Bloomberg
Law Reports®

February 14, 2012

Corporate and M&A Law

Corporate Governance

How Should Corporate Boards and General Counsel Deal with Cyber Risks?

STEPTOE & JOHNSON LLP

Contributed by Stewart Baker, Steptoe & Johnson LLP

The drumbeat of concern about cybersecurity is almost deafening today. And it should be. Many companies have been robbed blind, losing most of their competitive secrets to unseen intruders on their networks. Political leaders are demanding greater corporate disclosure of cyber-risks, and the Securities and Exchange Commission has released guidance[1] that will force more detailed and frequent disclosures. Laws requiring public notice when personal information has been compromised have spread throughout the United States[2] and are being adopted abroad[3] as well. Talk of cyberweapons[4] and cyberwar[5] is raising the prospect that domestic pipeline, refinery, and electric power companies will face cyberattacks in future conflicts, as well as liability for failing to prevent the attacks.

Despite the serious consequences of a cyberattack, corporate boards and general counsels, generally speaking, have trouble thinking about this problem, and they don't get the strategic help they need from their corporate security and IT departments. No one expects the general counsel or the board to give guidance on encryption algorithms, proxy servers, or network audit architecture. Instead, they need to provide meaningful guidance at a strategic level. Generally, presentations on corporate network security tend to focus on two strategic questions. Sometimes, security professionals measure themselves against abstract checklists of security standards or best practices ("We're 90 percent compliant with FIPS-140 and expect to be 100 percent compliant by March"). And sometimes they measure themselves against their corporate peers ("We're in the top quartile in our industry for security measure deployments, according to independent consultants who survey us and our peers").

The problem with relying on peer comparisons or security standards is pretty plain. If all of your peers are getting compromised too, imitating their security measures isn't a path to success. And the old joke holds true about security standards: what's best about them is how many there are to choose from. If you choose the wrong standard, all the compliance in the world won't prevent a breach.

Corporations should strive to do better. Network security isn't like piloting a plane, where risk can be avoided by checking off all the procedures necessary to ensure safe operation. And it isn't like advertising, where keeping up with your peers will help you hold your market position. Network security is different because there's a living, thinking adversary on the other side. If anything it's like litigation against an institutional opponent. Very few general counsels would tell the board that the company's strategy for avoiding large-scale tort liability is to follow a checklist for

Originally published by Bloomberg Finance L.P. in the Vol. 6, No. 8 edition of the Bloomberg Law Reports–Corporate & M&A Law. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

product development or to have a legal budget that matches the budget of other big players in the industry. Those are good things, but the general counsel also wants to know what legal theories the plaintiffs' bar has been pioneering recently, what kind of tactics have produced the biggest payoffs for plaintiffs, and what industries they have in their sights. Armed with that information, the general counsel can make far better decisions about which checklists are most necessary and how big the budget should be.

In short, we should measure corporate security not against a checklist or our peers; we should measure security against the adversary. Network security experts have not typically done that because they've pursued network security as though it were a single goal; we'll make the network secure and then just maintain that state. But bitter experience tells us that absolute security is beyond our reach. We can't afford it. But once that illusion is surrendered, the question becomes "how much security can we afford?" And neither checklists nor peer comparisons provides a particularly useful answer to that question.

Comparing ourselves to our adversaries, however, does provide a useful framework. As with litigation risk, you can begin by asking, "Who might sue us?" The candidates may range from personal injury lawyers to patent claimants to state regulatory commissions. With a list of candidates, you next ask, "What are these institutional actors targeting, and is my company in a target zone?" If you are, you look at the tools and tactics each of these actors uses to go after the companies they target. Finally, you take steps to minimize the risk that those tactics will work against you, including developing a plan detailing who you will call and what you will do when the adversaries show up on your doorstep.

Every one of those steps, borrowed from the adversary world of litigation, will also work in the adversary world of cyber-risk. There is an entire ecosystem of attackers today. Nation-states maintain contingents of hackers to serve their interests.[6] Cybercriminals steal information that will lead to money, such as credit card numbers.[7] Politically motivated hackers like Anonymous seek to embarrass companies who've earned their ire.[8] And disgruntled insiders steal information for their next job or leave behind code that sabotages corporate operations. Each of these adversaries has different motivations, seeks different targets, and calls for different remediation strategies.

What's new in the past year or two is how much we know about even the nation-state attackers. Attacks out of China in particular have grown so bold and persistent that fighting them has become a cottage industry.[9] As a result, the defenders have learned a surprising amount about the targets of nation-state hacking, as well as the tactics that the hackers use. The same is true for the other classes of hackers. And so, for the first time, it is possible for a company to analyze its risk by first asking, "Am I of interest to nation-state hackers?" If so, the company can then ask, "What's the worst that can happen to me if a nation-state compromises my network?" That sometimes produces some troubling answers. Nation-states are more likely to steal secrets than money or credit card numbers. But their persistent presence in a network may mean that they can steal even ephemeral secrets, like your company's most recent bid for a particular oil lease, or your bottom line in negotiations with a merger candidate. Or, worse, they might use access to your processes and source code to introduce vulnerabilities to be exploited later, once you've delivered your product to their real target. Combining these possibilities can give a targeted company a good sense of what cybersecurity is worth to them.

The next step is to ask what it will take to defeat the attackers. Again, for nation-state attackers, many tactics have become standard. Spear-phishing[10] with socially-engineered lures is followed by remote access tool uploads, lateral compromise of other machines in the network, acquisition of administrator privileges, and installation of multiple backdoors, at which point the attackers begin a leisurely collection and exfiltration of terabytes of encrypted data. Targeted companies must assume that the enemy is inside their network, because even a successful cleansing operation can be defeated by a second spear-phishing attack a few weeks after the cleaning specialists have gone home. The measures needed to deal with such attacks are quite different from the measures needed to fend off thieves looking for funds or credit card numbers. By focusing on the adversary, we can begin to assemble a strategically tailored checklist of security measures, prioritized according to the risks presented by each attacker.

What I find most appealing about this adversary-focused security framework is the way it allows corporate boards and general counsels to approach the cybersecurity problem strategically. By looking separately at each adversary's goals, it is possible for general counsels to analyze the legal risks associated with a successful attack. In some cases, a breach of personal data might result in hundreds of thousands of dollars in notices and legal defense costs, plus losses from reputational harm, which are harder to quantify.

That potential cost of a cyber attack can inform the board and top executives as to the kinds of security measures that make economic sense. It also allows the board to set broad goals and priorities at a strategic level, such as "Above all, make sure no nation-state can modify the source code that serves our customers."

This approach also permits a more useful set of disclosures to investors. Instead of saying, "Cybersecurity is a problem, and if our networks are compromised, we could suffer material harm," companies could say, "We're in an industry that has recently been targeted by nation-state attacks aimed at stealing bid information. If a significant portion of our bid information were compromised and provided to competitors, the impact would be material. We have taken special measures to prevent such compromises and to assess the effectiveness of those measures." This approach to disclosure is more meaningful than the empty generalities that many companies are now forced to rely upon.

Why isn't this approach already the standard, insisted upon by corporate boards, executives, and lawyers? I think the problem is mainly a lack of information. Boards are used to cybersecurity briefings that either make their hair stand on end or their eyes glaze over. Either way, they suspect that they're being asked to approve expenditures without any real ability to measure

the expenditures' value. As they begin to discover how much we know, even about nation-state attackers, the value of an adversary-based security analysis will become obvious, and the switch will happen quickly.

Stewart Baker is a partner in the Washington office of Steptoe & Johnson LLP, where he heads the National and Homeland Security practice. He returned to the firm following over three years at the Department of Homeland Security as its first Assistant Secretary for Policy. Previously, Mr. Baker served as the National Security Agency's general counsel.

[1] Securities and Exchange Commission, Division of Corporate Finance, CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011).
[2] National Conference of State Legislatures, State Security Breach Notification Laws (Oct. 12, 2010).
[3] *See, e.g.,* Mexico's Federal Law for the Protection of Personal Data Held by Private Parties (May 7, 2010). and South Korea's Act on the Protection of Personal Data at http://www.steptoe.com/assets/attachments/4255.pdf.
[4] Michael Riley and Ashlee Vance, *Cyber Weapons: The New Arms Race*, Bloomberg Businessweek, (Jul. 20, 2011).
[5] Ken Dilanian, *Virtual war a real threat*, Los Angeles Times (Mar. 28, 2011).
[6] Kim Zetter, RSA Blames Breach on Two Hacker Clans Working for Unnamed Government, Wired, (Oct. 11, 2011).
[7] Jason Ryan, *Three Charged in Largest Ever Credit Card Data Breach*, ABC News (Aug. 17, 2009).
[8] Chenda Ngak, *Megaupload Anonymous hacker retaliation, nobody wins*, CBS News Techtalk (Jan. 20, 2012).
[9] Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, prepared for the US-China Economic and Security Review Commission (Oct. 9, 2009)..
[10] Federal Bureau of Investigation, Stories, "*Spear Phishers – Angling to Steal Your Financial Info*," (Apr. 1, 2009).