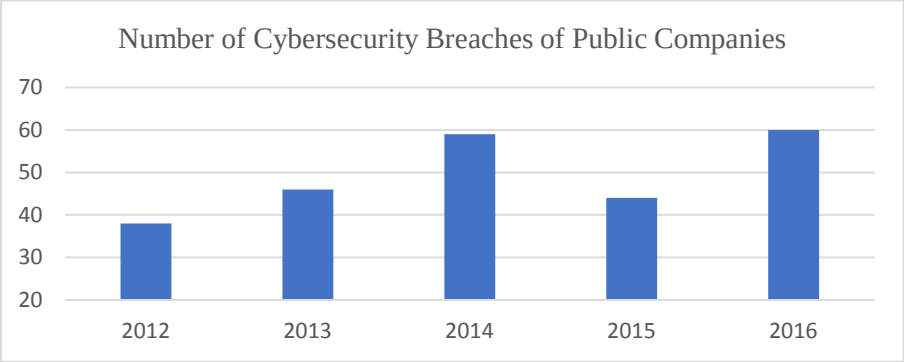
Discussion Draft Re: Cybersecurity and Risk Disclosure

(Note: This draft has not yet been approved by the Investor as Owner Subcommittee.)

Findings:

- In recent years, cyber-attacks on U.S. public companies have become more frequent and sophisticated.[1] In the last three years, over 150 U.S. public companies, including large and prominent companies such as Equifax, Yahoo, J.P. Morgan, Target, and Hyatt Hotels, have fallen victim to large-scale cyber-attacks.[2] In recently calling for "better disclosure" around cybersecurity risks, SEC Chairman Jay Clayton noted that he was "not comfortable that the American investing public understands the substantial risks that we face systemically from cyber issues."[3]

Figure 1.[4]



[1] During the December 9, 2013 Financial Stability Oversight Council meeting, former Assistant Treasury Secretary Cyrus-Amir-Mokri said that "[o]ur experience over the last couple of years shows that cyber-threats to financial institutions and markets are growing in both frequency and sophistication. The changing-nature of these cyber-threats prompted this Council last year to highlight operational risk, and cybersecurity in particular, as worthy of heightened risk management and supervisory attention." *See* Remarks of Assistant Secretary Cyrus Amir-Mokri on Cybersecurity at a Meeting of the Financial Stability Oversight Council, December 9, 2013, https://www.treasury.gov/press-center/press-releases/Pages/jl2234.aspx.

[2] On September 7, 2017, Equifax announced that a cyber incident affected 143 million U.S. customers. *Equifax Reports Cyber Incident, May Affect 143 Million U.S. Customers*, Bloomberg News, https://www.bloomberg.com/news/articles/2017-09-07/equifax-reports-cybersecurity-incident-potentially-impacting-143-million-u-s-customers. In 2014, Yahoo reported that hackers stole information on 500 million users. Robert McMillan, *Yahoo Says Information on at Least 500 Million User Accounts Was Stolen*, The Wall Street Journal, September 22, 2016, http://www.wsj.com/articles/yahoo-says-information-on-at-least-500-million-user-accounts-is-stolen-1474569637 Similarly, the 2014 J.P. Morgan data breach compromised data associated with 83 million customer accounts. Greg Farrell, *JPMorgan's 2014 Hack Tied to Largest Cyber Breach Ever*, Bloomberg News, https://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds.

[3] John McCrank, *SEC Chief Says Cyber-Crime Risks are Substantial, Systemic*, Reuters, September 5, 2017, http://www.reuters.com/article/us-sec-enforcement/sec-chief-says-cyber-crime-risks-are-substantial-systemic-idUSKCN1BH094.

[4] Figure 1 draws on data from Audit Analytics, *Cybersecurity Experts on the Board of Directors*, August 9, 2017, http://www.auditanalytics.com/blog/cybersecurity-experts-on-the-board-of-directors/.

- Cybersecurity breaches can lead to loss of intellectual property, operational disruption, decreased customer trust, tarnished reputation, and loss of investor commitment, all of which negatively affect shareholder value.[5] According to a 2017 study by IBM, each data breach on average compromises 24,089 confidential records and costs a company's shareholders $4 million.[6] Larger cyber-attacks have resulted in single incidents of shareholder wealth destruction of over $100 million, affecting millions of customers, and may lead to significant reputational harm.[7] A recent study by Cisco revealed that over one-third of organizations that experienced a breach in 2016 reported customer, opportunity, and revenue loss of more than 20 percent.[8]

- According to a survey of more than 600 corporate board members released by the National Association of Corporate Directors, ***only 19 percent say their boards have a "high level of understanding" of cybersecurity risks***.[9] In contrast to the data summarized above, which suggest that cyber-risk is serious at a growing and sizeable share of companies, a survey by the Harvard Business Review found that only 8% of board members view cybersecurity as a strategic threat.[10] The study also found that "[b]oards lack the processes and the expertise they need to surface, evaluate, and address cyberthreats."[11] According to a 2015 study by IBM, having board-level involvement reduces the average cost of a breach by $5.50 per compromised record, or by around $132,500 (3.5%) for the average breach.[12] The study also found that having business continuity management, which often includes board involvement, can reduce the average cost of a breach by $7.10 per compromised record, or by around $171,000 (5%) for the average breach.

---

[5] For example, after the recent announcement of Equifax's cyber breach, the company's shares dropped 14%. https://finance.yahoo.com/quote/EFX?p=EFX. *See also*, Cisco 2017 Annual Cybersecurity Report, January 31, 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1818259 (showing that cyber breaches lead to substantial losses in revenue, customer retention, and business opportunities).

[6] IBM Security and Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview*, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

[7] The attack on Target in 2014 led to $148 million in damages. *See* Sharone Tobias, *2014: The Year in Cyberattacks*, Newsweek, December 31, 2014, http://www.newsweek.com/2014-year-cyber-attacks-295876.

[8] Cisco 2017 Annual Cybersecurity Report, January 31, 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1818259.

[9] *See* Matt Hamblen, *Corporate Boards Aren't Prepared for Cyberattacks*, National Association of Corporate Directors, December 26, 2016, https://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=38735.

[10] J. Yo-Jud ChengBoris Groysberg, *Why Boards Aren't Dealing with Cyberthreats*, Harvard Business Review, February 22, 2017, https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats.

[11] *Id.*

[12] IBM Security and Ponemon Institute, *Cost of Data Breach Study: Global Analysis*, 27 May, 2015, http://www-03.ibm.com/press/us/en/pressrelease/47022.wss.

- Securities law disclosures could include substantive descriptions of cyber-attack risk or events and non-proprietary and non-sensitive descriptions of how issuers are responding to the threat of such attacks. Disclosures could also include descriptions of efforts to quantify potential risks, the scope and progress of programs of investment of corporate resources aimed at addressing those risks, and discussions of the board- and management skills and resources an issuer has to address the risks on an ongoing basis.

- Issuers could devote discrete portions of their management discussion and analysis to trends and known uncertainties associated with how cyber-attacks could result in losses. Issuers could disclose whether their boards include cyber experts, and if not, why a board does not believe such expertise is necessary for the issuer to address cyber risks. If required by SEC regulation, a disclosure obligation focused on board and management capabilities increase the level of board awareness and understanding of cyber risks at their own company, encourage boards directly to address cyber risk at least once per year, as part of the annual proxy statement disclosure cycle, and may usefully encourage boards to consider adding cyber expertise to board or senior management.[13]

- Although under the current regulatory regime companies disclose certain risks or loss events associated with cybercrime, such disclosures often appear to be minimal and/or boilerplate, and do not provide investors with sufficient information on the company's ability to address cybersecurity concerns.[14] The nature of the even past attacks is commonly described in terms so general investors have no ready way of assessing whether those attacks are likely to recur. Given the gravity of risks associated with cyberattacks, investors have a right to know whether public companies are prioritizing cybersecurity and whether they have directors who can play an effective role in cyber-risk oversight.

---

[13] This is the approach taken by the Cybersecurity Disclosure Act of 2017, S.536, 115th Cong. (2017), a bill introduced by U.S. Senators Jack Reed (D-RI) and Susan Collins (R-ME). If a company does not have a cybersecurity expert on the board, the bill prompts the SEC to require an explanation of the processes that went into the selection process.

[14] For example, Snap's cybersecurity risk disclosure in the most recent registration statement states "[m]obile malware, viruses, hacking, and phishing attacks have become more prevalent in our industry, have occurred on our systems in the past, and may occur on our systems in the future. Because of our prominence, we believe that we are an attractive target for these sorts of attacks. Although it is difficult to determine what, if any, harm may directly result from an interruption or attack, any failure to maintain performance, reliability, security, and availability of our products and technical infrastructure to the satisfaction of our users may seriously harm our reputation and our ability to retain existing users and attract new users." Snap Inc. S-1 Registration Statement, https://www.sec.gov/Archives/edgar/data/1564408/000119312517029199/d270216ds1.htm#rom270216_2. Similarly, Yext's recent registration statement states, "[w]e are vulnerable to computer viruses, break-ins, phishing attacks, attempts to overload our servers with denial-of-service or other attacks and similar disruptions from unauthorized use of our computer systems. Any such attack, or any information security incident from any other source affecting us or our services providers, including through employee error or misconduct, could lead to interruptions, delays, website or application shutdowns, loss of data or unauthorized access to, or use or acquisition of, personal information, confidential information or other data that we or our services providers process or maintain." Yext S-1 Registration Statement, http://otp.investis.com/clients/us/yext_inc/SEC/sec-show.aspx?Type=page&FilingId=11926612-66562-196141&CIK=0001614178&Index=17000. Neither Snap nor Yext's disclosures mention whether their directors or managers have expertise in cybersecurity.

Recommendation:

We note the last formal guidance from the SEC or its staff on cyber-risk was published in 2011. Since that time, the SEC has held a roundtable on the topic, and reflected to some extent cyber-risk in some of its rulemakings. Specific SEC Commissioners have spoken on the topic. Given Chair Clayton's public statements, we expect and would encourage the SEC and its staff will remain engaged with this issue. More specifically, in line with its mission to protect investors,[15] the SEC should respond to the growing concern over cyberattacks on public companies by enhancing disclosure requirements associated with cybersecurity risks, while respecting the need of companies to not reveal sensitive or proprietary information useful in combating those same risks. Specifically, we recommend that the SEC require public companies to include:

1) A more comprehensive description of company-specific cybersecurity risks, including a detailed description of trends and risks to future financial performance in the Management Discussion and Analysis portions of annual and quarterly reports.

2) Specific, non-proprietary and non-sensitive information about past cyber-attacks, including summary information derived from root-causes analyses of how the attacks were or were not successful, to clarify the nature and significance of ongoing risks. (We here note and commend the SEC's own recent disclosures regarding a cyber-attack at the agency as the kind of specific disclosures that provide assurance as to ongoing management and investigation of cyber-risk.)

3) A general description of the company's efforts to minimize cybersecurity risks and its capacity to respond to cyberattacks, including measures taken to elect or appoint special committees, response units, designated officers, or third parties responsible for securing company data and customer information. (We recognize that detailed descriptions of security systems may jeopardize cybersecurity efforts, and we do not advocate rules requiring disclosure of sensitive information. However, we believe that investors have a right to know whether the company has undertaken efforts to protect itself from cybercrime.)

4) Information on whether any member of the governing body, such as the board of directors of the reporting company, has experience, education, or expertise in cybersecurity, and if not, why a company believes that such board-level resources are not necessary for the company to adequately manage cyber risks. (Again, we recognize that such explanations would not be beneficial if they revealed proprietary or sensitive information that could increase a company's exposure, but we believe that more information than is currently being provided could be provided without jeopardizing company's security.)

[15] The mission of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. 15 U.S.C. § 78c(f) (2006).