Mutual INsurance

The New Fire in the Warehouse

By Patricia McHugh Lambert & Gregory Weiner

THE INCREASE IN CYBER DATA BREACH THREATS IS MAKING BOARD MEMBER, OFFICER, AND DIRECTOR LIABILITY COVERAGE AN EVEN MORE IMPORTANT PART OF A COMPANY'S PROFESSIONAL LIABILITY INSURANCE PACKAGE.

So much has been written about cyber liability that people can become numb to the topic. After all, how many times can we read about the 2013 data breach that impacted all of Target's United States locations and how that event is still impacting the company's operations, earnings, and brand? How many times can we read about data breaches at bars and restaurants such as the one that cost P.F. Chang's more than $50 million to resolve? Or how many times can we receive a new bank card in the mail because our financial institutions are worried about account hacking and are taking steps "to protect customers."

Consumers and business professionals, including those in the insurance industry, know that cybersecurity is important. Yet, too many people, with a relative shrug, move on to the other pressing matters, believing their only risk from cyberattacks is whether their own personal information has been hacked. This casual approach, particularly by executives and individuals who serve on boards of directors, belies the present, growing potential for personal cyber liability risk.

Officers, directors, and board members may have a personal duty to use reasonable efforts to protect:

- Names and addresses;
- Social Security and driver's license numbers;
- Health information;
- Bank routing and credit card information; and
- Hard drives and passwords.

Board members and C-level executives should know that they have a fiduciary duty to protect the financial integrity of the organization they serve as well as to prevent the company from unnecessary risk.

Think about this: the board of a company that stores its entire inventory in a single warehouse would know the business' financial future would likely be in jeopardy if a fire started in that warehouse. Its members would be remiss in fulfilling their fiduciary duties if the company did not have, at a minimum, insurance to protect against that loss. The board members could, under certain circumstances, have personal liability to the company's stakeholders if the risk is not considered and appropriately and reasonably mitigated.

CYBER LIABILITY IS THE NEW FIRE IN THE WAREHOUSE FOR BOARD MEMBERS.

As Jordan Reed Stark, a cybersecurity consultant, noted in an article for Cybersecuritydocket.com, "[E]very board now knows its company will fall victim to a cyberattack, and even worse, that the board will need to clean up the mess and superintend the fallout."

Thus, board members may likely have a fiduciary duty to protect a company against cyber risk just as much as they would against a fire in a warehouse. Prudence dictates that a board takes reasonable measures to provide adequate cybersecurity and to obtain appropriate insurance to cover potential losses. A board also needs to have plans for how to deal with security breaches, including how to deal with notification duties and brand protection issues. Given the multifaceted nature of potential risk exposures, board members need to take cybersecurity issues seriously and ensure the implementation of processes to prevent breaches and mitigate losses.

After a data breach occurred at Wyndam Worldwide Corporation, shareholders sued directors for "fail[ing] to take reasonable steps to maintain their customers' personal and financial security measures." The suit claimed that such failures were not disclosed in a timely manner in company Securities and Exchange Commission filings. Target also faced shareholders' derivative suits after its 2013 data breach. These complaints alleged that Target's officers and directors were aware of the risks of a data breach and of how important the security of private customer information was to all parties. The basis of these lawsuits is that the executives did not do enough when faced with a cyber risk. These suits make it clear that there is a substantial risk of personal liability exposure to the management team and the board of directors when a data breach occurs.

The risks of litigation, not to mention the damage caused by a data breach, should put everyone on notice. Planning is essential. Not exploring or mitigating the risks of a data breach means that if one does occur, a company's management team and board of directors will face an even more daunting, expensive, and time-consuming task after the breach. That could make for a public relations nightmare, all while the company may be dealing with government investigations and class action lawsuits. Therefore, instead of being reactive to a breach, a company needs to conduct pre-disaster planning that can mitigate risk to the organization and to personal liability.

Officers, directors, and board members face potential suits in a cyber attack for:

- Breach of duty of care;
- Breach of duty of good faith and loyalty; and
- Statutory duties for failure to notify customers of a breach.
- Breach of fiduciary duty;

To mitigate personal liability, the management team should obtain, if possible, insurance that appropriately covers cyber breaches. The efforts to acquire such insurance and the discussions with the cyber insurance professionals should be documented and retained. The underwriting process itself can help the management team uncover risks.

As noted by Stark in the Cybersecuritydocket.com article, "Interestingly, companies who maintain cyber insurance might also have the best cybersecurity policies and practices – probably because before obtaining cyber insurance coverage, a company is typically subjected to a fairly rigorous review by the proposed insurance company. Just like the physical exam typically required by insurance companies before issuing life insurance, which can prompt better personal wellness practices, a cyber insurance exam might trigger or prompt better corporate cybersecurity wellness."

Prior to a data breach, the management team should obtain appropriate directors' and officers' liability insurance and errors and omissions insurance so that management and board members have at least some personal liability protection. Companies that already have D&O and E&O policies should review them to make sure there is adequate and non-excluded protection for any data breach claims.

The management team also needs to create cyber liability prevention plans. In general, the idea is to review risk exposures so that the team can determine what is "reasonable and appropriate" based on its company's characteristics. The organization should consider a pre-loss plan that includes data prevention policies and security audits, and it should insist upon a systems review to make sure it has the appropriate firewalls and malware. Any company dealing with credit cards should make sure it has protocols consistent with federal, state, and local laws and credit card issuers' requirements.

To decrease potential personal exposure, officers, directors, and board members need to consider:

- Insurance for cyber breaches;
- Prevention plans for cyber breaches;
- Post-hack reaction team.
- nsurance for executives, officers, directors, and board members;
- Disaster planning; and

Of course, prevention cannot stop every data breach; therefore, a company should have a disaster plan for them. Just as companies practice for fires by having a disaster protocol for the protection of personnel and property, there needs to be a detailed, practiced disaster plan for the "new fire in the warehouse." That plan should potentially include a pre-determined cyber specialist who can help perform any needed forensic work, a public relations specialist, and a suitable legal team. This legal team can help conduct an investigation, make insurance claims, handle subrogation issues, conduct legal assessment of potential corporate and management team exposure, and make sure notification requirements are appropriately handled.

Executives and board members who fail to take such steps seem to be assuming that their companies will not suffer a cyber breach or a cyber loss, and they are taking on many risks. Professionals should find such unmitigated risks unacceptable.

Patricia McHugh Lambert *is a litigation principal with Pessin Katz Law in Baltimore, Maryland, who has served as chairman of the board for two insurance companies.* ***Greg Weiner*** *is a business and corporate lawyer principal with Pessin Katz Law with 15 years of experience in advising clients in legal issues related to technology licensing, intellectual property protection and development, mergers and acquisitions, and financing.*

In the Crosshairs

It is not just the mega corporations such as Target, P.F. Chang's, or Anthem that are in the crosshairs for cyberattacks. Mid-size companies and nonprofits are just as vulnerable.

Many security experts note that businesses with fewer than 250 employees represent the fastest growing sector for data breaches and cyberattacks.

One such small organization, Silversage Advisors of Irvine, California, a wealth management firm, had hard drives damaged when burglars hit a home where the hard drives were kept. They cracked open a safe bolted to the floor and made off with the financial records of many of the firm's most affluent clients.

A study by Verizon surveyed 855 data breaches to determine that 71 percent of breaches occurred at companies with fewer than 100 employees. Among other things, these companies have records of clients', employees', contributors' names, addresses, Social Security numbers, driver's license numbers, health information, and bank routing information.