Steps Directors and CIOs Can Take to Minimize Cyberattack Losses

This article was originally published in the *Wall Street Journal's CIO Journal* on October 6, 2014.

by Brian Finch and Sarah Good

Brian E. Finch
Public Policy
+1.202.663.8062
brian.finch@pillsburylaw.com

Brian E. Finch is a partner in Pillsbury's Public Policy practice in Washington, DC. He is a recognized authority on global security matters and is a leader of the firm's Global Security Services team.

Sarah Good
Litigation
+1.415.983.1314
sarah.good@pillsburylaw.com

Sarah A. Good is a Litigation partner in Pillsbury's San Francisco office. She is co-leader of the firm's Securities Litigation & Enforcement Team and is a member of the firm's Global Security Services team.

No director or officer can effectively carry out their duties today without considering the possibility of a cyberattack disrupting or damaging their company, and the fact that they will be the target of blame after the attack.

With the right amount of forethought and preparation, however, directors and officers can minimize the possibility of successful cyberattacks and also establish a record supporting that they acted reasonably and exercised due care in light of ongoing cyber threats.

Here are a few key points to consider:

You are the target.

After a cyberattack, the plaintiff's bar will doggedly allege that directors and officers helped contribute to the success of a cyberattack by being asleep at the switch. Directors and officers can therefore fully expect to be personally hit with shareholder derivative suits alleging a claim for breach of fiduciary duty and securities fraud class actions where the company's stock price has plunged in the wake of a cyberattack, among other third party suits.

Right or wrong, directors and officers need to prepare immediately for such litigation. Failing to do so will only intensify the immense financial pain associated with the expensive and protracted litigation.

Just as much effort therefore needs to be spent by directors and officers on documenting and justifying their cybersecurity measures as in choosing what steps to undertake. A key part of that will be utilizing lawyers as part of the cybersecurity planning process.

Directors and officers should consider having outside counsel assist in the planning, review, and implementation of security policies. After all, the plaintiff's lawyers are going to be all over the security decision-making process, so there is no reason why directors and officers shouldn't have their lawyers help them build a record that shows reasonable behavior and due care.

Stay focused on the problem.

Cyber losses come in any number of forms, but whatever shape it takes, leaders need to actively think about how to manage the threat. A key part of that will be dedicating time and expertise to the problem.

This is not simply a matter of hiring a good information or information security officer, much less buying the

"right" widget. Instead, this requires specific attention from directors and officers on a regular basis.

Some simple steps directors and officers could take include (1) receiving regular updates from the CIO or others addressing the company's cyber-security risks and what steps have been taken to manage/reduce those risks, (2) creating a separate board committee dedicated to cyber security issues that has the power to retain legal and security experts to advise it and could then report regularly to the entire Board of Directors. These steps can ensure that directors and officers become educated on cyber-security risks and are actively involved in management of those risks.

Set realistic expectations.

Just as no company wants to miss its earnings target, so too should directors and officers be wary of cyber security benchmarks that are impossible to meet. Remember, the cyber security fight is about risk management, not risk elimination. No one can possibly expect to stop every attack or prevent a single byte of data from being exposed; for heaven's sake the U.S. government cannot do that.

Cybersecurity directives should thus focus on stopping the stoppable and minimizing damage from inevitably successful attacks. Think of it this way: no municipal fire code is so complete that the city would say "well, no need for a fire department." The same is true for cyber threats. Any good cybersecurity plan will focus just as much on how to handle a successful attack as it will on preventing attacks. A company that knows how to respond and limit damage will be in far better shape than one that scrambles madly after the breach is discovered.

Process, not products, matter.

A consistent trend that has emerged is that cyber attackers are always a few steps ahead of defensive technology, and every new gadget introduces a different set of vulnerabilities. I have boiled this down to something I call "Finch's Law", which states that:

"Cyber defense cannot keep pace with the increasing sophistication or creativity of cyber-attacks."

The practical implication of Finch's Law is that the true measure of the effectiveness of a cybersecurity program is the thoroughness of the underlying process, not the dollars spent or widgets deployed.

More specifically, an effective cybersecurity program is one that is designed to rapidly respond to emerging threats. Directors and officers should regularly review threats, vulnerabilities, and consequences, and ensure the implementation of defenses that can be rapidly updated to deter or minimize cyber risks. Every company is different and while there are "best practices" that are evolving there is no "one size fits all" in cybersecurity.

Put simply –the process of designing and deploying security measures and procedures is what truly matters. If you place too much emphasis on simple technical goals, the threat will surpass your end-state even before it is completed.

Insurance is not just about insurance.

Here's an unfortunate reality check: the average cyber insurance policy is not going to make you whole after an attack. Cyber-attacks can result in billions of dollars in damages as well as reputational harm. Companies can typically only buy insurance for a fraction of the overall damages that may be caused – specifically, $350mm in coverage for their own use, and perhaps $1 billion in total insurance is available on the world market. Further, the larger the claim, the greater the likelihood of having to sue in order to obtain payment on claims. That said, while companies cannot rely on such insurance to fully protect them from losses caused by cyber-attacks, companies should still buy such insurance as part of their overall risk mitigation.

Given that, can directors and officers do anything to protect the company from massive financial harm following a cyber-attack? Actually, yes, they can.

One of the best step directors and officers can look into is ensuring the use of legal safe harbors, specifically the "SAFETY Act". Administered by the Homeland Security Department, this law limits or eliminates a variety of claims following cyber-attacks. The protections can only be obtained by applying to the Homeland Security Department, and apply to a wide variety of cyber security policies and products. Most importantly, the SAFETY Act is the only law in existence today that can proactively limit the fallout of lawsuits arising from cyber-attacks.

Beyond helping establish that the security measures taken by the company were "reasonable", and "due care" was exercised, the SAFETY Act also provides an excellent argument against personal liability for directors and officers. Pointing out that the federal government reviewed the company's cyber security measures and deemed them "effective" helps against courtroom second-guessing.

For whatever reason, after a cyberattack we seem to have adopted a "blame the victim" mentality. That is not likely to go away anytime soon. Directors and officers have to do everything they can then to show that they took all reasonable measures against cyberattacks.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | +1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP