Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY: CSC

Navigating the Cybersecurity Storm in 2016

Posted by Paul A. Ferrillo, Weil, Gotshal & Manges LLP, on Wednesday, November 25, 2015

Editor's note: Paul A. Ferrillo is counsel at Weil, Gotshal & Manges LLP specializing in complex securities and business litigation. This post is based on a summary of a Weil publication; the complete publication is available here.

> "Our nation is being challenged as never before to defend its interests and values in cyberspace. Adversaries increasingly seek to magnify their impact and extend their reach through cyber exploitation, disruption and destruction."
>
> —Admiral Mike Rogers, Head of US Cyber Command September 9, 2015

A very recent article in the UK publication *The Guardian*, entitled "Stuxnet-style code signing of malware becomes darknet cottage industry,"[1] raises the specter of bad actors purchasing digital code signatures, enabling their malicious code to be viewed as "trusted" by most operating systems and computers. Two recent high profile hacks utilized false or stolen signatures: Stuxnet, the code used to sabotage the Iranian nuclear program, allegedly jointly developed by America and Israel, and the Sony hack which was allegedly perpetrated by the government of North Korea. Both of these instances involve sovereign states, with effectively unlimited resources.

The *Guardian* article raises an interesting question that many in the cyber security industry have talked about this year, but have not discussed openly. To wit, "What if cyber maliciousness toolkits were to become available not just to nation-states (like they generally were before) but to ordinary cyber criminals and cyber gangs that might not have nation-state backing?" Or the random teenager living at home who is bored with his school work, and decides to do something more interesting one day? Doesn't this fact indicate that the stakes have been raised now even higher with the "more public" availability of these cyber attack tool kits, leaving attackers of all kinds with a potential huge return on a relatively meager investment if they were to pull off a successful attack? The answer, like Admiral Rogers notes above, is probably "Yes, Sir. Roger that!" The next logical question is, "So now what do we do?"

For the past year we extensively researched the most important cybersecurity issues facing United States boards of directors of public and private companies, and private equity and hedge fund managing directors. We did this not to critique or comment, but because in our view it is time to raise our cybersecurity game given the cyber threat actors and cyber threat vectors we are facing today. Though there have been some tremendously helpful articles written, none of them were in the same place, and many of them were written in "tech-speak," well beyond the bounds of comprehension of a mere mortal director (or even a mere mortal lawyer).

[1] This article is available at http://www.theregister.co.uk/2015/11/04/code_signing_malware/.

One of the more common complaints we heard was that the area of cybersecurity was too difficult to comprehend, too fast moving to catch up, and so far from being intuitive that directors did not have a good handle on what were the most important issues they were facing, and what were most important questions they should be asking of their company's executives and IT resources in order to help guide their company through the cybersecurity storm.

We are proud to announce the very recent publication of our book, Navigating the Cybersecurity Storm: A Guide for Directors and Officers. Founded upon many principle-based approaches like ISO 27001 or more recently the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, our book sets forth in "plain-English" format the most important cybersecurity questions that directors should be asking when faced with areas like cloud computing, cybersecurity federal and state regulatory and compliance issues (like those being generated today by the U.S. Securities and Exchange Commission ("SEC") and the U.S. Federal Trade Commission), information privacy issues for multi-national companies, and cyber insurance issues. These are not easy issues to address. There are probably no "right" answers to any of the questions we set forth in the chapters. But without knowing the right questions to ask, corporate and fund directors might be left on the bench during one of the most important periods of our lives—when the companies they guide are facing some of the most important threats to their corporate reputations, and indeed their corporate existence, they might ever face.

The book has multiple chapters covering most cybersecurity issues a board may face during their quarterly board meetings. Two of the most critical chapters deal with the NIST Cybersecurity Framework, and cybersecurity incident response planning. Why are they most critical? First, the NIST Cybersecurity Framework is probably the "de facto" if not "de jure" framework in the United States. It has been adopted by the U.S. Government, its agencies, and is required to be followed by its contractors. And it is referenced by many federal regulatory authorities, such as the SEC's Office of Compliance, Inspections and Examinations. The Framework sets forth many cornerstone issues of cybersecurity. Probably the most important issue in the Framework is a relatively simple one: "What are my most important data and informational assets, how do I rank them in terms of value, where are they located, and how am I protecting them today?" Indeed, if I don't know what are my most important assets and where they are located, then how can I consider better ways to protect them?

Finally, assuming the very good probability that most organizations have already been hacked at least once, our incident response chapter might be the most important one in the book.[2] Deploying robust antivirus software along with hardware and systems to detect anomalous activity on networks are prudent steps, but not enough. Time, effort and money must be invested to build and test a robust incident response plan to enable an organization to respond to a cybersecurity event effectively, maintain business operations and recover to full functionality as soon as possible. Sony Pictures as an organization was down for 3 weeks without having either computers or a functional phone system. This chapter should help all directors understand the cyber incident response planning process, the very critical element of cooperating with law enforcement, and potential and mandatory disclosure obligations relating to a sophisticated cybersecurity breach. Though this chapter is multi-faceted, its theme is practical: Use peacetime wisely! Prepare and plan for a cybersecurity breach well ahead of an incident, practice your plan

[2] It was written with the guidance of Austin Berglas, a former Assistant Special Agent in Charge of the Cyber Operations Division of the New York Field Office of the Federal Bureau of Investigations.
See https://www.k2intelligence.com/en/team/austin-p-berglas/.

(and different potential threats associated with today's cyber security threat vectors such as, e.g. DDoS attacks) and be prepared to not only react, but *proactively act* to limit the potential damage associated with a cyberattack in order to preserve not only the corporation's reputation, but the trust and confidence of its customer and investors. Armed with the knowledge contained in this accessible book, directors can confidently execute their duty of care with regard to cybersecurity in an informed manner. That truly, at the end of the day, is what this book is all about.