4 Things Lawyers Can Do to Improve Cyber-Risk Programs: You need to think of yourself as both a steward and a shepherd

The role of corporate counsel has been rapidly evolving in the past few years. The scope of responsibilities has expanded beyond legal administrative tasks to include companywide risk management, cost control, regulatory compliance and other areas that affect the company's reputation and bottom line. Data privacy and security, which used to sit squarely in the domain of the information technology department, now has the full attention of customers, shareholders and government regulators. As a result, senior management and the board are relying more and more on corporate counsel to be both the steward and the shepherd of cyber-risk governance programs.

This doesn't mean that counsel have simply inherited IT's responsibilities for managing cyber compliance. Quite the contrary. IT must still ensure that the computer systems they manage are properly secured. Counsel's role is to look beyond this hardening of IT systems to develop a more comprehensive cyber-risk governance program. Ideally, this program should consider cybersecurity from a broad perspective, and ensure that the company's statutory, contractual, regulatory and reputational liabilities are properly managed and minimized. Here are some best practices to consider to improve cyber-risk programs:

1. Take a top-down approach.

Most security professionals and practitioners would agree that total prevention is not possible. However, a top-down approach that embeds cybersecurity management throughout a company's infrastructure is the most effective way to mitigate risk. This means developing a governance model that starts at the board level, and then moves down through the C-suite and line managers to ensure accountability at all levels.

Many directors may not have the technical background to make decisions on their own, so the company should line up mechanisms to ensure that everyone has the assistance they need. These include the company deploying special cyber review or technology committees, and ensuring that other directors or advisory committee members have some technical or cyber experience as well. The committee can then perform periodic (typically quarterly) reviews and report to the board biannually. If it's not possible to create a dedicated technology committee, you should integrate the cybersecurity team into the audit or risk committee agendas for board reporting and decision-making. Determining which structure is most appropriate really hinges on the regulatory requirements, and the overall size and global footprint, of your company.

2. Make sure that the management team fully understands the risks.

You should conduct a full cyber-risk assessment that considers both the likelihood of various potential scenarios and the overall impact that each would have, using in-house resources and supplementing these with external assistance, where needed. To this end, it is important that you require senior management to know who the company's primary threat actors and stakeholders are. These can differ greatly across industries and geographies, and even across internal departments. It is therefore important that management provides a road map of the actual and potential actors or perpetrators they face.

The road map should also include the data privacy and security expectations of their key stakeholders and constituents. In addition, counsel should also require management to provide a clear and comprehensive map of company information assets that are susceptible to cyberattack. It's imperative to know what key assets are, where they are stored and what their internal and external values are in order to understand the controls needed to properly protect them. You should then ask some key questions, such as "How is the company positioned to handle any one of the identified adverse scenarios?" And "Is our current approach the optimal approach?"

3. Involve other departments.

Information assets and the risks they pose can differ greatly across the company. It is important to develop both a cross-disciplinary approach to cyber-risk management and a cross-segmental or divisional approach to cyber-risk management, including effective executive and board reporting. The information that each functional unit reports must be not only meaningful to more senior stakeholders, but also actionable.

The historic response to this challenge has been to use checklists, which are typically developed as a way for counsel to translate requirements into layman terms. Canned reports that IT professionals use to translate technological language into something others can understand and quickly review are equally common. But checklists and canned reports are unlikely on their own to give a clear picture of actual risk. This is especially true when they are just recycled metrics developed for other needs, such as the often-used common vulnerability scoring system (CVSS) reports, which were originally deployed for vulnerability response. Knowing how many vulnerabilities were reported and remediated in each quarter has very little value to a board that cannot discern if they were the right vulnerabilities or if their remediation had any impact on actual risk. (Sure, IT security closed 10,000 application vulnerabilities last period, but did that really help?)

More holistic risk reporting through a comprehensive portal that contains meaningful key performance indicators (KPIs) is essential to building an effective risk governance program. KPIs should be simple and easy to read. They should include, as a baseline, a road map that shows what your current risk profile is, where you want it to go in the future and what steps you are taking to get there.

4. Build cyber-risk partnerships.

Beyond leveraging internal resources, it is equally important that counsel build appropriate cyber-risk partnerships. These include actively engaging with your vendors and business partners, participating in both private-sector industry cybersecurity benchmarking and information-sharing programs. You should also monitor appropriate industry and government initiatives, and routinely engage outside advisers to take a fresh look at your cyber-risk governance program. In my sailboat racing days, we used to call this getting your head outside the boat. You can't hyper-focus on the tasks in front of you. To be successful, you have to also keep abreast of what is happening outside your company and what others around you are doing in response. It's important to look outside the organization and get constant feedback from experts with broader industry experience. Otherwise you will only focus on what you see in the boat, and probably completely miss that giant oil tanker headed straight at you.

Before leaving office, President Barack Obama called cyber-risk "one of most serious economic and national security challenges" facing America. As more and more critical company assets—including intellectual property, corporate strategies and consumer information—are stored electronically, developing robust cyber-risk governance programs could not be more important. As a result, general counsel and their legal teams must be proactive about taking a leadership role on cyber-risk governance. By staying properly informed about the company's cyber-risk profile and liabilities, they can provide the necessary guidance to the board of directors, senior management and other stakeholders. Counsel who assert their dual role as the steward and shepherd of these programs can ensure that their company's most important business assets remain secure and that its risks—legal and otherwise—are kept to a minimum.

AlixPartners LLP
Patron

David White

Topics

Special Sections:
Information Governance Insights
Featured Topics:
Cybersecurity
Other Topics:
legal operations
Web Topics:
AlixPartners