Cybersecurity and Financial Reporting
By Nicole Karp

In December 2013, Target reported a cybersecurity breach that affected more than 100 million customers. Attackers gained access to data stored on the magnetic stripes of customers' debit and credit cards.

One year earlier, a cyber-attack temporarily crippled the websites of Bank of America, Citigroup, Wells Fargo and other major U.S. Banks. In this case, hackers had remotely hijacked cloud service providers used by the banks.

And just this month, security experts identified a vulnerability called Heartbleed that was estimated to affect more than 70% of the world's web sites.

Because of these and other high profile security breaches, cybersecurity continues to capture the attention of the regulatory agencies, company boards and even the leader of the free world! Recently,

- President Obama signed an Executive Order calling for bolstered cybersecurity.
- The National Institute of Standards and Technology (NIST) published a framework for improving cybersecurity.
- The Center for Audit Quality issued *Cybersecurity and the External Audit* – a member alert that summarizes the responsibilities of independent external auditors in connection with cybersecurity.

The SEC also continues to play an important role in the oversight of cybersecurity matters. As a follow-up to its 2011 issuance of cybersecurity disclosure guidance, the Commission recently hosted a roundtable discussion on cybersecurity. A discussion around some of the topics addressed at this roundtable follows.

Cybersecurity and Financial Reporting

Companies are required to disclose *material* cybersecurity risk and incidents. Specifically, disclosure is mandatory to the extent that a company's business or operations give rise to *material* cybersecurity risks or that cybersecurity incidents experienced by a company are *material*. During the roundtable, however, Commissioner Stein challenged this approach. Her concern: Is one or more immaterial cybersecurity incidents an indication of a more significant, looming security risk? No final conclusions were reached, however.

Roundtable participants also debated whether a company should – or is technically required to – disclose the implications of a cyber-incident in the MD&A. MD&A rules require disclosure of any trend or uncertainty that is reasonably likely to have a material effect on a company's results. Although the actual costs of patching security holes (and perhaps offering credit monitoring services to affected parties) may be small, reputational damage may be enormous. Therefore, MD&A disclosure might be necessary, despite the challenges in quantifying future customer losses and other corollary effects of a cyber-event on the company's financial operations.

Finally, roundtable participants considered whether customer data should be regarded as assets. If so, participants discussed whether the safeguarding of such assets would fall within the scope of the internal controls (ICFR) to be reported on under Section 404 of the Sarbanes-Oxley Act. Linda Griggs of the law firm Morgan Lewis believes it is: "According to the SEC's adopting release on ICFR…the safeguarding of assets is one of the elements of internal control over financial reporting. Because customer data is an asset, a company's failure to have sufficient controls to prevent the unauthorized acquisition, use, and/or disposition of customer data may constitute a weakness in ICFR."

Cybersecurity and Board of Directors

Panelists at the SEC roundtable generally agreed that a company's Board of Directors must be involved in cybersecurity. In fact, given the current environment, companies should strongly consider appointing a board member with cybersecurity expertise. Cybersecurity oversight should also be one of the stated responsibilities of either a risk committee or the audit committee. Board involvement will help companies prepare a defense against a cyber-attack and coordinate a timely response in the event that cyber-attack takes place.

Final Thoughts

Cyber-risks are not going away. Instead, attackers are devising new and more powerful forms of attack.

Therefore, cybersecurity is not simply an IT issue. It's a major business risk, and companies should be prepared to discuss in their financial reports their processes for handling this threat.