CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW

OCTOBER 2019

MANAGING A COMPANY'S CYBER RISK IS A TEAM EFFORT

General counsel are often well positioned to play a leading role in the process.

BY KURTIS SUHS

The general counsel's role in managing cyber risk should start well before a cyber incident. From projects that may range from compliance work, third-party contract reviews and vendor due diligence to employee training and tabletop exercises, in-house counsel can be prime contributors to cyber risk readiness.

As the threats of significant financial loss and reputational damage continue to grow, lawyers can help drive the process to elevate their organization's cyber risk readiness. In the past three years, the role of in-house counsel has greatly expanded in response to increased civil litigation, regulatory scrutiny and a steady stream of new international, federal and state laws.

General counsel are often well positioned to help coordinate the efforts of their colleagues. That is because cybersecurity is not just an IT issue, but a business strategy that may create legal obligations for the organization. And no one group can build cybersecurity alone. This is definitely a team sport, and it requires a roster that is wide and deep. Let's review some of the players.

Board of Directors

Boards of directors are ultimately liable for a company's missteps and responsible for its survival, and in today's interconnected world, cyber resilience is a big part of that responsibility. General counsel today are seen as trusted board advisers who wield influence over their companies' legal and business strategy. Instead of reactively analyzing an issue from a purely legal perspective, GCs help remove obstacles and foster business objectives in a proactive manner. Meanwhile, they are expected to ensure that the organization maintains the highest standards of legal and ethical behavior, adroitly balancing the dual imperatives of company performance and corporate integrity.

The importance of the law department is reflected in the second of five principles listed below, which spell out what all corporate boards should consider as they seek to enhance their oversight of cyber risks. These appeared in the Director's Handbook on Cyber-Risk Oversight, published by the National Association of Corporate Directors (NACD).

• Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

• Directors should understand the legal and regulatory implications of cyber risks as they relate to their company's specific circumstances.

• Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the Board meeting agenda.

• Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

• Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Outside Counsel

In-house counsel should have a relationship with a law firm that has expertise and experience with data breaches, privacy laws and regulations. One of the most difficult challenges in responding to an incident is deciding whether it triggers statutory or contractual notification obligations that involve employees, customers, vendors, insurers, regulators and law enforcement.

But just as important, outside counsel should be hired by the company that has suffered the potential attack to retain the third-party vendors it will need to work with. This could ensure that discussions and work product are subject to attorney-client privilege. Without this attorney-client privilege, any third-party work product may be subject to discovery by the plaintiffs bar for use against the entity or the organization's directors and officers.

Information Security

In conjunction with their information security teams and other personnel, the general counsel can help develop key aspects of a cybersecurity program. These should include data inventories, risk assessments, compliance strategies and incident response plan testing through tabletop exercises and breach simulations. With guidance from the information security team, in-house counsel should ensure that the written information security plan is achievable and has a buy-in from all stakeholders. Furthermore, general counsel should ensure that it complies with and meets the minimum standards required by relevant states.

Risk Management

In-house counsel should work closely with their organization's risk management team to protect the company in the event of an attack. Insurance brokers and outside counsel should also be consulted to best match the types of coverage and policy terms that the organization needs. They can also help risk management evaluate cyber risk within each property and casualty insurance policy, examining for affirmative coverage, excluded coverage, sub-limited coverage or silent coverage (where cyber risk is neither affirmed nor excluded).

Human Resources

Given that a number of cyber incidents emerge due to the actions of an organization's own workforce, in-house counsel can play a crucial role in managing those risks. The lawyers can assist the human resources department to ensure that an organization's policies are not only drafted but followed, and that disciplinary measures are taken in the event of a violation. The areas covered should include cybersecurity, physical security, data security, security training and employee conduct.

Facilities Management

Physical security is a vital part of any written information security plan. Getting the right people involved will save valuable time and effort as plans and strategies are developed for new and existing resources. From the initial point of physical entry to the protection of an asset, general counsel can take an active role by offering oversight, marshaling resources and serving as an advocate for key stakeholders.

Law Enforcement

Organizations should also develop relationships with law enforcement before a cyber incident. General counsel can often serve as the initial point of contact and help agents access documents and witnesses. Time is of the essence, particularly with business email compromise through hacking and phishing attacks. If victims contact their local FBI field office within 48 hours of a loss, the FBI's Recovery Asset Team has a 75 percent chance of recovering those funds.

The Bottom Line

Just as technology, advanced persistent threats, litigation, legislation and the regulatory landscape are rapidly changing, so is counsel's role within the organization. By actively managing decision-making throughout the risk assessment and compliance process, counsel can help prepare their organizations to detect risk and effectively respond when threats arise.

Kurtis Suhs *is the Managing Director of Cyber Special Ops, LLC, a Georgia-based company that he founded to advance cybersecurity by using specialized teams and risk management techniques to prepare for and respond to a cyber event. He has over 33 years of experience in the insurance and financial services sectors, and helped launch the first cyber insurance product in 1997. Using the concierge medicine model, Cyber Special Ops provides guaranteed access to highly credentialed third-party providers for a modest annual membership fee.*