Financial Fraud Law Report

AN A.S. PRATT & SONS PUBLICATION FEBRUARY 2014

The FINANCIAL FRAUD LAW REPORT is published 10 times per year by Matthew Bender & Company, Inc. For subscription information and customer service, call 1-800-833-9844. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., PO Box 7080, Miller Place, NY 11764, smeyerow@optonline.net, 631.331.3908 (phone) / 631.331.3664 (fax). Material for publication is welcomed — articles, decisions, or other items of interest.
POSTMASTER: Send address changes to the *Financial Fraud Law Report*, LexisNexis Matthew Bender, 121 Chanlon Road, North Building, New Providence, NJ 07974. Direct inquiries for editorial department to catherine.dillon@lexisnexis.com. *ISBN: 978-0-76987-816-4*

Cybersecurity: Amid Increasing Attacks and Government Controversy, a Framework to Reduce Risk Emerges

STUART D. LEVI

The author reviews 2013 developments in cybersecurity and advises companies and their executives to stay focused on cybersecurity risks in the coming year.

Last year likely will be considered a watershed period in the role of cybersecurity in corporate strategy and management. While there were few significant legislative developments, a marked increase in cybersecurity attacks sensitized companies to this growing threat.

Companies are more cognizant that cyberattacks are not limited to the unauthorized access to and use of personal information; attacks that focus on the theft of intellectual property and corporate business plans have become equally prevalent. In addition, attacks from state-sponsored hackers are increasing at an alarming rate. The ability of companies to protect themselves against such cyberattacks is becoming a competitive differentiator.

A LACK OF U.S. CONGRESSIONAL ACTIVITY

In a year when both houses of Congress had difficulty agreeing on a number of critical national issues, it is not surprising that cybersecurity legis-

Stuart D. Levi is a partner at Skadden, Arps, Slate, Meagher & Flom LLP, where he is co-head of the firm's Intellectual Property and Technology Group. He may be contacted at stuart.levi@skadden.com.

Published by Matthew Bender & Company, Inc. in the February 2014 issue of *Financial Fraud Law Report*.

lation gained little traction. The reality is that many organizations, let alone legislators, have trouble agreeing on what type of cybersecurity regulation is necessary or even appropriate. Many companies believe that they are already taking steps to address this risk, and do not require legislation to compel their actions. Congress also is reluctant to mandate specific technological solutions out of a concern that it might be seen as backing certain technology vendors over others.

Congressional activity instead has focused on amending laws that restrict information sharing among companies so that businesses can exchange cybersecurity data. The expectation is that increased sharing of information, especially about cybersecurity intrusions, will allow companies to coordinate security efforts and take their own prophylactic measures. Such information sharing would be required only of "critical infrastructure" industries, which include the energy, telecommunications and financial services sectors. While a focus on information sharing, as opposed to new regulation, increases the likelihood of some type of cybersecurity legislation emerging from Congress, many hurdles remain. Sharply divergent views on which entities would be covered by this information sharing, what form it would take, and what sort of legal protection companies would have if they shared information likely will be debated in 2014.

Some have suggested that the recent attack on Target Corp., resulting in the theft of credit and debit information of some 40 million customers, will be the "tipping point" incident that incentivizes Congress to take a more aggressive approach on enacting cybersecurity legislation. However, it remains unclear what type of laws would have prevented such a breach. To date, there has been no suggestion that Target lacked industry-standard cybersecurity protections. The reality is that, in the current environment, hackers continuously outsmart such protections.

PRESIDENT OBAMA'S EXECUTIVE ORDER AND ITS RAMIFICATIONS

The executive branch has stepped into the void created by the lack of any meaningful congressional activity. On February 12, 2013, President Obama signed an executive order and a presidential directive that together set forth

the administration's approach to two key issues: regulating critical infrastructure network security and sharing cyberthreat information between the public and private sectors.

The executive order discusses the cybersecurity of "critical infrastructure" — private sector systems and assets so vital to the U.S. that their incapacity or destruction would have a debilitating impact on security, the economy or public health. The executive order initiated a new process through which the administration asked federal agencies to assess the need for new regulation of cybersecurity standards at critical infrastructure companies. There are three key components: actions by the Department of Homeland Security ("DHS"), actions by the National Institute of Standards and Technology ("NIST"), and actions by sector-specific regulators named in the associated presidential directive. Of these three, NIST actions have done the most to shape the cybersecurity agenda.

The NIST Framework

The executive order required NIST to coordinate the development of a "framework" to reduce cybersecurity risks to critical infrastructure. Over the course of 2013, the institute solicited public comments and drafted a preliminary NIST Framework, which highlights the difficulty of enacting comprehensive cybersecurity legislation. Rather than prescribing specific requirements, the framework is far more open-ended. As NIST noted, there is no "one-size-fits-all approach for all critical infrastructure organizations."

The framework highlights five core functions that NIST considers part of a comprehensive view of cybersecurity risk:

- identifying which systems, assets and data require protection;
- protecting those systems, assets and data by implementing appropriate safeguards;
- detecting the occurrence of cybersecurity events;
- responding to cybersecurity events detected; and
- recovering capabilities impaired through a cybersecurity event.

The framework subdivides these core functions into categories and subcategories and provides cross-references to a number of different existing industry and government standards that address each subcategory within the functions. Organizations can review these references and select the standard that best addresses their particular needs.

The framework also includes implementation tiers describing the level of sophistication an organization applies to each core function. There are four tiers, ranging from partial, in which an organization does not have a formal risk management process, to adaptive, in which an organization regularly incorporates new information into its approach. Organizations that adopt the framework determine a desired tier at each function and category level based on organizational goals, expected reduction in cybersecurity risk and feasibility of implementation. For example, an organization may choose to put more resources into robust recovery from cybersecurity events and fewer into asset protection.

Once an organization selects tiers across all functions and categories, it has developed a framework profile — a cybersecurity risk mitigation response strategy. It can then regularly compare its current framework profile to its target version and take action as required.

Incentives for framework compliance remain unclear. In August 2013, the DHS made public a preliminary list that the government may offer to companies that opt to comply. How those incentives may be deployed in practice is uncertain.

While the preliminary framework does not propose new cybersecurity standards, the executive order mandates that agencies use it (once finalized) as the basis for reviewing critical infrastructure cybersecurity within regulated sectors. The executive order also asks those agencies to consider whether they have the legislative authority to enact any regulations that might be required.

THE FTC BECOMES INCREASINGLY PROACTIVE

In 2013, the Federal Trade Commission ("FTC") continued to take an aggressive approach in pursuing certain companies that suffered data breaches. This stance surprised many because there is no existing cybersecurity standard that such a company could have violated.

Instead, the FTC has taken the position that certain companies misled consumers (thereby violating Section 5 of the FTC Act) by purporting to have adequate security processes in place when, as "established" by the breach, they clearly did not. While at least two companies have challenged the FTC's tactic as exceeding the agency's jurisdiction, we anticipate that the FTC will continue this aggressive approach in 2014. At the end of 2013, the FTC also announced that in 2014 it will focus increased attention on "Big Data" (*i.e.*, the pooling of vast stores of data, often without consumer knowledge, let alone consent), mobile devices and protection for sensitive data, which includes health and financial information, as well as data about children.

WHAT COMPANIES SHOULD CONSIDER IN 2014

The 2014 cyberthreat environment requires that companies implement, audit and update robust security measures frequently. Companies also should make organizational and policy changes that insulate them as best as possible from regulatory challenges and class actions:

At the Board and C-Suite Level

Board and company executives need to treat cybersecurity as another critical audit and control function of the organization. Long gone are the days when executives could dismiss cybersecurity questions by responding that this was the purview of the IT department. Instead, as part of their fiduciary responsibility to protect their corporations, board and C-suite executives need to be well-versed in the steps their companies are taking to safeguard systems and be involved in all major decisions in this regard. Boards also should receive regular reports on the state of the organization's security. It is important to note that corporate audit committees increasingly are focusing on the critical nexus between cybersecurity and an organization's financial health and controls. These committees realize that, in today's environment, financial controls are heavily dependent on, and threatened by, cybersecurity issues.

Data Breach Response Planning

Organizations need to develop data breach incident response plans. If a

company fails to do so and suffers a data breach, it runs the risk of a class action claim that it was ill-prepared to deal with cybersecurity, and any resultant harm could have been avoided if such a plan were in place.

Developing a Security Standard

Although the NIST Framework only provides general cybersecurity guidelines, merely points to existing standards and is limited to "critical infrastructure" companies, it does offer the first government-generated comprehensive overview of cybersecurity standards. Organizations should assume that plaintiffs' lawyers, the FTC and regulators may view the framework as an important baseline document to measure an organization's cybersecurity practices. Regardless of industry or existing cybersecurity policy, companies may want to carefully review the framework and technical standards it discusses.

Reviewing Security Assurances

The FTC's actions provide an important reminder that organizations should be mindful of how they present their security standards to customers. Organizations understandably are tempted to laud their state-of-the-art security systems as a means to assuage customers' concerns and provide a competitive advantage. However, these statements may come back to haunt organizations in the event of a data breach. We are in an era where more circumspect comments may be warranted.

Closely Track Third Party Agreements

Third party vendors have become increasingly cautious about cybersecurity issues, particularly in agreements through which they will handle client data. Therefore, vendors likely will seek limitations on liability, narrower indemnities and possibly even liability exclusions for any data breaches. Legal departments and procurement groups need to carefully review agreements for these clauses. Organizations also should consider establishing risk policies regarding whether they are willing to accept any such limitations or exclusions.

Cyberinsurance

For the last few years, organizations have asked whether cybersecurity was an insurable risk. Despite the demand, insurance companies initially struggled with creating a commodity insurance product for a risk that was so dependent on how a company secured its systems. Without performing company-by-company audits, which would be cost-prohibitive, selling insurance products against this risk seemed challenging. However, in 2013, the market for cyberinsurance products expanded dramatically. While premiums and scope of coverage vary widely, organizations may want to consider this option.

CONCLUSION

In 2014, companies and their executives need to stay focused on cybersecurity risks. While Congress has offered little direction on the levels of security required, aggressive plaintiffs' lawyers, and an active FTC have created an environment where security policies and activities are being closely scrutinized.