TheChertoffGroup
Enabling A More Secure World

CHERTOFF GROUP POINT OF VIEW ON SEC GUIDANCE

Updated 2018 Guidance on Public Company Cybersecurity Disclosure Requirements Under Federal Securities Laws

WWW.CHERTOFFGROUP.COM

On February 21, the U.S. Securities and Exchange Commission (SEC) released updated guidance on public company cybersecurity disclosure requirements under Federal securities laws.[1] While news articles have focused on the guidance's emphasis on timeliness and insider trading prohibitions, a foundational question is whether the cyber risks and incidents are "material." Making informed decisions on materiality demands, in part, active and continuing understanding and management of underlying cyber risks.

Timely disclosure of material risks and incidents, and no insider trading. The guidance focuses on two topics: (1) the importance of maintaining comprehensive cyber policies and procedures, particularly on timely disclosure of material cyber risks and incidents, and (2) the application of insider trading prohibitions to material cybersecurity risks and incidents.

The guidance implicitly responds to controversy around how senior management and boards of directors addressed recent incidents at Yahoo, Uber and Equifax. In the cases of Yahoo[2] and Uber[3], a significant time lapse occurred between the discovery of a compromise and notification to the public. In the case of Equifax, several senior executives sold stock immediately after the breach was discovered but before it was publicly disclosed.[4]

Materiality and board oversight. A threshold disclosure question is one of materiality – i.e., if there is a "substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available." The SEC guidance states that, as part of a materiality analysis, "a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity." According to the SEC, potential consequences include "harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities."

While the Commission provides that "[w]e do not expect companies to publicly disclose specific, technical information about their cybersecurity systems," there is an expectation that public companies should "disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure." A key question is thus how senior management and Boards are advancing their understanding of cyber risk such that they can make informed judgments about materiality.

Several recent disclosures are (notwithstanding that they mostly predate the Guidance) instructive.

- Equifax's 2017 earnings report included reference to its data breach throughout the report. It reported $99.1 million in costs to investigate and remediate the cybersecurity incident, plus legal and other professional services. It also reported $50.7 million in additional costs for credit monitoring and related services, while also noting that it was the subject of multiple class action lawsuits and government inquiries.[5] As a point of reference, Equifax reported $3.4 billion in 2017 revenue and $587 million of net income.[6] Less obviously, the report also noted that revenue declined in 2017 due to the impact of the cybersecurity incident:

    - "Certain of our customers have determined to defer or cancel new contracts or projects and others could consider such actions unless and until we can provide assurances regarding our ability to prevent unauthorized access to our systems and the data we maintain. Many of our customers are requiring security audits of our systems and any negative results of such audits may cause further losses of customers. In addition, some of our current and potential customers and the contracts governing certain customer relationships, as well as certain of our data suppliers, require us to maintain International Organization for Standardization ("ISO") certifications, such as ISO 27001 certification, that specify requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system. Due to the 2017 cybersecurity incident, certain of our ISO certifications have been suspended and we will be required to take additional remediation steps to retain such certifications, which efforts may not be successful. Additionally, certain of our payment card industry certifications have been suspended which could result in fines and loss of access to data if we are not able to complete the necessary remediation steps to retain these certifications, which would adversely affect our ability to offer certain products to customers. If we are unable to demonstrate the security of our systems and the data we maintain and rebuild the trust of our customers, consumers and data suppliers, and if further negative publicity continues, we could experience a substantial negative impact on our business."[7]

- While much recent focus and attention has been directed at data breaches, attacks aimed at compromising the integrity or availability of systems may be more pernicious. A number of major global companies were impacted by notPetya, a ransomware campaign originating in Ukraine in June 2017. The U.S. Government has since attributed notPetya to the Russian Federation as "part of the Kremlin's ongoing effort to destabilize Ukraine."[8] Companies impacted by notPetya included pharmaceutical giant Merck, FedEx and Danish shipping company Maersk – each to the tune of hundreds of millions of dollars.

- In its most recent quarterly report, FedEx reported a cumulative $400 million impact to earnings. Interestingly, the impact was "primarily from loss of revenue due to decreased shipments" as well as associated remediation costs.[9] As a point of reference, FedEx reported $60 billion in consolidated 2017 revenue and roughly $3 billion in net income.[10] Moreover, FedEx went on to note that, while critical operational systems have been fully restored, "not all customers are shipping at pre-attack volume levels."

- Likewise, Merck reported a cumulative $590 million 2017 loss -- divided between revenue and expense impacts – based on impacts to its manufacturing, research and sales operations. While Merck took the position that the impact of the attack on the company's operations and financial condition "has not been material to date," the company reported a $260 million unfavorable impact on sales based on an inability to fulfill orders in certain markets.[11] In particular, Merck reported that "the temporary production shut-down from the cyber-attack contributed to the Company's inability to meet higher than expected demand for [HPV vaccine] Gardasil 9, which resulted in Merck's decision to to borrow doses of Gardasil 9 from the U.S. Centers for Disease Control and Prevention Pediatric Vaccine Stockpile."[12] As regards expense, Merck reported $330 million in gross expense due to manufacturing variances and remediation efforts-related expenses.[13] Merck is also forecasting another $200 million adverse impact to sales in 2018 based on order backlogs.[14] As a point of reference, Merck reported $40 billion in consolidated 2017 revenue and $2.4 billion in net income.[15]

Probability. What can we learn from these disclosures? Returning to the Guidance's focus on probability and impact, let's start with probability. In all cases, the intrusion vector appears to have involved the exploitation of an unremediated vulnerability inside the victim organization's environment. Tempting as it is to blame the victim for what was obviously a fateful delay in vulnerability remediation, the fact is that patching can break things, thus underscoring the importance of careful remediation planning. Of course, careful planning is not license for indefinite delay and inaction – the adversary does not offer time-outs – and a key question revolves around risk-based defensive measures to limit the spread of an infection inside the environment. This dynamic also calls for focused education for senior management and then boards on key questions – and likely implementation challenges – in managing cyber risk. Have we identified our crown jewels? Do we have the right talent in place? Can we execute? How do we evaluate effectiveness? The more confidence we have in program and control effectiveness, the lower we can ascribe probability of a cyber harm. Are we seeking advice from outside counsel and auditors on "materiality" thresholds?

Impact … and opportunity. Turning to impact, each of the three above-cited incidents offer important insights into the changing nature of cyber harms. Historically, with data breach cases, a narrative has developed that companies don't suffer long term impacts – yes, incidents entail significant (non-recurring) remediation and litigation expenses, but customers still keep doing business. However, in all three of the above cases, the reported impact extends beyond remediation costs, litigation and other expenses … to an immediate revenue impact. Merck couldn't fulfill orders. FedEx couldn't deliver packages. Equifax customers deferred contract renewals.

The FedEx and Equifax incidents also point to two potentially important long-term trends: (1) substitution effect and (2) changing customer drivers. In FedEx's case, the impairment of the company's operations appeared to cause customers to switch to competitor package delivery services. Having switched, some percentage will (for whatever reason) simply never return. In Equifax's case, an increasing number of commercial customers are imposing formalized, auditable cybersecurity requirements as a condition of contract. Moreover, these requirements are often unique to the buyer. So imagine the post-incident challenge of satisfying a diverse group of customers that the victim organization has an effective program in place.

In this challenge also lies an opportunity: to invest in cybersecurity as a differentiator with customers. Boards understand value creation. Thus, when presented with a cybersecurity investment roadmap, questions should not only revolve around "will this investment advance our effectiveness?" but also, "how can we position this investment as a customer advantage?"

Preparedness … and its relationship to timeliness. . Since there is no such thing as risk elimination (even the SEC's own EDGAR database was breached[16]), resiliency becomes critical. Management and boards should thus have a firm view of the effectiveness of preparedness, response and recovery capabilities, for two reasons. First, being prepared helps limit the extent of actual harm to the company. Second, management's ability to effectively manage a crisis – cyber or otherwise – serves as a proxy for its broader management capabilities and thus influences the brand's reputation. Years ago, in its 2012 Reputation Review Report, Oxford Metrica analyzed long-term market value impacts of major corporate crises (cyber and non-cyber) found that "[a]t times of crisis, substantially more information is forthcoming on a company and, in particular, on its management, than is usually available. This new information is used by investors and other stakeholders to re-assess their expectations of future behaviour and performance." The report went on to conclude: "It is in the first few days following an event that the market makes its judgement on whether a company is going to emerge as a Winner or a Loser."[17]

Most large companies now understand that having an incident response plan is table stakes. But having an incident response plan is no guarantee of effectiveness. Rather, key escalation triggers must be defined and understood – for example when a vulnerability crosses over into a breach. Key personnel must, through training and exercises, understand their roles and key decisions to be made in a crisis – including when to call in outside help (consider the changes recently announced by Uber, such as having "more stakeholders involved in the decision-making process for how to handle security incidents, and informing law enforcement of potential security incidents right away"[18]). And technology should be architected to anticipate that incidents will occur and thus facilitate quick response response and recovery. In this way, the SEC's timeliness expectation

becomes less of an issue because the incident investigation does not linger over an extended period. Likewise, expectations around materiality and insider trading are anticipated as part of preparedness-related planning.

Active engagement with U.S. Government. Finally, these cases all suggest the need for a more active management and Board engagement in demanding active U.S. Government support for defending the private sector. Of the above-cited examples, all but one (Uber) have been either explicitly (Yahoo[19], Merck, FedEx[20]) or implicitly (Equifax[21]) tied to a hostile state actor. The U.S. Director of National Intelligence's 2018 Annual Worldwide Threat Assessment recently warned that "[t]he risk is growing that some adversaries will conduct cyber-attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war."[22] Moreover, the notPetya attack reportedly leveraged vulnerabilities used for offensive purposes by the U.S National Security Agency but subsequently leaked.[23] While there is little expectation that U.S. Government agencies would be playing a defensive operational role inside a public company, there are a number of steps the Government can take, including timely sharing of actionable cyber threat information, more actively disclosing vulnerabilities, advancing research and development efforts, and imposing consequences on those actors to whom it can attribute malicious cyber activity.

[1] See https://www.sec.gov/news/press-release/2018-22. This guidance expands on 2011 guidance that provided the Division of Corporation Finance's views on cyber risk-related disclosure obligations, which is available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] See Oct. 3, 2017 Oath press release updating a December 2016 disclosure and announcing that all 3 billion Yahoo accounts by an August 2013 data theft, available at https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/.

[3] See Nov 21, 2017 blog by Uber CEO Dara Khosrowshahi disclosing a late 2016 incident in which information on 57 million customers and 600,000 drivers was inappropriately accessed and downloaded by external actors, available at https://www.uber.com/newsroom/2016-data-incident/?state=4XD-binlsTek0dVDiYww--pamS55UaDsd_D4IUnh_Ak%3D&_csid=H9m412OrGzOp9I9sC6kR7A#._

[4] See https://www.npr.org/sections/thetwo-way/2017/09/08/549434187/3-equifax-executives-sold-stock-days-after-hack-that-wasnt-disclosed-for-a-month. See also Equifax Inc., Form 10-Q for the Quarterly Period Ended September 30, 2017, p. 41, where the company noted that "we have received subpoenas with respect to investigations by the SEC and the U.S. Attorney's Office for the Northern District of Georgia regarding trading activities by certain of our employees in relation to the cybersecurity incident." Available at https://investor.equifax.com/financial-information/sec-filings

[5] See Equifax Inc. Form 10-K for 2017, available at https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?Type=html&FilingId=12595195&CIK=0000033185&Index=10000. Moreover, in a recent earnings call, Equifax said it expects costs related to the 2017 data breach to grow by $275 million this year. See https://www.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUSKCN1GE257.

[6] See Id.

[7] See Id.

[8] See Statement from the Press Secretary, the White House, Feb. 15, 2018, available at https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

[9] See FedEx Form 10-Q for the Quarterly Period Ended November 30, 2017, available at http://investors.fedex.com/financial-information/sec-filings/default.aspx.

[10] See FedEx 2017 Annual Report, available at http://d18rn0p25nwr6d.cloudfront.net/CIK-0001048911/7fba0d15-1c88-4aeb-a941-4b86fb1163af.pdf.

[11] See Merck Form 10-K for the Fiscal Year Ended 2017, available at http://s21.q4cdn.com/488056881/files/doc_financials/2017/Q4/2017-Form-10-K_FINAL-wo-Exhibits_Filed-022718.pdf.

[12] See Id.

[13] See Id. The net loss was $285 million based on insurance recoveries.

[14] See Id.

[15] See Id.

[16] See Chairman's Statement on Cybersecurity, Sept. 20, 2017, available at https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

[17] See http://www.aon.com/attachments/risk-services/Aon-OM-Reputation-Review-2012.pdf.

[18] See Testimony of John Flynn, Chief Information Security Officer, Uber Technologies, Inc., Senate Commerce Committee, Feb. 8, 2018, available at https://www.commerce.senate.gov/public/_cache/files/7d70e53e-73e9-4336-a100-67b233084f12/75728554E990488D71625DFA69B05494.uber---john-flynn---testimony.pdf.

[19] See https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

[20] See https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

[21] See https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

[22] See https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[23] See https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/.

TheChertoffGroup
Enabling A More Secure World

1399 NEW YORK AVENUE NW, SUITE 900 | WASHINGTON, DC 20005
T. 202.552.5280 | F. 202.330.5505 | WWW.CHERTOFFGROUP.COM