**Westlaw Today**
*powered by Reuters*

# Cyber and D&O insurance: maximizing coverage for companies and executives from cyber incidents

**By Lorelie S. Masters, Esq., Andrea DeField, Esq., Geoffrey B. Fehling, Esq., and Charlotte Leszinske, Esq., Hunton Andrews Kurth**

**SEPTEMBER 5, 2023**

Cyber incidents are growing in frequency and severity. Enforcement, too, is ramping up. The DOJ, FTC, and SEC are all involved in investigating potential violations of law following cyber incidents and prosecuting companies who fail to protect data.

Executives are right to worry about these risks, particularly because agencies, and shareholders, have shown willingness to pursue individual directors following an incident. Insurance policies providing cyber and directors and officers ("D&O") liability coverage can reduce corporate and individual exposure in the event of a cyber incident.

*Recently, Uber's former Chief Information Security Officer Joe Sullivan became the first executive to be criminally prosecuted, and then convicted, for failing to disclose a data breach.*

But these policies are not one-size-fits-all, and companies would be well-served by reading their policies carefully to determine, and proactively address, potential weaknesses or gaps that could mean the difference between the insurer accepting or rejecting a claim for coverage.

## I. Why cybersecurity should matter to executives and boards

In 2023, nearly every organization, in every industry, is at risk of cyber incidents. Cisco found that nearly two-thirds of reporting organizations experienced major security incidents that jeopardized business operations.

These incidents have significant financial ramifications — IBM Security and the Ponemon Institute's 2022 cost of a data breach report found that the average cost of a data breach in the United States is $9.44 million — significantly higher than the global average cost of a data breach, at $4.82 million. The effects of a cyber incident can linger. Bitglass found that following a data breach, stock prices for publicly traded companies dropped an average of 7.5% and took an average of 45 days to recover to pre-breach levels.

Further, incidents like ransomware attacks can encrypt some or all of a company's systems, resulting in companies facing lost profits in the several millions of dollars because of system outages and ramp-up time when systems begin to be restored.

Recently, regulators have begun cracking down on companies who fail to secure data and/or fail to promptly disclose cyber incidents. In October 2021, Deputy Attorney General Lisa Monaco announced[1] the launch of the Civil Cyber-Fraud Initiative, led by the Fraud Section of the DOJ Civil Division's Commercial Litigation Branch. The Civil Cyber-Fraud Initiative was created to "utilize the False Claims Act ('FCA') to pursue cybersecurity related fraud by government contractors and grant recipients."

Since the program was announced, the DOJ has done as promised. Just last month, it announced a settlement[2] with Jelly Bean Communication Design LLC and manager Jeremy Spinks, individually, for failing to secure data on HealthyKids.org.

Other federal agencies have also taken action. The FTC, for example, has ramped up enforcement of data privacy standards under Section 5 of the FTC Act, coming after large companies like BetterHelp[3] ($7.8 million) for failing to safeguard data. In addition to civil penalties, many of these companies will be subject to FTC oversight for an extended period of time (BetterHelp will be monitored for twenty years) and may have to comply with additional requirements.

The FTC[4] and SEC[5] have also engaged in rulemaking on cybersecurity issues. In March 2023, the SEC proposed three new cybersecurity rules,[6] which would require covered entities and systems to undertake certain cybersecurity-related actions such as reforming security programs and procedures and providing notice of cyber incidents. As of June 13, 2023,[7] three sets of proposed SEC cybersecurity rules are in the Final Rule Stage.[8]

Not just companies, but individual executives, may be vulnerable. Recently, Uber's former Chief Information Security Officer Joe Sullivan became the first executive to be criminally prosecuted,[9] and then convicted, for failing to disclose a data breach.

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

THOMSON REUTERS®

At the time, Uber was being investigated by the FTC for an earlier data breach. Rather than reporting the breach, Sullivan and his team paid the hackers' ransom and had them sign a nondisclosure agreement; the FTC was not informed of the breach until 2017. Sullivan was subsequently convicted on federal charges of obstructing an FTC investigation and misprision (concealing a felony); in May 2023, he was sentenced to three years' probation and ordered to pay a $50,000 fine.

Executives may also be held liable under state law. Delaware recently ruled[10] that in addition to directors, officers owe a duty of oversight, opening the door for civil breach of oversight claims to be brought against both directors and officers.

## II. Cyber vs. D&O insurance: distinct and complementary protections

Companies worried about these risks can reduce exposure with cyber and D&O insurance. These two types of policies provide distinct, but sometimes overlapping, protections for the types of liability arising out of cyber incidents discussed above.

**Cyber insurance** protects an organization against many different risks associated with cyber incidents. Cyber policies typically include both "first-party" and "third-party" coverages:

- First-party coverages help respond to and defray costs associated with responding to cyber incidents. Policies may cover breach response costs (money spent to stop a threat actor, investigate the cause, scope, and extent of the incident, and to restore security systems), business interruption loss (revenue lost while systems were interrupted during the attack and for ramp up following restoration), cyber extortion expenses (for example, ransom demands, and costs to retain an extortion specialist), digital asset restoration costs (spent to restore stolen or destroyed data), legal expenses for privacy and cybersecurity advice, costs to notify impacted individuals and provide credit monitoring or identity theft services, and public relations costs, among other costs. First-party coverage may also include business interruption loss arising out of outages or cyber incidents on a key vendor or supplier's system, such as a cloud service provider.
- Third-party coverage, in contrast, protects against claims and lawsuits asserted by others. Policies may cover defense costs (costs to defend against a lawsuit), settlements, and other costs arising out of third party claims, regulatory investigations and formal actions (*e.g.*, FTC enforcement actions), and media or IP violations.

**D&O insurance** protects an organization's directors and officers, and sometimes the organization itself, from claims arising out of alleged wrongful conduct by directors, officers, or employees in making decisions and otherwise managing the company. Common D&O exposures include alleged breach of fiduciary duties by the board, securities class actions or claims alleging regulatory violations, reporting errors, and inaccurate disclosures.

In addition to defense costs, private company D&O insurance may also cover costs arising out of regulatory investigations.

## III. Evaluating the strength of cyber and D&O insurance programs

Adding both cyber and D&O insurance to an insurance program may protect an organization and its officers and directors from common costs arising out of cyber incidents. But simply purchasing both types of coverage is not enough, as not all policies are created equal. To the contrary, insurance forms can have material differences that determine whether a cyber-related insurance claim will be accepted or rejected.

*D&O insurance protects an organization's directors and officers, and sometimes the organization itself, from claims arising out of alleged wrongful conduct by directors, officers, or employees in making decisions and otherwise managing the company.*

Moreover, even the best standard-form language can often by modified by endorsement to further expand coverage, narrow exclusions, or strengthen terms in significant ways to help guard against uncovered exposures (or, the opposite — endorsements can materially limit coverage that was otherwise available in the main policy form).

Dozens of provisions can help or hurt the chance of recovery in the event of a claim. For organizations evaluating their current program, some provisions to look out for are:

- **Cyber exclusions**. With cyber incidents on the rise, some insurers have added broad "cyber" exclusions to D&O policies. While the purpose of those exclusions is to shift true cyber exposures to cyber policies, many times in practice the exclusions are far too broad and limit or negate large swaths of coverage for D&O claims based on remote connections to a cyber event. Narrowing those exclusions, especially broad lead-in and causation language, can help minimize those risks.
- **Pre-approval of key vendors**. If a cyber incident occurs, organizations will need to quickly retain many key vendors, including legal counsel, IT forensics, public relations, and potentially an extortion specialist. Some insurers require the insured to use their panel vendors. Organizations should check their cyber policies for such a requirement and ensure that they are either comfortable using the insurer's panel or should move to a policy that will allow the organization to choose its own vendors. For the latter, the organization should seek pre-approval of its preferred vendors by endorsement onto the policy to ensure there is no dispute with the insurer in the critical hours following discovery of a cyber incident.
- **Conduct exclusions**. In data privacy actions, public and private plaintiffs commonly allege misconduct by the company or its executives, for example in the BetterHelp and Uber/John Sullivan cases mentioned above. Conduct


©2023 Thomson Reuters

exclusions in D&O policies may bar coverage for claims arising out of fraudulent or criminal conduct, or the willful or deliberate violation of the law. While some type of conduct exclusion is usually unavoidable, these exclusions can be narrowed by inserting final adjudication requirements.[11] Coverage is not barred until there is a final, nonappealable adjudication that the insured's conduct was wrongful.

- **Insured v. insured exclusions**. These exclusions, commonly found in D&O policies, bar claims[12] by one insured (*e.g.*, an organization) against another insured (*e.g.*, the organization's director). The exclusion should contain an exception for whistleblower claims, for example, if a director reveals that their organization improperly covered up a cyber incident.
- **Exclusions for violations of securities laws, or unfair trade practices**. Securities law exclusions in technology errors and omissions or cyber policies should contain a carve-back for otherwise-covered privacy claims. Exclusions for unfair trade practices claims in D&O policies should contain exceptions for claims arising out of data breaches and failures to disclose cyber incidents in violation of applicable law, including regulatory actions.
- **Contractual liability exclusions**. Many organizations, when contracting with clients or vendors, must make representations and warranties regarding their security systems or ability to protect data. These organizations should ensure that exclusions for contractual liability exempt liability that would exist in the absence of contract.
- **Other exclusions**. The list above is by no means exhaustive. Policyholders may also run into claim disputes arising from exclusions for professional services, terrorism, intellectual property, and bodily injury and property damage, just to name a few. Each policy form and endorsement should be scrutinized to fully understand not only how a particular policy may respond to a claim but also how a particular coverage grant (or exclusion) operates within the insurance program as a whole.

Organizations should carefully review existing policies to determine which coverages exist and whether additional or modified terms are warranted. Each line of coverage should be carefully analyzed and, if needed, modified before a claim arises.

## Notes

[1] https://bit.ly/3YSoGxl

[2] https://bit.ly/3Pc11ET

[3] https://bit.ly/3qO4LDf

[4] https://bit.ly/3QVqqUJ

[5] https://bit.ly/3EaVqlM

[6] https://bit.ly/3qQHz7p

[7] https://bit.ly/3QWjwia

[8] https://bit.ly/44GGtJv

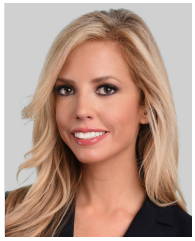
[9] https://bit.ly/3OPSXs8

[10] https://bit.ly/3PaATue

[11] https://bit.ly/3szkh6n

[12] https://bit.ly/3OJrjNi

## About the authors

(L-R) **Lorelie S. Masters** is a partner with **Hunton Andrews Kurth** in Washington, D.C. A nationally recognized insurance coverage litigator, she advises clients on a wide range of liability coverages, including insurance for environmental, employment, directors and officers, fiduciary, property damage, cyber, and other liabilities. She has written two textbooks on insurance coverage and is a founder and past president of the American College of Coverage Counsel. She can be reached at LMasters@HuntonAK.com. **Andrea DeField** is a partner in the firm's insurance coverage practice in Miami, where she co-leads the cyber insurance practice. She was named an "Elite Woman" by Insurance Business America, a "Next Generation Partner" by The Legal 500, and a "Rising Star" in insurance by both Law360 and The Legal 500, and received the American Bar Association Young Lawyer Division's "On the Rise" Award. She can be reached at adefield@HuntonAK.com. **Geoffrey B. Fehling** is a partner in the firm's Boston office, where he advises corporate policyholders and their directors and officers in insurance coverage matters, from placement of complex insurance programs and policy reviews to claim advocacy through arbitration, litigation, trials and appeals. He is a prolific author on insurance and risk management topics and co-chair of the American Bar Association Business Law Section's Director and Officer Liability Committee. He can be reached at gfehling@HuntonAK.com. **Charlotte Leszinske,** an associate in the firm's Washington, D.C., office, represents policyholders in insurance coverage actions in federal and state courts across the country. Her work includes environmental liability, mass torts, product liability, cyber incidents, D&O coverage and bad faith. She can be reached at cleszinske@HuntonAK.com. This article was originally published July 25, 2023, on the firm's website. Republished with permission.

**This article was first published on Westlaw Today on September 5, 2023.**

© 2023 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.