BITSIGHT

EBOOK

Cyber Risk Protection and Resilience Planning for Boards

What cybersecurity questions should directors be asking?

Cybersecurity is a top risk for corporate directors to understand and navigate. The implications of cyber events for a company are many and growing: instantly damaged reputations that erode years of credibility and trust with customers and investors, impaired profitability from customer attrition and increased operating costs, lost intellectual property, fines and litigation, and harm to a company's people and culture.

According to a recent survey from Diligent[1], nearly half of surveyed organizations experienced a cyber breach in 2022, resulting in an average of nearly $1 million per organization in lost revenue.

Consequences for companies can be significant. For example, in 2022, the SEC announced cybersecurity enforcement actions against major firms based on failure to comply with core obligations, including record-keeping and safeguarding customer information. Persistence and vigilance, combined with education, preparedness and transparency, are key to ensure a holistic program of cyber protection and resilience is in place.

Current State of Cybersecurity

A focus on cybersecurity is critical for boards, from both an investor and an operational perspective. Institutional investors are concerned about the impact of cybersecurity threats on their investments, making it a top ESG risk. Investors are also focusing on how to integrate cyber risk into valuations and pricing. As proxy advisors increase their focus on a company's cybersecurity risk, activist investors' attention may be drawn there as well.

Operationally, directors should understand how the use of third-party vendors exposes the company to additional risks. Roughly 62 percent of companies[2] that have experienced a breach reported that the attacker accessed their network through a vendor, a partner or another third party.

At the same time risks are rising, cyber insurance has become more costly and harder to obtain. One important driver for the change in cyber insurance coverage is the dramatic increase in ransomware and ransomware payments, which increased by 220 percent in 2021[3]. The U.S. Department of the Treasury reported that U.S. banks and financial institutions processed roughly $1.2 billion in ransomware payments in 2021[4], a new record and almost triple the amount of the previous year.

[1] https://www.diligent.com/news/diligent-finds-73-percent-of-risk-professionals-are-concerned-about-meeting-the-changing-demands-of-regulatory-compliance/
[2] https://www.verizon.com/business/resources/reports/dbir/
[3] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a
[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-243a

Transparency Is Coming

New cybersecurity regulations from the SEC are being considered (with similar rules anticipated in Europe) and are expected to come into effect in the first half of 2023. These regulations will require board members to participate more closely in cybersecurity oversight, so it is crucial for directors to enhance their knowledge of cybersecurity to effectively govern significant enterprise-wide risks and have meaningful conversations with functional leaders.

According to a recent survey of U.S. directors, improving cybersecurity and data privacy is one of the top priorities for boards in 2023 and 2024. At the same time, 38 percent of directors identify cyber risk and data security as the issue most challenging to fulfilling their oversight responsibilities, and 47 percent are engaging in director education programs to prepare for proposed regulatory requirements surrounding cybersecurity disclosures.

A cyber risk and strategy certification[5] is a straightforward way of achieving this goal. Courses like this help corporate directors enhance cyber literacy to effectively govern significant enterprise-wide cyber risks and have meaningful conversations with management.

Prioritization Is Key

Spending on information security and risk management products and services is expected to reach more than $188.3 billion in 2023[6]. That is a lot of money, particularly considering that incidents continue to occur at an alarming rate. Are organizations spending in the right areas to reduce risk?

Trusted analytics can help organizations make more informed and data-backed decisions regarding their cybersecurity programs. For example, organizations can use their Bitsight cybersecurity rating to better understand their exposure to key cyber events such as ransomware and data breaches. Armed with the right information, security leaders can prioritize increasingly stretched technology resources to improve the critical elements of their cybersecurity program and more confidently report metrics to the board and senior leaders. In turn, directors will be more confident in their deliberations if they know their organizations are spending critical resources on the right activities to enhance protection and resilience will create more confident directors.

[5]https://www.diligent.com/landing/cyber-risk-strategy-leadership-certification/?utm_campaign=COE-GL-Multi-OP-YOY-Cyber_Risk_Certification_Registration&utm_medium=email&utm_source=eblast&utm_content=LP&mkt_tok=OTQ2LUFWWC0wOTUAAAGJePdoPE82TEHH73nh0TT-sovxiREX4VTFJsq8ZrFwyFtU-X7T2krHv_9jFaPfQDRssS6ELM7m6F9MEWQhDm8jOquQR1Pv7_I5tWac0UDTEApNXIA

[6] https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i

Putting It All Together

As boards confront the risks and increased focus on cybersecurity, there are specific actions directors can take to protect themselves and their companies:

- **Assign board committee risk oversight responsibility guided by subject matter experts.** Responsibility for cybersecurity oversight should be allocated to the current board committee charged with general risk oversight (often the audit committee). Risk management experience and continuing education are crucial for managing cyber risk; companies should hire senior personnel with cybersecurity expertise who retain primary responsibility and regularly report to the board.

- **Engage third-party partners to measure status and progress.** These trusted third parties—including data providers and consultants that report to the board — should conduct periodic assessments (e.g., penetration tests) and benchmark against comparable companies and best-in-class measures. Leveraging quantitative data is critical to obtain independent, objective analysis.

- **Stay abreast of disclosure rules and shareholder expectations.** Review with counsel the latest SEC-proposed disclosure rules and expectations from ISS, Glass Lewis, and other proxy advisors to proactively address new information that may be required.

- **Track key metrics**. Identify metrics for the board to regularly evaluate the risk profile of the business, key assets that require protection, the adequacy and effectiveness of existing security controls, and best practices to limit and mitigate cyber risk associated with strategic plans. Discuss regularly at the board level.

- **Practice incident response and have concrete plans.** Finalize time-sensitive policies on business recovery and continuity (even cyber ransom), and conduct "fire drills" (including a "break glass" plan) with the board to prepare for time-sensitive situations.

Key questions boards should be asking include:

- Which executive(s) are responsible for cyber risk, and how often is the executive committee and the board being briefed on cybersecurity? Is there clear accountability linked to performance objectives?

- What measurements does the company use to determine whether our investments in cybersecurity are reducing our risk in a cost-effective manner? Are we clear on spend and value for money?

- Has management benchmarked the cybersecurity program performance against industry peers? If not, why not? If so, how do we measure up?
- Which cyber risk scenarios pose the greatest risk to our business? Are we more exposed to ransomware or data breach?
- Do we have a cyber insurance policy in place? If not, why? If so, with whom, how much, and have the premium and coverage terms changed recently? Do we understand the exclusions and whether we have coverage that will pay if an incident occurs? (If unclear, then you may be self-insuring.)
- Do we have a comprehensive vendor cyber risk management program that includes cyber reviews during the vendor/supplier onboarding process? Do we have a handle on who is accessing our systems and data?
- Are we communicating our cybersecurity performance to critical external stakeholders, including investors, insurers and business partners? If so, what are they being told?
- Have we quantified our cyber risk in financial terms (and under what scenarios) so that we can make informed decisions about risk mitigation and risk transfer? What are we getting for our money?
- Have we tested our preparedness by using cyber tabletop exercises? At what point during a cybersecurity incident would the board be engaged? Is there a "break glass" communication plan?
- How have we adjusted our plan to attract and retain cyber talent to keep up with the market?
- When launching new business initiatives (including M&A), how is cyber considered?

Cybersecurity risk is now a mainstay of corporate risk management and director responsibilities. Persistence and vigilance, alongside the right software solutions, education, preparedness and transparency, are key to ensure a holistic program of cyber protection and resilience is in place.

This article was written by the following individuals and originally published on directorsandboards.com

David Platt is chief strategy officer at Moody's Corporation
Bill Anderson is senior managing director at Evercore
Dottie Schindlinger is executive director of Diligent Institute
Steve Harvey is CEO of Bitsight

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT