CORPORATE COUNSEL

An ALM Website

corpcounsel.com | June 2, 2016

5 Steps to Better Prepare for a Cyberbreach

From the Experts

Donna Balaguer

Is your company feeling pressured by the near daily barrage of news about the latest cyberbreach or other compromising data hack? Gone are the days when only the IT department was tasked with worrying about and managing cyber risks. Senior management can no longer shrug their shoulders when IT employees speak in a technical language they cannot follow, and hope that appropriate security measures are in place.

The good news is that more companies are making cybersecurity a top priority companywide. My firm recently conducted a survey of in-house counsel which showed that executives and boards are increasingly engaged in cybersecurity preparedness and risk mitigation. The bad news is that many find the actual task of getting prepared daunting.

The survey asked in-house counsel to rate the level of senior management and board of director support for cybersecurity preparation, and to specify hurdles to cybersecurity implementation and oversight. More than two-thirds of respondents claim the level of instilled culture of security is either very high companywide (22 percent) or at least high across the most affected departments (47 percent). In addition, 79 percent of respondents agree that their company has strong support across senior management for robust cybersecurity/data privacy policies, and 72 percent believe that their boards are increasingly engaged in cybersecurity preparedness and risk mitigation.

Yet, even with this high level of support, the results also showed that most companies – including those with over $1 billion in annual revenue and global operations – are not sufficiently prepared for a cybersecurity event or data compromise. The survey evaluated 10 cybersecurity preparedness measures, and only three of those measures (creating data security policies/procedures, creating an incident response plan and annually auditing policies/procedures) were fully implemented by at least half of the respondents. Other critical measures, such as developing companywide training programs and annually auditing vendors' data security practices, have not yet been fully implemented by at least half of the respondents.

So why do companies say they are committed to cybersecurity, yet fail to adopt the best practices to achieve it? Lack of resources and lack of technical expertise were cited as two main issues hindering the legal department's oversight of, and involvement in, cybersecurity risk. In addition, over 80 percent of respondents said the volume and variety of data privacy laws and regulations make compliance extremely difficult.

Cybersecurity preparedness can certainly feel overwhelming. The U.S. has a myriad of federal and state laws governing data security and privacy issues, and understanding which ones apply to your company is challenging. Companies with international operations need to understand that many country-specific laws may apply. The security landscape is complex, and in-house counsel need to develop a working knowledge of the technical issues in order to effectively participate in cybersecurity conversations.

The key to making all this manageable is to break it down into concrete steps and develop a written cybersecurity plan that addresses each step. The plan should be a living document. Given the constant changes in the laws, best practices, security measures and more, the plan must be routinely reviewed and updated.

As you develop your plan, make sure to follow these five practices:

1. Know what data you are collecting and how the company takes care of that data. This means polling all relevant departments in the company, including reviewing the paper and electronic systems and methods that employees in those departments use. Sometimes, particularly in the federal government, this is called completing a privacy impact assessment (PIA), which is a useful tool to analyze how data is collected, used, shared, maintained and destroyed. Companies often mistakenly take a limited view of the data that should be included in the PIA. They may think only about high-profile customer data like credit card numbers or other information that might be considered personally identifiable information (PII). But companies need to protect not only the data they collect from third parties like customers, but also their own data, including employee records and trade secrets and other intellectual property.

2. There is no such thing as too much oversight of your vendors. Data breaches by vendors are common. Your company is likely to shoulder the blame in both the public's and government's eyes if the vendor has a breach involving data collected by or on behalf of your company. But it can be difficult to control the execution of vendor contracts in a large company. Company employees negotiating the contract have other immediate objectives, such as procuring a needed product or service, and are often not thinking at all about the vendor's data security practices or interactions with company's systems. The company should create a written vendor policy, including mandatory data security language that must be included in all vendor contracts (without modification unless an upper-level approval is obtained). The language should include representations and warranties ensuring good data security practices, notification and indemnification requirements for breaches and insurance.

3. Consider obtaining an independent security assessment. Sometimes company employees are too close to, and too vested in, the systems they created to view them on a macro level. For example, perhaps the company has become lax on allowing employees to use third-party email services to transmit company data, or has not enforced a bring your own device (BYOD) security policy, because employees have resisted these measures as inconvenient to them. An objective security audit

will identify these gaps, which can then be brought to upper management's attention for resolution.

4. Take training to a new level. Many companies know they must train their employees on data security and privacy issues, but the training sessions are often inadequate and not reinforced on an ongoing basis. Don't take a one-size-fits-all approach. It only makes sense that employees who manage the security systems should have more in-depth, technical training. They, along with the parties identified in the company's breach notification plan, should participate in additional exercises, such as simulated drills on handling a breach. On the other hand, training for non-technical employees should not be so cluttered with technical jargon and details that the employee loses the overall message on how to comply with the company's cybersecurity plan. Another mistake companies make is to offer the training once a year, and then basically ignore cybersecurity at the employee level until the next year. There should be ongoing interaction with all employees, reminding them of good data security practices and updates to the cybersecurity plan.

5. The best offense is a good defense. When government security personnel are falling victim to "phishing" efforts, it would be naive to think that anyone is immune. Make sure your employees know about the recent spate of very sophisticated phishing emails. Employees need to hear the anti-phishing message enough that they will view the next slightly odd email with deep suspicion. Another defense is to ensure that company systems are designed to prevent scammers from getting the funds or data that they want. For example, it's easy for a scammer to fake a company executive's email address and send an email to the company controller requesting the disbursement of funds to a vendor. Not only should the controller be trained to be suspicious of such requests, but the company procedures should prevent the transfer without further verification or a secondary approver's signature.

When it comes to cybersecurity, the name of the game is preparation, preparation, preparation. It is easy to get overwhelmed by the amount of information, the technical details and the work required to get on top of and stay on top of cybersecurity issues. But this is an area where the pursuit of perfection will only get in the way. Companies should work step-by-step to create their cybersecurity plans, and if they already have a plan, there is no time like the present to review and update the plan to make sure it's keeping pace with the rigors of a constantly changing cybersecurity environment.

Donna Balaguer is *a principal in Fish & Richardson's office in Washington, D.C. She advises clients on a full range of privacy and data security laws and best practices, from the early stages of developing a privacy plan to handling a cyberbreach. She counsels clients across multiple industries, including hospitality, healthcare, media, communications, manufacturing and retail. Balaguer is a member of the International Association of Privacy Professionals and a Certified Information Privacy Professional (CIPP/US). She previously served as in-house counsel in the technology sector. She can be reached at balaguer@fr.com.*