Harvard Law School Forum on
Corporate Governance and Financial Regulation

SUPPORTED BY:
pwc

Grading Global Boards of Directors on Cybersecurity

Posted by Paul Ferrillo, Weil, Gotshal & Manges LLP, on Sunday, May 1, 2016

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 Weil publication by Mr. Ferrillo and Christophe Veltsos.

On April 1, 2016 NASDAQ, along with Tanium (a leading-edge cybersecurity consultant), released a detailed survey of nonexecutive (independent) directors and C-suite executives in multiple countries (e.g., the US, UK, Japan, Germany, Denmark, and the Nordic countries) concerning cybersecurity accountability.[1] NASDAQ and Tanium wished to obtain answers to three basic questions: (1) how these executives assessed their company's vulnerabilities to cybersecurity threat vectors; (2) how they evaluated their company's readiness to address these vulnerabilities; and (3) who within the company was held "accountable" for addressing these cybersecurity vulnerabilities.

This report is a must-read for directors, officers, and IT executives, as well as risk professionals, insurers, and brokers. Many of its findings are to be expected, in that some companies "get it, some don't, and many won't." Yet some results are startling. Outside of the US and UK, cybersecurity knowledge and awareness are reported as very low, which does not bode well for these countries, given the rise of cybercrime and cyber terrorism on a global scale. Among the executives and directors in non-US/UK countries, "98 percent of … business leaders are not confident their organization can monitor all devices and users at all times, which means information is traveling through unknown places," and some "91 percent of board members [of these] respondent companies are unable to interpret a cybersecurity report."[2] In total, the cost of cyber-crime is staggering. "Crimes in cyberspace will cost the global economy $445 billion in 2016— more than the market cap of Microsoft ($411 billion), Facebook ($314 billion) or ExxonMobil ($332 billion)—according to an estimate from the World Economic Forum's 2016 Global Risks Report."[3]

And while US and UK company directors and officers are further along in their knowledge than their counterparts in other countries, there is still a lot of room for improvement.

1. Despite obvious knowledge of catastrophic data breaches during the past three years, 40% of all those surveyed in all countries admit that they did not feel responsible for the repercussions of a cyberattack. Whether this indicates a "blame IT" mentality, or whether it's a basic lack of understanding of cybersecurity risks by directors (which is somewhat

[1] See "Bridging the Accountability Gap: Why We Need to Adopt a Culture of Responsibility," available here.
[2] *Id.* See also, "Taking on the Cyber Pirates," available here. ("Cyber attacks pose a growing threat in Germany, damaging businesses and ministries and recently even temporarily forcing a hospital emergency ward to close.")
[3] See "The Global Risks Report," available here.

suggested by the survey)[4], this figure represents wrong-headed thinking. All directors and executives within a company are responsible for defending against cybersecurity attacks, and especially the directors, who are generally charged with responsibility for oversight of cybersecurity.

2. The cybersecurity literacy of executives in the US and UK was generally high. However, we would note that *independent director* cybersecurity literacy lagged behind that of other groups of executives. Their knowledge of the implications of a cybersecurity breach (such as reputational damage) also trailed that of other groups of executives. Officer cybersecurity literacy and awareness was higher in both the US and UK than in other countries.
3. Only 68% of all directors and executives surveyed have assessed their potential losses arising from cyber-attacks.
4. Company directors and executives in the US and UK generally received more impactful threat intelligence than their peers in other countries.
5. The US and UK directors and executives surveyed in the report exhibited greater knowledge about the resiliency of their company's computer networks, along with their ability to respond to a cybersecurity incident.
6. As we would expect, given the lack of real-time cybersecurity disclosure in the European Union, director and executive knowledge of cybersecurity risks and responsibilities significantly lagged behind that of other countries. As the European Union progresses toward a disclosure-based regulatory regime, directors and executives of E.U. countries are going to have to improve their working knowledge or else face stiff fines and penalties.

Conclusions To Be Drawn from the NASDAQ/Tanium Report:

Despite apparently being way ahead of their contemporaries in the E.U. countries surveyed, US and UK directors and executives clearly have work to do. One cybersecurity executive aptly noted: "Cyber security is 'no longer a dark art but an everyday business practice that must pervade every level of the organization.'"[5]

One clear finding we worry about is the apparent lack of cybersecurity literacy, awareness and risk assessments among US and UK independent directors surveyed. We would have thought that in the two-and-a-half-plus years since the Target breach and the six months since the infamous TalkTalk breach in the UK,[6] US and UK directors would be more cognizant of their company's cybersecurity posture and how that posture could relate to a significant data breach. What is the cause of this apparent lack of independent director knowledge regarding cybersecurity? A general lack of time spent at board meetings on cybersecurity? A lack of the right level and amount of information being imparted to directors by CISOs and CIOs at board meetings? Or just a plain old "failure to communicate"? As we have written before (and as other studies have confirmed), it appears that many times "directors are from Mars, and IT executives are from Venus." Whether their interplanetary vectors cross paths at some point remains to be seen.

---

[4] See "The Accountability Gap: Cybersecurity & Building A Culture of Responsibility," at pg. 9, available here. ("43% of all respondents can't interpret a cybersecurity report at the same level of a financial report."

[5] See "CEO email scam is wake-up call for boards," available here.

[6] See "TalkTalk breach could be good for cyber security in the long run," available here.

One clear path forward to get US and UK directors on the same page would be the adoption and implementation of the National Institute of Standards and Technology's Cybersecurity Framework (the Framework). Three of the Framework's core elements, ("Identify, Protect, and Respond") cut across nearly all of the cybersecurity attributes surveyed by Tanium and NASDAQ. "Identify" means "what are the company's most important IT and IP assets and where are they located." "Protect" means "how are these assets being protected" by whatever means are available to the company through the right balance of technology and employee awareness and training. "Respond" means what it says: does the company have a cyber-incident response plan that is battle-tested and ready to implement at a moment's notice? The Framework has a "common language" element that allows everyone in the company (directors, officers, and IT staff) to have these important discussions as often and frequently as required to keep the company out of harm's way.

Adopting and implementing the Framework at a board level would go a long way toward improving the cybersecurity literacy and awareness of directors. Allowing sufficient time at quarterly board meetings to discuss cybersecurity issues would also be very useful. Finally, we place the responsibility on everyone in the company to have cybersecurity discussions in such a way that all who are involved can participate and make decisions. As recently noted by SEC Commissioner Mary Jo White, in a speech to mutual fund directors, "As areas such as cybersecurity, derivatives, liquidity, trading, pricing and fund distribution become increasingly complex, boards need to assure that they are equipped to address those challenges…."[7] As stated in the Tanium report by a Silicon Valley investment visionary, "At the board level, there is ignorance and a sense that 'techies' should take care of that. It is a technical problem, which is of course completely wrong."

No tech speak should be allowed in these cybersecurity briefings. No acronyms. Just plain-English reporting on the cybersecurity posture, readiness, and effectiveness of the company. A "failure to communicate" can no longer be accepted at the board of directors level at any company. Two years ago, former SEC Commissioner Luis Aguilar made a definitive statement regarding board duties when it comes to cybersecurity. The SEC has said nothing to suggest that it is changing its view regarding board responsibilities for cybersecurity:

Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues. According to one survey, boards were not undertaking key oversight activities related to cyber-risks, such as reviewing annual budgets for privacy and IT security programs, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks. Even when boards do pay attention to these risks, some have questioned the extent to which boards rely too much on the very personnel who implement those measures. In light of these observations, directors should be asking themselves what they can, and should, be doing to effectively oversee cyber-risk management.[8]

[7] See "Fund Boards Face Broad Threats, SEC's White Warns," available here.
[8] See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," available here.