AmWINS Group, Inc.

CYBER LIABILITY: THE D&O DILEMMA

CONTACT

To learn more about how AmWINS can help you place coverage for your clients, reach out to your local AmWINS broker or marketing@amwins.com.

LEGAL DISCLAIMER

ABOUT THE AUTHOR

This article was authored by Megan North, a member of AmWINS' national Professional Lines Practice.

One click is all it takes to order goods, exchange payment, and have the items shipped and delivered to a doorstep within hours.

But what happens when that one click is not used to facilitate commerce, but rather used to intentionally or even accidentally disrupt a network? When one click releases a malicious code causing an assembly line to come to a screeching halt? When one click transfers millions of dollars to a fraudulent account? When one click by a rogue employee disseminates the contents of personal files to the public? In these instances, who is ultimately responsible?

In recent cases, fingers have pointed directly at the board of directors. Since 2013, several shareholder derivative suits have been filed following network security breaches. Defendants have included Home Depot, Horizon Blue Cross Blue Shield, Target, Wyndham, and Wendy's. Technology is changing at a rapid pace, and it is clear that consumers and shareholders have high expectations for businesses and those who run them.

Allegations in these network security cases have included breach of fiduciary duty, negligence, breach of implied contract, and violation of various state and federal statutes. Interestingly, most of the aforementioned cases have been dismissed (or settled) – apart from Wendy's, which is still in its early stages. These dismissals are showing that the plaintiffs are having difficulty: (1) proving corporate mismanagement as a direct cause of harm from a data breach, and (2) showing actual compensatory injuries as a direct result of the breach. Courts have been dismissing cases in which actual damages have not been proven.

Cases alleging executive mismanagement are subject to the business judgment rule, which presupposes that the individuals on the board acted in good faith, on an informed basis, and in the best interests of the company. Absent insurmountable proof that D&O's acted in self-interest or were grossly negligent in their actions with regard to preventing a breach, those allegations have not been holding up.

Additionally, plaintiffs must prove actual economic harm has occurred as a result of a breach. Judges in recent cases have proven strict on this requirement, as evidenced by the Wendy's case in which the original complaint was dismissed as allegedly fraudulent charges to the plaintiff's debit card were not sufficient grounds upon which to bring suit. To further clarify that requirement, U.S. District Judge Claire Cecchi of the District of New Jersey (who presided over the Horizon BCBS case) said the individual plaintiffs "cannot rely on their increased likelihood of future harm as a basis for their case."

Despite the dismissals, this litigation highlights several concerns for Directors & Officers (D&O's). Not all cases or allegations are being dismissed. Some financial institutions and regulators have found success in their lawsuits brought against D&O's. Settlements have been made to avoid extensive litigation in certain cases. Even when allegations don't stick, there may still be hefty defense costs. The relentless pursuit by plaintiff attorneys highlights that there exists a pervasive expectation of, and onus placed upon Directors & Officers with relation to cyber exposures. These individuals are collectively responsible for making important decisions on behalf of their organizations and may be held personally liable in the event that these decisions produce egregiously negative effects on the company as a whole.

(continued on next page)

ON YOUR TEAM.

AmWINS Group, Inc.

CYBER LIABILITY: THE D&O DILEMMA

(continued from previous page)

D&Os remain particularly susceptible to plaintiff claims in relation to cyber exposures. These individuals are *collectively responsible* for making important decisions on behalf of their organizations and may be held *personally liable* in the event these decisions produce egregiously negative effects on the company as a whole.

It is imperative that directors and officers secure a comprehensive executive liability insurance program to protect themselves, but appropriate coverage is just one component of effective protection. As security and privacy breaches continue, and subsequent suits emerge, it is paramount that D&O's can show they've taken the necessary steps to protect the information of their customers, as well as the interests of their companies.

So what can be done? How can D&O's effectively mitigate their cyber liability exposure and that of the companies they are charged to lead?

1) Understand the risk.
- Know the types and value of your data, where the data is held, and how much of that data is held or utilized during the day-to-day transaction of business
- Obtain an overview of the systems and networks used
- Require regular updates of vulnerabilities and threats to these systems

2) Minimize the risk.
- Create awareness of potential threats for all data handlers in the organization
- Develop security protocols; educate employees on and track compliance with these procedures
- Require full compliance with security protocols; emphasize that deviation is unacceptable under any circumstance
- Empower employees to question a request when it does require them to deviate from protocol (even if that request purports to have come from an executive or manager)

3) Be prepared.
- Develop a breach response plan with detailed instructions and procedures
- Test the breach response plan
- Document these preparation efforts. This step is not only worthwhile in the event of a breach, but also demonstrates that diligent cyber-security efforts were made, in the event of litigation. Regulators will ask what happened, what prevention steps were taken and how the organization responded.
- Ensure designated procedures exist surrounding public relations and access to the public in the event of a breach incident
- Limit the individuals with authority to speak with media concerning these events.

Incidents are inevitable, and while the above measures can help mitigate liability in the event of a breach, no plan is foolproof. Dealing with a cyber-security incident is complicated, expensive, and time-consuming. A comprehensive privacy & network liability insurance policy provides valuable protection for a company, as well as pre-breach loss mitigation services.

How does a network security & privacy policy help?

- **Pre-Breach Services**: Many insurers will offer pre-breach coaching and table top exercises to help recognize threats and establish response plans.
- **Breach Response Services (during/post)**: In the event of a breach, insurers have partnered with experienced vendors to aid their policyholders in responding to the incident and navigating the complex legal and regulatory environments. In addition to the tangible benefits of a team of experts working on their behalf, policyholders also benefit from discounted rates negotiated with these vendors.
- **Balance Sheet Protection**: The policy can provide a mechanism for transferring some of the financial burdens incurred from a covered incident. These may include: indemnity obligations, regulatory fines and penalties, costs to notify affected individuals, defense costs, and costs for public relations services to mitigate reputational damage. Additionally, Cyber Liability policies respond where a D&O policy will not. Cyber Liability policies assist with handling the breach, and D&O policies protect the D&O's for the decisions they made regarding network security and in response to a breach.
- **Recovery**: In the event of a data breach, some of the most costly damage is related to reputational harm. Some cyber liability carriers include coverage for services to aid with public relations and reputation recovery after a breach.

D&O and Cyber Liability policies are specifically designed to address different elements of cyber risk. Whether created to respond to a breach or to protect D&O's for their business judgments, these policies should be evaluated by an insurance broker who specializes in these lines of insurance. AmWINS Brokerage employs a nationwide team of product experts ready to assist in the analysis and placement of D&O and Cyber Liability insurance.

ON YOUR TEAM.