ALM LEGAL INTELLIGENCE

Cybersecurity and Corporate Counsel: Ignorance is Risk

Brought to you by Infinite Spada

infinite·spada

EXECUTIVE SUMMARY

According to federal authorities and cybersecurity experts, the majority of big companies have been hacked and may not even be aware of the breach.[1] In fact, while the average total cost of a data breach has been estimated at $6.5 million, since 2014 there have been payouts into the billions of dollars (including Anthem at between $100 million and $16 billion, and JPMorgan Chase at $1 billion dollars).[2]

Faced with an uptick in cybersecurity attacks and potential costs, corporations and their legal departments are scrambling to implement policies and procedures to adequately prepare for this fast-moving, multi-dimensional threat, starting by both heightening preventive awareness and improving detection after the fact. Meeting the threat necessitates involving legal departments more deeply in the formation of policy and process from the outset.

Cybersecurity challenges are explored in depth in this research, including an overview of the current state of the cybersecurity landscape, the role of in-house counsel, company benchmarks, and analysis of where industries appear to be headed to meet current and impending threats. Also included is a set of tools to enable the adoption of cybersecurity best practices, an overview of the current regulatory environment, and a list of cybersecurity trends to monitor.

This research reveals why cybersecurity matters to each and every company and the ways companies and corporate counsel departments can prepare for and react to inevitable cyber attacks.

1 Walters, Riley, "Cyber Attacks on US Companies in 2014," The Heritage Foundation, October 27, 2014; According to cybersecurity expert Mikko Hyponnen, every single Fortune 500 company has been hacked. Slater-Robins, Max, "A Security Researcher Claims That All Fortune 500 Companies Have Been Hacked," *Business Insider*, October 26.

2 "2015 Cost of Data Breach Study: Global Analysis," IBM, Ponemon Institute, May 27, 2015; "Data Breaches," Identity Theft Resource Center (www.idtheftcenter.org).

ABOUT THE AUTHORS

Lead Author – Daniella Isaacson
Senior Analyst, ALM Legal Intelligence
Phone: *516-209-8240 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 Bachelors of Arts in international affairs (magna cum laude) from the George Washington University's Elliott School of International Affairs.

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.

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 industry trends.

RESEARCH METHODOLOGY

This report relied on a number of research avenues, including results of the ALM inaugural Corporate Counsel Cybersecurity Survey, and four weeks of one-on-one interviews with corporate counsel; law firm attorneys; and information security officers, consultants, and industry experts. This was supplemented by cybersecurity market research and the authors' practical knowledge from working in the legal industry. For purposes of this report, cybersecurity is defined as "whether and how electronic data and systems are protected from attack, loss or other compromise."[3]

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 corporate counsel survey. In total, ALM surveyed 369 companies on their cybersecurity practices.

For the corporate counsel survey, ALM Legal Intelligence collected survey information from 50 participants, the majority of whom identify as corporate counsel (69%). Industries represented included technology (29%), industrials (19%) and financial services (17%). The gross revenue of companies represented was predominantly (80%) above $2 billion – 40% noted their gross revenue was between $2 billion and $5 billion, while 40% noted that their gross revenue was greater than $10 billion. Interviews typically lasted 60 minutes and covered a range of topics related to cybersecurity preparedness, breach management, and the role corporate counsel and law firms play in helping manage these threats.

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

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

OVERVIEW

The Critical Hour: The Importance of Incorporating and Supporting Cybersecurity

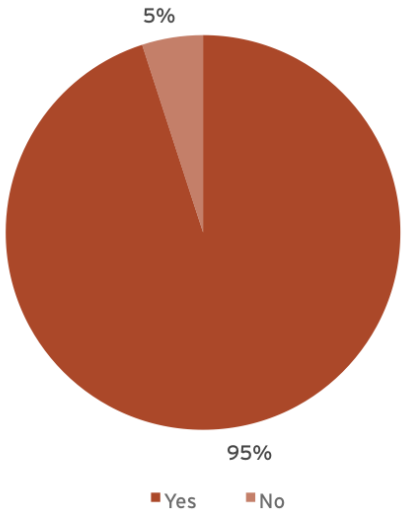
Cybersecurity is a top concern for corporate legal departments, but despite the cost and frequency of the threat, most executives do not believe that their companies are equipped to respond.[5] Moreover, many directors lack confidence in the GC's ability to oversee cyber risk.[6]

"There are two kinds of big companies in the United States. There are those who've been hacked...and those who don't know they've been hacked."

– FBI Director James Comey[4]

Corporations and law departments struggle with the opaque nature of the cybersecurity threat. Liability for breaches is wide-ranging, including financial, reputational and intellectual property costs, and financial liability often does not correlate with company size or the volume of breached records.[7] While the average total cost of a data breach is estimated at $6.5 million, this approximation is highly sensitive to the idiosyncrasies of particular breaches and is nearly impossible for companies to predict in advance.[8] Notable attacks since 2014 include Anthem (which cost the company between $100 million and $16 billion), JPMorgan Chase ($1 billion), Ashley Madison ($850 million), eBay ($200 million), and Home Depot ($80 million).[9] In worst-case scenarios, particularly relevant to the legal department, breach of trade secrets can result in a loss of more than four times the median cost of a payment card information breach.[10]

Do You Believe Cyber Attacks Are Increasing In Frequency?



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

Companies are not unaware of these risks. In fact, 95% of survey respondents agreed that cyber attacks are increasing in frequency (see graph). This awareness notwithstanding, most survey respondents and interviewees reported feeling uncomfortable with their company's ability to withstand a cyber breach.

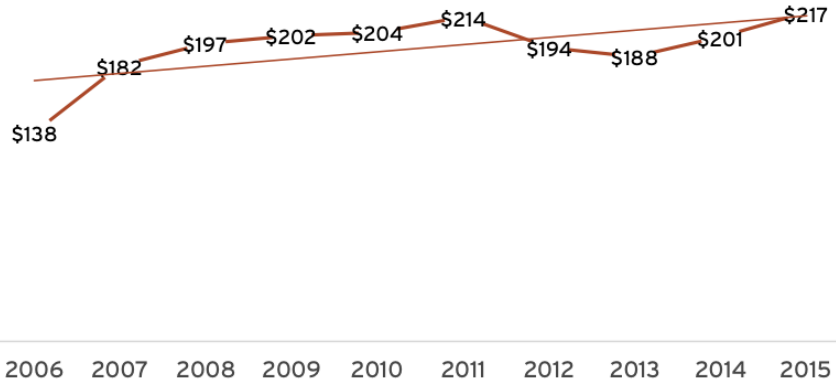
4 Walters, Riley, "Cyber Attacks on US Companies in 2014," The Heritage Foundation, October 27, 2014.
5 According to a recent survey, cybersecurity ranks as the "No. 1 worry for both directors and general counsel, with 90% of directors and 86% of GCs indicating that they are either extremely concerned or concerned about this issue." "Law in the Boardroom in 2015," Corporate Board Member, FTI Consulting, May 20, 2015; Mintzer, Rebekah, "Executives' Self-evaluation on Data Security: We're Coming Up Short," *Corporate Counsel*, ALM Media, November 12, 2015.
6 Less than 50% of directors were confident in the GC's ability to oversee risk. "Law in the Boardroom in 2015," *Corporate Board Member*, FTI Consulting, May 20, 2015.
7 "2015 Data Breach Investigations Report," Verizon Enterprise Solutions (www.verizonenterprise.com); "NetDiligence 2015 Cyber Claims Study," NetDiligence, September 2015 (netdiligence.com).
8 "2015 Cost of Data Breach Study: Global Analysis," IBM, Ponemon Institute, May 27, 2015.
9 "Data Breaches," Identity Theft Resource Center (www.idtheftcenter.org).
10 "NetDiligence 2015 Cyber Claims Study," NetDiligence, September 2015 (netdiligence.com).

OVERVIEW

The Critical Hour: The Importance of Incorporating and Supporting Cybersecurity

In the aftermath of these recent attacks and countless others, the global cybersecurity market is estimated at more than $100 billion and is projected to grow to more than $170 billion within the next five years, at a compound annual growth rate of 9.91%.[11] As can be seen in the chart at right, based on the 2015 Cost of Data Breach Study by Ponemon Institute and IBM, the average per capita cost of a data breach has risen dramatically since 2006 and is poised to continue to rise.[12]

Average Per Capita Cost of a Data Breach



Source: "2015 Cost of Data Breach Study: Global Analysis," IBM, Ponemon Institute, May 27, 2015

11 Harrison, Erin E., "Hackers Help Grow Cybersecurity Market to $170B by 2020," *Legaltech News*, ALM Media, August 28, 2015.
12 "2015 Cost of Data Breach Study: Global Analysis," IBM, Ponemon Institute, May 27, 2015.

OVERVIEW

Cybersecurity Threats

One reason for this growth stems from the fact that corporations have not gotten a good handle on how to manage the multitude of threats encompassed within cybersecurity.[13] As can be seen from the following table, companies must account for a wide array of threats in managing cybersecurity.

Potential Threats	Description
Data Volume and Location	Companies often keep confidential information on online or internal databases for convenience, which also makes it easy for attackers or malicious employees to access.[14]
Employee Error or Malice	Employees have been found to be a source of cyber risk due to errors or malicious intent (see graph).
Third-Party Vendors	Third-party vendors, including outside counsel, often pose an enormous risk to companies, both due to weak controls within their organizations and as an entry point to the company's systems (see graph).
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 (see graph below).
Hackers, Phishers, DDoS and Other Stealthy Lurkers[15]	Hacking is the single most frequent type of data breach, but all malicious threats pose a risk (see graph below).[16]
External Access	In the digital age of working from different devices and locations, including mobile and bring your own device (BYOD), accessing the system remotely from a variety of platforms creates security concerns.[17]
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.[18]
Lack of Resources	Lack of resources makes it more difficult for companies to adequately prepare against cyber threats, particularly for smaller organizations.[19]

Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

13 In 2014 alone, there were 783 recorded data breaches at companies from all industries, exposing over 85 million records including social security numbers, bank details, health information and credit cards. Hess, Amanda, "'Everything Was Completely Destroyed': What It Was Like to Work at Sony After the Hack," *Slate*, November 22, 2015.
14 Fitch, Elizabeth S., and Theodore M. Schaer, "The Year of the Cyber Breach," *IADC Committee Newsletter*, March 2015.
15 Hopkins, Curt, "A Definitive Guide to Hacking Terms," *The Daily Dot*, September 23, 2013.
16 Hackers were found to be the most frequent cause of loss (31%). "NetDiligence 2015 Cyber Claims Study," NetDiligence, September 2015 (netdiligence.com).
17 "2015 Data Breach Investigations Report," Verizon Enterprise Solutions (www.verizonenterprise.com).
18 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
19 "NetDiligence 2014 Cyber Claims Study," NetDiligence, December 2014 (netdiligence.com).

OVERVIEW

Cybersecurity Threats

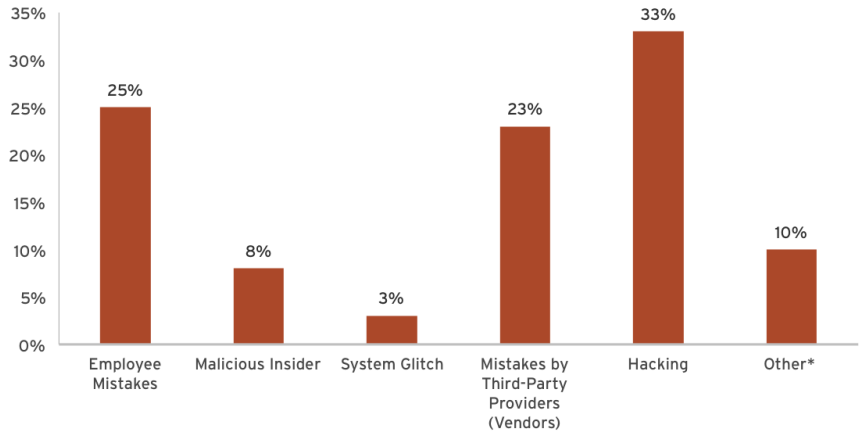
According to survey respondents, the top three risk areas are hacking (33%), mistakes by third-party vendors (23%) and employee mistakes (25%).

According to survey respondents, personal information represented 50% of breached assets, but financial information (38%) and health information (25%) were also reported to be heavily affected.

It is often difficult for companies to keep pace with the changing nature of cyber risk and the rising expenses necessary to protect the company.[20] This holds true particularly for smaller companies, which often do not have the resources or time to devote to cybersecurity, and have thus frequently been a target of cyber attacks.[21] In fact, companies with 250 or fewer employees accounted for 31% of cyber attacks in 2014.[22]

Further, unlike many other corporate risks, companies can be subject to multiple attacks over time.[23] As seen in the graph below, 84% of survey respondents who suffered a breach had suffered multiple ones.

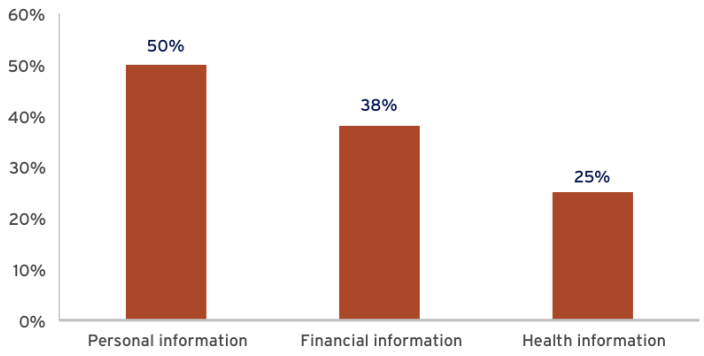
Believed to Be Primary Source of Data Breaches



*Other includes I don't know, multiple reasons, and phishing

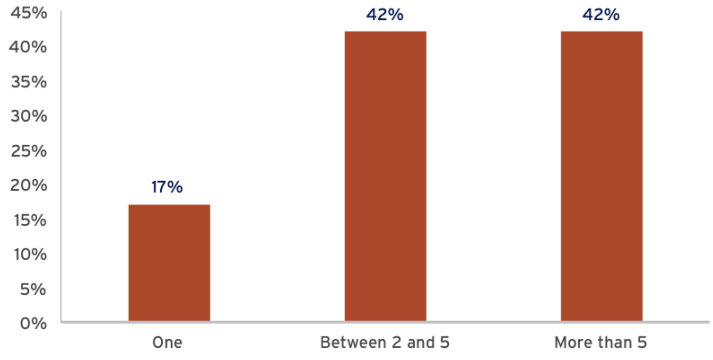
Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

Type of Information Stolen



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

How Many Breaches Has Your Company Experienced?



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

20 Warren, Zach, "Survey: Just 19% of Banks 'Highly Prepared' for Cyber Attack, Executives Say," *Legal Tech News*, ALM Media, September 30, 2015.
21 "NetDiligence 2014 Cyber Claims Study," NetDiligence, December 2014 (www.netdiligence.com).
22 Proppe, Jim, "Think Only Big Companies Get Hacked? Wrong," Thomson Reuters, April 14, 2015.
23 Moreover, in 60% of attacks, an organization is compromised within minutes. "2015 Data Breach Investigations Report," Verizon Enterprise Solutions (verizonenterprise.com).

OVERVIEW

Corporate Response to Cybersecurity

Companies have made headway in this fight against cyber threats, but many have a long way to go in achieving a level of comfort with their ability to counter an attack.[24]

While it is critical that companies achieve better cybersecurity preparedness, it is nearly impossible to develop a one-size-fits-all approach to cybersecurity.[25] The size of the organization, the number of data 'crown jewels,' the type of information, the level of industry risk, the business judgment of company leadership and many other factors all contribute to the risk tolerance level of the organization and reasonableness of cybersecurity standards.[26]

Even so, companies should strive to achieve a level of best practice that adequately prepares the company in case of crisis. For instance, in a 2015 IT Security and Privacy Survey, one-third of companies surveyed lacked policies for data governance, and 71% of respondents did not even understand their own data or which data was most sensitive.[27] This is a basic requirement of cybersecurity preparedness in any organization.

To best incorporate cybersecurity into the corporate DNA, the board and senior management should own the initiative and implement a top-down approach. It seems unlikely that this is being accomplished just yet. In a recent survey, only 28% of respondents indicated that there is currently a high level of engagement by the board, compared to 30% in the 2014 survey.[28] However, according to another recent survey, 69% of public company board members reported greater involvement with cybersecurity than they were one year prior and have expanded the budget on average by 22% to meet this growing threat.[29]

24 Harrison, Erin E., "Hackers Help Grow Cybersecurity Market to $170B by 2020," *Legaltech News*, ALM Media, August 28, 2015.
25 Some interviewees reported the creation of a dedicated cybersecurity team, but the placement of that team varied; typically it was a stand-alone business vertical, but in some instances, it was a team within the legal department, compliance and risk department, the board, or underneath the IT function.
26 More heavily regulated industries (such as healthcare and financial services) typically have higher data breach costs associated. "2015 Cost of Data Breach Study: Global Analysis," IBM, Ponemon Institute, May 27, 2015.
27 Harrison, Erin E., "Law Firms Lacking Cybersecurity Measures Have 'Significant Ground to Make Up,'" *Legaltech News*, ALM Media, October 1, 2015.
28 Harrison, Erin E., "Law Firms Lacking Cybersecurity Measures Have 'Significant Ground to Make Up,'" *Legaltech News*, ALM Media, October 1, 2015.
29 Harrison, Erin E., "Law Firms Risk Replacement as Boards Focus on Cybersecurity Policies," *Legaltech News*, ALM Media, November 4, 2015.

THE ROLE OF IN-HOUSE COUNSEL

While the final decision for cybersecurity role assignment and policies should lie with senior management and the board of directors, corporate counsel can and should be an integral part of a company's cybersecurity response.[30] According to experts, the question has largely shifted from whether or not in-house counsel should be involved at all to *when* the legal department should become involved.[31]

The key shift is from reaction to prevention and preparation. Companies often use corporate counsel post-breach, when it is clear that legal minds are required to ascertain next steps in preparing for litigation. However, excluding corporate counsel from the pre-breach preparation process is a missed opportunity. In-house counsel should be involved proactively and strategically, not just reactively and contractually. One corporate counsel interviewed noted that in-house counsel are primed to look for legal and compliance issues throughout the process, which business-focused minds may not see. Moreover, preparing the legal department pre-breach will make the post-breach process more efficient and less costly.[32]

In fact, if the company has not achieved a level of due diligence that internal counsel believes is sufficient, most interviewees felt it was appropriate for in-house counsel to make that argument to the board and own the process if necessary.

30 Hulme, George V., "Is the Board's Involvement in Cybersecurity Really That Critical?" *CSO Online*, November 12, 2015.
31 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
32 Ibid.

THE ROLE OF IN-HOUSE COUNSEL

Why Legal Has Not Been Invited to the Table

According to a recent study, one reason why the legal department might be underutilized pre-breach is due to confusion over role division. Some work divvied up to the IT, risk or compliance departments might actually be better suited to the legal department, given its enhanced understanding of local and federal laws and its privilege.[33]

Companies should right-source the cybersecurity workload to the appropriate functions as much as possible, whether through an internal process or by asking a third party to assist. The National Institute of Standards and Technology (NIST) framework also addresses this issue and separates cyber duties into three categories: technical, managerial and operational. Companies struggling to divide roles might look to this framework for assistance.[34]

"The field of cybersecurity is so technical and changes so often, it is problematic to rely upon resources who do not have the appropriate technical background as well as the time to devote to staying current on the topic."

- Jason Straight, Senior Vice President and Chief Privacy Officer, UnitedLex

Another barrier to the legal department's involvement has been in-house counsel's level of comfort with the technical aspects of cybersecurity. When interviewed, Jason Straight, Senior Vice President and Chief Privacy Officer at UnitedLex, explained, "The field of cybersecurity is so technical and changes so often, it is problematic to rely upon resources who do not have the appropriate technical background as well as the time to devote to staying current on the topic." In a recent survey, only one-third of law departments reported being "moderately" or "slightly familiar" with the issue.[35] In another survey, two-thirds of GCs reported needing more information on cybersecurity risk, and about one-third reported not knowing the right questions to ask management about the company's IT/cybersecurity strategy.[36]

It is critical that the legal department receives sufficient training to be able to at least ask the right questions of other functions, or to know when to bring in outside forces.[37] Legal departments should invest in more resources and training, or hire outside counsel or consultants to assist in bridging this gap.

Similarly, lack of resources has been cited as a concern by some GCs. While the legal department may want to assist as much as possible, it may be difficult to devote resources to the fast-changing and complex world of cybersecurity preparedness, particularly since market cybersecurity resources are few and far between.[38] Short of hiring more specialized resources, legal departments should rely on outside counsel or third party consultants to bolster gaps in resources.[39]

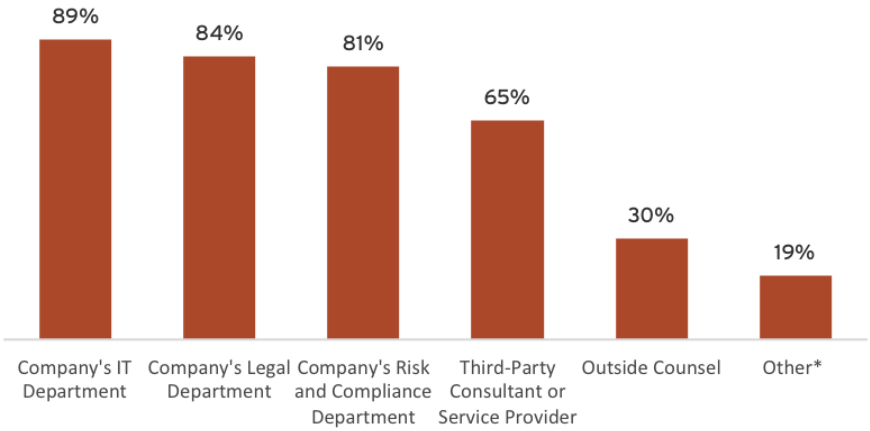
33 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
34 Ibid.
35 Ibid.
36 "Law in the Boardroom in 2015," *Corporate Board Member*, FTI Consulting, May 20, 2015.
37 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
38 Schlesinger, Jennifer, "This Career Field Has Thousands of Unfilled Jobs," Thomson Reuters, December 6, 2015.
39 "Consero July 2015 General Counsel Data Survey," Consero Group, July 17, 2015; Zurkus, Kacy, "Why Every CIO Needs a Cybersecurity Attorney," *CIO*, August 4, 2015; Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.

THE ROLE OF IN-HOUSE COUNSEL

Legal's Current Role

Reassuringly, there seems to be some movement toward bringing legal into the discussion. Survey respondents felt that second only to IT, the legal department was the most involved in creation of a formal information privacy and security risk assessment (84%).

People Involved In Security Assessment



*Other includes corporate security department, operational technology department, finance, HR, internal audit, store operations and I don't know (8%).

Source: ***Cybersecurity and Corporate Counsel: Ignorance is Risk***

THE ROLE OF IN-HOUSE COUNSEL

Vendor Management

One important cybersecurity task that falls to in-house counsel is vendor management.[40] In-house counsel are often in charge of contracts with vendors that shift risk away from the company. In this role, in-house counsel should strive to define the protected data in the agreement, detail the obligations of the vendor to protect the data, and specify the obligations in the event of a security breach.[41]

"Vendors that do not comply with ABC's cybersecurity and information security policies are not given access to any sensitive data and may be banned from working with the company entirely."

- Evan Farber, Chief Legal Officer, The Advisory Board Company

A critical component of this task is to ensure that vendors are vetted thoroughly and the company retains audit rights.[42] Evan Farber, Chief Legal Officer at The Advisory Board Company, stated that "vendors that do not comply with ABC's cybersecurity and information security policies are not given access to any sensitive data and may be banned from working with the company entirely."

Another task for the legal department is to push back on risk-shifting contracts *as a vendor*. In the words of one corporate counsel, risk-shifting provisions often trickle down to corporate law departments based on customers' more stringent cyber policies. It is the law department's job to ensure that the risk level and audit rights the company agrees to are reasonable and will not compromise its own security by giving clients too much access to internal systems.

"Outside counsel can fill in any lingering question marks in risk-shifting provisions. For instance, outside counsel can advise on how to structure contracts with different vendors and how others in the industry are structuring their contracts."

- Kristine Devine, Associate, Harris, Wiltshire & Grannis

For companies that outsource any internal functions (such as HR, or, particularly, IT), developing third-party contractor agreements that protect the company's data while allowing the third party to perform its job will be an ongoing challenge for legal departments. Any third-party contractors with access to sensitive data should be audited semi-regularly.[43] Some experts report that companies are now pulling back from outsourcing for fear of data and security concerns.[44]

Interviewees reported that the risk-shifting provision process slows down the sales cycle considerably but is vital. Deciding what information the company will and will not share to potential customers regarding internal security will continue to be a thorny issue for in-house counsel.[45]

Outside counsel can be a resource for the in-house legal department in drafting risk-shifting provisions. Kristine Devine, an associate at Harris, Wiltshire & Grannis, who specializes in communications and regulatory compliance, noted that "outside counsel can fill in any lingering question marks in risk-shifting provisions. For instance, outside counsel can advise on how to structure contracts with different vendors and how others in the industry are structuring their contracts."

40 Wilson, Donna L., Linda D. Kornfeld, and Rebecca Perry,"Data Security Best Practices for In-house Counsel," Association of Corporate Counsel, August 6, 2015.
41 Bloom, Michael L., Julian Bulaon, and Monica Steinberg, "Drafting Data Security Provisions: 3 Key Elements," *Corporate Counsel*, ALM Media, November 30, 2015.
42 Straight, Jason, "Get a Handle on Third-Party Cybersecurity Risks," *The Recorder*, ALM Media, July 8, 2015; Harrison, Erin E., "Law Firms Risk Replacement as Boards Focus on Cybersecurity Policies," *Legaltech News*, ALM Media, November 4, 2015.
43 Based on industry interviews.
44 Based on presentations at ASCEND: Elevate Your Cybersecurity Event at Bloomberg BNA.
45 Based on industry interviews.

THE ROLE OF IN-HOUSE COUNSEL

Cyber Plans, eDiscovery, Communication and Other Tasks

While contract review is a good start for the legal department's involvement in pre-breach preparation, one interviewee noted that, "If contract review is the only role for lawyers [in cybersecurity], the company is likely not in a great place in managing cybersecurity. Lawyers should be playing a much more strategic role than just contract drafting."

In-house counsel can play a critical role in drafting cybersecurity policy and as a member of the cybersecurity response team. Primarily, in-house counsel bring a perspective on risk that does not exist within other business units: they are aware of applicable laws that may need to be considered in drafting a policy and response.

Further, in-house counsel can and should be in charge of discovery hygiene.[46] Experts recommend focusing on both physical and electronic data in this exercise.[47] The legal department's understanding of discovery policies and concerns should set the tone for the organization on how to best address discovery internally. Through managing the discovery program, attorneys can also assist in accomplishing cybersecurity best practices, such as data mapping and ensuring that confidential information is segmented into different systems, helping the organization understand the location and scope of its data (See Appendix 2).[48]

Post-breach, in-house counsel, in conjunction with outside counsel and other experts as warranted, should be in charge of communication (depending on applicable state and federal regulations), to ensure regulatory compliance and to preserve privilege.[49] Communication tasks include gathering information on the breach and the data compromised, determining if notice is necessary, deciding which parties should be notified (including regulators and the public), determining when notice must be provided, and drafting and sending notices and communication regarding the breach.[50]

46 Sweeney, Marlisse Silver, "Corporate Counsel, Get Thee in Touch With Your Inner IT Director,"*Corporate Counsel*, ALM Media, November 12, 2015.
47 Wojcik, Christina, "Are Your Contracts Ready for a Cybersecurity Breach? From the Experts," *Corporate Counsel*, ALM Media, October 31, 2014.
48 Sullivan, Casey, "The Data That Isn't Used...," Big Law Business, Bloomberg BNA, October 20, 2015 (bol.bna.com).
49 Harrison, Erin E., "Law Firms Risk Replacement as Boards Focus on Cybersecurity Policies," *Legaltech News*, ALM Media, November 4, 2015.
50 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.

THE ROLE OF IN-HOUSE COUNSEL

Cyber Plans, eDiscovery, Communication and Other Tasks

In sum, the following are sample tasks for in-house counsel: [51]

Sample Tasks for In-House Counsel
Drafting the cybersecurity incident response plan and membership on the cybersecurity response team
Liaising with compliance, IT, the business units and the C-suite regarding regulatory compliance
Discovery hygiene and understanding the corporation's data
Creating a data retention policy that complies with local and federal regulations
Protecting sensitive data stored in the legal department, such as IT and M&A information
Communications internally and externally as a result of any breach
Management of risk-shifting provisions in contracts both as a vendor and for third-party vendors
Partnering with law enforcement and other companies to better understand cybersecurity best practices and benchmarking against others in the industry
Liaising with outside counsel and third-party vendors to determine contract provisions, pre-breach requirements and post-breach requirements, as well as to determine if a breach has occurred
Keeping tabs on changes in the law and educating the company on any changes
Taking action post-breach as regulations, laws and company policies require

Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

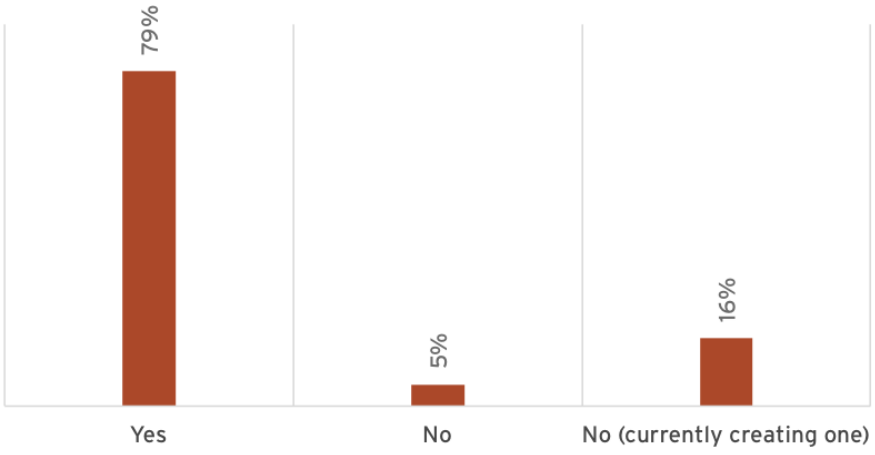
51 "Legal Departments Getting Proactive on Cybersecurity," *Corporate Counsel*, ALM Media, February 24, 2015.

FULFILLING DUE CARE

Utilizing Best Practices and Regulations in an Unclear Environment

Given cybersecurity's ambiguous requirements under state and federal law, fulfilling this requirement becomes more common sense than prescriptive. At the same time, there are certain baseline best practices, and some that are based on business-judgment decisions on risk and cost.[52] The bottom line is that it is necessary to embed an understanding of cybersecurity — the risk, response and action plan — within the corporation.[53] Appendices I and II detail some best practices and cybersecurity regulations to keep in mind in structuring a cybersecurity policy.

Company Currently Has Data Breach Plan In Place



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

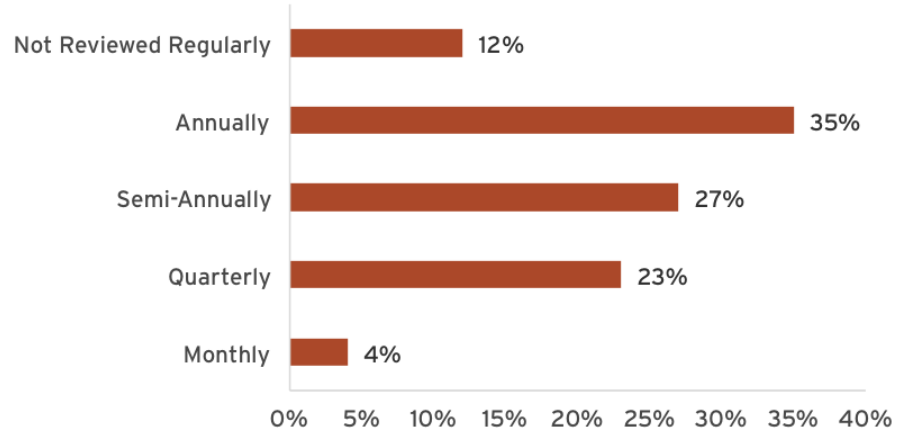
Benchmarking Best Practices

One important component of cybersecurity is benchmarking against peers. The following are some best practices that survey respondents reported were effective, and some that could be improved upon:

1. Cybersecurity plan in place

Seventy-nine percent of respondents currently have a cyber plan in place, and 16% are creating one. Only 5% do not have one and are not planning on creating one. While the number of companies that have a plan should be no less than 100%, 95% of repondents have analyzed and are in the process of implementing cybersecurity procedures.

How Often Is The Plan Reviewed Or Revised?



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

One area for improvement here is the frequency with which the plan is updated. Cybersecurity is a fast-changing field and problems do not remain static. Twelve percent of respondents do not review the plan regularly, and 35% only review the plan annually.

Further, only 67% of respondents reported that their plan identifies specific outside counsel to contact in case of breach. The cybersecurity plan and team should incorporate roles and responsibilities, including outside counsel.

52 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.
53 Hogan Lovells, "Cybersecurity: The Corporate Counsel's Agenda," Bloomberg BNA, November 15, 2012.

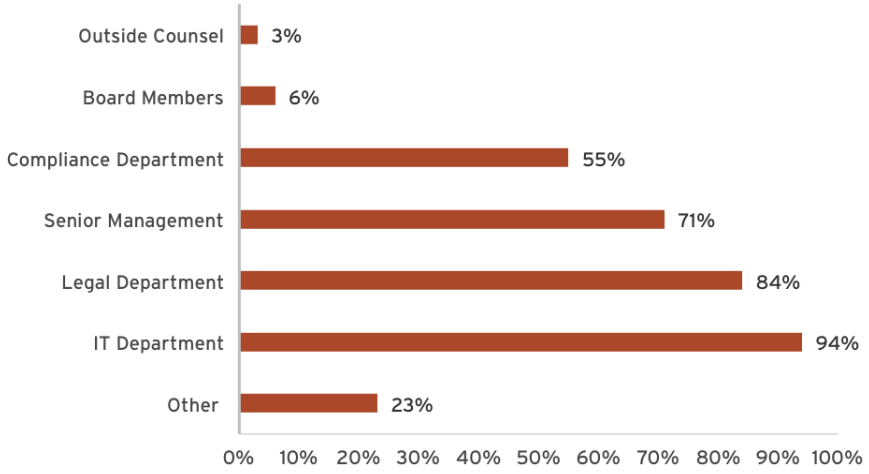
FULFILLING DUE CARE

Benchmarking Best Practices

Since cyber attacks move quickly, a lack of foresight can result in wasted time post-breach.

Similarly, companies should provide for a forensics expert in the plan. Eighty-six percent of respondents reported having a forensic partner. Having a crisis panel in place allows for faster mobilization in case of crisis and lowers crisis management costs.[54]

Team Representatives



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

2. Cybersecurity team in place

Eighty-two percent of respondents have a team or committee in place, suggesting that the majority of respondents have begun to create a cyber response with roles and responsibilities allocated.

While most teams comprise the IT department (94%), the legal department (84%), senior management (71%) and compliance (55%), only 6% involve the board and only 3% involve outside counsel. These data points suggest that cybersecurity teams are too limited in scope — and may fail to engage top-level organizational leadership and critical advisors.

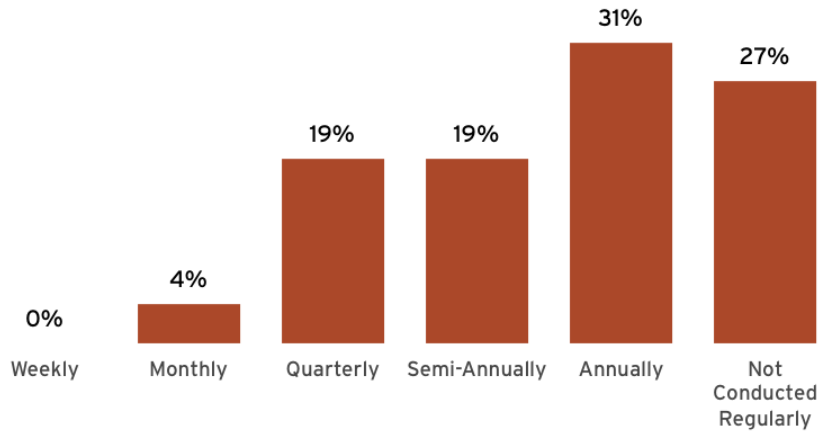
Other includes corporate security, HR, internal audit, I don't know, research and development, and manufacturing.

3. Training

Ninety-five percent of respondents reported training employees on processes and policies to prevent data breaches.

However, the practice of running "fire drills" — training employees on what to do in case of a real breach — leaves room for improvement. Most respondents (31%) stated that they perform drills annually, followed by "not conducted regularly (27%)." Companies should strive to implement fire drills more regularly, at least semi-annually if not more frequently.

How Often Company Conducts Fire Drills on Data Breaches



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

54 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

Benchmarking Best Practices

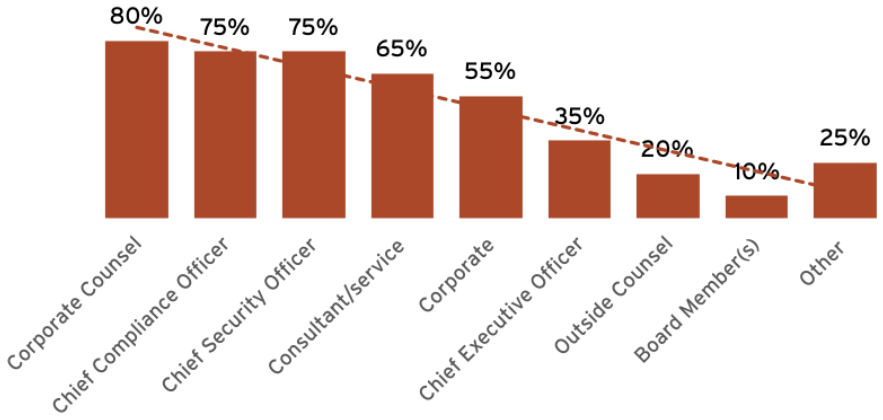
Moreover, the team members involved in fire drills should be much more robust. For instance, only 10% of respondents reported board member involvement. Since cybersecurity as a whole should be an initiative that rests with the C-suite and board, this number suggests that the fire drill training is lacking upper-management buy-in.

4. Using technology and cybersecurity experts

Should the company feel that it is lacking in cybersecurity expertise, companies can implement technology and hire internal or external vendors to address cyber gaps.[55] Respondents noted that they most often increase readiness to potential breaches by increasing technology investments (73%) and hiring more internal IT staff (62%).

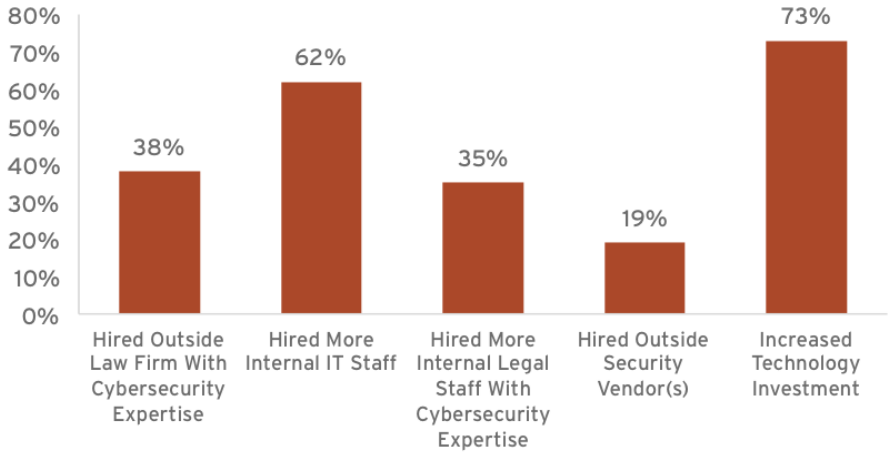
However, only 35% hired more internal legal staff with cyber expertise, and only 38% hired outside law firms with cyber expertise. Companies with a high-risk profile should reexamine whether to invest in more internal or external legal staff focused on cybersecurity.

Who Is Involved When Fire Drills Are Conducted?



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

How Has Your Company Increased Its Readiness In Handling Potential Security Breaches?



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

55 "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

Benchmarking Best Practices

5. Audits

Ninety percent of survey respondents agreed that the company performs formal information privacy and security risk assessments.

6. Liaise with regulators

Thirty-six percent of respondents have not yet identified or documented the regulatory bodies that will likely be involved in a data breach, suggesting room for improvement.

Further, after experiencing a breach, only 64% of respondents notified regulators about the breach. Regulators left out of the loop are far more likely to react negatively when news of a breach reaches them, especially if notice comes from a source other than the company itself.

7. Liaise with the public

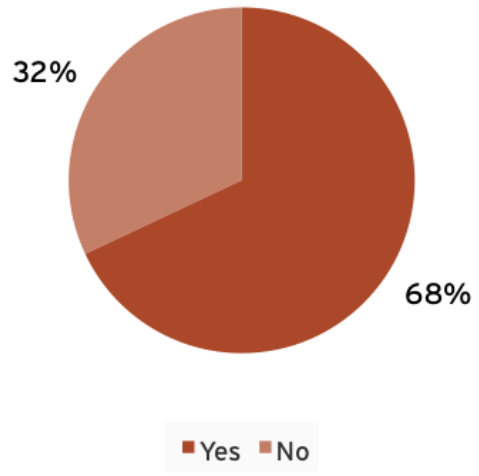
Similar to the best practice of notifying regulators, another best practice, and often a requirement, is notifying the public. After experiencing a breach, 73% of respondents have not notified their customers or the general public.

8. Cyber liability insurance

Only 68% of respondents have purchased cyber liability insurance. This area calls for some improvement. Companies should buy stand-alone policies from a cyber insurance provider and ensure that the provider meets the company's requirements for coverage. Since this field is rapidly changing, it makes sense to shop around and consult different providers before purchasing.[56]

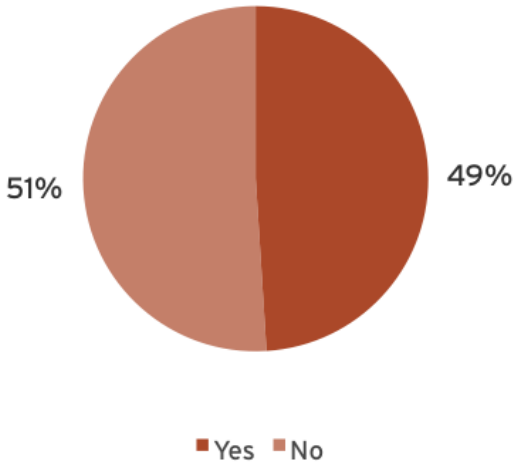
Organizations should also ensure that third-party vendors add them as a beneficiary to their cyber insurance. Only 49% of respondents ensured that third parties even carry cyber liability insurance.

Company Purchased Cyber Liability Insurance



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

Do You Require Third Parties to Carry Cyber Liability Insurance?



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

56 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 (bol.bna.com); Interviews with industry experts.

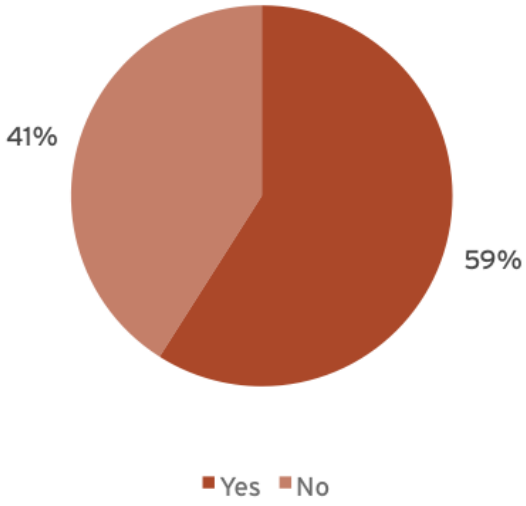
RELATIONSHIP WITH OUTSIDE COUNSEL

Outside counsel's relationship with in-house counsel is a tenuous partnership when it comes to cybersecurity. Outside counsel is often a tool in managing cybersecurity but can also be a potential security weakness, given that such third-party vendors have access to some of the company's most sensitive information and trade secrets, including patent applications, deal memos, M&A information and strategy memos.[57]

Outside Counsel as a Data Weak Spot

According to Mandiant, a cybersecurity firm, 80 of the 100 biggest law firms in the US have experienced a data breach since 2011.[58] Citibank, too, has cautioned, "It is reasonable to expect law firms to be targets of attacks by foreign governments and hackers because they are repositories for confidential data on corporate deals and business strategies."[59] Further, only 59% of survey respondents felt comfortable with outside counsel's ability to withstand a cyber attack.

Comfortable With Outside Counsel's Ability To Withstand A Cyber Attack



Source: *Cybersecurity and Corporate Counsel: Ignorance is Risk*

Law firms will likely continue to be a source of data-breach targeting, given their hold on confidential client information, but what should give in-house counsel pause is whether law firms are concerned with incorporating cybersecurity. In a recent survey, more than 80% of survey respondents from large firms did not know if the firm had cyber insurance, 52% of respondents did not know if a client had ever asked for a security audit of the firm, and the majority of respondents did not even know if the firm had ever had a security assessment by a third party.[60] Further, a Chase Cost Management survey reported that Am Law 200 firms rarely spend more than 1.9% of gross annual revenue on information security, and almost half of respondents reported that spending on security was insufficient.[61]

Law firms might have a hard time incorporating cyber best practices into their DNA, since the security practices necessary are often the antitheses of the traditional law firm working environment. As a growing concern for clients, law firms have become better at addressing these issues, but they remain a potential weakness that in-house counsel must manage.[62] Some interviewees reported telling outside counsel that if they do not follow company protocols, they will cease doing business with them. Further, many financial institutions are requiring firms to fill out a questionnaire on cyber practices, while others are doing audits and even on-site inspections.[63]

57 Fadem, Steven, "How to Secure Data From Hackers," *Corporate Counsel*, ALM Media, November 10, 2015; Breedlove, Scott, "Protecting Trade Secrets in an Age of Cyber Insecurity," *Corporate Counsel*, ALM Media, November 3, 2015.
58 Simmons, Christine, "Cybersecurity Data Sharing Is Now Available to Law," *New York Law Journal*, ALM Media, August 19, 2015.
59 June, Daniel, "ABA Survey Exposes Law Firm Ignorance Over Information Security View Count: 995," *JD Journal*, October 21, 2015.
60 Friedman, Gabe, "ABA Survey: Data Breaches Rising at Large Firms," Big Law Business, Bloomberg BNA, September 23, 2015 (bol.bna.com).
61 Lopez, Ian, "'Tis the Season for Identity Theft: Considerations for Consumers and Legal Pros," *Legaltech News*, ALM Media, November 30, 2015.
62 "2015 Client Advisory," Citibank and Hildebrandt Consulting, December 2014.
63 Goldstein, Matthew, "Law Firms Are Pressed on Security for Data," DealBook, *Wall Street Journal*, March 26, 2014.

CANDIDATE SOURCING

Certain law firms attempt to avoid the conversation entirely by proactively proving that they have achieved a higher standard of cybersecurity, such as by becoming ISO-27001 certified.[64]

Law departments should also inquire as to whether law firms use a cloud provider and if they have security in place to protect information stored on the cloud. A recent LexisNexis survey found that three quarters of firms will likely use the cloud this year, and as one interviewee explained, most contracts with cloud providers do not provide damages for loss of trade secrets.[65] As such, law departments should press law firms as to whether the cloud provider has controls in place when handling sensitive information.

Outside Counsel as Cybersecurity Protector

When a breach occurs, outside counsel or a third party provider should be brought in to assess the damage and help the company decide next steps, in conjunction with the legal department. Seventy-three percent of respondents confirmed that outside counsel was engaged as a result of the breach.

While the relationship with outside counsel is generally focused on post-breach management and litigation, outside counsel should be brought in much earlier in the process to assist in preparing for a cyber attack and to help benchmark the organization against others in the industry. Outside counsel can help determine how best to devote time, resources and assets on cybersecurity initiatives; advise on risk-shifting provisions; educate the legal department on changing cyber regulations; and help decipher regulatory requirements in case of breach.[66]

Interestingly, most interviewees did not report using outside counsel with specific cybersecurity expertise. Rather, they turned to trusted law firm generalists for both cyber preparedness and breach response. Some outside counsel interviewed explained that their information security officer or technology staff is often on call to help bolster technical expertise in case a technical question arises.

64 Silverstein, Ed, "Goodwin Procter Latest Am Law 100 Firm to Earn ISO Security Certification," *Legaltech News,* ALM Media, October 28, 2015.
65 Ciccatelli, Amanda, "The Law Society Warns UK Law Firms about Cloud Computing Risks," *Inside Counsel*, ALM Media, April 10, 2014.
66 Interviews with industry experts.

CONCLUSION

The Future of Cybersecurity

Corporations and law departments must do more to ensure they are as protected as much as possible in the event of a breach. The cybersecurity threat to corporate financial, reputational and IP interests continues to rise, but most companies have not yet successfully implemented a top-down, proactive cybersecurity plan or response.

While cybersecurity readiness and best practice specifics vary by industry and jurisdiction, the bottom line is that companies need to embed cybersecurity practices into their corporate DNA. To do so, cybersecurity initiatives should start with the C-suite and bring in different functions and outside parties — notably, the legal department, compliance and risk management functions, technology leadership, outside counsel, and consultants and third-party advisors. As for when to involve the legal department in cybersecurity, the answer is, "As early as possible." Legal departments can and should be playing a more strategic and proactive role in cybersecurity programs and processes.

As companies become more adept at risk planning for cybersecurity and as regulations mature, ambiguity around best practices and how to manage confusing regulatory mandates will resolve. However, the dynamic nature of the current threat landscape illustrates that there will always be new trends to monitor (see Appendix 3). Companies must continue to update policies and processes to ensure they are constantly confronting and defending against this evolving threat. Proactively preparing for and responding to cybersecurity will continue to be a critical concern for in-house counsel and the broader organization for the foreseeable future.

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.[67]

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[68]

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:*[69] Federal agencies

67 Fitch, Elizabeth S., and Theodore M. Schaer, "The Year of the Cyber Breach," IADC Committee Newsletter, IADC Law, March 2015.
68 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.
69 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[70]

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."[71]

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.[72]

70 Hanover Research, "The Emergence Of Cybersecurity Law," Indiana University Maurer School of Law, February 2015.
71 Silverstein, Ed, "Goodwin Procter Latest Am Law 100 Firm to Earn ISO Security Certification," *Legaltech News*, ALM Media, October 28, 2015.
72 "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:[73]

Pre-Breach

1. Risk profile data

Figure out what the "crown jewels" implement discovery hygiene - -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.[74]

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.[75]

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).[76]

** Denotes a task that may best lie under in-house counsel's purview*

73 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.

74 Mackay, Sheila, "How to Pass a Cybersecurity Audit in 10 Steps," Big Law Business, Bloomberg BNA, September 17, 2015.

75 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.

76 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.[77]

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.[78]

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.[79]

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.[80]

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.

** Denotes a task that may best lie under in-house counsel's purview*

77 Fadem, Steven, "How to Secure Data From Hackers," *Corporate Counsel*, ALM Media, November 10, 2015.
78 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.
79 Mackay, Sheila, "How to Pass a Cybersecurity Audit in 10 Steps," Big Law Business, Bloomberg BNA, September 17, 2015.
80 "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.[81]

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*

** Denotes a task that may best lie under in-house counsel's purview*

81 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.[82]

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.[83] As well, the FTC has developed 10 model recommendations based on its experience in handling cybersecurity.[84]

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.[85]

** Denotes a task that may best lie under in-house counsel's purview*

82 Selby, Judy, and Austin P. Berglas, "Combating the Insider Threat," Big Law Business, Bloomberg BNA, October 2, 2015.
83 "FFIEC Cybersecurity Assessment Tool Overview for Chief Executive Officers and Boards of Directors," FFIEC, June 2015.
84 "Start with Security: A Guide for Business," Federal Trade Commission, June 2015.
85 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.[86]

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.[87]

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.

** Denotes a task that may best lie under in-house counsel's purview*

86 One law department interviewee reported having a group of industry peers on a cybersecurity email chain should questions or concerns arise.
87 "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

** Denotes a task that may best lie under in-house counsel's purview*

Appendix 3: Cybersecurity Trends to Monitor

Certain cybersecurity trends remain wild cards in the future market.[88] Based on this research, the following are trends to monitor.[89]

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 cyber threats, 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 cyber threats
6. Whether companies will start using fake data security environments to catch cyber threats
7. How cloud services will respond to and protect against cyber threats
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 Corporate Counsel: Ignorance is Risk*

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