MARSH JLT SPECIALTY

INSIGHTS | MARCH 2019

What Boards Need to Know About Cyber Insurance and Regulatory Change

The pace and scale of cyber-attacks continue to grow, as do the financial stakes, with companies facing revenue losses, recovery expenses, liability costs, and potentially severe regulatory fines.

The specter of 2017's NotPetya event, the most devastating cyber event in history, still haunts business leaders: The malware caused more than $10 billion in economic damages and disrupted business operations, production, and logistics for several major multinational companies. The insured losses from that attack alone have been estimated at more than $3 billion.

NotPetya and other cyber events are forcing companies to make cyber risk a corporate priority. In the 2019 *Marsh Microsoft Global Cyber Risk Perception Survey*, 80% of organizations ranked cyber threats among their top five risks. And companies are slowly but surely shifting their view of cyber risk from a problem to be solved by spending more on technology, to a more realistic view of cyber threats as risks that must be actively managed across the entire company. That shift in mindset has increasingly brought cyber insurance into companies' overall approach to cyber risk management.

But cyber risk is not only on the agenda of C-suites and boards. Regulators also are more actively looking at how organizations address cyber risks and how they manage their responsibilities to key stakeholders. So even as the financial costs of cyber threats grow, the regulatory stakes are likewise poised to rise as more regulators, particularly the US Securities and Exchange Commission (SEC), begin to impose stricter requirements on businesses.

The increasing adoption of insurance to transfer cyber risk and a more rigorous regulatory approach to cyber risk management dovetail in numerous ways. Many of the new regulatory requirements and guidance around cyber risk assessment, prevention and management, executive and board-level ownership, and event disclosure and response are the same practices that should inform an organization's decision-making around cyber insurance investment. These same best practices are what underwriters increasingly expect and value.

MARSH

SEC Guidance

The SEC's interpretative guidance focuses on five main areas:

- **Pre-incident disclosure.** The guidance calls for transparency around the identification, quantification, and management of cyber risks by the c-suite and oversight by the board of directors. Often, growth in technology and the global operating environment impede 360-degree visibility into a company's vulnerable spots, with lack of data contributing to compromised security.
- **Board oversight.** The board is expected to understand, quantify, and oversee cyber risk. The SEC advises companies to disclose in their proxy statement the board's role and engagement in cyber risk oversight. Board members have to be privy to and understand the company's overall cybersecurity exposure, with a particular focus on how this could impact the company's financial situation, integrating this insight into their 360-degree view of the company's risks.
- **Incident disclosure.** Companies are required to "inform investors about material cybersecurity risks and incidents in a timely fashion." To do so, companies must have structures in place to identify and quantify cyber risk — tools that allow them to rapidly determine whether the impact of compromised systems were, in fact, material and require disclosure to regulators and investors.
- **Controls and procedures.** The guidance also tasks companies with assessing whether their enterprise risk management (ERM) process is sufficient to safeguard the organization from cyber disasters. This requires a step-by-step playbook for cyber events, including identifying who needs to be contacted and how and with whom the business will share information about a breach. Given the evolving nature of cyber risk, ongoing due diligence exercises should occur to identify and manage new risks — especially during a merger or acquisition. Most companies have long done this for other perils such as natural disasters, and it is imperative they extend this process to cyber risk.
- **Insider trading.** New to the 2018 guidance is a reminder to companies, directors, officers, and other parties of insider trading prohibitions. In practice, this means that directors, officers, and other executives who are aware of a company's cyber vulnerabilities or a breach could be liable if they sell company stock, or instruct anyone else to do so, before such a breach or vulnerability is divulged.

The SEC Strengthens Its Stance

Cybersecurity has been on the SEC's agenda for several years. In 2011, the commission's Division of Corporation Finance issued guidance calling on companies to assess their disclosure obligations regarding their cybersecurity risks and cyber incidents.

While a good starting point, the guidance did not go far enough in setting clear expectations for both proactive and reactive cyber risk management and oversight. In 2018 the SEC approved new interpretative guidance that outlines requirements for publicly traded companies to disclose cybersecurity risks and material incidents (see sidebar).

The cost of noncompliance can be substantial. In 2018, the SEC leveled a $35 million penalty against a large technology company it said misled investors when the company failed to disclose the theft of the personal data from hundreds of millions of user accounts.

Congress, which holds the SEC's purse strings, is placing mounting pressure on the agency to improve cybersecurity. Private investors are also pressing for more stringent cybersecurity controls at the companies they hold. It is, therefore, likely the SEC will start coming down on companies with more vigor, especially in the wake of major breaches.

Risk Transfer: A Core Cyber Risk Management Tool

Technology alone can't address the full spectrum of risks that businesses face. Insurance has historically stepped in to provide the financial backstop for that residual risk that cannot be eliminated through process, procedure, and mitigation.

Cyber risk is no different and organizations increasingly recognize that cyber threats cannot be managed through technology alone. It is an operational risk that needs to be incorporated into an overall enterprise risk management (ERM) framework that includes risk transfer, as well as mitigation and resilience planning.

The insurance market now offers risk transfer solutions for cyber risk that address both ever-evolving technology risk and the recent retreat of traditional insurance products from adequately addressing firms' evolving cyber risk profile.

Cyber risks include both the direct loss that a firm can suffer in terms of lost revenue or assets, as well as the liability that can arise from a data breach or failure to comply with myriad new domestic and international regulations.

Cyber insurance has also been at the forefront of pushing for better understanding of cyber risk's financial implications to help the industry improve modeling of potential loss scenarios. Such a financial assessment is also a critical foundation for businesses' risk management planning: Cyber risk quantification helps organizations assess the economic impact of a range of cyber events, and on that basis, make informed investments in technology, insurance, and response resources. Quantification of cyber risk also allows for cyber risk to be analyzed within an organization's overall risk framework and integrated into its overall risk management planning.

The assessment, evaluation, and modeling processes that are essential foundations for purchasing cyber insurance are, in many ways, aligned with the practices called for in the SEC's guidance. Given the likelihood of an increasingly active regulatory agenda, organizations are advised to align their policies and practices to abide by the SEC's recommendations and to consider insurance market coverage that can help protect against cyber event-related losses and regulatory liabilities.

A version of this article was originally written for NACD BoardTalk, the official blog of the NACD.

For more information, send an email to cyber.risk@marsh.com, contact your Marsh representative, or contact:

BOB PARISI
US Cyber Product Leader
+1 212 345 5924
robert.parisi@marsh.com