FISH.
FISH & RICHARDSON

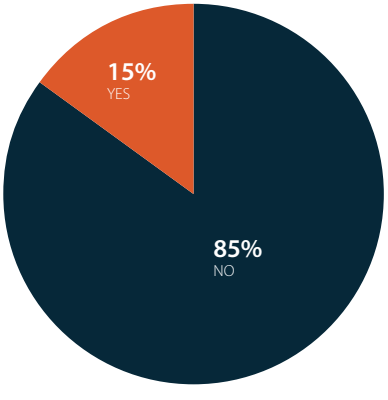
ALM-FISH & RICHARDSON SURVEY SHOWS COMPANIES STRUGGLING TO PREPARE FOR CYBERBREACHES, DESPITE EXECUTIVE SUPPORT

In September 2015, ALM Marketing Services and Fish & Richardson conducted an online survey of in-house counsel to gain insight into the current state of U.S. corporate involvement and preparedness for cybersecurity events. The results show that, while the C-suite and board of directors support a culture of security, there is still a lot of work to be done.

Disconnect between buy-in and action

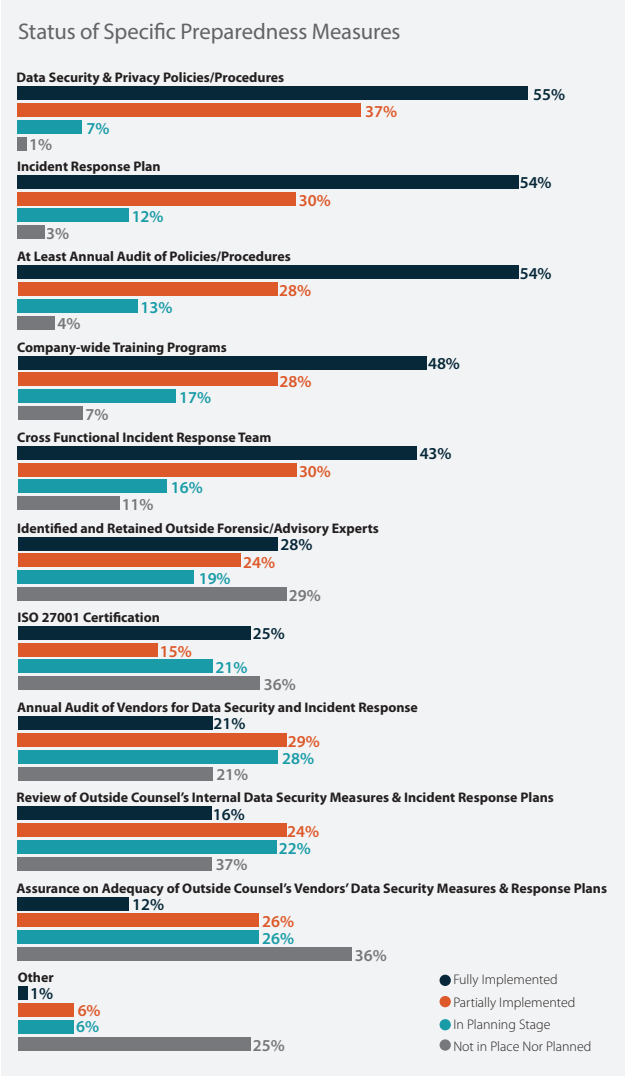
While data breaches are in the news almost every day, only about 15% of those surveyed report a significant cybersecurity incident or data compromise over the past 18 months.

Based on their experience, companies may perceive that the odds of an incident occurring are low, and therefore have not aggressively prepared. Yet, nearly half of the respondents reported having over $1 billion in annual revenues, with the average revenue across all respondents well over twice that amount. Over half of the respondents reported having global business interests. Although any company can suffer a breach, no matter its size, one would expect that large and global companies would be prepared for what some would call an inevitable breach.



Incidence of Cybersecurity Incident or Breach in Past 18 Months

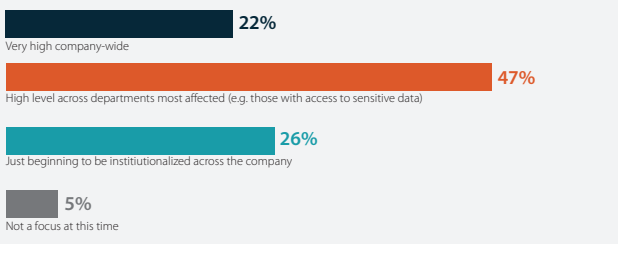
Respondents were given a list of ten specific preparedness measures that are considered best practices by cybersecurity experts. The results show that companies are not nearly as prepared as they should be. Only three measures have been fully implemented by at least 50% of respondents—(1) creating data security policies/procedures, (2) creating an incident response plan and (3) annually auditing policies/procedures. Even though most companies know by now to put these policies in place, approximately a third of respondents reported only partially implementing these measures. Policies are not fully effective unless employees know what they are and how to follow them, but less than half of respondents have fully put company-wide training programs in place. Near the bottom of the list, only 21% of respondents have implemented an annual audit of vendors for data security and incident response, one of the most critical components of an effective preparedness plan.



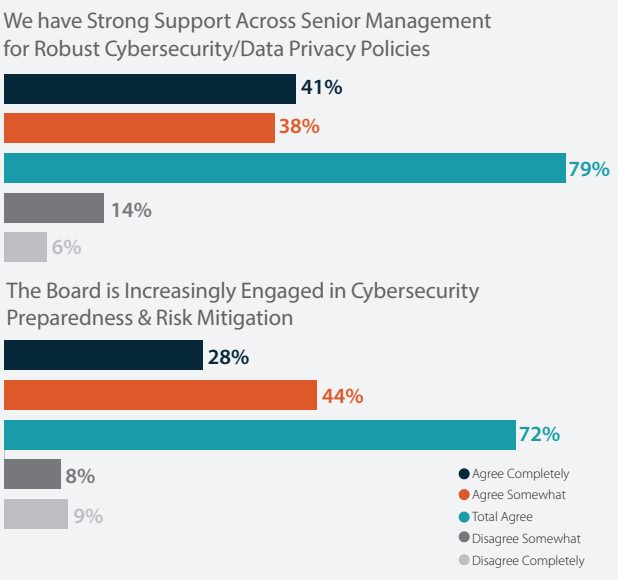
Companies that hold any type of valuable information typically receive two key pieces of advice from cybersecurity experts. The first is not to wait for the breach. It is likely that a crisis will hit eventually, so companies should prepare in advance when they are in a calm mode. Most respondents have not fully implemented the best practices above, and will end up scrambling to manage a breach.

The other piece of advice is to start at the top. Protecting the company from cyberbreaches and privacy invasions requires vigilance at every level. Resources must be allocated and attention must be paid. These requirements will only take place should leadership—and this means the C-suite and board of directors—buy in.

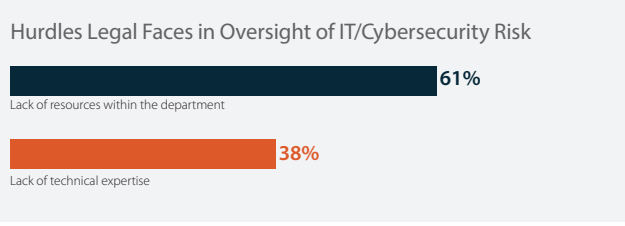
The good news is that, for the most part, they have. More than two-thirds of respondents claim that the level of instilled culture of security is either very high company-wide (22%) or at least high across the most affected departments (47%).



As further evidence, 79% of respondents agree that their company has strong support across senior management for robust cybersecurity/data privacy policies and 72% believe that their boards are increasingly engaged in cybersecurity preparedness and risk mitigation.



So why is actual preparedness so weak if management buy-in is so strong? Cyber-preparedness can be overwhelming. Over 80% of respondents said the volume and variety of data privacy laws and regulations makes compliance extremely difficult. The risks are constantly changing and the problems are difficult to address, often creating "analysis paralysis." Not only does this diminish the sense of urgency, but without a specific plan, it can be hard to marshal resources. In fact, when respondents were asked about what hinders their department's oversight of and involvement in IT/cybersecurity risk, the leading response by far was lack of resources.



How should the office of general counsel respond?

The results of the ALM-Fish & Richardson Survey Report on U.S. Companies Cybersecurity Preparedness show that companies want to be prepared, but actually aren't. What can in-house counsel do to fix this gap?

1. Allocate resources. While time and effort of employees will account for most of the resources required for a preparedness program, a budget is necessary for technology, consultants and outside counsel. Start by contacting experts to get a general estimate of what it may cost to build a program. Ask them for help in estimating what internal resources will be required. Make sure the C-suite and board of directors commit to provide needed internal and external resources.

2. Form a privacy committee. A critical early step is the formation of a cross-functional privacy committee. Legal, Security and IT should be represented, but the committee should also include representatives from other departments that handle data, such as sales, marketing, customer support, and research and development. It may make sense to have outside counsel represented as well. The committee should meet regularly (perhaps monthly). If a company has a Chief Privacy Officer, that person is an obvious choice to chair the committee. Otherwise, the Chief Information Security Officer or a knowledgeable representative from the legal department might be chosen.

3. Identify data collected and how it is handled. Almost all departments collect data, and there needs to be a uniform mechanism for knowing what is collected, where it is located, who can access it and how it is transferred, stored and destroyed. Typically, representatives from each department should be interviewed to obtain this information. The privacy committee should review the results with the IT team to ensure it is aware of all intra-company activities.

4. Identify what risks are posed, both internally and externally. Once the nature and handling of data is determined, the next step is to identify potential risks. Risks can be internal or external. Internal risks are often overlooked but they are one of the most common reasons for data breaches. These risks include rogue employees, file folders kept in open unlocked areas, lost laptops and mobile devices, collection of unnecessary data, and storage of data for longer than necessary.

External risks are what many people think of when they hear about data breaches. These risks expose a company's network to hackers and other bad actors, including through the use of soft passwords, unchanged passwords, unencrypted data and security flaws.

Companies must also focus on the risks posed by third party vendors that maintain their data. With the increasing rise of breaches due to vendor relationships, companies must do more than simply get a contractual promise that the vendor will keep their data secure. Appropriate due diligence should be conducted to ensure that vendors have, and will maintain, appropriate security standards and practices. Companies should seek the contractual right to audit their vendors. They should verify that vendors have adequate insurance in place to cover a data breach. Finally, vendor contracts should be reviewed regularly as technology and other risks change frequently.

5. Patch security holes that are identified. Once the internal and external risks have been identified, a plan must be developed to mitigate those risks. While a technology fix may be required—such as improving encryption technology or intrusion detection systems—many problems can be solved by clearly articulating and enforcing some basic policies. For example, a common security risk arises when employees email documents to their personal email accounts, which removes all of that data from the company's secure environment. Simply establishing and communicating a policy that such actions are not permissible will help. Again, vendors must be included if the risk assessment reveals security risks with vendor systems or the interaction of such systems with the company's own systems.

6. Put policies in writing. Establishing a security policy is not enough. The policy must be written and appropriately distributed. The policy should cover internal security practices, internal privacy practices, and incident response. If the company maintains a website and interacts with the public, there should be a separate externally facing privacy policy.

One policy that should be built early on is the breach response plan. Even the best security is not 100% effective, so it is critical to plan in advance how to respond. The plan should include who is in charge and who is on the response team (legal department, outside counsel, privacy office, forensics team, public relations etc.). The plan should also include the necessary steps to comply with relevant laws and regulations, including breach notification laws. Companies don't want to start reviewing and deciding how to comply with 47 different state breach notification laws in the midst of a breach. There may be other notifications where time is of the essence, such as those required under insurance policies. Having this plan in place will go a long way to easing the anxiety of and pressure on those dealing with the breach.

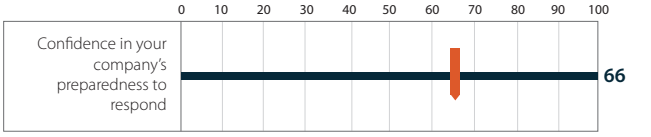
7. Educate, train and monitor. Companies should create a culture of employee accountability when it comes to privacy and data security. Again, this is a place to leverage management's buy-in as a message "from the top" which will carry greater weight with employees. All involved employees should be formally trained on the policies. At the same time, penalties for mistakes should not be so severe as to impede the reporting of potential incidents (e.g., if employees are at risk of getting fired if they lose a flash drive, they may not report the incident).

Once policies are in place and employees are trained, an ongoing monitoring protocol should be put in place. Some of the elements can be simple, such as requiring managers to walk through their areas at the end of the day to ensure data is locked down, properly disposed of, etc. The IT department should be using sophisticated tools to monitor their network. They should know if someone, for example, copies an entire hard drive to a personal device and they should use these tools to keep everything in check.

8. Revisit at least once a year. The privacy committee should remain in place and regularly meet in order to periodically review policies and any incidents, and ensure the policies are actually being followed and enforced. A formal review of all policies and practices (indeed, almost a repeat of all of the above steps) should be conducted at least annually.

Conclusion: Action needed to leverage management support

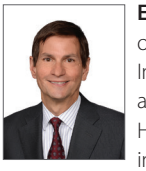
Despite the fact that there seems to be a large gap between management buy-in and actual company-wide action, most survey respondents are confident, on average, in rating their companies' preparedness at 66 out of 100. Yet, considering the other responses on the survey, a deeper review internally may show that they are not as prepared as they think.



Data breaches are on the rise and can cause significant harm including interrupted business, regulatory penalties, class action lawsuits and intellectual property theft. Although cybersecurity preparedness can seem overwhelming, it can be tackled through a methodical step-by-step approach—and it should not be delayed.

ABOUT THE AUTHORS:

Donna Balaguer is a Principal in the Washington, DC office of Fish & Richardson. She is a member of the International Association of Privacy Professionals and a Certified Information Privacy Professional (CIPP/US). She advises clients on the full range of privacy and data security laws and best practices, from the early stages of developing a privacy plan to handling a breach. She served as in-house counsel in the technology sector and has the technology savvy needed to navigate complex cybersecurity issues. She advises clients across multiple industries, including hospitality, healthcare, media, communications, manufacturing and retail.



Ed Lavergne is a Principal in the Washington, DC office of Fish & Richardson. He is a member of the International Association of Privacy Professionals and a Certified Information Privacy Professional (CIPP/US). He advises clients on data security and privacy issues including geo-location tracking, online behavioral advertising, data breach and incident response planning, internal data security and privacy policies, and external privacy statements. His clients include media and entertainment companies, book publishers, hotels, resorts and casinos, colleges and universities, and non-profit organizations.

ABOUT THE FIRM:

Fish & Richardson is a global patent, intellectual property (IP) litigation, and commercial litigation law firm with more than 400 attorneys and technology specialists across the U.S. and Europe. For more information, visit **www.fr.com**.