LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

July 2018

In-House Counsel's Growing Role in Data Protection and Security Risk Management

***Building an Intelligence-Led Program* — With reports of major breaches surfacing with alarming frequency, boards and C-Level management are now looking to counsel to implement programs that help the corporation prepare for, quickly recover and reduce fallout from, inevitable cyber incidents. In-house counsel is facing growing responsibility to minimize damage to the corporate reputation, loss of key data, and legal and regulatory penalties. And many worry their organization is stuck in a game of catch-up.**

By Deana Uhl

The increasing damages of global ransomware have grown from $325 million in 2015 to an estimated $5 billion in 2017, as reported by IDG. With reports of major breaches surfacing with alarming frequency, boards and C-Level management are now looking to counsel to implement programs that help the corporation prepare for, quickly recover and reduce fallout from, inevitable cyber incidents. In-house counsel is facing growing responsibility to minimize damage to the corporate reputation, loss of key data, and legal and regulatory penalties. And many worry their organization is stuck in a game of catch-up.

The current threat landscape is affecting nearly every corporation around the world. There has been a more than 27% increase in the average number of security breaches (per Accenture's 2017 Cost of Cyber Crime Study), which can lead to brand damage, enforcement actions from regulators and decreased market value.

In the latest ALM/Morrison Forrester Crisis Management In-Depth Report, 67% percent of respondents indicated that they were well prepared for a cyber crisis, which was an improvement on earlier figures. Still, in our experience, many organizations continue to struggle to implement a repeatable and effective crisis management playbook for data breach events. A proactive, intelligence-led corporate data protection program is the only way to increase resilience against evolving threats, and counsel must continually evaluate ways to strengthen their defenses.

Mapping the Risk

The first step in doing this is for the legal team to champion the effort to map out the organization's risk landscape and evaluate the organization's enterprise risk management model. This exercise identifies the types of possible breaches and threat level unique to the organization, so the response can be appropriately focused. Threats can span a wide range across nation-state activity, financially motivated malicious actors, hackers looking to steal intellectual property, or inadvertent data loss from employee negligence.

The legal team should drive the organization to answer questions including: What type of data and information does the company manage and store, that if lost or stolen result in a major impact? What and where are the company's crown jewels? What type of best practices are already in place? What systems, including those that are unique to the organization's business or industry, are likely to be primary targets by adversaries? For example, financial services organizations will likely focus on thwarting attempts to steal money, healthcare providers will focus on their significant regulatory obligations, while pharmaceutical companies will work to reduce their risk around trade secret theft.

Regardless of industry, organizations that have operations in Europe also must address and prioritize privacy under the General Data Protection Regulation (GDPR). Enforcement of the GDPR was activated on May 25, and states that

Deana Uhl is a Senior Director in the FTI Technology practice and is based in Houston. Ms. Uhl provides consulting to corporate clients, with a focus on designing, implementing and enabling change management for information governance, data privacy, data security and e-discovery programs.

organizations not compliant with its extensive requirements may be fined up to 4% of annual global turnover, or €20 million (whichever is greater). Counsel must review requirements and applicability, and, with other key stakeholders, identify gaps and areas of risk across people, process and technology.

In the energy industry, every company has an emergency response team, with detailed playbooks and regular drills. This is part of an innate culture to plan and prepare for safety and environmental crises. Today's landscape requires organizations in any industry, of any size, to take a similar approach with their cybersecurity and data privacy programs.

With the knowledge that results from a risk evaluation exercise, a company can begin putting together the many pieces of an effective corporate data protection program. This should be approached as a dynamic process, with policies that can evolve rapidly alongside the constantly changing landscape. Enabling cultural, operational and technology changes must all be viewed as equal priorities. Sound programs include the following elements:

• ***Policies and standards:*** A strong framework of policies must be the foundation. Often there are a number of standards in different parts of a company, but they are not coordinated. It is important to take a top down approach, so a common security, privacy and data protection taxonomy and standards are in place holistically across the organization.

• ***Identification and classification:*** Not all data is equal across a company, and a map of the data landscape is critical. Critical assets should be identified and grouped together, separate from the less sensitive information stored within the organization.

• ***Governance:*** The policies established must include built-in enforcement measures. Processes and technologies can be leveraged to track internal compliance with policies and ensure they are sustained across the organization and with third parties.

• ***Regulatory considerations:*** Most multi-national organizations are dealing with a patchwork of regulations, and data protection programs must address compliance with any industry and cross-border requirements that apply.

• ***Change management:*** The entire workforce must be on board for programs to be effective. Change management and training are critical elements to any such program and will drive awareness so that everyone from the board members to the interns understand what must be done.

Developing Incident Response

In addition to the elements above, one of the critical things a legal team must do to strengthen a data protection program is to champion the development and standardization of a cyber incident response playbook. When a breach or other incident of high potential impact occurs, from the first minute and for the months following, the public will scrutinize how the organization responds. With an incident response plan in place, recovery can occur swiftly and damages minimized by everyone working in a coordinated and collaborative way to respond to the incident. Also, it helps the organization demonstrate what was done to prevent, prepare for, respond to, and minimize the impact, which may be critical in defending against litigation that results from a breach or other such incident.

Effective incident response plans provide a guide that help counsel and other stakeholders anticipate the unexpected, and should encompass:

• ***Assessment:*** The plan should outline the organizational environment, including identified roles and responsibilities for who will be involved in certain incidents based on the risk model. This also includes defining a broader governance committee of stakeholders across legal, IT, executive leadership, information security, etc.

• ***Defense:*** The plan implements and manages defensive best practices, including access control, network maintenance and deployment of proactive technology. Continuous monitoring to identify threats rapidly and proactively (a result of knowing in advance the main areas of risk) helps keep the organization one step ahead of threats.

• ***Response:*** Even a huge investment of time, budget and energy into cybersecurity will not make an organization immune. Response must be viewed not as an IT problem, but as a business operations activity. It should ensure proper notification of authorities and impacted parties, as required by the various laws to which the organization is subject.

• ***Recovery:*** This is where practice drills and lessons learned come into play. Teams must holistically look at the nuances of the breach to learn from it and strengthen the position so it does not happen again.

Conclusion

An intelligence-led strategic approach is necessary and must be enacted as a proactive priority, before a breach occurs. Adopting a data protection governance and policy posture and sharing that responsibility across the organization will ensure protection of the organization's crown jewels. Beyond mitigating cyber risks, these activities help strengthen the overall corporate culture around privacy and security, allowing for improved trust among clients and partners.

—❖—