New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 261—NO. 41

MONDAY, MARCH 4, 2019

Role of In-House Counsel In Incident Planning And Response

BY AVI GESSER, MATTHEW A. KELLY AND SAMANTHA J. PFOTENHAUER

UFABIZPHOTO VIA SHUTTERSTOCK

Until recently, corporate cybersecurity was viewed as essentially an IT concern, with some limited involvement from other functions such as Risk and Compliance. Except in situations requiring interaction with law enforcement, cybersecurity was not usually an area of substantive responsibility for in-house attorneys. But in the last five years, the role of in-house counsel in cybersecurity matters has expanded dramatically in response to increased risks of civil litigation, regulatory investigations, and congressional inquiries, as well as a stream of new state, federal, and international regulations. In 2019, effective management of cyber risk requires coordination and communication across a range of internal departments, at multiple levels within the corporate hierarchy, informed by the timely advice of competent in-house counsel.

As companies expand their preparation for cyber incidents, in-house counsel may be expected to play a role in an increasing number of disparate tasks, including:

- Assessing disclosures of prior incidents and material risks;
- Drafting and testing the company's incident response plan and other cybersecurity policies;
- Facilitating employee training and tabletop exercises;
- Ensuring the adequacy of insurance coverage;
- Developing contacts in law enforcement;
- Overseeing communications with threat-sharing groups;

AVI GESSER *is a partner in Davis Polk & Wardwell's litigation department, representing clients in a wide range of cybersecurity issues and counseling companies that have experienced cyber events. He is a frequent writer and commentator on cybersecurity issues.* MATTHEW A. KELLY *is an associate and* SAMANTHA J. PFOTENHAUER *is a law clerk in the department.*

• Assisting with cyber-focused due diligence of vendors and potential merger partners;

• Reviewing third-party contracts regarding cybersecurity-related undertakings and notification obligations; and

• Crafting strategies and submissions on public policy issues and proposed legislation.

When a cyber incident does occur, counsel may also be expected to:

• Ensure appropriate document preservation;

• Conduct witness interviews;

• Manage risks associated with insider trading;

• Help weigh the risks of paying and not paying cyber-ransom demands;

• Consider voluntary outreach to law enforcement and regulators;

• Direct efforts to have websites and search engines remove any stolen data; and

• Assess potential litigation and regulatory implications of the incident.

In this article, we explore three important aspects of in-house counsel's duties related to cybersecurity incident preparation and response: (1) providing advice regarding the company's legal and regulatory obligations, especially with respect to breach notification; (2) engaging and coordinating external resources, including outside counsel and consultants; and (3) coordinating and managing internal and external communications.

Saying What the Law Is (or May Be)

Not surprisingly, counsel's core cybersecurity-related function is to understand the company's statutory, regulatory, and contractual obligations, and to provide advice on the adequacy of the company's efforts to satisfy these obligations. For incident preparation, counsel should be able to advise as to which regulators have (or may claim) jurisdiction over the company—both for its cybersecurity compliance and in the event of a cyber incident—and what those regulators expect from the companies they regulate.

Often, the applicable regulations require that the company have a detailed written incident response plan (IRP), which counsel should assist in preparing. The document should provide pragmatic instructions for handling a cyber event, with a balance between real-time flexibility and the institutional need for internal accountability and consistency of approach. Because a company's response to an incident may be judged in part by its adherence to its IRP, counsel should ensure that the IRP sets out a framework that is achievable and has buy-in from the various stakeholders who may be involved in incident response. Counsel should also ensure that the IRP is practiced and tested through tabletop exercises, and is updated in response to changed circumstances, new threats, and lessons learned.

One of the most difficult aspects of incident response planning for counsel is trying to determine when a particular cyber event may trigger statutory or contractual notification obligations, including requirements to notify one or more of the company's customers, regulators, insurers, auditors, and vendors, as well as the market. There are now breach notification regimes in each of the 50 U.S. states, as well as federal, international, and industry-specific notification regulations. And unfortunately for anyone trying to navigate this labyrinth, the various regimes differ in their notification triggers, content requirements, and deadlines. In addition, many of these regulations are subject to regular amendments, and new notification regimes are popping up with some frequency. So counsel should not wait for an actual incident to begin the process of figuring out the company's obligations under these rules, especially because a failure to comply can lead to regulatory and civil liability, reputational harm, and the perception among regulators, the press, and the public that the company's overall management of the incident was lacking.

Engaging and Coordinating External Resources

Another key role for counsel in cyber incident planning and response is to engage and coordinate external resources, which may include retaining outside counsel, cybersecurity consultants, and public relations firms.

Counsel should be prepared to advise the company on how best to structure such arrangements in order to shield potentially sensitive communications from unwanted disclosure, particularly those taking place in the period immediately after the discovery of a potential incident. Claims of privilege or work product

protection are likely to be strongest where the company begins by engaging outside counsel to advise it on its legal obligations in connection with a cyber event, and outside counsel then retains other external resources to assist the law firm in providing legal advice to the client.

This is not to say that every engagement of a consultant related to cybersecurity should be privileged or should flow through outside counsel. In each instance, in-house counsel should be prepared to advise the company on the risks and benefits of trying to maintain privilege, and how best to achieve the desired outcome.

Managing Communications Regarding an Incident

A final key role of in-house counsel in responding to a cyber event is monitoring and managing internal and external lines of communications. At first glance, this may not appear to be a legal function. But inaccurate, inconsistent, or simply ill-considered internal and external communications can be sources of significant liability, even in contexts involving relatively insignificant cyber events. Helping to manage this risk is therefore an increasingly important role for in-house counsel. Where an incident—or information regarding the incident response process itself—could be material, risks related to information leaks, selective disclosure, and insider trading require careful consideration of who should be told about the incident, and what instructions they should be given about further sharing of information. Counsel should be involved in these discussions and should remind those who become aware of the incident—particularly the core incident response team—that their communications may be scrutinized later, and that extra care should be taken to ensure that their statements are accurate, informed, and professional.

To ensure that senior leadership is getting adequate and accurate information on a timely basis, counsel should provide, or be consulted in connection with, upward reporting regarding an incident to management and the board. Where feasible, counsel should review and approve any status reports or other summaries of information related to the incident prior to distribution.

Externally, counsel should review and approve any communications with insurers, auditors, customers, regulators, and the public to ensure consistency and accuracy. As discussed above, counsel should also monitor and advise on relevant notification triggers, and assist in drafting or reviewing any required notifications before they are released.

Finally, counsel should oversee any interactions with third parties whose cooperation may be needed in connection with the company's response to an incident, such as vendors, former employees, content hosts (e.g., Github), and internet service providers (ISPs), as well as federal or state law enforcement authorities. Here, too, it may be helpful to leverage the expertise and resources of outside counsel. But careful consideration should be given to the strategic and optical implications of counsel liaising directly with any third parties regarding the incident.

Conclusion

In preparing for and responding to a cyber incident, in-house counsel may be required to work with the company's various departments to neutralize active threats, identify and address areas of potential risk, and avoid creating additional liability. In the course of this work, counsel must take care to stay in their lane—identifying and focusing on performing the legal department's key functions. Although these may be varied and expanding, they generally include advising the company as to its legal and regulatory obligations (especially with respect to breach notification), engaging and coordinating with outside resources, as well as helping to manage internal and external lines of communication during an incident.