COVINGTON

Five Cybersecurity Questions that General Counsel Should Consider In Light of the Sony Breach

January 22, 2015

Privacy & Data Security

In the wake of the much publicized North Korean cyber-attacks against Sony—as well as recent favorable rulings for the plaintiffs in class action lawsuits pending against Target—cybersecurity is at the forefront of many corporate boards' and general counsel's agendas in the coming year. We expect the focus will only increase in light of the legislative proposals announced by the President last week, which were also featured in this week's State of the Union address. This is a complex topic that crosses multiple legal disciplines and business functions, and cybersecurity risk-mitigation requires thorough planning tailored to the particular data, business practices, and infrastructure of an organization, taking into consideration the threats facing the organization. Nevertheless, there are five foundational questions that every general counsel should understand when evaluating his or her organization's legal and business cybersecurity risk profile:

1. **What actions has your company taken to reduce the likelihood and impact of potential cyber intrusions?**

Many companies implement controls that focus on protecting their networks and systems against incursions by external attackers, but have less developed approaches to security once an attacker gets into the network. Such an approach may not adequately safeguard the "crown jewels" of a company's enterprise (e.g., valuable trade secrets, sensitive personal information, financial information, business plans and health records). Indeed, given the multiple potential sources and vectors for compromise—and the prevalence of attacks in today's world—a more progressive approach that assumes some form of compromise and develops heightened security controls around the most sensitive data and assets is essential to reduce the risk to the organization. This is important not only for managing the business risks associated with cybersecurity, but also reducing exposure to legal risks, as business partners, regulators, and other finders of fact may all increasingly consider such a defense-in-depth approach to security a necessary and reasonable standard of care. In turn, counsel can play an important role in working with internal IT and security experts and other critical business functions to develop an appropriate data classification approach and ensure that the most sensitive data and assets receive heightened protection.

2. **Has your company established and tested an incident response plan?**

There is, of course, no such thing as perfect security, and even the companies with the best-in-class information security practices suffer incidents. A critical aspect of minimizing the costs of incidents, therefore, is preparing for them in advance—which requires the development and maintenance of a written incident response plan as part of an overall information security program, and testing the plan through table-top exercises. Such a plan ultimately will not be a precise script for when an incident occurs, but it will help ensure preparedness and that the right team and procedures have been identified in advance of the incident. In our experience, this is important not only to help expedite a response, but also to address regulatory risks, and to

ensure that the company can be prepared to preserve applicable legal privileges in the event of a breach. If a breach becomes subject to regulatory scrutiny, the company will need to demonstrate that it had a reasonable plan in place to address incidents and made a good faith effort to follow that plan.

3. What resources are in place to assist incident response?

Cybersecurity incident response often requires organizations to draw upon multiple resources and address the interests of various constituents. For example, it frequently is necessary to engage external forensic resources to collaborate with the in-house incident response team and help develop the remediation plan. Efforts to stay in front of an incident may also involve a public communications strategy and, in turn, necessitate engagement with public relations consultants to assist with a company's notifications and responses to media and customer inquiries. These engagements can be crucial to an effective incident response; equally crucial, they should be structured in a manner that helps preserve privileges while still allowing the experts to optimize the assistance they can provide. In our experience, the most effective incident response plans identify the potential additional resources before an incident occurs, and contemplate how such resources will be engaged upon the occurrence of an incident, including the extent to which legal privileges may attach to the work of the consultants.

Other constituent parties that may become involved in cybersecurity incidents include law enforcement and a company's board of directors. Addressing the interests of these constituents—and potentially benefiting from their perspectives—requires a thoughtful approach to engagement informed by strong relationships and experience. In turn, having counsel who understand the interest of law enforcement officials and have experience in addressing and managing those interests, and who also can present credibly to the board of directors, can be an invaluable aspect of an effective and timely incident response.

4. Do your company's insurance policies cover data security incidents?

Another important aspect of cyber risk management is to ensure that the company's insurance policies provide the strongest possible basis to recover the potentially significant costs and liabilities associated with cyber incidents—ideally, before an incident happens. Covington has a top-ranked policyholder practice in the U.S., and deep experience not only in advising companies on policyholder terms, but also pursuing recovery under policies in some of the largest documented security breaches.

5. Is your company prepared for litigation arising out of a cybersecurity incident?

Cybersecurity incidents increasingly result in class action litigation. The plaintiffs' bar often takes a "kitchen sink" approach to these lawsuits, asserting various theories of liability in an attempt to see what may stick for discovery. Among other claims, these lawsuits often allege: (1) violations of federal securities laws (for publicly traded companies); (2) breaches of agreements to protect personal information; (3) other breach of contract claims; (4) various state tort-law claims, including negligence and fraud or misrepresentation claims; (5) state-law claims based on the failure to provide reasonable security for personal information; (6) state-law claims based on the failure to provide timely notice of a data breach; and (7) state-law claims based on "deceptive" or "unfair" trade practices.

To help address the risks associated with such lawsuits, it is prudent for internal counsel to understand the nature of these claims, and to identify potential resources to assist in defending against such claims in the event of an incident. To this end, it often is useful for a company to work with its internal and external counsel to ensure that they are fully apprised of its data

handling and privacy practices, as well as its infrastructure and potential risks, before any incident, so that if it ever becomes necessary to defend against a lawsuit, counsel guiding the company already are well-informed on key factual aspects of the matter.

* * *

Covington combines deep expertise working complex cyber- and national security matters and related policy issues. With more than a decade of practical experience working with numerous Fortune 500 companies across a range of industries on legal compliance matters, we regularly help clients prepare for and defend against security risks, both internal and external, to their systems, assets and data. Indeed, we have assisted clients in responding to scores of security breach situations, ranging from insider breaches involving millions of records containing personal information to multi-year breaches of sensitive commercial information from sophisticated external attackers, including advanced persistent threats ("APTs"). These incidents have involved among the largest and most complex cybersecurity breaches and have covered a diverse range of industries, including media and Internet content companies, retail, technology/communications, financial services, defense, energy, software, pharmaceuticals, travel-related services, and data-based services companies. These experiences inform our identification and approach to each of the foregoing questions.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Privacy & Data Security practice group:

David Fagan	+1 202 662 5291	dfagan@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Mythili Raman	+1 202 662 5929	mraman@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Jeffrey Kosseff	+1 202 662 5489	jkosseff@cov.com
Libbie Canter	+1 202 662 5228	ecanter@cov.com