July 7, 2014

Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
Re: Public Comments on Cybersecurity Roundtable
File No. 4-673

To Whom It May Concern:

I offer this submission as a comment to the Cybersecurity Roundtable held on March 26, 2014. Though each of the Roundtable topics is important, my submission specifically focuses on public company disclosure issues.

Given the importance of cybersecurity to public companies and investors alike and given the inconsistency with which businesses disclose cyber risks and incidents to investors today, I believe the SEC is obligated to take the following steps in order to protect investors and maintain fair and efficient markets:

- Create an education and awareness campaign to raise awareness of the existing disclosure laws, including disclosure obligations and investors' rights to obtain information;
- Work with business and investors to develop a material cyber risk and incident reporting structure for registrants;
- Request the Financial Accounting Standards Board (FASB) develop recommendations with respect to cybersecurity accounting issues;
- Enforce existing disclosure laws; and
- Consider issuing additional guidance.

I am currently a consultant with Good Harbor Security Risk Management, LLC, a firm providing cyber risk management advice to corporate leaders. I previously served as legal advisor to Senator John D. Rockefeller, IV, Chairman of the Senate Commerce Committee, where I acted as Sen. Rockefeller's lead negotiator on cybersecurity legislation and led his initial inquiry into corporate disclosure practices that resulted in the SEC's 2011 cybersecurity guidance. Prior to working in the Senate, I worked in the House of Representatives as the Staff Director for the Homeland Security Committee's Subcommittee on Emerging Threats, Cybersecurity, Science and Technology. I have written and spoken extensively on cybersecurity issues, particularly on breach liability, corporate responsibility for cyber risk management, disclosure obligations, and the importance of cybersecurity to investors. The views I express here are my personal views and do not reflect those of my company or any client that my firm or I advise.

Respectfully submitted,

Jacob S. Olcott

(1) Cybersecurity is a critical issue for businesses and their investors, though information asymmetry exists.

It is now commonly understood that businesses around the world are under attack in cyberspace, and the threat is growing more severe. Attackers are targeting consumer information, financial information, and sensitive business information, including corporate secrets and transactional data. Some attackers seek to cause operational disruption to businesses. Many organizations have been victims of an external cyber attack, though insiders can also inflict significant harm.

Cyber incidents can have a significant financial impact on a business. Though definitive numbers about actual costs of cyber incidents are difficult to discern, studies and expert opinion estimate that cybercrime costs businesses exceeds $400 billion globally.[1] Financial loss related to cyber crime includes actual money stolen, cost of intellectual property stolen, recovery cost of repairing or replacing damaged networks and equipment, regulatory fines, litigation costs, reputational harm, reduced competitiveness, and failed expansion in emerging markets.

With real value at risk, businesses and their investors share a common interest in cybersecurity, though their access to cybersecurity information is quite different. Corporate executives and their investors are interested in growing business value and earnings, each of which can be jeopardized by a malicious cyber incident. As evidenced by the recent cyber attack against Target Corporation, businesses and investors can both suffer harm from a cyber incident.[2] However, as the following sections suggest, investors often do not have access to relevant and material information related to cyber risks and incidents. This information asymmetry is creating an inefficient market where investors accept significant risk without being properly informed or compensated. Investors are entitled to and deserve more information about cyber risks and incidents from public companies.

(2) Businesses inconsistently disclose cyber risk and incident information to investors today.

Though the SEC clearly described the legal obligations of public companies to disclose material cyber risks and incidents in its 2011 staff guidance, cyber risk and incident disclosure is performed inconsistently by businesses today. The result is that investors are taking on significant, uncompensated risk, and are often left unaware of critical cyber-related risks or incidents that have or may result in large financial loss. There are many reasons for the inconsistency in disclosure today, including the following:

---

[1] McAfee and the Center for Strategic and International Studies, "Net Losses: Estimating the Global Impact of Cybercrime," June 2014, available at http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

[2] Following a major security incident impacting millions of credit card numbers, Target experienced a 5.5 percent drop in number of transactions, 3.8 percent decline in sales year over year, and estimated hundreds of millions of dollars in losses related to the breach incident. Paul Ziobro, "Target Earnings Slide 46% After Breach," Wall Street Journal, Feb. 26, 2014, available at http://online.wsj.com/news/articles/SB10001424052702304255604579406694182132568. There

- **Many businesses are unaware that cyber incidents are occurring.** Many companies, including some of the largest public companies, do not have the capability to detect a cyber incident in real time and respond appropriately. Though corporate spending on cybersecurity technologies continues to increase, many companies still lack full situational awareness over their information environment, a reality confirmed in annual data breach surveys which suggest that the vast majority of businesses who experience breaches do not discover them on their own, but instead are notified months later by a third party.[3]

- **Many businesses infrequently and inconsistently account for cyber incidents and related losses.** Businesses, including financial departments and independent auditors, infrequently and inconsistently account for cyber incidents and related financial losses, making it difficult for investors to determine the scope or impact of cyber incidents.

  Many companies do not consider the long-term impact of certain types of data theft on their business' revenue and profitability. Not all cyber incidents result in immediate financial loss: some incidents involving intellectual property or trade secret theft may take months or years to negatively affect a company's competitiveness and earnings.[4] This distinction can be lost on or ignored by executives who are focused exclusively on short-term earnings.

  Many businesses that suffer attacks do not appropriately assess the value of the data that they have lost. Businesses do not perform damage assessments to determine the business significance of potentially compromised data or assets. A damage assessment should consider the value of the stolen data, the likelihood that the data will be used to harm the company or the source, and any costs (e.g. financial, legal, operational, reputational harm) associated with the incident. Damage assessments would be particularly useful for companies to perform after

[3] Verizon's 2013 Data Breach Investigations Report found that approximately 70 percent of breaches were discovered by external parties (down from 92 percent the previous year), and 66 percent of breaches took "months" to discover, resulting in significantly larger losses for a business than if the breach was discovered quickly. "2013 Data Breach Investigations Report," Verizon, 2013. Unfortunately, third party notification often occurs long after attackers have had a chance to identify and exfiltrate sensitive data from the victim company. A delay in discovering an incident can also prevent a company from using computer forensics to discover the true impact of the event. IT and business outsourcing also creates incident detection challenges. Many businesses use third party providers to operate and maintain their IT systems or provide sensitive corporate data to third parties like law firms, consulting firms, or other vendors. In these situations, cyber incidents may go unnoticed or unreported if those third party vendors lack detection capabilities. Furthermore, if a business fails to incorporate a contractual provision requiring the third party service provider to disclose data breaches affecting the client's data, the provider is typically under no legal obligation to disclose a breach incident to the business. As a result, the business can be completely unaware that her company's most sensitive information, which has been entrusted to a third party, has been compromised.

[4] See the case of American Superconductor Corp., a computer system manufacturer, which had software trade secrets stolen by a Chinese competitor that caused AMSC to lose significant market share and stock price. Michael Riley and Ashlee Vance, "China Corporate Espionage Knocks Wind Out of US Companies," Bloomberg, March 15, 2012, available at http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html

incidents involving theft of corporate trade secrets and strategy information, where the value of the data is typically difficult to determine. The business is in the best position to perform damage assessments, which can be shared with investors in order to provide a more thorough and accurate financial assessment of a breach incident. Damage assessments are important but difficult; even companies who do attempt to perform damage assessments have difficulty predicting how their stolen data will be used by an attacker, particularly one who successfully maintains his anonymity.

Cyber loss accounting is infrequently performed for many reasons, including unclear standards, lack of internal awareness, and valuation challenges. Those few companies that do account for cyber losses do so inconsistently. According to one recent survey, those that do some form of cyber loss accounting utilize historical cost data (how much money the company spent to create a trade secret, e.g. salaries and supplies) to estimate trade secret losses rather than measuring asset value or economic benefit (how much the company planned to earn from the trade secret, including lost profit, reasonable royalty, and other income/economic benefits). The inconsistency in accounting can create significant confusion for investors.[5]

- **There is inconsistent understanding and interpretation of the material cyber risk and incident disclosure standard among corporate lawyers.** There is very broad and confused understanding and interpretation of the SEC's cybersecurity disclosure requirements in the legal community, and additional training and education by the SEC about these requirements is likely necessary.

  Disclosing material cyber risk and incident information is required by the Securities Act and the Securities Exchange Act. The SEC's 2011 staff guidance on cyber disclosure clearly states the legal obligation to disclose material cyber risks and incidents. The guidance should not be viewed by attorneys or businesses as voluntary. Nevertheless, some businesses remain ignorant of these newly clarified obligations.

  Businesses who are aware of their obligation to disclose maintain varying interpretations of materiality when it comes to cyber incidents. Some companies appear to use an artificially high threshold for materiality when it comes to cyber incidents. Though countless government officials have described the vast penetration of businesses by cyber attackers today there is surprisingly little

[5] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011, p. 3-4, available at http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. Corporate organizational structures present hurdles that limit the adoption of cyber loss accounting mechanisms: the financial accounting and IT security functions do not typically collaborate within a business, even when cyber incidents do occur.

disclosure of cyber incidents to investors.[6] Corporate attorneys recognize that cyber incident disclosure may have market repercussions, and are therefore likely to set a very high materiality threshold for cyber incident disclosure. In the recent data breach involving Target Corporation, for instance, the attorneys' conclusion that the breach would not have a material impact seemed to run counter to the company's actual reported financial condition.[7] Policymakers, including Senator John D. Rockefeller, IV, have suggested that Target Corporation's failure to provide information to investors was inconsistent with the company's legal obligations.

The legal community's confusion about what constitutes a material cyber risk and incident was evident at the SEC Cybersecurity Roundtable. During the Roundtable, Washington Gas & Light General Counsel Leslie Thornton suggested that a breach by a nation state of her company would not be a disclosable incident, in part because it would not involve the disclosure of personally identifiable information (e.g. credit cards).[8] But as other Roundtable participants suggested, different shareholders have different levels of risk tolerance; WG&L shareholders and investors, for instance, might expect to receive information about such incidents because they represent increased risk to the company and their investments. While the SEC's guidance requires reporting of any incidents likely to have a material effect on operations, liquidity, or financial condition, including but not limited to credit card breaches, given the confusion in the legal community, additional education and clarification is necessary to ensure reliable reporting to investors.

(3) Current cyber risk and incident disclosure has limited value to investors.

Investors do care about cybersecurity information and the impact of cyber incidents on a business, but cyber risk and incident disclosure today has very little value to the average investor. Disclosures are boilerplate, vague, unhelpful to investors, inaccurate, and sometimes non-existent. The information that would be truly important for investors – specific information about cyber risk management and internal oversight, as well as quantitative information about cyber incidents and their real or expected financial impact – is rarely disclosed.

---

[6] Former Federal Bureau of Investigation Director Robert Mueller and US Attorney General Eric Holder have suggested that every US company has been the victim of a cyber attack; former National Security Agency Director Keith Alexander stated that US companies have experienced "the greatest transfer of wealth in history," a fact that, if true, would certainly be a surprise to investors given the relatively low level of incident disclosure in filings. See testimony of Gen. Keith Alexander before the US Senate Committee on Armed Services, 12 March 2013, available at http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf.

[7] Target experienced a 5.5 percent drop in number of transactions, 3.8 percent decline in sales year over year, and estimated hundreds of millions of dollars in losses related to the breach incident. Paul Ziobro, "Target Earnings Slide 46% After Breach," Wall Street Journal, Feb. 26, 2014, available at http://online.wsj.com/news/articles/SB10001424052702304255604579406694182132568

[8] US Securities and Exchange Commission Cybersecurity Roundtable, Mar. 26, 2014, available at http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt

Investors can and should demand greater transparency with respect to cyber risk and incident data, just as they have done in areas like environmental risk and governance. But without further assistance from the SEC, the asymmetry in information access may continue to create great challenges to investors in obtaining the information that they need. In the case of cyber risk and incident data, investors are entirely reliant on market participants to provide adequate data because the company is the only real source of the data. When an incident occurs, investors should not be expected to calculate the value of the data lost and the costs to mitigate the exposure; they do not have the data necessary to perform those calculations. The registrant is clearly in the best position to perform this analysis and provide that information to investors. Unfortunately, this type of analysis does not happen today; investors, instead, are typically provided a limited statement from a company that nearly always states that a breach occurred but it will not have a material impact on the business. Registrants owe their investors more sophisticated analysis of the risks and incidents than what they are currently providing, and the SEC is the proper organization to reduce that asymmetry and enforce that information disclosure.

(4) The SEC must take additional steps to establish consistency and value in cyber risk and incident disclosure.

Given the SEC's role in protecting investors and maintaining fair, orderly, and efficient markets, there are specific steps that the SEC must take with respect to cyber risk and incident disclosure:

- **Create an education and awareness campaign to raise awareness of the existing disclosure laws, including disclosure obligations and investors' rights to obtain information.** With respect to cyber risk and incident disclosure, the SEC should seek to educate three main groups: registrants, investors, and attorneys. The SEC took a very strong first step by holding its Cybersecurity Roundtable in March, and Commissioner Aguilar's speech at the New York Stock Exchange in June was a very important initiative. The SEC should consider holding more roundtables, but also attend and deliver remarks at investors conferences and legal seminars, as well as provide more reminders to registrants about cyber risk and incident disclosure besides the occasional cybersecurity comment letter. This education campaign will highlight the information asymmetry that many investors likely did not previously recognize existed.

- **Work with business and investors to develop a material cyber risk and incident reporting structure for registrants.** Though the staff guidance was a very important initiative, the SEC can do more to create consistency in material risk and incident reporting. Working with key participants, the SEC can create a basic, consistent, and standard reporting structure for registrants to disclose material cyber risks, incidents, and other relevant information about cybersecurity in order to provide adequate information to investors.

  Standardizing the cyber risk and incident disclosure process will create significant confidence and greater assurance for both investors and registrants. A consistent reporting structure will be beneficial to reduce information asymmetry for

investors, who will gain access to better, more reliable, and more easily consumable information. Registrants will benefit from the procedural clarity as well as the ability to distinguish themselves in the marketplace.

The SEC can provide a list of items that registrants should disclose and a template for the disclosure. As suggested by the SEC's cybersecurity guidance, information disclosure should not compromise ongoing cybersecurity efforts. A list of items relevant to investors may include:

- The organization's overall assessment of its risk (assessed perhaps against the National Institute of Standards and Technology's new cybersecurity framework)
- The organization's approach to cyber risk management, including organizational structure (e.g. roles/responsibilities, organizational chart)
- Key policy and technical controls
- Third party security evaluations and/or ratings
- Accounting standards used by the organization to estimate cyber risk and incident impact
- Actual assessed losses from a cyber incident
- Damage assessment process utilized by the organization to provide insight and assurance to investors about how the company arrives at its materiality determination in the cybersecurity context
- Post-incident "best estimates" of financial costs and damage, prepared by the organization or a third party that would provide analysis to investors of the expected financial losses that the company reasonably expects to incur from the incident (including short-, medium-, and long-term losses from trade secret or intellectual property theft)

The SEC should consider facilitating meetings with interested investor groups and registrants to help shape the list of relevant material information that investors desire from registrants as well as presentation format.

- **Request the Financial Accounting Standards Board (FASB) develop recommendations with respect to cybersecurity accounting issues.** Accounting for cyber-related losses of data including intellectual property and trade secrets presents a difficult and significant challenge for companies, and greater attention must be placed on this critical issue. The SEC should request the FASB: 1) review cyber risk and incident accounting standards currently employed by public companies, 2) report their findings to the SEC, and 3) examine any gaps in practices or standards that should be addressed in order to improve public accounting of cyber incidents and losses.

- **Enforce existing disclosure laws.** There are now several public examples of data breaches that appear to be material cyber incidents that were not contemporaneously reported to investors. Failure to enforce disclosure laws in highly public cases sends a signal to investors and registrants alike that materiality

standards will not be enforced by the SEC. Enforcement of existing disclosure requirements should be a priority for the SEC in order to provide greater stability and certainty for investors and market participants. The SEC can leverage public reporting of breach incidents as well as other data security tools currently available to the private sector to ensure that market participants and investors are being protected.

- **Consider issuing additional guidance.** Additional guidance from the SEC to registrants may be necessary to improve the quality and quantity of material risk and incident disclosure. The 2011 staff guidance is an excellent and thoughtful approach to the difficult issue of cyber risk and incident disclosure, properly documenting the analysis that a company should consider when considering an incident is material. Comment letters have been helpful to give registrants a greater understanding of their obligations and potential disclosure shortcomings. More, however, may be required from the SEC to ensure the proper consideration of these issues within public companies. For instance, the SEC may consider issuing interpretive guidance on the matter to consolidate some of the outstanding issues and provide the Commissioners' imprimatur on the subject. Interpretive guidance on climate change, issued by the SEC in 2010, appears to have had a significant and positive impact on the quality and timeliness of sustainability disclosure.