BCLP. Client Intelligent

Insights

CYBER – MORE THAN JUST BREACH RESPONSE

Mar 06, 2025

"*The true hero in the Black Swan world is someone who prevents a calamity and, naturally, because the calamity did not take place, does not get recognition or a bonus for it.*" - Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder*

The vast majority of commentary and public advice concerning data breaches surround, deservedly, the breach itself. This focus is only natural; it is the breach itself that requires victims to bring enormous resources to bear through the investigation, technical remediation and potential notification to individuals and regulatory authorities, and it is the breach itself that can cause reputational harm both internally and externally and lead to investigations, fines and costly class action lawsuits. But cyber is more than just breach response, and companies that focus solely on responding to breaches have lost the opportunity to be a true, if unsung, hero by taking steps to prevent, prepare for and mitigate data breaches and security incidents.

With this in mind, we have identified below five steps organizations can take now to improve their preparation and limit their risk in the arena of cybersecurity:

1. **Map Reporting Requirements:** Most organizations are aware that they have reporting obligations in the event of a qualifying data breach to individuals and to state regulators. But organizations must also identify any other regulators, such as regulators focused on particular sectors, that may require notification. Organizations may be required to report under accelerated time frames or via different methods, and this process will vary significantly by company. For example, is the organization or its data regulated by any federal regulators? Is the organization a Covered Entity under HIPAA? Is the organization a licensee under NYDFS? Is the organization public, thus requiring compliance with new data governance and cybersecurity reporting requirements in the company's yearly 10-K? These requirements are evolving (and increasing) each year, so even if your team has done this analysis in the past, it is wise to revisit the issue and identify the relevant timing and notification requirements. Otherwise, it is possible that a new obligation can be missed in the pressure of a data breach.

2. **Revisit Procurement Strategies:** Many data breaches suffered by organizations do not actually happen on their own systems, but on those of their service providers (g., a third party central HRIS system). Nevertheless, the reporting obligations and primary liability generally run to the

organization rather than the service provider. Thus, protection of data means more than hardening company servers, endpoints and other assets, and training employees. As important, if not more, is the development of a procurement strategy that ensures: (i) that the company is protected contractually, through indemnification and other risk-shifting provisions, in the event of a breach; (ii) that the company has received sufficient assurances through actionable representations and warranties concerning the service provider's security standards and protection of the company's sensitive data; and (iii) that the company has a meaningful audit strategy for key vendors. Indeed, an inventory of key vendors ranked by risk and an audit strategy for those vendors is one of the more valuable (and rare) mitigation strategies.

3. **Revisit Insurance Coverages and Resources:** Most companies now have insurance for cybersecurity events but few periodically revisit their coverage to determine if it is sufficient, and competitively priced. Moreover, many insurers now offer free or low-cost resources to harden their insureds' systems and controls. This is a win-win because the insurer gets a lower risk insured-controller and the insured-controller receives free or low-cost resources to aid in the development of their cybersecurity program.

4. **Board and CISO Considerations:** While individual liability for data breaches is rare, it is not impossible. The SEC has brought actions against individuals, and particularly CISOs, in relation to data breaches in the past. Though many of these claims were later dismissed, the mere attempt sets a precedent that should concern CISOs and other employees. Companies should review whether and to what extent CISOs and other key personnel in the cyber ecosystem are covered by traditional D&O policies, and should of course establish a process for thoroughly vetting public statements and board communications. The SEC's recent guidance and requirements concerning cybersecurity governance may provide a good roadmap in this area, even for non-public entities. In addition, every organization should consider thresholds and parameters for Board reporting, both with respect to breaches themselves and of course with respect to Board oversight of cybersecurity programs, risks, and strategy. The clear trend, as evidenced by the SEC's 10-K reporting requirements, is toward more Board involvement and accountability.

5. **Remember Your Broader Compliance Program:** For companies that are unfortunate enough to suffer a significant data breach, the occurrence can often be an opportunity for regulators to make inquiries concerning the victim's broader compliance program. As one example, the FTC recently has taken a very expansive view of its enforcement authority deriving from the FTC Act's prohibition of "unfairness" to require data brokers to comply with a number of specific privacy compliance objectives in recent consent orders. Moreover, the FTC recently has amended the Health Breach Notification Rule (the "HBNR"), 16 C.F.R. 318, to expand its scope, and has reached multiple settlements in recent years challenging data sharing practices by invoking HBNR. Even with the change in administrations, we expect this focus to continue from FTC. And of course, as noted above, the SEC has issued a final rule that requires both breach reporting and additional,

yearly reporting relating to cybersecurity controls and processes. Training and review of existing policies and procedures, with the assistance of counsel, can help ensure that the company is meeting more general regulatory expectations in this area, not to mention complying with the patchwork array of state and federal laws.

Preparing for the breach itself and knowing what to do is important, but so too is positioning your organization to be in the best place possible to avoid the breach in the first place and to mitigate collateral risks. By reducing the possibility of a breach in the first place, you too can be like Taleb's true hero. As the steps above make clear, this is not just a technical goal. Counsel can assist in these preventative activities. Should you have any questions concerning any of this material, please do not hesitate to contact the authors below.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535
