Protecting Directors and Officers in the New World of Cyberthreats

by Joshua Gold and Daniel J. Healy

By now, most directors and officers are acutely aware of the exponential growth of cyberrisks. They may be less aware that the very ubiquity and familiarity of cyberattacks has exposed them to greater personal risk than they faced when such attacks were more of a novelty. Insurance coverage for such known threats, and the scrutiny of directors and officers that often follows, must be prioritized.

Evolving regulations and investor expectations put the onus on directors and officers to take responsibility for prevention, mitigation and recovery from cyberattacks. Regulators are insisting on it. Corporate boards must address the issue, engage and vet competent outside vendors handling data or accessing systems, test corporate security measures, ensure that the appropriate insurance coverage is in place, and continually re-assess their company's risk.

Such accusations have grown increasingly likely. The Federal Trade Commission (FTC) has gone on record stating that, in a post-breach investigation, it looks at whether a company investigated appropriate cybersecurity vendors and did not "unreasonably" hire vendors that failed to competently protect the company. The Securities and Exchange Commission, Federal Communications Commission and state attorneys general have launched numerous investigations into the efforts of corporate boards and senior management to prevent data breaches and make fair disclosures about the corresponding risks. The number and diversity of regulators is a good indication that a corporation, and its management, may need a diverse set of coverages to rely upon if a cyber-related loss is suffered.

When a breach does occur, directors and officers and their companies should not expect to be treated like victims, even though they and their company may have been victimized by an outside or internal threat. They must prepare in advance to answer tough questions about the steps they took to reasonably protect their company against such loss. Part of that preparation involves appropriate insurance coverage.

Directors and officers should ensure that the insurance purchased is suited to the risks specific to their industry and individual business. Among the myriad breaches that reach the news, the facts are rarely the same and the nature of the business suffering the attack often dictates the type of attack, the nature of the compromised data and the type of loss suffered. For example, a breach of a bank's credit card data involves different losses than breach of a health insurance company's medical records for patients, even though both breaches could lead to similarly enormous losses and liability.

Regardless of a company's industry, however, a few types of insurance should always apply to situations where directors and officers are accused of not taking appropriate and reasonable steps to protect against cyber loss. Directors and officers coverage and errors and omissions coverage may be vital if regulators, shareholders, customers or others accuse the board and management of failing to reasonably safeguard data or systems.

One prudent step is to assess coverage already purchased and compare it to the company's risk profile. At a minimum, coverage should be in place to protect the company and the individual directors and officers—as the class action suits and derivative shareholder suits against Target Corporation demonstrate. Without appropriate coverage, directors and officers could be left on their own to defend against lawsuits and pay any potential liability. That risk is even greater for smaller companies that may not have the same resources to voluntarily indemnify directors and officers.

Similarly, directors and officers will want to understand whether their D&O coverage covers regulatory investigations, interviews and non-formal inquiries. If it can be expected that a data breach will lead to an investigation, it is worth the time to determine whether a D&O policy covers such risks, and whether coverage may also be found under dedicated cyber policies, business package policies, errors and omissions policies, or possibly some other form of insurance.

As many policyholders have discovered in the non-cyber arena, regulator inquiries, investigations and proceedings can be lengthy and costly. Boards, officers, their risk managers and consultants need to spend time analyzing the available coverage

from the perspective that they will likely suffer a data breach.

Whether appropriate coverage was in place prior to a breach is one of many questions that those who scrutinize the board's conduct once a breach has occurred are likely to ask. Already, legislators and regulators have suggested that the purchase of cyber insurance needs to be a consideration. Directors and officers should take steps not only to avoid assertions that they did not adequately protect their companies against risks, but also to avoid personal liability for such losses. ■

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.*

Daniel J. Healy *is a partner in Anderson Kill's Washington D.C. office where he exclusively represents policyholders in insurance recovery matters.*

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com