate/Business; Int'l & Cross-Border; Consumer/Retail

Source: ALM Legal Intelligence Analysis of RivalEdge Data

RivalEdge data reveals that CIPP certified attorneys are more common, though still not prevalent, with McGuireWoods leading the way among Am Law 200 firms, with nine on staff. Washington, DC (34), followed by San Francisco (16), and New York (13) are the top locations for attorneys with CIPP certifications among Am Law 200 firms.

Am Law 200 Firms with Five or More CIPP Certified Attorneys

Firm	CIPP Certified Attorneys
McGuireWoods	9
Ropes & Gray	7
Wilson Sonsini	7
Crowell & Moring	6
Jackson Lewis	6
Mintz Levin	5
Alston & Bird	5
Ice Miller	5

Source: ALM Legal Intelligence Analysis of RivalEdge Data

Top 10 Locations for CIPP Certified Attorneys in Am Law 200 Firms

Location	CIPP Certified Attorneys
Washington, DC	34
San Francisco, CA	16
New York, NY	13
Chicago, IL	10
Los Angeles, CA	9
Atlanta, GA	9
London	9
Brussels	4
Minneapolis, MN	4
Indianapolis, IN	4

Source: ALM Legal Intelligence Analysis of RivalEdge Data

CONCLUSION

For Big Law, cybersecurity presents both risks and opportunities, and it is up to firm leadership to choose their path. While cybersecurity preparedness and best practices vary by organization, the bottom line is that law firms should strive to implement a holistic approach to data security, one that starts with management and crosses disciplines, notably including more than IT. Though cyber attacks are constantly evolving and there will always be new trends to monitor and new challenges to confront (see Appendix 3), those firms that invest in data security best practices have an opportunity to distinguish themselves from their peers by demonstrating a true commitment to protecting the attorney-client relationship. Further, firms that pursue building credible expertise in cybersecurity have an opportunity to gain competitive advantage in the burgeoning data, privacy and information security legal market; however, time is of the essence. There are clear indications that some firms are beginning to establish themselves as leaders in the field and are in a position to leave the competition behind.

Appendix 1: Regulatory Overview

1. State Privacy Laws

Forty-seven states, the District of Columbia, Puerto Rico, Guam and the Virgin Islands have all enacted statutes requiring companies to provide notification if a breach of personal information occurs. A breach may involve multiple state statutes. State laws are not industry-specific and are, therefore, broader than many federal regulations on cybersecurity.

Companies should first evaluate if a breach has occurred, what data has been compromised, and whether the type of data compromised requires disclosure under state breach notification laws. The legal team will likely take ownership of determining if a breach warrants public notification under relevant laws.[37]

Some states have adopted stricter laws or are set to adopt stricter laws than just breach notification statutes. For instance, the New York Department of Financial Services has warned companies that it plans to implement cybersecurity regulation addressing cyber concerns.

2. Federal Regulations[38]

There are some regulations that encompass all industries, but most federal regulations are industry-specific, including the following:

- *Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act:* Healthcare
- *Family and Educational Rights and Privacy Act:* Education (schools that receive federal funds)
- *Securities and Exchange Commission's Regulation S-P:* Financial services
- *Cable Communications Policy Act of 1984:* Cable operators
- *Video Privacy Protection Act:* Videotape service providers
- *Federal Information Security Modernization Act of 2014:* Federal agencies and third-party contractors
- *Office of Management and Budget Cybersecurity Mandates:*[39] Federal agencies

37 Fitch, Elizabeth S., and Theodore M. Schaer, "The Year of the Cyber Breach," IADC Committee Newsletter, IADC Law, March 2015.
38 Klein, Sharon R., Jan P. Levine, Angelo A. Stio III, and Brian R. Zurich, "How to Avoid and Respond to a Cybersecurity Breach," Pepper Hamilton, September 11, 2015.
39 Walker, Molly Bernhart, "New OMB Cybersecurity Plan Plots Quick Deadlines for Agencies," FierceGovernmentIT (www.fiercegovernmentit.com), Questex, November 2, 2015.

Appendix 1: Regulatory Overview

Other broader regulations include:

- *Federal Trade Commission Act, Section 5:* The FTC uses this provision to give itself wide berth in prosecuting "unfair" data security and privacy practices.
- *Other FTC Authority Statutes, including the Fair Credit Reporting Act and the Children's Online Privacy Protection Act:* The FTC applies a combination of 60 different sets of laws to pursue security and data privacy violations.

3. Case Law

Case law continues to impact the cybersecurity framework.

4. Frameworks and Tools[40]

FTC "Start with Security": To avoid an FTC violation, companies should implement the FTC "Start with Security" model rules.

NIST: The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is a response to an Executive Order from President Obama related to protecting critical infrastructure sectors. It has become a de facto standard of care and can serve as a place to turn amid the confusing patchwork of existing regulations.

ISO 27001 Certification: Becoming International Organization for Standardization (ISO)-certified indicates achieving a higher standard of cybersecurity expertise. The process includes a "risk assessment, impact analysis, updated controls and policies, as well as audits."[41]

Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool: The FFIEC has created a Cybersecurity Assessment Tool to help financial institutions gauge cyber preparedness and mitigate cyber risk.[42]

40 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
41 Silverstein, Ed, "Goodwin Procter Latest Am Law 100 Firm to Earn ISO Security Certification," *Legaltech News*, ALM Media, October 28, 2015.
42 "FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors," June 2015.

Appendix 2.1: Best Practices

Best Practices to Follow to Ensure Compliance with Due Care:[43]

Pre-Breach

1. Risk profile data

Figure out what the "crown jewels" are, including, but not limited to, confidential client information (personally identifiable information, protected health information and payment card information), trade secrets, IPO information, and M&A data. Classify the data, create a data map and enforce a usage policy for that data.[44]

Best Practice: Identify data crown jewels and only allow a limited number of people to access that data. Enforce usage policies for accessing the data.

2. Determine necessary data for business purposes

When doing a risk assessment, keep in mind what data is necessary to carry on the business, and what may be extra liability. For instance, collecting Social Security numbers when that is not a core element of the business may be an unnecessary risk.[45]

Best Practice: Identify confidential data necessary for business purposes and recalibrate, as needed, to remove data that is not necessary to maintain the business.

3. Implement discovery hygiene

The company should implement discovery hygiene relating to both physical and electronic information.

Best Practice: The legal department is best suited to implement a discovery hygiene policy, in conjunction with outside counsel or third-party consultants, to best preserve and protect required sensitive data, while also removing any non-requisite sensitive data.

4. Conduct a risk assessment to determine where sensitive data is in the system

Identify where this information lies and if it is at risk for exposure. For instance, does it lie in the same system as non-sensitive information?

Best Practice: Segment confidential data into separate systems and only allow access by a limited number of people who require that information.

5. Keep in mind that the data might be accessed from different types of devices

Determining where the data lies should include reviews of all devices that might have access to the data and the manner in which they can access the data – for instance, mobile phones, iPads and personal computers (either personal or company-owned).[46]

43 Stevens, Mark, "Raising a Digital Defense," *Law Technology Today*, American Bar Association, October 30, 2015; Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015; Hogan Lovells, "Cybersecurity: The Corporate Counsel's Agenda," November 15, 2012.
44 Mackay, Sheila, "How to Pass a Cybersecurity Audit in 10 Steps," Big Law Business, Bloomberg BNA, September 17, 2015.
45 Smith, Jordan, and Micah Lee, "Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege," The Intercept (theintercept.com), November 11, 2015.
46 Chickowski, Ericka, "Privileged Account Control Still Weak In Most Organizations," Dark Reading (www.darkreading.com), *Information Week*, November 11, 2015.

Appendix 2.1: Best Practices

Best Practice: Limit the number of access points to the confidential data from any device. Consider locking particularly sensitive data down to physical or restricted access only.

6. Encrypt sensitive data

Companies should encrypt valuable information to make it more difficult for outside parties to access or leverage.[47]

Best Practice: Encryption is first step to protect confidential information.

7. Implement good password hygiene

Use password management technology, such as second-factor identification, and train employees on password safety (such as changing passwords semi-frequently, protecting where passwords are stored, and using a standard of password difficulty) to make it more difficult for hackers or non-users to gain access to confidential information.[48]

Best Practice: Implement advanced password hygiene, such as second-factor identification and other technologies.

8. Develop an incident response plan and team

Companies should develop a cybersecurity plan replete with roles and responsibilities for team members and cybersecurity policies for the company and third-party vendors to follow. One person should be designated as the responsible party for the company's cybersecurity policy.[49]

Best Practices: The cybersecurity plan and team should be an initiative spearheaded by upper management and the board and provide for varied roles and functions, including the board, senior management, a dedicated cybersecurity team if applicable, IT, risk and compliance, the legal department, outside counsel, crisis services, and others.

9. Use technology to assist in preparing against cyber attacks

Technology helps and hinders cybersecurity — by enabling attackers to leverage advanced techniques to access systems, but also by enabling companies to implement more advanced controls against attacks. Companies can use technology, such as second-factor identification and creation of a fake data environment designed to catch cyber attackers, to better protect the company.[50]

Best Practice: Use technology where applicable to better protect the company against cyber attacks.

10. Use metrics to determine success of the cybersecurity policy and make changes as necessary

Big Data is an often-discussed tool for organizations to prove success. Analytics should be used in the cybersecurity context to help gauge success and improve performance.

47 Fadem, Steven, "How to Secure Data From Hackers," *Corporate Counsel*, ALM Media, November 10, 2015.
48 Second-factor identification is defined as follows: "In order to log in, you must have something you know (usually a password), as well as one additional factor, usually something you have (usually your cellphone) or something you are (usually a fingerprint or faceprint)." Solove, Daniel J. and Woodrow Hartzog, "Should the FTC Kill the Password? The Case for Better Authentication, 14 Bloomberg BNA Privacy & Security Law Report 1353 (2015), GWU Law School Public Law Research Paper No. 2015-33, GWU Legal Studies Research Paper No. 2015-33, July 27, 2015.
49 Mackay, Sheila, "How to Pass a Cybersecurity Audit in 10 Steps," Big Law Business, Bloomberg BNA, September 17, 2015.
50 "Future Prospects — Global Megatrends and Opportunities," Ponemon Institute, Raytheon, February 2015.

Appendix 2.1: Best Practices

Best Practice: Implement carefully considered data analytics to assist in gauging success and weak spots in cybersecurity preparedness.

11. Hire external specialists

Hire a specialist such as a data loss prevention security provider, cybersecurity experts to audit data security, network monitoring specialists, and third party consultants.

Best Practice: Determine where among the team there are weaknesses and look outside for third-party specialists to help fill those gaps.

12. Use outside counsel as necessary

Keep outside counsel on call to assist in planning cybersecurity policy and incident response.

Best Practice: There are a number of ways to use outside counsel. Outside counsel should be brought in the process pre-breach to help create the cybersecurity plan, and after the fact as necessary to determine the severity of a cyber breach and craft a breach response.

13. Train employees on cyber policies

Employees are one of the primary causes of data breaches, through mistakes or malicious access. One of the best ways to combat misuse of data by employees is by providing training on cybersecurity issues and responses.

Best Practice: Bring employees in early. Train employees on proper data governance and policy violations. Audit employees and practice "fire drill" situations to teach employees how to respond to a crisis in a simulated environment.

14. Retrain employees on a regular schedule

A one-off course on cybersecurity will not suffice. Companies should employ a periodic update of cybersecurity risk assessments and training.

Best Practice: Be proactive. Train and retrain employees using different media.

15. Ensure that third-party vendors comply with security policies

Third-party vendors should be vetted for cybersecurity practices and should uphold the company's stated cybersecurity policy. Vendors that do not comply should be removed from the company's Rolodex or should be given extremely limited and carefully watched access. Vendors with access to confidential data should also be subject to audits by the company.[51]

Best Practice: The legal department should ensure that third party vendors comply with cyber policies by putting risk-shifting language to that effect in their contracts and by maintaining audit rights.

16. Classify vendors according to access level, and maintain more stringent oversight over higher-risk vendors

51 Mukherji, JD, Aditi, "5 Ways In-house Counsel Can Improve Vendor Cybersecurity," In House, FindLaw Corporate Counsel Blog (lp.findlaw.com), February 4, 2014.

Appendix 2.1: Best Practices

Vendors should be classified by risk type (and since risk level may change, this should be a constant exercise), and be monitored based on risk level.

Best Practice: The legal department should own classification of vendor risk, given their input into contracting with third-party vendors.

17. Monitor networks

One way to determine if a security system has been breached is to monitor access to the system. Those monitoring the system should understand who should and should not have access and be able to determine when a non-user has accessed the system.[52]

Best Practice: Monitoring the system is one way to determine if there has been a breach to the system. The only way to effectively employ monitoring of the system is to risk-profile data, determine access rights and enforce those rights.

18. Keep up to date with local and federal regulations

Companies should look to current guidance locally and federally but should also keep abreast of recent developments in the law.

Best Practice: Use in-house counsel to tailor the response to current regulations, predict future regulations, and keep abreast of changing requirements. In-house counsel should bring in outside counsel and external specialists as necessary.

19. Use existing frameworks and tools

Companies should turn to existing frameworks and tools as a means of establishing due care. Frameworks such as the National Institute of Standards and Technology (NIST) have often been used as a test by regulators to determine if companies have established a minimum level of due care. The Federal Financial Institutions Examination Counsel (FFIEC) has also created a Cybersecurity Assessment Tool to help financial institutions gauge cyber preparedness and mitigate cyber risk.[53] As well, the FTC has developed 10 model recommendations based on its experience in handling cybersecurity.[54]

Best Practice: Incorporate frameworks and tools such as NIST, FFIEC, and the FTC "Start with Security" Recommendations, to improve cyber preparedness.

20. Purchase cyber liability insurance

Companies should purchase cyber liability insurance and also ensure that third-party vendors have cyber liability insurance. As this is still a burgeoning field, companies should risk-profile their assets and ensure that providers meet their requirements before finalizing which company and plan to purchase.[55]

52 Selby, Judy, and Austin P. Berglas, "Combating the Insider Threat," Big Law Business, Bloomberg BNA, October 2, 2015.
53 "FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors," FFIEC, June 2015.
54 "Start with Security: A Guide for Business," Federal Trade Commission, June 2015.
55 Privacy & Data Security Law Resource Center, "Views on Corporate Cybersecurity Insurance Options From Thomas H. Bentz Jr. of Holland & Knight LLP," Big Law Business, Bloomberg BNA, August 18, 2015.

Appendix 2.1: Best Practices

Best Practice: Purchase cyber-specific insurance, and ensure that third-party vendors use cyber insurance and have the company listed as a beneficiary.

21. Partner with other organizations and law enforcement

Discourse on cybersecurity with other organizations and law enforcement might help share potential threats, response strategies, and best practices. Further, it is often necessary to liaise with regulators in dealing with a cyber attack.[56]

Best Practice: In-house counsel might be best suited to address cybersecurity within the market and with regulators. In-house counsel, aware of the risks of divulging too much information on potential breaches, can get further information on how to craft a cybersecurity plan benchmarked against others in the industry.

Post-Breach

1. Tailor internal and external communications

Companies should communicate internally and externally with caution. Given the delicate balance of requiring disclosure by local or federal regulations, the importance of protecting privilege, and the potential for reputational harm, the company should tread cautiously when divulging a breach internally or externally.[57]

Best Practice: Communication might best sit within in-house counsel's wheelhouse, in conjunction with outside counsel, PR, marketing and other specialists, as they have the best understanding of the delicate nature of divulging a breach due to local and federal regulations, privilege, and potential reputational harm.

2. Treat a potential breach with caution – get forensics in early

It is critical that, in the early days of a potential breach, protocols allow for sufficient time to determine the access point of the breach, potential data loss, and identification of who breached the system.

Best Practice: Call in the experts immediately. Forensic experts should be designated and on-call pre- breach, for immediate mobilization in determining the extent of a breach.

3. Call in a pre-defined team to assist with breach management

Companies should have a breach response team on call, including crisis services such as forensics, PR, outside counsel and others. This team should be mobilized and ready to go with predefined tasks to follow in case a breach occurs.

Best Practice: This team should be defined and expansive, including the C-suite, the board, in-house counsel, cybersecurity business units, IT, compliance, risk management, forensics, PR, and outside counsel. The exact members will vary based on the company but should include a wide range of skills.

56 One law department interviewee reported having a group of industry peers on a cybersecurity email chain should questions or concerns arise.
57 "The Battle Continues: Bridging the Data Security Chasm: Assessing the Results of Protiviti's 2015 IT Security and Privacy Survey," Protiviti, 2015.

Appendix 2.2: Best Practices Checklist

Pre-Breach

- ❑ Risk profile data
- ❑ Determine necessary data for business purposes
- ❑ Implement discovery hygiene
- ❑ Conduct a risk assessment to determine where sensitive data is in the system
- ❑ Keep in mind that the data may be accessed from different types of devices
- ❑ Encrypt sensitive data
- ❑ Implement good password hygiene
- ❑ Develop an incident response plan and team
- ❑ Use technology to assist in preparing against cyber attacks
- ❑ Use metrics to determine success of the cybersecurity policy and make changes as necessary
- ❑ Hire external specialists
- ❑ Use outside counsel as necessary
- ❑ Train employees on cyber policies
- ❑ Retrain employees on a regular schedule
- ❑ Ensure that third-party vendors comply with security policies
- ❑ Classify vendors according to access level and maintain more stringent oversight over higher-risk vendors
- ❑ Monitor networks
- ❑ Keep up to date with local and federal regulations
- ❑ Use existing frameworks and tools
- ❑ Purchase cyber liability insurance
- ❑ Partner with other organizations and law enforcement

Post-Breach

- ❑ Tailor internal and external communications
- ❑ Treat a potential breach with caution – get forensics in early
- ❑ Call in a pre-defined team to assist with breach management

Appendix 3: Cybersecurity Trends to Monitor

Certain cybersecurity trends remain wild cards in the future market.[58] Based on this research, the following are trends to watch for.[59]

Cybersecurity Trends
1. Whether the role of in-house counsel or outside counsel will expand or contract
2. Whether companies will increasingly turn to third-party consultants or outside counsel to assist in cyber planning
3. Whether technology will help and/or hinder cybersecurity preparedness, by both detecting and responding to cyberthreats, and by creating cyber attacks with more advanced technology
4. How companies will use data analytics to measure and streamline data security
5. How machine learning will assist in predicting, understanding and protecting against cyberthreats
6. Whether companies will start using fake data security environments to catch cyberthreats
7. How cloud services will respond to and protect against cyberthreats
8. Whether backup and recovery will be streamlined as cybersecurity standards
9. The direction of the cyber-liability insurance market
10. Whether there will be tension between contract rights in risk-shifting provisions and federal and state regulations
11. Audit rights of third-party vendors
12. Whether federal and state governments will create more clear and concise regulations for cyber preparedness to remove some of the confusion around ensuring due diligence

Source: *Cybersecurity and Law Firms: Ignorance Is Risk*

58 *Future Prospects - Global Megatrends and Opportunities, Ponemon Institute*, sponsored by Raytheon, February 2015.
59 Goldman, Jeff, "Industry Experts Predict the Top Cyber Security Trends for 2016," ESecurity Planet, ITBusinessEdge, December 2, 2015.