CYBER EVENTS AND DIRECTORS & OFFICERS

Understanding Liability Risks and Insurance Coverage

Brought to you by: BRP Management Liability Practice and BRP Cyber Practice

With technology becoming an integral part of how businesses of all sizes and industries operate and conduct business, over the years, the scope of cyber risk has evolved immensely. While in the past, the assumption might have been that cybersecurity solely fell under the purview of IT departments, in the present, that is certainly not the case. Because of the complexity of cyber risk today, organizations need to include various stakeholders beyond IT leaders to build an effective cyber resiliency strategy, and this includes executives and board members.

In order to effectively protect digital assets, profitability, and reputation, companies buy-in from all levels of the organization, and especially leaders and board members, becomes critical. If a cyber event occurs at a company and directors and officers are found to not have done their part, there may be significant personal liability implications for these individuals.

This is why cybersecurity has become a significant Directors and Officers (D&O) claims concern.

CONSIDER THIS:
Since 2017, there were 31 security class action lawsuits related to a cyber attack or data breach filed against public companies. Though many of these suits have been dismissed, plaintiffs continue to bring forth suits and the threat of litigation comes with a price, both monetary and reputational.

REGULATORY ENVIRONMENT

The regulatory environment surrounding board members' and executives' responsibilities regarding cybersecurity is also becoming more stringent.

SECURITIES AND EXCHANGE COMMISSION (SEC)

The SEC recently proposed new requirements for companies to address cybersecurity risks. This proposed rule, which is inching closer to becoming a reality in 2023, would significantly increase the requirements and expertise of cybersecurity for boards of directors. With this rule, public companies will be required to disclose their board's cybersecurity experience, governance methods, and details about cyber incidents. This development follows efforts from the SEC throughout 2022 to protect investors from the impacts of cyber incidents, with both entities and individuals being held to task for wrongdoings related to cybersecurity breaches.

FEDERAL TRADE COMMISSION (FTC)

The FTC is another Federal entity that has shown greater interest in directors' and officers' roles in cybersecurity incidents.

EXAMPLE:
in 2022, the FTC took action against Drizly, currently a privately held company, and its CEO over allegations that the company's lax security measures led to a data breach that exposed the personal information of about 2.5 million customers. The order binds CEO James Cory Rellas to certain data security requirements that will follow Rellas even if he leaves Drizly.

BOARD SENTIMENT

Considering the circumstances, how do boards feel about cybersecurity risks? Harvard Business Review recently surveyed 600 board members about their attitudes and initiatives around cybersecurity, and the results were concerning. The research revealed these notable takeaways:

65% of directors still believe their organizations are at risk of a material cyberattack within the next 12 months, and almost 50% believe they are unprepared to cope with a targeted attack.

47% of survey participants who serve on boards interact with their CISOs regularly, with about 33% of them only seeing their CISOs at board presentations, which speaks to a disconnect and communication gap between cybersecurity teams and boards.

Only 67% of board members believe human error is their biggest cyber vulnerability, though findings from several organizations over the years indicate that human error accounts for 95% of cybersecurity incidents. This could indicate that some boards do not see the widespread organizational risk they face.

Because of our litigious society and changes in the regulatory environment, boards and executives should consider the following as they navigate the overlay of cyber and executive risks.

WHAT ARE BOARDS' RESPONSIBILITIES REGARDING CYBERSECURITY?

At a basic level, these are the expectations for boards and executives regarding cybersecurity:

1. Boards need to take reasonable steps to protect customers' sensitive data.
2. Directors and officers are also expected to support the implementation of controls to detect and prevent a data breach.
3. Following a data breach, entities need to follow the advice of privacy counsel and notify affected parties.

BRP

Directors and officers have a fiduciary duty of oversight. When it comes to cybersecurity, boards at both public and private companies have a duty to establish effective cybersecurity oversight and monitoring. Should a cyber breach occur, the actions of the board and senior executives might come under intense scrutiny. D&O personal liability has become an alarming concern since many recent lawsuits have made claims that directors and executives collude and enable each other in violating their respective responsibilities.

Failure to implement appropriate cybersecurity controls and adequately monitor them can result in breaching fiduciary duties to the company and its shareholders. The board and management may also face questions about how they handle disclosing a cyberattack or data breach to relevant authorities, financial markets, and affected parties, which is why it's essential to establish responsibilities for implementing and managing cybersecurity before and after a cyber event.

Though there are a few exceptions, private companies are subject to the same legal duties and standards as large public companies. One such exception is this: public companies must make timely, extensive disclosures about cybersecurity risks to the SEC, while this usually isn't the case for the boards of smaller private businesses due to their limited size and scale.

Prioritizing cybersecurity for the board requires continuous dedication, not just an annual update. It involves discussing it in every board meeting, obtaining cybersecurity updates between meetings, and inquiring beyond what is presented. Board members' personal actions also send a message to senior leadership, which is why they should also demonstrate a personal interest in cybersecurity, such as being secure themselves, raising questions, sharing stories, and recognizing individuals who exhibit the behaviors that the board wants to encourage.

HOW DOES INSURANCE FIT INTO THE PICTURE?

Transferring risk via insurance can be an effective risk management tool that provides financial safeguards for boards and companies in the event of a cyber breach.

There are two coverages that come into play: cyber liability and D&O liability.

Though there's no such thing as a standardized cyber liability policy, cyber insurance will typically offer financial protection and remediation services to a company from the fallout arising after a breach or cyber event compromise its systems, and/or sensitive, third-party data. Cyber policies may cover litigation fees, regulatory fines, notification costs, recovery efforts, and more. It's essential to assess the level and extent of coverage of a cyber policy to guarantee that it aligns with the company's cyber risk.

Beyond ensuring that a company has adequate cyber coverage in place as part of its cyber resiliency strategy, directors should also look at D&O insurance coverage. If a company's cybersecurity is inadequate and leads to a data breach, customers or shareholders may view it as negligence or a breach of duty by the board and try to hold directors accountable for any damages.

In most cases, a cyber liability policy likely won't offer the protection directors and officers need after a data breach, which is where a D&O policy comes into play. In the absence of D&O coverage, your individual assets may be at risk and might be surrendered to cover legal expenses.

A D&O policy can respond to investigations or personal claims made against board members in the event of a cyber incident. It is critical to confirm if the company's D&O policy would provide protection to its directors and officers if they face litigation alleging breach of fiduciary duties associated with a cyber event or data breach. A standard D&O policy covers the individual directors' acts, errors, and omissions associated with their conduct as directors, which may involve matters related to a cyber incident, but again, not all insurance policies offer the same protection. Always be on the look out for overly broad cyber exclusions on a D&O policy, which may leave you uncovered after a cyber event.

Be sure to consult with your insurance advisor about these coverages, ensuring that they are tailored to the needs of both the company and the board. You'll also want to understand how both a cyber and D&O policy define a loss, and how this impacts which policy responds to claims after a cyber breach. Never assume that a policy will provide necessary coverage for a company and its board – always be sure to verify the terms for coverage.

PRIVATE VERSUS PUBLIC COMPANIES: ARE THERE NOTABLE COVERAGE DIFFERENCES?

Both public D&O and private D&O policies protect individuals if they're named in a suit, and also cover the company where they have to indemnify those individuals. However, private D&O policies tend to provide broader coverage than a public D&O policy, barring explicitly stated exceptions. Additionally, a public D&O policy will usually only provide coverage when there is a securities class action against the public company.

WHAT ARE SOME STEPS BOARDS CAN TAKE TO CONTAIN CYBER RISK?

Though there isn't a standardized way to contain cyber risk, there are frameworks that boards can refer to when setting standards or cybersecurity governance. These include the National Institute of Standards and Technology (NIST) framework, the SEC's guidance, the FTC's recommended cybersecurity guidelines, FINRA principles, the U.S. DOJ's best practices for reporting cyber incidents, and more.

As a starting point, boards can take the following steps to help reduce their exposure to cyber risk:

- Include cybersecurity experts on the board.
- Make cybersecurity updates and discussions a regular part of board meetings, and ensure that meeting notes reflect this.
- Protect all board meeting minutes and records by storing them in a secure, encrypted platform. Have guidelines in place about storage practices and who can access which information.
- Train board members periodically so that directors understand the evolving cybersecurity and data privacy landscape.
- Establish cybersecurity oversight via committees to manage the company's cyber risks.
- Create a consistent reporting structure and cadence for oversight, such as quarterly reports from company executives, or external experts.
- Regularly evaluate the company's digital systems and assets, the risks that they pose, and ways to contain those exposures.
- Have a crisis preparedness plan for cyber events, and review and enhance that plan on a regular basis.
- Provide security and information teams the resources and budgets they need to implement cybersecurity best practices.
- Lead by example. If you, as a board director, have sensitive data stored in your electronic devices, know what you can do to be cybersecure.
- Break down silos within the company and create a culture where cybersecurity is everyone's responsibility, not just IT. Thoroughly review your cyber and D&O policies to ensure that your insurance program will respond in tandem if a cyber event occurs.

STAYING AHEAD OF CYBER RISK

Ultimately, boards need to understand that cyber risk is not just a technology issue, but rather a significant financial liability, They should discuss their organization's digital risks, implement plans to manage those risks, and take action now to protect against both D&O lawsuits and cyberattacks.

Connect with our Management Liability and Cyber experts for a comprehensive review of your coverages and to explore your available options.

Insurance products offered through one or more licensed insurance agency affiliates of Baldwin Risk Partners, LLC.

BRP