FINE PRINT

# New Cyber Risk Management Concerns for Directors & Officers

by Joshua Gold

Never has senior management been faced with so many daily organizational threats stemming from computer-enabled perils. Risk management for protection of senior officers and the board has taken on new dimensions with unparalleled cybercrime and sweeping new data privacy regulations. The coronavirus pandemic compounds the challenge of maintaining computer security, as ever-growing numbers of workers follow directives to work from home.

## INCREASING REGULATION AND OVERSIGHT

The enactment of regulations like GDPR overseas and the California Consumer Privacy Act in the United States has made cyber risk management increasingly difficult. Regulators now require that organizations have reasonably designed and implemented security around their online systems. The SEC continues to up the ante over board-level obligations to safeguard against cyber perils, fining some and admonishing others. In 2018, the SEC fined one public company $35 million for its failure to timely disclose (and refrain from "misleading" investors about) a massive hack of computer systems in which hundreds of millions of customer accounts were compromised. Subsequently, the same public company was forced to settle shareholder litigation for $80 million (in addition to significant legal expense incurred in defending itself, no doubt).

Previously, Home Depot had thwarted derivative shareholder litigation against it, winning a dismissal of the suit at the trial court level. Nevertheless, before appeals were heard, Home Depot relented, and ended up settling after its data breach prompted not only shareholder litigation, but consumer privacy litigation too. The seven-figure settlement (of a case it had originally won) plus agreement to institute numerous cyber governance reforms at the executive level, portends a greater threat landscape for directors and officers.

## THE NEED FOR D&O INSURANCE

Directors' and officers' insurance has already been called upon to cover the significant costs of defense representation against shareholders and regulators over cyber incidents. D&O insurance is absolutely essential when the cyber stakes rise for officer and director liability exposures. Organizations cannot solely rely upon dedicated (standalone) cyber insurance products. Directors and officers will still need their D&O insurance protection since many cyber policies may impose an express exclusion for securities claims. Thus, noticing a cyber securities lawsuit for coverage under a cyber policy will surely trigger a coverage fight with many cyber insurance companies.

Further, D&O insurance remains one of the broader liability insurance policies, offering a strong scope of coverage for an officer's or director's (and sometimes a corporation's) "wrongful acts." Outside of a few select exclusions (e.g., ERISA, asbestos and nuclear claim exclusions), almost all perils leading to allegations and claims of wrongful acts committed by an insured in their management capacity are covered. Thus, in the ever more perilous cyber environment, it is essential that boards and the executive management team maintain the availability of D&O insurance for cyber-related claims.

RISK MANAGEMENT

Reprinted with permission from Risk Management.
Copyright © 2020 Risk and Insurance Management Society, Inc.
All Rights Reserved.
**www.rmmagazine.com**

March 2020

## SAFEGUARDING D&O INSURANCE FOR CYBER CLAIMS

With increases in cyber exposures for senior management, D&O insurance underwriters may begin to impose exclusions, sub-limits and other coverage conditions. In addition, policyholders need to be careful in responding to insurance applications that may be used by insurance companies post-claim to seek a forfeiture of coverage.

They should also pay strict attention to D&O policy retroactive coverage dates. Where at all possible, push for better terms on this front. The problem is that some cyber threats occur well before the policyholder actually discovers evidence of an intrusion. Further, class action complaints routinely make vague allegations of a long-standing corporate environment of lax cybersecurity that may stretch back years before the lawsuit's commencement (as well as long before the date of the cyber incident). We now know all too well that hackers can intrude into computer systems weeks, months and even years before the policyholder becomes aware of the threat. Purchasing insurance coverage with a retroactive date that pre-dates the policy period, especially by a number of years, removes a potential coverage fight from the menu.

The following are some key risk management steps for board-level and officer cyber exposures:

- Stay informed about cyber exposures generally and your organization's security for online systems and storage devices specifically—these days, regulators and investors are demanding an informed executive suite in this area).
- Ensure that adequate resources are committed to combating the cyber threat. Cost-cutting here will not be well received when a serious breach has to be explained and defended to regulators, law enforcement, investors and other stakeholders.
- Ensure that reasonable steps are followed for telecommuting due to coronavirus, so that remote access and off-site data use is implemented and managed in as secure a manner as possible.
- Provide notice to your insurance companies quickly after a breach—including your D&O insurance companies. Early in the process of responding to a breach, the meter will be running on costs, and some of those costs may be to protect, investigate and defend the board.
- Ensure, in the first instance, that D&O insurance coverage (including primary, excess, Side A, etc.) remains free of cyber-related exclusions or sub-limits. Management will be highly concerned with any argued "gap" in coverage should a cyber event ensue—especially with the advent of cyber derivative shareholder litigation. ■

**Joshua Gold** is a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

Copyright © 2020 Risk and Insurance Management Society, Inc.

All Rights Reserved.

**www.rmmagazine.com**

FINE PRINT

RISK MANAGEMENT

Reprinted with permission from Risk Management.

Copyright © 2020 Risk and Insurance Management Society, Inc.

All Rights Reserved.

**www.rmmagazine.com**

June 2020