Bloomberg Law

Corporate Law & Accountability Report™

DATA BREACHES

Hack Attack: Reducing the Risks of Stockholder Litigation Arising From Data Breaches




BY EDWARD R. MCNICHOLAS, ALEX J. KAPLAN, JAMES HEYWORTH, AND CHARLOTTE K. NEWELL

Cyberattacks and data breaches are increasingly the subject of front-page headlines and can have material effects on our personal lives. And yet, reports suggest that many corporate directors and managers remain relatively unaware of important cybersecurity issues, risks, and strategies that directly relate to their organizations.

Edward R. McNicholas, Alex J. Kaplan, James Heyworth, and Charlotte K. Newell are lawyers at Sidley Austin LLP. Edward R. McNicholas is a co-leader of the firm's Privacy and Cybersecurity practice, Alex J. Kaplan and James Heyworth are both partners in the firm's Securities and Shareholder Litigation and Complex Commercial Litigation practices, and Charlotte K. Newell is an associate in the Securities and Shareholder Litigation practice.

For example: imagine that your company has fallen victim to a successful cyberattack and customer data was stolen. In the aftermath, the securities plaintiffs' bar undoubtedly will be searching for stockholders to (among other things) pursue claims for violations of state and federal securities laws and/or for breaches of fiduciary duty against the company's board. Are you, your colleagues, managers, and directors prepared to respond to and manage this type of incident and the subsequent litigation and regulatory investigations? Have you documented your diligence in governing cybersecurity risk? For many, the answer may be no.

This article discusses the scope of this problem, how it can directly impact you and your company, and steps you can take now to help prepare for the unknown. It is certainly true that even the best cybersecurity programs cannot guarantee deterrence of all attacks. But such programs unquestionably mitigate the risk of a breach, support organizational resilience, and help control the fallout should one occur.

I. The Scope of the Problem: A Substantial Risk

Cyberattack statistics are sobering. In 2014, reported cyberattacks were up 48 percent from the prior year (to 42.8 million, or 117,339 per day), and the *average* loss sustained was $2.7 million. *See Lloyd's Cyber Strategy* (2015) *available at* https://www.lloyds.com. By 2016, these damages were estimated to be a whopping $450

 ISSN 2330-6300

billion per year globally. *See Lloyd's: Counting the Cost* (2017) *available at* https://www.lloyds.com. And news of ever larger breaches at internet companies, professional services firms, credit reporting agencies, and retailers continue to hit news cycle after news cycle.

Not surprisingly, the scope and severity of these issues makes them top-order items for government and corporate entities alike. In 2014, for example, then-Securities and Exchange Commission Chair Mary Jo White deemed cyber threats to be ''of extraordinary and long-term seriousness'' and noted that the FBI expected ''resources devoted to cyber-based threats . . . 'to eclipse' resources devoted to terrorism.'' *See M.J. White Opening Statement at SEC Roundtable on Cybersecurity* (Mar. 26, 2014) *available at* https://www.sec.gov. IBM's CEO has called these issues the ''greatest threat to every company in the world.'' *See* Forbes, *IBM's CEO on Hackers* (Nov. 24, 2015) *available at* https://www.forbes.com. And as Chairman Jay Clayton recently echoed at his Senate Banking Committee confirmation hearing: ''In terms of whether there is oversight at the board level that has a comprehension for cybersecurity issues, I believe that is something that investors should know, whether companies have thought about the issue, whether it's a particular expertise the board has, I agree. It's a very important part of operating a significant company.'' *See* Reuters, *Clayton Backs Improvements to Cybersecurity Disclosures* (Mar. 27, 2017) *available at* tax.thomsonreuters.com [hereinafter *Improvements*].

II. Legal Consequences of a Successful Cyberattack

The cyber-intrusions of the last few years teach that those in control of public companies should anticipate stockholder derivative and/or securities litigation (among other things) should a breach occur. Indeed, the securities laws provide an angle for plaintiffs to argue that cyber risks were not adequately disclosed, particularly should a stock price fall when a breach is announced. Similarly, longstanding common law fiduciary standards require that corporate boards adequately oversee the enterprise and maintain appropriate risk management structures. This obligation extends to IT systems and cybersecurity. As a result, while each stockholder claim stemming from cyberattacks raises unique issues of fact, they are grounded in longstanding legal doctrine.

The SEC has pursued investigations against public companies after major breaches on theories of inadequate disclosure and/or inadequate risk governance oversight. Recently, Chairman Clayton has openly questioned ''whether the disclosure is where it should be'' with respect to the ''discussion and understanding of cyber threats and their possible impact on companies'' and has pointed to guidance from the Division of Corporate Finance ''to help public companies consider how issues related to cybersecurity should be disclosed in their public reports.'' *See Improvements; see also* S.E.C., *Statement on Cybersecurity* (Sept. 20, 2017) *available at* https://www.sec.gov/news.

In the last ten years, a number of companies (and, their boards) have also been subject to stockholder, securities, or other commercial litigation stemming from cyber intrusions. Thus far, no stockholder plaintiff has succeeded at trial, but because a number of these cases have settled, the incentive for plaintiffs' counsel to pursue these claims remains. For example, in late 2013, a major retail company fell victim to a point-of-sale attack, in which roughly 40 million credit and debit card accounts used at its stores were compromised, revealing customer name, card number, expiration date, and security code information. A wave of lawsuits followed, ultimately consolidated in a federal multi-district litigation in the District of Minnesota. These included:

■ Stockholder derivative suits, alleging the company's board failed to properly oversee the enterprise and manage the risk of a possible cyberattack. As Minnesota law permits, in response, the company created a special litigation committee which dedicated nearly two years to an investigation (including completion of roughly 70 interviews), funded by the company and assisted by outside counsel. Its final report concluded that pursuing such litigation would not be in the company's interests. On this basis, the derivative claims were dismissed. *Davis v. Steinhafel*, No. 14-cv-203, Order (D. Minn. July 7, 2016).

■ Tens of additional class actions were filed raising a range of consumer protection and negligence claims. The company was also beset by banks and credit unions, which alleged significant damages from the reissuance of credit cards or reimbursement of fraudulent transactions. The company agreed to a settlement with each (of roughly $10 million and $40 million, respectively). The terms of the settlement were challenged by objectors; on limited remand from the Eighth Circuit, the District Court granted the renewed motion to certify the class, paving the way for the settlement to go forward. *In re Target Corp. Customer Data Sec. Breach Litig.*, 2017 BL 165484, 2017 WL 2178306 (D. Minn. May 17, 2017).

Further, the company disclosed in its annual report expenses of nearly $300 million related to the breach. Beyond the financial impact, the company's CFO testified before Congress about the breach, and several board members faced an outside challenge to their re-election.

Thus far, these types of stockholder and securities claims have largely been settled or dismissed, suggesting that these companies' cybersecurity policies and procedures (and, associated disclosures) largely withstood the test. Nevertheless, this ''success'' still comes at significant literal and reputational cost. And it begs the question: is your company ready?

III. Seven Key Steps: Planning Ahead

Given the statistics about cyberattacks, the question is not ''if?'' but ''when?'' With that, we suggest keeping in mind at least the following principles:

First, at a macro-level, consider how your cybersecurity awareness, practices, and procedures compare to other issues that are a focus in your business (*e.g.*, financial planning or compliance). If, by comparison, your cybersecurity prowess or reporting has been given insufficient weight, act now, knowing you are not alone. Recent studies indicate that a lack of board-level focus on cybersecurity is relatively common. For example, a Harvard Business Review survey of 340 directors ranked their cybersecurity processes ''dead last.'' *See* Harvard Business Review, *Why Boards Aren't Dealing with Cyberthreats* (Feb. 2017), *available at* https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats.

   ISSN 2330-6300

Second, focus on your company's board-level expertise and reporting on these issues. Boards should consider adding directors with cybersecurity expertise; here again, the data suggests many boards have not yet done so. *See, e.g.*, Audit Analytics, *Cybersecurity Experts on the Board of Directors* (Aug. 9, 2017) *available at* http://www.auditanalytics.com/blog/ cybersecurity-experts-on-the-board-of-directors/#_ftnref1. Regardless, all corporate boards should be receiving regular reports about a company's specific cyber risk profile, exposures, and solutions. Ideally, such reports should come from a dedicated internal cybersecurity expert (such as a Chief Information Security Officer) who can communicate directly with the board. Cybersecurity data and presentations should be provided in a standardized fashion, using a model similar to the form created by the National Institute of Standards and Technology, which identifies and standardizes key cybersecurity functions: identify, protect, detect, respond, and recover. This standardization promotes regular self-assessment that can be tracked over time.

Third, boards should regularly assess their formal cybersecurity policies and procedures. These policies should be created in conjunction with internal and external cybersecurity experts and identify and prioritize key risks. Such board-level policies can then (i) be regularly updated and (ii) serve as the framework for more detailed, tailored, division-specific policies to help ensure uniformity across an organization. Critically, these policies and procedures should include a formal response plan to streamline any response to a negative event. Such a plan should expressly identify the individuals responsible for leading a response, include representatives from all key stakeholder constituencies within the company, and set forth methods to mitigate the business, reputational, technical, and legal fallout. Such concrete plans are far more effective in guiding a necessarily time sensitive, difficult response and encourage the sort of cross-functional collaboration that is key for successful incident response.

Fourth, boards should assess the implementation of cybersecurity policies and procedures. Policies will be effective only if they are adhered to, and failing to implement stated policies not only undercuts their purpose, but provides fodder for plaintiffs in any future litigation. Thus, it is important to assess adherence to policies.

Fifth, boards must document their governance mechanisms and consideration of these issues. Not only must policies be properly documented and readily accessible, but it is also important for boards to maintain a clear paper trail of their receipt of cybersecurity briefings and actions on those briefings. It may also be helpful to institute regular training so that these policies and procedures (and any updates) are understood and remain top of mind for necessary parties.

Sixth, boards should consider their cybersecurity insurance coverage. If data breaches are an inevitable consequence of the growth of data as a valuable corporate asset and driver of business models, it is essential for boards to assess whether insurance coverage is adequate.

Seventh, keep in mind that, at times, third parties will play a pivotal role in your cybersecurity efforts. If third parties have access to your systems and they lack adequate protection, you could inadvertently decrease your preparedness. The excellent technologists who built and maintain your network are most likely not the forensic specialists who will be crucial during a breach response. Thus, your current and future third-party vendors should be expressly addressed in your firm's policies and procedures. In a similar vein, cybersecurity issues need to be considered as part of the diligence in any formative corporate transaction, like a merger or acquisition.

Unfortunately, even the best cybersecurity efforts cannot guarantee safety. But, developing these key policies and procedures should prove rewarding. They will improve prevention efforts. And, should such an attack succeed, your company will be better served by following a concrete response plan (with the guidance of cybersecurity experts and counsel) to navigate the situation and interact with law enforcement, regulators, and clients. Finally, it is these policies and procedures—and, the company's response to any breach—that will serve as the company's best defense in any subsequent litigation should a breach occur. In sum: plan now. The old saying ''an ounce of prevention is worth a pound of cure'' is exemplified by the area of cybersecurity.