New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 265—NO. 89

MONDAY, MAY 10, 2021

Time Well Spent: Cultivating a **Broad Cybersecurity Team**

By **Julia Brickell**

The call comes Friday before the holiday. Your in-house IT lead tells you there has been a cyber-attack on the company. You know speed matters. "When are we convening?" you ask. "Fifteen minutes—I'm sending an invite. The core team is aware."

You join the call, listen to the debrief from the security team and to IT's initial impact assessment. The team runs through its list of steps: detect, analyze, contain, eradicate, recover, improve. You discuss which pre-identified advisors to call. You discuss privilege and preservation. You agree on the level of notice to the extended response team (executives, sales, PR, finance, HR, consultants). You pull out your insurance policy. You pull out your legal department response checklist (e.g., notify breach and privacy counsel, notify your insurer). The team confirms the actions to be taken immediately. You set a time to reconvene.

Smooth sailing? More like a well-outfitted boat in stormy waters. What process led to that boat with that crew who knew what to do in what order? Thought, planning, practice—all of which requires determination and lead time.

Threats Are Increasing, With 'Dismal' Preparedness. The threat of a cyber-intrusion or other cyber-incident is known and looming, and if it isn't giving in-house counsel and the C-suite restless nights, they may be sleeping on the job. Remote work and circumstances related to the COVID-19 pandemic have only intensified the threat. Forbes has reported that 2020 broke all records for data lost in breaches and numbers of cyber-attacks on companies, government, and individuals (at an estimated cost of $6 trillion dollars annually) and opined that the readiness state of most companies is "dismal."

This is surely cause for concern. Even for companies in industries that are not regulated, clients and regulatory authorities are increasingly imposing obligations relating to data security. The 2016 California Data Breach Report, prepared by the California Department of Justice under the leadership of then Attorney General Kamala Harris, positioned securing personal data an entity collects as a duty of the entity. The report established a standard of care, opining "[t]he *failure* to implement all the [CIS Top 20 Critical Security]

JULIA BRICKELL *is executive managing director and general counsel at H5.*

Controls that apply to an organization's environment constitutes a *lack of reasonable security*." The FTC may view a failure to implement reasonable security to be an unfair business practice under the FTC Act and has brought numerous enforcement actions on that basis. State-imposed privacy protection statutes, such as the CCPA and New York Shield Act, similarly oblige entities to implement reasonable security to protect personal information of customers and clients.

While protection is most important, response to a breach ranks high as well. Indeed, the Ponemon Institute 2020 Cost of a Data Breach research published by IBM Security concluded that an incident response plan and an identified incident response team were the two of the top three factors that most reduced breach costs. An undoubtedly related metric, time to identify and contain a breach, also factored into cost: a quicker response saved money. Most of the downside consequences—business interruption, revenue loss, reputational damage, customer/employee harm—can be mitigated by speed. Are you prepared?

Scope of Required Preparedness Is Often Under-Estimated. Back to that boat. During a cyberattack, a time of substantial stress, many parts of the enterprise need to come together with speed and camaraderie. Imagine the pressure of a ransomware attack, for example. Attackers are threatening, business data is unavailable, systems are down, employees are unable to work, customers need to be handled, employee data may be compromised, insurers need to be notified, external advisors need to be brought in. You may be calling law enforcement and media may be calling you. Containment, analysis, and remediation planning are underway and breach notification needs to be evaluated and planned. Executives must rely on information from these various teams to make critical decisions on pay or don't-pay tactics.

Sound security is axiomatic. But that takes time and attention from trained security professionals, not your IT staff alone. Having an IT contractor or even an in-house IT team to keep your technology running likely won't plug the holes in the hull. Just as lawyers have specialties, so too do technology professionals. Security is a specialty. Engage the specialists.

Next, identify the internal team, a critical part of both prevention efforts and breach response. The scope goes far beyond the obvious IT and Security candidates. Business teams have information regarding data acquisition, composition, storage location, needed access, and use. HR has a role in hiring and background checks. Sales may be informative on clients' evolving expectations, legal would be informative on contract requirements including security standards, limitations on access, data retention, and breach notice. A group should be in charge of training (often Compliance or HR), an integral component of security. Indeed, human error reportedly was the root cause of 23% of breaches in 2020; separately, by falling for phishing and social engineering and creating weak passwords and other mistakes, humans admitted a large percent of malicious attackers, the cause of most breaches.

Work To Align and Share Perspectives, Knowledge and Vocabulary. With today's business operations often siloed, employees may lack shared perspectives, knowledge, or vocabulary, especially where systems and data are concerned. As counsel, we often eschew deep technological discussions. Marketing and IT rarely interact. Security and HR may not converse and align.

Both for prevention and response, collaboration among these groups is imperative. Time is your friend before a breach occurs, but not after; breach response must be swift and

certain. The key is to nurture *in advance* relationships among the appropriate in-house (and external) teams to enable them to work together effectively on prevention and to plan and practice for a coordinated response, should that critical moment come.

For the company to have responded so effectively to the hypothetical cyber-attack described at the beginning of this article, plenty of work would have occurred in advance. For example, there would have been purposeful, weekly meetings among representatives of in-house technical, legal and compliance teams, expanded quarterly to include others (e.g., PR/marketing, HR, business division leadership, company leadership, sometimes with outside counsel and consultants/vendors).

Ongoing interaction, with discussion of technology assets and projects, types of possible (or actual) security incidents and legal and compliance obligations and concerns can serve to familiarize team members with both risks and the planned methods to address them (including technical, policy, and training methods). Frequent conversations enable different teams to describe approaches, consider implications, and ask for clarification. Over time, recurring meetings keep teams current, support mutual understanding of vocabularies and goals, and help develop a shared sense of purpose.

Practice, Practice, Practice. A periodic cybersecurity tabletop exercise, in which the team walks through a mock incident, provides yet another opportunity to keep processes fresh and visions aligned. These exercises demand that team members articulate their anticipated responses at each step of the unfolding scenario. They enhance group understanding and expose weaknesses or gaps, enabling remediation and improved planning.

Conclusion

The National Institute of Standards and Technology (NIST) breaks the incident response lifecycle into four phases: preparation; detection and analysis; containment, eradication and recovery; and post-event activity. Although much of the responsibility for a cyberattack does fall within the information security technical function, the overall effort of a company toward prevention and response has a significant impact on reputation, losses, and costs.

The bottom line? Cyberthreats require deliberate prevention techniques, enterprise-wide awareness, and a well-planned incident response. This requires, in turn, a cultivated interaction among teams. A purposeful effort to share knowledge and develop camaraderie can keep the boat afloat.