Managing Data-Related Enterprise Risks

Submitted by AprilHall on Fri, 09/25/2020 - 09:19

As COVID-19 continues to disrupt and challenge “normal life” around the world, the pandemic has also emboldened cybercriminals and nation-state actors to adapt and strengthen their targeting of various organizations. These include companies operating in the healthcare and medical research sectors, small to medium-sized family businesses, and publicly traded companies operating in a diversity of industries. Such attacks aim to steal data through traditional hacking methods, such as phishing scams or scanning for unpatched systems, but also prioritize targeting services that have seen increased use during the pandemic, namely video teleconferencing technologies and remote access tools.

These threats have placed additional pressure on boards in this challenging time, in part due to the level of attention and adverse scrutiny directed at data security incidents. This includes scrutiny from shareholder advisory service firms as well as a number of federal government agencies, and state attorneys general, who routinely investigate data security incidents.

In order to thwart such opportunistic criminals, it is as important as ever for boards to be proactive and implement steps to protect one of their organizations’ most prized assets: data.

Programs and Procedures

Boards should ensure that their company has a current data compliance program in place and have regular assessments to ensure that they are prepared to evaluate, govern, and mitigate data risks. This includes the assurance that every employee understands how to handle sensitive data and how to protect against risks. In light of the current pandemic, this is particularly important given the increased frequency of teleworking and remote work. Many employees might not have a home office, a reliable broadband internet connection, or access to a printer. This state of play presents unique security risks. For example, boards must ensure that data compliance programs are being utilized that account for increased use of public WiFi networks, or productivity-related software installations, and the handling of confidential business information on potentially unsecure technology infrastructures.

Oversight

Boards should practice proactive oversight and should not wait to monitor data risks only after a breach occurs. Instead, be prepared to have regular oversight, and request routine reports from your organization's Chief Information Officer (CIO). In *Marchand v Barnhill*, the Delaware Supreme Court set the standard that boards of directors have risk oversight responsibilities and could be subjected to liability if they fail to "make a good faith effort to implement an oversight system and then monitor it." In addition, boards' consideration and deliberation about their organizations' new systems and processes should be documented through written records.

Effective Communication with CIO and IT Teams

Boards and executives must identify the questions to ask chief information security officers (CISOs) to empower boards to remain fully informed. In addition to the questions the Cybersecurity and Infrastructure Agency (CISA) recommends every CEO ask about cyber risks, boards should begin by asking their CISOs to list the top five to 10 common mistakes similarly situated organizations make. These often include using the wrong metrics to measure cybersecurity risk, focusing on security over cyber hygiene, a disconnect between security and business development, and a failure to recognize information technology dependencies.

Boards need to be familiar with their company's risk tolerance and approach to information security to develop a better understanding of its security posture. Boards should ask their organization's CISOs basic questions, such as:

- Do we use multifactor authentication? How are we enforcing complex-password rules?
- Are our laptops encrypted?Are our systems set to retain log files that would be useful when investigating a cyber-intrusion?
- Do we have an out-of-band method for communication in the event that our corporate email system is compromised?

If those have been answered, the tough questions need to be examined:

- Why haven't we addressed the data security concerns raised in last year's audit?
- Do we utilize network segmentation?

The limitations of remote work extend to the company's onsite IT teams, limiting hands-on trouble shooting with employees who are working from home and not being able to provide the same level of support as they would to employees

present in the office. Boards must plan for these limitations now by ensuring incident response protocols are clear, incidents continue to be appropriately flagged and escalated as appropriate, and the incident response team can communicate using off-band communications if needed. In order to accomplish this, companies need clear, reliable communication channels for both internal and external parties.

Continued and proactive monitoring

Boards should be asking what additional obligations and steps their organization should be taking in light of evolving data security decisions and laws, such as the recent Schrems II decision from the Court of Justice of the European Union concerning data transfers from the EU to the United States, New York's Stop Hacks and Improve Electronic Data Security (SHIELD) Act, and California's Consumer Privacy Act (CCPA).

In July 2020, the CJEU invalidated the EU-U.S. Privacy Shield and cast a cloud over Standard Contractual Clauses and, by implication, all other data transfer mechanisms between the EU and United States. The decision will have significant implications for companies' data transfer arrangements. Boards will need to ask questions about the type of data that the company transfers from the EU to other countries and the nature of the agreements pursuant to which the data is transferred.

In the United States, despite the expansive disparate patchwork of state laws, there are growing commonalities that may signal coalescence around prevailing security and breach notification standards and a gradual shift toward increased uniformity.

This monitoring extends to breach notices, which are driven by federal and state laws (and often non-U.S. laws). There are federal breach requirements (e.g., the Gramm-Leach-Bliley Act for financial institutions and the Health Insurance Portability and Accountability Act for healthcare data), and there are unique/individual requirements in every U.S. state and most U.S. territories.

Notice in a nationwide incident can be complicated, especially given the evolution of applicable laws over the last few years, and now given the uncertainty endemic to the current COVID-19 situation. Boards should make an effort to stay abreast of the current landscape of breach-related requirements and ask for a presentation on the company's current standing with these laws. In addition, breaches that affect subsidiaries, affiliates, or individuals outside the U.S. are even more complicated. Be aware that the number of jurisdictions with breach-notification

obligations is growing and, in many instances, includes the unauthorized disclosure of any type of personal information. Moreover, a growing number of countries now require that notice be provided to regulators within 72 hours of a company learning of a breach.

Healthy response and contingency planning

As the world adapts to an ever-evolving COVID-19 “new normal,” boards will need to continue to manage their COVID-19 response plans. Boards should consider what questions to ask to better support an entirely remote workforce long-term, how that creates data vulnerabilities, and what boards can do to help mitigate risks. Many companies have an incident response plan, but many now must be updated in light of the new realities of incident response in a remote workplace but questions to consider for a long-term audit of processes include:

- Does the plan need to be updated based on the current breach environment?
- Would it actually be helpful in responding to a high-profile, global or nationwide security breach?
- Does it have a list of key contacts and their contact information?

The short and long-term effects of this current upheaval neither are close to being over, nor fully understood. While data security and risk management may seem like an overwhelming and daunting responsibility, a careful review and assessment of your organization’s level of preparedness for cybersecurity risks and implementation of the steps above will help mitigate risks to your organization and make you less vulnerable to the whims and exploits of cyber criminals and hackers.

John Carlin *is chair of the Global Risk and Crisis Management practice,* ***Miriam Wugmeister*** *is co-chair of the Global Privacy and Data Security practice,* ***Alex Iftimie*** *is of counsel in the National Security practice, and* ***Reema Shocair Ali*** *is a national security analyst at law firm Morrison & Foerster.*