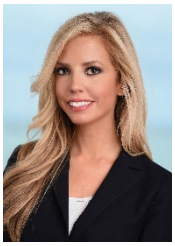
HUNTON ANDREWS KURTH

Lawyer Insights

How Cyber, D&O Insurance Can Mitigate Risk to C-Suite and Board Following a Cyber Attack

By Andrea DeField, Geoffrey Fehling and Sima Kazmir
Published in Corporate Counsel | September 3, 2021



Since the start of the pandemic, cyber criminals have become increasingly brazen. An unfortunate byproduct of these emboldened criminals is that fallout from their cyber attacks has become increasingly public, disruptive, and detrimental to public and private companies. Board members are rightfully concerned, since both the company and its officers and directors can face potential liability following a cyber attack, including board turnover, shareholder derivative claims, consumer lawsuits, and now, more frequently, regulatory enforcement actions. Fortunately, cyber insurance and directors and officers liability insurance can help mitigate these liabilities.

Why Should Your C-Suite and Board Care About Cyber Attacks?

IBM Security and the Ponemon Institute's 2021 cost of a data breach report found that the average cost of a data breach in the United States is $9.05 million—significantly higher than the global average cost of a data breach, $4.24 million. Cyber attacks have become an unavoidable business risk. Board members and the C-Suite must prepare to deal with the potential ramifications of an attack—loss of business and/or consumer data; interruption to business operations, often on a global scale; investigation and response costs; reporting and notice obligations; consumer and/or shareholder suits; potential ransom payments; increased public scrutiny; and damage to reputation and the public's trust.

Perhaps even more worrisome, federal and state regulators have begun to crack down on companies' cybersecurity disclosures. For example, in February 2018, the SEC published a statement and guidance on public company disclosures, noting that, due to the "frequency, magnitude and cost of cybersecurity incidents, the commission believes it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion."

Previously, the SEC has fined public issuers for failures to disclose known breaches within two years of discovery. In June 2021, however, the SEC went one step further and fined a company over $485,000 for its failure to maintain adequate procedures and controls for disclosure. The SEC's enforcement against First American Financial Corporation related to a vulnerability discovered by a cybersecurity journalist on May 24, 2019. First American disclosed the incident to the SEC in a Form 8-K four days later. Despite the seemingly prompt disclosure, the SEC concluded that the company had failed to maintain required disclosure controls and procedures because First American had failed to inform its senior executives that the company's own information security personnel had identified the vulnerability several months earlier and failed to remediate.

How Cyber, D&O Insurance Can Mitigate Risk to C-Suite and Board Following a Cyber Attack
By Andrea DeField, Geoffrey Fehling and Sima Kazmir
Corporate Counsel | September 3, 2021

Then, in August 2021, the SEC announced that Pearson plc had agreed to pay a $1 million fine to settle charges that it had repeatedly misled its investors about a 2018 cyber attack that involved the theft of student records, including dates of birth and email addresses. In this action, the SEC similarly alleged that Pearson had inadequate disclosure controls and procedures.

The increased regulatory scrutiny of cyber incidents is not limited to the SEC. In early 2017, the New York Department of Financial Services promulgated 23 NYCRR Part 500, which established cybersecurity requirements for certain financial services companies and required they adopt programs to protect consumers' private information. First American was the first charged in connection with this regulation, in relation to the same vulnerability identified in the June 2021 SEC action. Though the First American action has not yet been heard, and a second amended statement of charges was recently filed, the NY DFS recently fined another entity, Residential Mortgage Services, $1.5 million in connection with violations of 23 NYCRR Part 500.

The SEC and NY DFS's recent conduct makes clear that federal and state regulatory agencies are increasingly scrutinizing cyber attacks and initiating enforcement actions based on how companies their directors, officers, and information security personnel respond to cyber threats. These are just a few examples—the Federal Trade Commission regularly investigates and takes enforcement action against companies that fail to live up to promises to consumers that they will safeguard their personal information. For example, Equifax, Inc. agreed to pay $575-$700 million as part of a global settlement with the FTC, Consumer Financial Protection Bureau, and 50 U.S. states and territories to settle allegations that it failed to take reasonable steps to secure its network, leading to the widely publicized 2017 data breach that affected 147 million people.

Given the rash of ransomware and other cyber attacks in 2021, companies should anticipate that government agencies and regulators will take a more active role in the future. Indeed, potentially signifying further focus on corporate response to cyber attacks, in June 2021, the SEC conducted an enforcement sweep of SolarWinds customers following the public disclosure of a major cyber attack. The SEC sent information requests to issuers and other regulated entities, in which they offered amnesty for reporting failures (subject to limitations) and asked for information about previously undisclosed compromises.

How Can Your Cyber and D&O Insurance Help Protect Your C-Suite and Board From Certain Risks?

When purchasing or renewing cyber and D&O insurance, companies must look at their program as a whole to ensure that there are no gaps in coverage for liabilities that directors, officers, and the company may face in the aftermath of a cyber attack. While cyber, D&O, and other liability insurance policies are meant to work together, the actual coverage afforded across a company's insurance program can lead to a patchwork of policies resulting in significant coverage limitations or, even worse, critical gaps in protection for cyber-related exposures.

The following are a few of the key issues and gaps that corporate policyholders should look out for in renewing or procuring a cyber policy.

- Liability coverage should be triggered by not only suits and arbitration proceedings, but also formal and informal investigations.

How Cyber, D&O Insurance Can Mitigate Risk to C-Suite and Board Following a Cyber Attack
By Andrea DeField, Geoffrey Fehling and Sima Kazmir
Corporate Counsel | September 3, 2021

- Policies should cover fines and penalties. To help avoid an insurer's argument that such fines or penalties are uninsurable and thus not covered, corporate policyholders should negotiate a "most favored jurisdiction" clause, such as one stating that civil fines or penalties will be covered where insurable by the applicable law which most favors coverage.

- Any exclusions for violations of securities laws should contain an express exception for claims arising out of a privacy event or a failure to disclose a cyber incident in violation of breach notification laws.

- Exclusions for unfair trade practices or FTC actions should similarly be carved back so as to not apply to regulatory actions or claims arising out of an otherwise covered cyber attack.

- Policyholders should also consider optional coverages, such as reputation loss coverage and public relations and crisis management coverage, to help mitigate the fallout from any cyber attack.

The company's D&O insurance should complement its cyber insurance coverage. A major cyber incident may exhaust available limits of cyber insurance, so it is imperative to ensure that the D&O policy does not have cyber exclusion and will respond to traditional D&O risks, even those arising out of a cyber-event. If D&O insurers will not remove exclusions for claims arising out of cyber or privacy incidents, public companies should try to carve back at least some coverage, such as for securities claims. Corporate policyholders should also request that affirmative coverage for investigations be added to the D&O policy, including for investigations of the company and not just investigations of directors and officers.

For both cyber and D&O coverage, policyholders should also:

- Review terrorism or war exclusions to make sure they cannot be used by an insurer to deny coverage for common cyber attacks. Companies should request that any terrorism and war exclusions contain exceptions for cyberterrorism.

- Ensure contractual liability exclusions contain carve-outs for liability that would exist in the absence of contract. Many companies are required to make contractual representations or warranties on cyber security programs or standards as part of contacts with clients and vendors and these representations may be alleged in a suit following a cyber attack. Consumers also often assert quasi-contract theories of liability regarding safeguarding of data.

- Make sure that exclusions for bodily injury or invasion of privacy are carved back so that they do not apply to otherwise covered claims arising out of a privacy breach. Exclusions for bodily injury should expressly contain a carve-out for emotional distress arising out of a breach.

- Assess intellectual property exclusions to ensure that broadly defined exclusions covering patents, trade secrets, or other IP could not be triggered if bad actors hack a company for the purpose of gaining access to the companies IP portfolio. Similar to contractual liability exclusions, careful attention must be given to IP exclusions and how they may be triggered based on exfiltration of client-side data possessed by third parties.

- Evaluate any exclusions, especially in D&O and professional liability policies, that reference a failure to maintain "adequate" insurance, which can operate in the same manner as an explicit cyber exclusion where a company is alleged to have failed to procure (or to have procured inadequate) cyber coverage.

The potential coverage gaps discussed above are just a few of the traps for the unwary director, officer or company. Companies are best served by working with experienced insurance coverage counsel and insurance brokers to analyze coverage and fill any gaps with appropriate endorsements at renewal.

Andrea DeField *is a partner in the firm's Insurance Coverage group in the firm's Miami office. Andrea has dedicated her career to helping clients manage risk and maximize insurance recovery. She can be reached at +1 (305) 810-2465 or adefield@HuntonAK.com.*

Geoffrey B. Fehling *is Counsel in the firm's Insurance Coverage group in the firm's Washington D.C. office. Geoff represents corporate policyholders and their officers and directors in insurance coverage disputes involving directors' and officers' (D&O), errors and omissions (E&O), and other professional liability claims, cybersecurity and data breaches, representations and warranties, employee theft and fidelity claims, government investigations, breach of fiduciary duty, environmental liabilities, and property damage. He can be reached at +1 (202) 955-1944 or gfehling@HuntonAK.com.*

Sima Kazmir *is an associate in the firm's Insurance Coverage group in the firm's New York office. Sima is a proactive commercial litigator whose practice focuses on complex consumer finance, insurance coverage and business litigation. She can be reached at +1 (212) 309-1112 or skazmir@HuntonAK.com.*