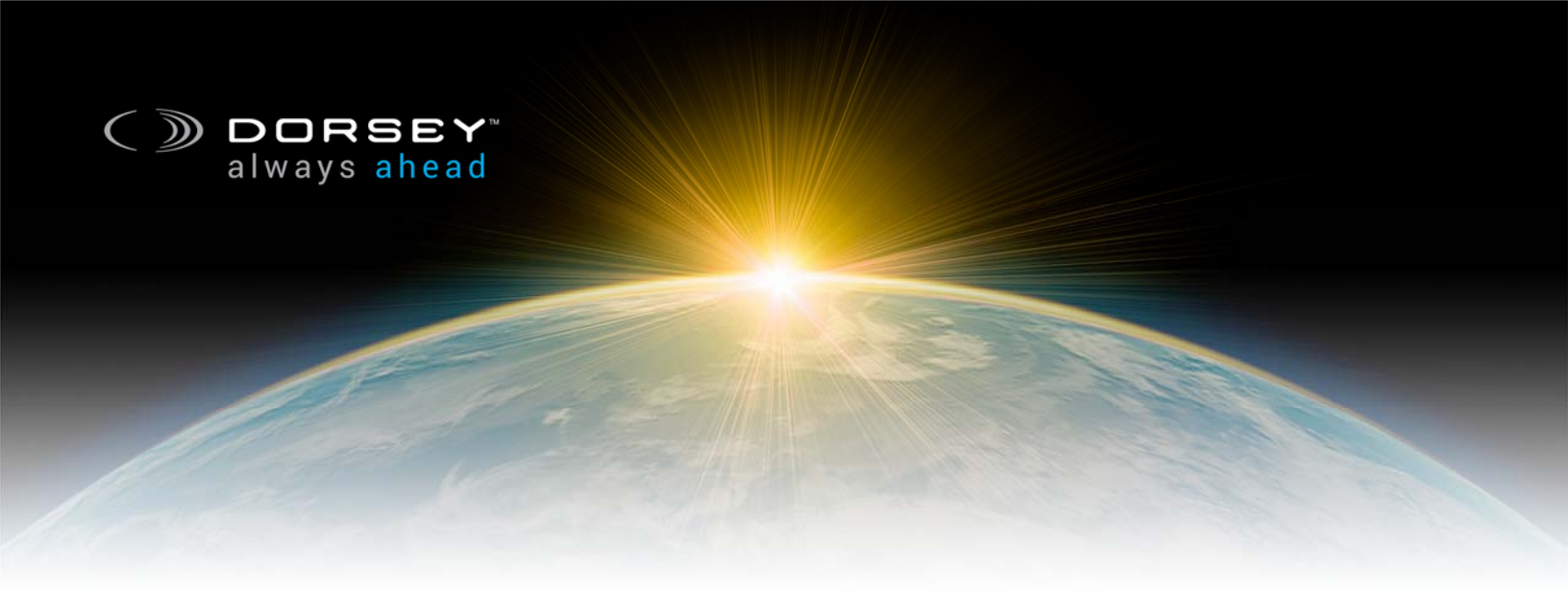


Corporate Governance & Compliance

SEC Guidance on Cybersecurity Disclosure and Policies

June 5, 2018

Dorsey & Whitney Speakers

Gary Tygesson
Cam Hoang
Bob Cattanach

Corporate Governance & Compliance

SEC Guidance on Cybersecurity Disclosure and Policies

Contents

Other Resources

Dorsey's Corporate Governance and Compliance Blog
Available at: http://governancecomplianceinsider.com/

U.S. Department of Commerce Presentation on GDPR (March 28, 2018)
Available at: https://www.dorsey.com/~/media/files/uploads/images/cattanach_gdpr.pdf?la=en

The Sedona Conference Incident Response Guide to Data Breach Compliance, Robert Cattanach (March 23, 2018)
Available at: https://www.dorsey.com/newsresources/publications/client-alerts/2018/03/robert-cattanach-editor-in-chief-data-breach

Seminar Playback: *The EU General Data Protection Regulation (GDPR): The Time to Act is Now*, Robert Cattanach, Ron Moscona and Jamie Nafziger (December 4, 2017)
Available at: https://www.dorsey.com/newsresources/events/videos/2017/12/seminar-playback-the-eu-general-data-protection

Bloomberg BNA Interview: Dorsey & Whitney Partner Bob Cattanach on Cybersecurity Incident Response & Mitigation (May 15, 2017)
Available at: https://www.bna.com/dorsey-whitney-partner-m73014450936/

Dorsey vUpdate: *Five Steps to Prepare for a Data Breach*, Robert Cattanach (August 2015)
Available at: https://www.dorsey.com/newsresources/publications/client-alerts/2015/08/five-steps-to-prepare-for-a-data-breach

Corporate Governance & Compliance

SEC Guidance on Cybersecurity Disclosure and Policies

Speaker Biographies

Robert Cattanach
Partner
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 340-2873
cattanach.robert@dorsey.com

Bob helps clients navigate the complexities of regulatory law, especially in the area of cybersecurity and compliance, and provides the perspective and skills of a seasoned trial lawyer to protect their interests in the courtroom. His technical background enables him to understand the complex business challenges associated with today's cyber world, and provide the strategic acumen to achieve success. Bob's decades of experience as a trial lawyer also enable his clients to achieve their business objectives if other means of resolution cannot be achieved. Bob has an active trial docket in courts around the country, where his innovative thinking, collaborative client approach, and keen strategic insights have provided his clients with a long string of successful verdicts and appeals. Under Bob's leadership, Dorsey teams have helped our clients achieve precedent-setting results, especially in the complex area of constitutional challenges to government overreach.

Cam Hoang
Partner
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 492-6109
hoang.cam@dorsey.com

Cam helps clients with corporate matters including governance and SEC compliance, securities offerings, and mergers and acquisitions. Prior to her return to Dorsey, Cam was Senior Counsel and Assistant Secretary at General Mills, Inc., where she helped the company achieve its corporate governance and SEC compliance objectives, worked on securities offerings and M&A transactions, risk management, foundation governance, and general corporate and commercial matters. Before joining General Mills in 2005, Cam was an associate for five years in the Dorsey Corporate Group in Minneapolis. Cam is a co-editor of Dorsey's corporate governance and compliance blog, http://governancecomplianceinsider.com/.

Gary Tygesson
Partner
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 340-8753
tygesson.gary@dorsey.com

Gary helps clients access the capital markets to achieve their financing objectives and advises on corporate governance, shareholder activism and sec compliance matters. Gary is Co-Chair of Dorsey's Capital Markets and Corporate Compliance Group with extensive experience advising public companies on a wide range of securities financing, reporting and compliance matters. Gary also regularly advises clients and their Boards of Directors with respect to corporate governance, SEC compliance, public company disclosure, shareholder activism and executive compensation. Gary served as Co-Chair of the firm-wide Corporate Group from 1997 to 2002 and as a member of the Firm's Management Committee from 1997 to 2002.

DORSEY™ always ahead

SEC Guidance on Cybersecurity Disclosure and Strategies

Gary Tygesson
Cam Hoang
Bob Cattanach

Presenters

GARY TYGESSON

Gary is the Co-Chair of Dorsey's Capital Markets and Corporate Compliance Group. He has extensive experience advising public companies on a wide range of securities financing, reporting and compliance matters. Gary also regularly advises clients and their Boards of Directors with respect to corporate governance, SEC compliance, public company disclosure, shareholder activism and executive compensation. tygesson.gary@dorsey.com

CAM HOANG

Cam, a partner in our Corporate Group, advises clients on governance and SEC compliance matters, equity plans and executive compensation, securities offerings, and mergers and acquisitions. Prior to her return to Dorsey, Cam was Senior Counsel and Assistant Secretary at General Mills, Inc., where she helped the company achieve its corporate governance and SEC compliance objectives, worked on securities offerings and M&A transactions, risk management, foundation governance, and general corporate and commercial matters. Before joining General Mills in 2005, Cam was an associate in the Dorsey Corporate Group in Minneapolis. hoang.cam@dorsey.com

BOB CATTANACH

Bob a partner in our Trial Group, helps clients navigate the complexities of regulatory law, especially in the area of cybersecurity and compliance, and provides the perspective and skills of a seasoned trial lawyer to protect their interests in the courtroom. Bob practices in the areas of regulatory litigation, cybersecurity and privacy. He also counsels clients on privacy and information security compliance requirements, incident response, and international regulatory compliance. **cattanach.robert@dorsey.com**

DORSEY™ always ahead

Overview

- Changing landscape of cybersecurity
- SEC guidance
- Shareholder expectations and claims
- SEC enforcement actions
- Regulatory and legislative initiatives
- Equifax case study

DORSEY™ always ahead

3

Changing Landscape of Cybersecurity

- Technological advances
- Hackers generally considered to be a generation ahead
- Greater sophistication of and collaboration among attackers
- The human factor remains the largest risk: it can be improved through training, but we will never be perfect
- IoT has broadened the perimeter you have to defend
- Inherent tension: improving efficiency versus maintaining security

DORSEY™ always ahead

4

Changing Landscape of Cybersecurity

- **Regulatory and legislative initiatives**
- **Shareholder expectations and claims**
- **Equifax highlighted need for clearer guidance:**
  - Lack of urgency in disclosing
  - Insider trades before public disclosure

DORSEY™ always ahead

5

SEC 2011 Guidance

- **CF Disclosure Guidance: Topic No. 2 – Cybersecurity (October 13, 2011)**
- **While SEC regulations do not specifically address cybersecurity they are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.**
- **Disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents:**
  - Risk factors
  - MD&A
  - Description of business
  - Legal proceedings
  - Financial statements
  - Disclosure Controls and Procedures

DORSEY™ always ahead

6

SEC 2018 Guidance

- **Commission Statement and Guidance on Public Company Cybersecurity Disclosures (*Rel. No. 33-10459*) (February 21, 2018)**
  - Issued by Commission
  - Reinforced 2011 guidance, but more urgent in tone
  - Enhanced guidance on disclosure of cybersecurity issues, but within the existing disclosure framework
  - New focus on policies and procedures

DORSEY always ahead

7

General Disclosure Obligations: Materiality

The standard for disclosure remains MATERIALITY:

- Is there a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that the disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available? *(TSC Industries v. Northway)*
- 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. *(Basic v. Levinson)*

- **According to the 2018 SEC guidance, the materiality of cybersecurity risks or incidents depends on:**
  - their nature, extent and potential magnitude, and
  - the range of harm that such incidents could cause, including reputation, financial performance, customer and vendor relationships, and the possibility of litigation or regulatory investigations or actions

DORSEY always ahead

8

General Disclosure Obligations: Materiality

- **Omitted information can be material**
- **Materiality is a judgment call:** No bright lines, unlike the state law notification requirements
- **Technical and compromising information should not be disclosed**
- **The SEC staff may contact company counsel for an analysis of why a breach was not material**, when they see a news report that a hack has occurred (according to recent Congressional testimony by Bill Hinman, SEC Chief of Division of Corporation Finance)

DORSEY™ always ahead

9

General Disclosure Obligations: Timing

According to the SEC's 2018 guidance:

- **Ongoing investigation is not a basis for delaying disclosure:** The SEC recognizes that a company may require time to discern the implications of a cybersecurity incident…however, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.
- **Disclosure prior to securities offering:** Where a company has become aware of a material incident or risk, SEC expects appropriate disclosure sufficiently prior to the offer and sale of securities and steps to prevent insider trading.
- **Use Current Reports**: Timely disclosure may require a current report on Form 8-K. Item 8.01 may be used to report information not otherwise called for by the form, but of importance to securityholders.

DORSEY™ always ahead

10

General Disclosure Obligations: Timing

According to the SEC's 2018 guidance:

- Companies may have a **duty to correct** prior disclosure that the company determines was untrue, or where the company omitted a material fact necessary to make the disclosure not misleading, at the time it was made.
- Companies may have a **duty to update** disclosure that becomes materially inaccurate after it is made (for example, when the original statement is still being relied upon by reasonable investors).
- But the 2018 guidance cites a case holding that there is **no duty to update before the next quarterly report** (*Higginbotham v. Baxter Intern., Inc. (7th Cir. 2007)*)

DORSEY always ahead

11

Risk Factors

(Item 503(c) of Reg. S-K; Item 3.D of Form 20-F)

- **Consider the following issues in evaluating cybersecurity risk factor disclosure in an annual or quarterly report:**
  - Prior incidents, including severity and frequency
  - Probability and potential magnitude of future incidents
  - Adequacy of preventative actions, including limits on the company's ability to prevent or mitigate certain risks
  - Aspects of business and operations that give rise to material risks, including industry-specific, third-party and service provider risks
  - Costs associated with protections, including insurance coverage
  - Potential for reputational harm
  - Compliance with laws and regulations and associated costs
  - Costs of litigation, investigations and remediation
- **It may not be sufficient for a company that had a previous material cybersecurity breach to disclose simply that there is a risk that a breach could occur. The company may also need to discuss a prior or ongoing cybersecurity incident to provide context for its cybersecurity risks.**

DORSEY always ahead

12

MD&A

(Item 303 of Reg. S-K; Item 5 of Form 20-F)

- **In an annual or quarterly report, discuss cybersecurity events, trends or uncertainties that are reasonably likely to have a material effect on the company's results of operations, liquidity and financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition.**
- **Costs and other consequences of incidents, and risks of potential incidents, could inform the analysis:**
  - Preventative measures and insurance coverage
  - Immediate costs of an incident
  - Litigation and regulatory investigations and related costs
  - Compliance with laws
  - Remediation efforts
  - Loss of intellectual property
  - Effect of any possible reputational damage and loss of competitive advantage
- **Consider impact on each reportable segment, if applicable**

DORSEY™ always ahead

13

Description of Business and Legal Proceedings

(Item 101 of Reg. S-K; Item 4.B of Form 20-F) (Item 103 of Reg. S-K)

Description of business in an annual report. Disclose any material impact of cybersecurity risks or incidents on:

- Products
- Services
- Relationships with customers or suppliers
- Competitive environment

Legal proceedings in an annual or quarterly report

- Material pending legal proceedings, including cybersecurity lawsuits and investigations, must be disclosed in annual and quarterly reports
- Watch for interplay between materiality determinations and timing for SEC disclosure and other agencies' reporting requirements

DORSEY™ always ahead

14

Financial Statement Disclosures

(Reg. S-X)

- **Financial statement disclosures in annual and quarterly reports about cybersecurity incidents may include information about:**
  - Expenses for litigation, investigations, breach notification and remediation
  - Loss of revenue and goodwill
  - Claims related to warranties, breach of contract, product recall and indemnification
  - Insurance premium increases
  - Diminished future cash flows
  - Possible impairment of IP or other assets and recognition of liabilities
  - Increased financing costs
- **A company's financial reporting and control systems should be designed to provide reasonable assurance that information about the range and magnitude of the financial effects of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.**

DORSEY™ always ahead

15

Board Risk Oversight

(Item 407(h) of Reg. S-K; Item 7 of Schedule 14A)

- **SEC proxy rules require the company to disclose the extent of the Board's role in the risk oversight of the company, such as how the Board administers its oversight function.**
- **To the extent cybersecurity risks are material to a company's business, this discussion should include the nature of the Board's role in overseeing the management of that risk.**
- **The SEC believes that disclosures regarding a company's cybersecurity risk management program and how the Board engages with management on cybersecurity issues allow investors to assess how a Board is discharging its risk oversight responsibility.**
- **<u>Practice Point</u>: Consider next year's proxy disclosure now and update protocols as necessary.**

DORSEY™ always ahead

16

New Focus on Policies and Procedures

- **Comprehensive policies and procedures related to cybersecurity**
- **Disclosure controls and procedures related to cybersecurity disclosure**
- **Insider trading policies and procedures**
- **Regulation FD and selective disclosure policies**

DORSEY™ always ahead

17

Comprehensive Policies and Procedures Related to Cybersecurity

- **Companies are encouraged to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including disclosure controls and procedures (EU now mandates)**
- **Guidance does not specify IT-related policies and procedures, but examples would include:**
  - Network security
  - Security governance
  - Compliance
  - Risk management
  - Incident response
  - Business continuity

DORSEY™ always ahead

18

Disclosure Controls and Procedures Related to Cybersecurity Disclosure

- **Companies are required to establish and maintain appropriate and effective disclosure controls and procedures (*Exchange Act Rules 13a-15 and 15d-15*).**
- **Controls and procedures should ensure that the relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate effective operation of insider trading policies.**
- **Companies should review their disclosures controls and procedures to make sure they capture cybersecurity matters for consideration of possible disclosure.**

DORSEY™ always ahead

19

Insider Trading Policies and Procedures

- **Antifraud provisions of federal securities laws prohibit trading on the basis of material nonpublic information, which can include information about a company's cybersecurity risks and incidents.**
- **Companies are encouraged to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents.**
- **The SEC believes it is important to have well-designed policies and procedures to prevent such trading.**
- **While investigating and assessing significant cybersecurity incidents, should consider whether and when it may be appropriate to implement restrictions on insider trading.**

DORSEY™ always ahead

20

Insider Trading Policies and Procedures

- Does your company have one and have you reviewed it lately?
- Important items to consider:
  - Be clear on covered persons and how policy applies to each class of persons
  - Articulate and enforce pre-clearance procedure
  - Establish blackout periods related to quarterly financial reporting calendar
  - Provide for (and implement) event-specific blackouts
  - Provide examples of material nonpublic information (including cybersecurity)
  - Consider prohibiting certain transactions (standing orders, pledging, hedging)
  - Address use of Rule 10b-1 plans
  - Identify a contact for questions
  - Remind insiders of the policy at least annually
- See enclosed Dorsey eUpdate

DORSEY™ always ahead

21

Regulation FD and Selective Disclosure Policies

- The SEC expects companies to have policies and procedures to ensure that any disclosure of material nonpublic information related to cybersecurity risks and incidents are not made selectively and that any Reg FD required public disclosure is made in a timely fashion.
- Interplay of Reg FD requirements with breach notification laws

DORSEY™ always ahead

22

Regulation FD and Selective Disclosure Policies

- **Does your company have one and have you reviewed it lately?**
- **Important items to consider:**
  - **Establish authorized spokespersons and monitor for compliance**
  - **Be clear about application and protocol to various settings:**
    - ✓ Press releases
    - ✓ Earnings calls
    - ✓ Day-to-day communications
    - ✓ One-on-one meetings with analysts
    - ✓ Presentations at conferences and road shows
    - ✓ Social media
  - **Articulate role of legal department**
  - **Provide examples of material nonpublic information (including cybersecurity)**
  - **Provide periodic reminders and training to management**

DORSEY™ always ahead

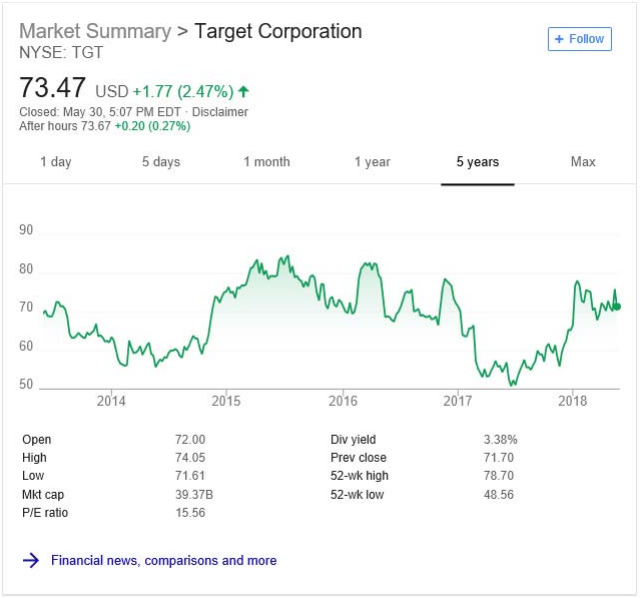
23

Shareholder and Securities Fraud Claims

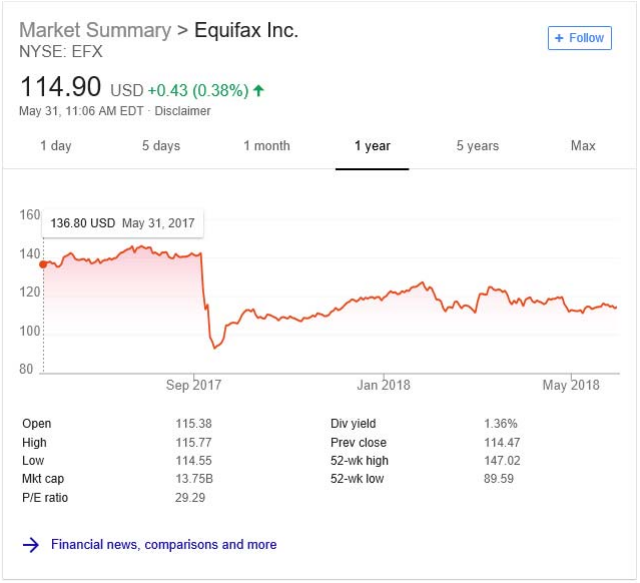
- **Any major cyber event will attract claims**
- **Breaches are having a greater impact on stock price**
- **Shareholder derivative claims initially attempted, but hard to win**
  - **Shareholder claims against Target dismissed**
- **Securities fraud claims increasingly common, easier to survive**
  - **Nine cases filed in 2017 (none in 2016)**
  - **High profile breaches (Equifax, Intel, Yahoo!, Advanced Micro Design, PayPal)**
  - **Potentially larger settlements**
- **$80 million settlement recently approved for Yahoo! shareholder class action**

DORSEY™ always ahead

24



DORSEY™ always ahead



DORSEY™ always ahead

SEC Enforcement Actions

- **Yahoo! settlement**
  - Yahoo! successor Altaba Inc. reached a $35 million settlement with SEC in April to resolve claims that it delayed telling investors about a massive data breach.
- **Equifax insider trading charge**
  - Former CIO of Equifax business unit allegedly used confidential information to conclude that Equifax had suffered a major data breach, and then exercised options and sold shares prior to public disclosure of the breach.
- **SEC Cyber Unit Chief Robert Cohen**
  - Focus on cybersecurity cases where the "facts are particularly bad and when the conduct really violates the statute very clearly"
  - Expect continued enforcement in the areas of insider trading, market manipulation and accounting fraud
  - "We're not looking to bring dozens and dozens of cybersecurity cases every year."

DORSEY™ always ahead

27

Challenges Posed by Post-breach Claims

- **Courts are still defining the boundaries of cyber "reasonable care"**
- **Hindsight will suggest that the vulnerability could have been detected and mitigated earlier**
- **Failure to timely disclose may be difficult to explain**
  - For example, Intel clearly knew of risk well prior to public disclosure (China told)
  - Failed to include any mention of chip flaw in earlier public disclosures
  - The longer a company waits, the longer the class period becomes
- **What is your story when (not if) an incident happens?**
  - Demonstrating that the steps the Board took to ensure that the company's protections against data breaches were adequate
  - Explaining the delay between initial discovery and later public disclosure

DORSEY™ always ahead

28

Existing Regulatory Requirements

- All 50 states now have state-specific data breach notification laws
  - Disclosure of personally identifiable information (PII) triggers
  - Many different, sometimes conflicting, requirements for notice
  - ***Customer's*** state of residency will determine what law applies
- Some states mandate data protection requirements
- Industry-sector reporting obligations for personal health information (PHI) or personal financial information (PFI)
  - Employee data may include PHI and PFI

DORSEY™ always ahead

29

Regulatory Initiatives to Monitor

- The EU's General Data Protection Regulation (GDPR)
  - Extraterritorial effect: ***offering*** goods or services to EU residents
  - Elevates personal privacy to a "fundamental right"
  - Serious sanction exposure: 4% of *worldwide* turnover
- New York's Department of Financial Services Cyber Regulation (NYDFS)
  - Any "financial institution" doing business in New York
- Even if a company is not *directly* regulated, regulatory mission creep via demands on supply chains and contracts

DORSEY™ always ahead

30

Complicated Interplay Among GDPR and NYDFS Notices and SEC Requirements

- **GDPR: Notice to Supervisory Authorities *within 72 hours* of discovery *unless* unlikely to result in risk to the rights and freedoms of natural persons**
- **NYDFS: Notice to Superintendent *within 72 hours* if**
  - **Reasonable likelihood of *materially harming***
  - **Notice is required to *any government body* (see GDPR!)**
  - **Confidential notice allowed**
- **When must a company:**
  - **Disclose publicly?**
  - **Impose a trading blackout?**

DORSEY always ahead

31

Equifax Case Study

- **May-July 2017:** Hackers access personal information of nearly 44% of US population on Equifax's servers.
- **July 2017:** Security department becomes aware of a data breach; they know it's a material breach, but they do not know the full scope.
  - Management assembles a breach response team consisting of security, legal and IT personnel to address the breach; the team is subject to a special trading blackout and instructed not to share information on the breach with anyone outside the response team.
  - Management assembles a second response team charged with designing a notification and remediation plan; team members are told that this plan is for a client; they are not told about Equifax's data breach, and they are not subject to the special trading blackout.

DORSEY always ahead

32

Equifax Case Study

- **August 2017:** North American CIO is on the second response team, but through conversations with colleagues, comes to the conclusion that Equifax is the victim of the data breach.
  - Text to direct report: "[o]n the phone with [global CIO]. Sounds bad. We may be the one breached…Starting to put 2 and 2 together."
  - He conducts Internet searches on prior breaches and their impact on stock price.
  - He proceeds to exercise all vested stock options and sells them on the market prior to public announcement of the breach, avoiding a loss of $117,000.
- **September 7, 2017:** Data breach publicly announced. Equifax shares plunge 13.7% in first day of trading after announcement.
- **March 2018:** Equifax announces that an additional 2.4 million people's information was stolen.

DORSEY™
always ahead

33

DORSEY
always ahead

CORPORATE UPDATE
A PUBLICATION OF THE CORPORATE GROUP OF DORSEY & WHITNEY LLP

April 27, 2018

Failure to Disclose Leads to $35 Million Penalty in the Yahoo! Cybersecurity Breach

Cam Hoang

The Securities and Exchange Commission (the "SEC") announced Tuesday that Altaba, the entity formerly known as Yahoo! Inc., has agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts. The SEC's release is available at https://www.sec.gov/news/press-release/2018-71.

According to the SEC's order, within days of the December 2014 intrusion, Yahoo's information security team learned that Russian hackers had stolen what the security team referred to internally as the company's "crown jewels": usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts. Although information relating to the breach was reported to members of Yahoo's senior management and legal department, Yahoo failed to properly investigate the circumstances of the breach and to adequately consider whether the breach needed to be disclosed to investors. The fact of the breach was not disclosed to the investing public until more than two years later, when in 2016 Yahoo was in the process of closing the acquisition of its operating business by Verizon Communications, Inc.

In the order, the SEC finds that Yahoo's post-breach disclosure in quarterly and annual reports was too general, stating that the company faced only the risk of, and negative effects that might flow from, data breaches. The company failed to disclose the actual breach or its potential business impact and legal implications.

In addition to deficiencies in Yahoo's disclosure to investors, the SEC's order found that Yahoo did not share information regarding the breach with its auditors or outside counsel in order to assess the company's disclosure obligations in its public filings.

Finally, the SEC's order found that Yahoo failed to maintain disclosure controls and procedures designed to ensure that reports from Yahoo's information security team concerning cyber breaches, or the risk of such breaches, were properly and timely assessed for potential disclosure.

In its Statement and Guidance on Public Company Cybersecurity Disclosures, released earlier this year, the SEC reiterates that public companies are required to disclose material risks and incidents, including those related to cybersecurity, in their current and periodic reports available at https://www.sec.gov/rules/interp/2018/33-10459.pdf. The SEC encourages companies to

continue to use current reports to disclose material cybersecurity-related information promptly as this practice reduces the risk of selective disclosure. Furthermore, beyond requirements explicitly found in SEC regulations, companies are also required to disclose material information and revisit previous disclosure, especially during a cybersecurity investigation, as may be necessary to ensure the company's filings are not misleading. Notably, perhaps in recognition of how rapidly the scope of a breach may evolve, the SEC provides that companies "have a duty to correct prior disclosures that the company determines were untrue at the time it was made, or a duty to update a disclosure that becomes materially inaccurate after it is made." See our earlier memo for a summary of the SEC's guidance available at https://www.dorsey.com/newsresources/publications/client-alerts/2018/03/sec-issues-new-cybersecurity-guidance.

In evaluating the range of potential disclosure for quarterly and annual reports, companies should consider that cybersecurity breaches or the risk of such breaches may trigger disclosure in the Management's Discussion and Analysis, if the breach presents a material event, trend or uncertainty that has had or is reasonably likely to have a material effect on results of operations, liquidity or financial condition. Furthermore, financial statements may need to reflect costs incurred, insurance proceeds and contingent liabilities resulting from claims. A cybersecurity breach may also need to be addressed in the description of business, discussion of legal proceedings and effectiveness of internal controls and disclosure controls and procedures.

Even before the next quarterly or annual report, companies should consider whether the information available on the cybersecurity breach is material and should be communicated to investors in a current report in order to reduce the risk of selective disclosure in violation of Regulation FD. If material information on a cybersecurity breach is not publicly disclosed in a current report, companies should consider whether it is appropriate to impose an event-specific blackout on trading in the company's stock, in accordance with applicable insider trading policies. Determining the population of employees and other individuals who know, or in hindsight should have known, about the breach, and who should be subject to the event-specific blackout, deserves careful consideration, as demonstrated by the Equifax experience, where high-ranking executives traded in the company's stock after a cybersecurity breach was discovered but before it was announced.

CORPORATE UPDATE
A PUBLICATION OF THE CORPORATE GROUP OF DORSEY & WHITNEY LLP

March 1, 2018

SEC Issues New Cybersecurity Guidance

Cam Hoang and Imeabasi Ibok

On February 26, in the wake of significant and far-reaching cybersecurity breaches (e.g., the Equifax Data Breach), the SEC published interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. The SEC recognizes that cybersecurity threats present an "ongoing risk" to all public companies which can lead to "substantial costs and other negative consequences" including liability for stolen assets or information and repairs of system damage; increased cybersecurity protection costs, litigation and legal risks; increased insurance premiums; and damage to the company's reputation, competitiveness, stock price and long-term shareholder value.

The SEC's new guidance reinforces and expands on its October 2011 guidance, emphasizing the importance of adopting sound cybersecurity policies and procedures and safeguards against insider trading in the event of a potentially material cybersecurity breach.

Public Disclosure Requirements

The SEC provides that "although no existing disclosure requirement explicitly refers to cybersecurity," periodic reports, current reports and Securities Act and Exchange Act obligations all require public companies to disclose material risks and incidents including those related to cybersecurity. The SEC encourages companies to continue to use current report Form 8-K or Form 6-K to disclose material cybersecurity-related information promptly as this practice reduces the risk of selective disclosure.

Beyond requirements explicitly found in SEC regulations, companies are also required to disclose material information and revisit previous disclosure, especially during a cybersecurity investigation, as may be necessary to ensure the company's filings are not misleading. Notably, companies "have a duty to correct prior disclosures that the company determines were untrue at the time it was made, or a duty to update a disclosure that becomes materially inaccurate after it is made."

The obligation to update prior disclosure is the subject of some debate, and perhaps will merit further guidance from the SEC. According to a footnote in the guidance, the SEC bases this duty to update in Backman v. Polaroid Corp., 910 F.2d 10 (1st Cir. 1990), but acknowledges that other circuits have not found a duty to update. Furthermore, the Private Securities Litigation Reform Act expressly disclaims any duty to update forward-looking statements. 15 U.S.C. §§ 77z-2(d) and 78u-5(d) ("Nothing in this section shall impose upon any person a duty to update a forward-looking statement."). A duty to update prior disclosure, and the associated work and potential liability, may constrain future disclosure of cybersecurity risk.

The SEC provides the following examples of factors companies should consider when evaluating their cybersecurity risk disclosure: 1) the occurrence of prior cybersecurity incidents, including their severity and frequency; 2) the aspects of the company's business and operations that give rise to

material cybersecurity risks and the potential costs and consequences of such risks; 3) the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers; and 4) existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies.

The SEC cautions that this guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts. There is no general requirement to expose potential system vulnerabilities in such a way that would make the company more susceptible to risk. However, the SEC expects that companies will provide disclosure that is tailored to their particular cybersecurity risks and incidents using company-specific, useful information as opposed to boilerplate language.

The SEC guidance suggests companies adopt comprehensive policies and procedures related to cybersecurity and assess their compliance regularly. Companies should have adequate disclosure controls and procedures in place to ensure that relevant cybersecurity information is processed and reported to the appropriate personnel to enable senior management to make disclosure decisions and certifications. These policies will not only allow the company to adhere to the SEC's disclosure requirements but will also facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.

Insider Trading

The SEC guidance provides that companies and their corporate insiders should be mindful to adhere to the federal antifraud provisions as well as other applicable rules (such as codes of conduct required by exchanges) related to insider trading in connection with information about cybersecurity risks and incidents. The SEC guidance advises companies in the midst of investigating significant cybersecurity incidents to consider implementing restrictions on insider trading in their securities to prevent corporate insiders from trading on the basis of material nonpublic information before the incident has been publicly disclosed, and to avoid the appearance of improper trading.

Conclusion

Companies are facing rapidly evolving cybersecurity threats. It is increasingly important for companies to investigate and refine their own disclosure policies and procedures to ensure a momentary lapse in cybersecurity judgment does not culminate in unnecessary damages to the company or SEC enforcement actions. The new SEC cybersecurity guidance can be found in its entirety at https://www.sec.gov/rules/interp/2018/33-10459.pdf.

CORPORATE UPDATE
A PUBLICATION OF THE CORPORATE GROUP OF DORSEY & WHITNEY LLP

September 14, 2017

Equifax Data Breach: Preliminary Lessons for the Adoption and Implementation of Insider Trading Policies

Gary Tygesson and Cam Hoang

Insider trading allegations have surfaced at Equifax, a credit rating agency that last week announced a data breach that could potentially affect 143 million consumers in the United States, nearly half of the country's population. SEC filings show that three Equifax executives – Chief Financial Officer John Gamble Jr., Workforce Solutions President Rodolfo Ploder and U.S. Information Solutions President Joseph Loughran – sold nearly $2 million in shares of the company's common stock days after the cyberattack was discovered but before the news was publicly announced. It was unclear whether their share sales had anything to do with the breach. None of the SEC filings list the sales as being conducted as part of pre-established10b5-1 trading plans. Equifax said in a statement that the three executives sold a "small percentage" of their shares on August 1 and August 2, adding they "had no knowledge that an intrusion had occurred at the time they sold their shares." Following the company's announcement of the data breach on September 9, Equifax shares traded down by almost 14 percent. The SEC has not commented on the share sales.

While all of the facts are not yet public, the situation as reported raises a number of fundamental questions. Under Equifax's insider trading policy, was there a mandatory pre-clearance policy requiring the executives to get approval prior to placing their sell orders? If so, why were the sales approved in light of the existence of a data breach? Did Equifax invoke a blackout period as soon as it knew of the data breach and, if not, why not?

These questions and the developing circumstances at Equifax serve as a reminder for public companies to consider the following practices when adopting or revising an insider trading policy:

- Make sure that your company has a policy and procedures in place that cover the purchase and sale of securities by insiders. The anti-fraud provisions of U.S. securities laws (Section 10(b) and Rule 10b-5 of the Securities Exchange Act of 1934 (the "Exchange Act")) prohibit individuals with material nonpublic information from trading in the company's securities on the basis of that information and from providing the information to others who may trade in the securities. Directors and executive officers of public companies are also subject to the reporting requirements and short-swing trading restrictions of Section 16 of the Exchange Act. A well-crafted and implemented insider trading policy can help prevent insiders from inadvertently violating these laws and incurring civil and

criminal liability, and can protect the company from circumstances that would otherwise result in premature disclosures or "control person" liability. Keep in mind that the outcomes in these situations are typically determined with the benefit of 20/20 hindsight, and they can be costly not only in financial terms but also to the reputations of the insider and the company.

- Be clear on which individuals are subject to the insider trading policy, and how it applies to each class of persons. The policy may apply to anyone who has a fiduciary duty to the company (including directors, executive officers, other employees, and potentially advisors, consultants and contractors, and their related persons), and none of these individuals should be trading securities based on material nonpublic information. Restrictions on trading activities by these individuals, however, will vary depending on their level and function at the company. For example, many insider trading policies only require directors, executive officers and designated insiders with regular access to material nonpublic information to pre-clear their transactions. Companies must apply judgments on risk and feasibility of policy implementation in defining the set of "designated insiders" beyond directors and executive officers who are subject to additional restrictions not placed on rank-and-file employees.

- Articulate and enforce pre-clearance policies for directors, executive officers, other designated insiders and their related persons. Pre-clearance is the most effective procedure to prevent sales by insiders during a blackout period or at other times when they might be in possession of material inside information. Insiders should be encouraged to pre-clear transactions before they are discussed with their brokers or financial planners. The policy should also be clear on the types of transactions that require pre-clearance. Some transactions that require pre-clearance may not be intuitive, such as an intra-401(k) plan transfer into or out of the company stock fund and changes in the form of ownership or the manner in which ownership is recorded, such as transfers in or out of joint ownership; transfers into or out of a trust; and transfers into or out of a custodial account. Similarly, there may be exceptions related to employee stock purchase programs, dividend reinvestment plans or other arrangements where the individual does not control a market transaction in the company securities.

- Establish clear blackout periods related to the quarterly financial reporting calendar. Directors, executive officers and those involved in the company's external financial reporting process should be restricted from trading in company securities during pre-established blackout periods tied to the company's financial reporting calendar. Blackout periods generally commence at a time prior to the end of a fiscal quarter, as determined by each company based on its internal information gathering and processing timetable, and continues until 24 to 48 hours following the public release of the company's quarterly results.

- Provide for (and implement) event-specific blackouts to allow the company to impose trading restrictions outside of scheduled blackout periods when material nonpublic information is known within the company. The importance of event-specific blackout periods cannot be understated. The anti-fraud provisions the federal securities laws generally do not impose an affirmative duty on public

companies to disclose material inside information unless, among other things, the company or its insiders are trading in the company's securities. Therefore, trading by insiders essentially forces a company to disclose material inside information at time when it may be disadvantageous to the company and would not have otherwise been required. The law department should have a procedure in place to notify designated individuals subject to such a blackout that they may not trade in company securities, and that they should not disclose the existence of the blackout to other individuals. However, the failure to designate or notify these individuals does not relieve these individuals of an obligation not to trade while in possession of material nonpublic information.

- Provide examples in the policy of material nonpublic information. A simple statement that information may be considered material if a reasonable investor would consider it important in making a decision to buy, hold or sell securities may provide insufficient guidance. Instead, a set of specific examples can make the policy easier to understand. In addition, individuals should be reminded that their obligations extend to material nonpublic information about other companies that do business with the company, which were obtained in the course of their business activities on behalf of the company.

- Avoid standing orders to buy or sell company securities at a particular price, because they may be triggered when the individual is in possession of material nonpublic information. These concerns may be avoided by establishing a Rule 10b5-1 plan.

- Explain how trades may be exempt from the insider trading policy if they are made under a properly pre-established and maintained trading plan, known as a 10b5-1 trading plan, and articulate the criteria for a properly pre-established and maintained plan. In brief:

    - the plan must be established when the individual was unaware of material nonpublic information;

    - the plan must be established in good faith and not as part of a scheme to evade the prohibitions of Rule 10b5-1;

    - the plan must specify the number or dollar value of company securities to be purchased or sold, the price at which the shares are to be traded, and the date of the trade; provide a written formula, algorithm or computer program for determining these variables; or not permit the individual to exercise any subsequent influence over how, when or whether to effect purchases or sales, provided that any other person exercising such influence must not be aware of material nonpublic information when doing so; and

    - the purchase or sale must be pursuant to the plan (without deviation and without a corresponding or hedging transaction with respect to the securities).

- At least annually, remind directors, executive officers and designated insiders of trading restrictions, including restrictions under the insider trading policy, Section 16 of the Exchange Act and any anti-hedging and anti-pledging policies, and remind them of the scheduled blackout periods. Periodic educational sessions for the various classes of individuals subject to the insider trading policy are advisable.

- Identify a contact for questions concerning the insider trading policy. Generally, this would be the company's General Counsel or another person who manages the disclosure of material information to the public.

October 31, 2017

U.S. v. Microsoft: Supreme Court to Review Scope of Search Warrant Compliance in a Digital Age

Robert E. Cattanach

The U.S. Supreme Court has granted certiorari to review a decision by the Second Circuit Court of Appeals, which reversed a District Court's refusal to quash a warrant issued by the Department of Justice to Microsoft that would have required it to produce information housed in an overseas server. The case underscores the increasingly challenging nature of our digital world in the context of "searches" and "seizures". Until recently, the law was straightforward: a warrant could require the recipient to produce to law enforcement anything in its possession responsive to the scope of the warrant, e.g., paper documents stored in its files. All of that changed with the advent of digitized information. Would the recipient have to produce information stored on a server located at the facility where the warrant was served? Of course. What about a server located outside of the jurisdiction of the court issuing the warrant, but which it could easily access? Technically, that information would still be within the "custody and control" of the recipient, and probably would have to be produced.

What about information stored overseas?? Now that's getting a bit more tricky. Arguably it's still within the custody and control of the recipient. But. What if the jurisdiction in which it is located has other limitations on whether it should be produced, and under what circumstances? Now turn the situation around. Does information about US citizens, or even foreign nationals, located in US servers have to be produced in response to a subpoena issued overseas by a foreign government? What if it's North Korea or Iran seeking information on dissidents?

Plainly there are many significant policy issues at play, and it's not clear whether our system for obtaining search warrants adequately reflects the nuances of a digital age. This will be a very closely-watched case, and one hopes the US Supreme Court will shed some light on this increasingly shadowy area of the law.

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2

Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.

Introduction

For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity[1] have also increased, resulting in more frequent and severe cyber incidents. Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. As a result, we determined that it would be beneficial to provide guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances.

We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk. We are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts -- for example, by providing a "roadmap" for those who seek to infiltrate a registrant's network security -- and we emphasize that disclosures of that nature are not required under the federal securities laws.

In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or

insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents

The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.[2] Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. In addition, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.[3] Therefore, as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.

The following sections provide an overview of specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.[4] In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this

evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Consistent with the Regulation S-K Item 503(c) requirements for risk factor disclosures generally, cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure.[5] Depending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

A registrant may need to disclose known or threatened cyber incidents to place the discussion of cybersecurity risks in context. For example, if a registrant experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised, it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur. Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences.

While registrants should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material

effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[6] For example, if material intellectual property is stolen in a cyber attack, and the effects of the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues, an increase in cybersecurity protection costs, including related to litigation, the registrant should discuss these possible outcomes, including the amount and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cybersecurity protection expenditures, the registrant should note those increased expenditures.

Description of Business

If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's "Description of Business."[7] In determining whether to include disclosure, registrants should consider the impact on each of their reportable segments. As an example, if a registrant has a new product in development and learns of a cyber incident that could materially impair its future viability, the registrant should discuss the incident and the potential impact to the extent material.

Legal Proceedings

If a material pending legal proceeding to which a registrant or any of its subsidiaries is a party involves a cyber incident, the registrant may need to disclose information regarding this litigation in its "Legal Proceedings" disclosure. For example, if a significant amount of customer information is stolen, resulting in material litigation, the registrant should disclose the name of the court in which the proceedings are pending, the date instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.[8]

Financial Statement Disclosures

Cybersecurity risks and cyber incidents may have a broad impact on a registrant's financial statements, depending on the nature and severity of the potential or actual incident.

Prior to a Cyber Incident

Registrants may incur substantial costs to prevent cyber incidents. Accounting for the capitalization of these costs is addressed by Accounting Standards Codification (ASC) 350-40, *Internal-Use Software*, to the extent that such costs are related to internal use software.

During and After a Cyber Incident

Registrants may seek to mitigate damages from a cyber incident by providing customers with incentives to maintain the business relationship.

Registrants should consider ASC 605-50, *Customer Payments and Incentives*, to ensure appropriate recognition, measurement, and classification of these incentives.

Cyber incidents may result in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts. Registrants should refer to ASC 450-20, *Loss Contingencies*, to determine when to recognize a liability if those losses are probable and reasonably estimable. In addition, registrants must provide certain disclosures of losses that are at least reasonably possible.

Cyber incidents may also result in diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Registrants may not immediately know the impact of a cyber incident and may be required to develop estimates to account for the various financial implications. Registrants should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements. A registrant must explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be material to the financial statements.[9] Examples of estimates that may be affected by cyber incidents include estimates of warranty liability, allowances for product returns, capitalized software costs, inventory, litigation, and deferred revenue.

To the extent a cyber incident is discovered after the balance sheet date but before the issuance of financial statements, registrants should consider whether disclosure of a recognized or nonrecognized subsequent event is necessary. If the incident constitutes a material nonrecognized subsequent event, the financial statements should disclose the nature of the incident and an estimate of its financial effect, or a statement that such an estimate cannot be made.[10]

Disclosure Controls and Procedures

Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective.[11] For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.

Endnotes

[1]Cybersecurity is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. Whatis?com available at http://whatis.techtarget.com/definition/cybersecurity.html. See also

Merriam-Webster.com available at http://www.merriam-webster.com/dictionary/cybersecurity.

[2] The information in this disclosure guidance is intended to assist registrants in preparing disclosure required in registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934. In order to maintain the accuracy and completeness of information in effective shelf registration statements, registrants may also need to consider whether it is necessary to file reports on Form 6-K or Form 8-K to disclose the costs and other consequences of material cyber incidents. See Item 5(a) of Form F-3 and Item 11(a) of Form S-3.

[3] Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9. Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available. See Basic Inc. v. Levinson, 485 U.S. 224 (1988); and TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438 (1976). Registrants also should consider the antifraud provisions of the federal securities laws, which apply to statements and omissions both inside and outside of Commission filings. See Securities Act Section 17(a); Exchange Act Section 10(b); and Exchange Act Rule 10b-5.

[4] See Item 503(c) of Regulation S-K; and Form 20-F, Item 3.D.

[5] Item 503(c) of Regulation S-K instructs registrants to "not present risks that could apply to any issuer or any offering" and further, to "[e]xplain how the risk affects the issuer or the securities being offered." Item 503(c) of Regulation S-K.

[6] See Item 303 of Regulation S-K; and Form 20-F, Item 5. A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056] Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746]; Management's Discussion and Analysis of Financial Condition and Results of Operations; and Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427].

[7] See Item 101 of Regulation S-K; and Form 20-F, Item 4.B.

[8] See Item 103 of Regulation S-K.

[9] See FASB ASC 275-10, *Risks and Uncertainties*.

[10] See ASC 855-10, *Subsequent Events*.

[11] See Item 307 of Regulation S-K; and Form 20-F, Item 15(a).

http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229 and 249

[Release Nos. 33-10459; 34-82746]

Commission Statement and Guidance on Public Company Cybersecurity Disclosures

AGENCY: Securities and Exchange Commission.

ACTION: Interpretation.

SUMMARY: The Securities and Exchange Commission (the "Commission") is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

DATES: Applicable: February 26, 2018

FOR FURTHER INFORMATION CONTACT: Questions about specific filings should be directed to staff members responsible for reviewing the documents the company files with the Commission. For general questions about this release, contact the Office of the Chief Counsel at (202) 551-3500 in the Division of Corporation Finance, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION:

I. Introduction

A. Cybersecurity

Cybersecurity risks pose grave threats to investors, our capital markets, and our country.[1]

[1] The U.S. Computer Emergency Readiness Team defines cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#C (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May

Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks. Companies today rely on digital technology to conduct their business operations and engage with their customers, business partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.

As companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased.[2] Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century. Cybersecurity incidents[3] can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and "hacktivists."[4] Companies face an evolving

---

2009).

[2] See World Economic Forum, Global Risks Report 2017, 12th Ed. (Jan. 2017), available at https://www.weforum.org/reports/the-global-risks-report-2017 (concluding that "greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyber-attacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways."). See also PwC, "Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016" (Oct. 2015), available at https://www.pwccn.com/en/retail-and-consumer/rcs-info-security-2016.pdf. (finding that in 2015 there was a reported 38% increase in detected information security incidents from 2014).

[3] A "cybersecurity incident" is "[a]n occurrence that actually or potentially results in adverse consequences to … an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#I.

[4] One study using a sample of 419 companies in 13 countries and regions noted that 47 percent of data breach incidents in 2016 involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures. See

landscape of cybersecurity threats in which hackers use a complex array of means to perpetrate cyber-attacks, including the use of stolen access credentials, malware, ransomware, phishing, structured query language injection attacks, and distributed denial-of-service attacks, among other means. The objectives of cyber-attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners. Cyber-attacks may also be directed at disrupting the operations of public companies or their business partners. This includes targeting companies that operate in industries responsible for critical infrastructure.

Companies that fall victim to successful cyber-attacks or experience other cybersecurity incidents may incur substantial costs[5] and suffer other negative consequences, which may include:

- remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;[6]
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;

Ponemon Institute and IBM Security, 2017 Cost of Data Breach Study: Global Overview (Jun. 2017), available at https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.

[5] The average organizational cost of a data breach in the United States in 2016 was $7.35 million based on the sample in the study. Id. However, the total costs a company may incur in connection with a particular cyber-attack or incident could be much higher.

[6] A company's costs may also include payments to perpetrators of ransomware attacks in order to attempt to restore operations or protect customer data or other proprietary information. But see Federal Bureau of Investigation, "How To Protect your Network from Ransomware," Ransomware Prevention and Response for CISOs, available at https:/ /www.justice.gov/ criminal-ccips/file/872771 /download.

- lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;[7]
- increased insurance premiums;
- reputational damage that adversely affects customer or investor confidence; and
- damage to the company's competitiveness, stock price, and long-term shareholder value.

Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack. Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.[8] In addition, the Commission believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has

[7] See, e.g., New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies; European Union General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 1.

[8] See Section II.B.1 below for further discussion of disclosure controls and procedures.

faced or is likely to face.

Additionally, directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company. Public companies should have policies and procedures in place to (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information.[9] In addition, we believe that companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material. We recognize that many companies have adopted preventative measures to address the appearance of improper trading and we encourage companies to consider such preventative measures in the context of a cyber event.

B. CF Disclosure Guidance: Topic No. 2

In October 2011, the Division of Corporation Finance (the "Division") issued guidance that provided the Division's views regarding disclosure obligations relating to cybersecurity risks and incidents.[10] The guidance explains that, although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be

[9] See Section II.B.2 below for further discussion of insider trading.

[10] See CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

obligated to disclose such risks and incidents.[11] After the issuance of the guidance, many companies included additional cybersecurity disclosure, typically in the form of risk factors.[12]

C. Purpose of Release

In light of the increasing significance of cybersecurity incidents, the Commission believes it is necessary to provide further Commission guidance. This interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies.[13] While the Commission continues to consider other means of promoting appropriate disclosure of cyber incidents, we are reinforcing and expanding upon the staff's 2011 guidance. In addition, we address two topics not developed in the staff's 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make

---

[11] Id.

[12] For example, Willis North America released a 2013 report that found that approximately 88% of the public Fortune 500 companies and about 78% of the Fortune 501-1000 companies included risk factor disclosure regarding cybersecurity in their annual reports filed in 2012. See Willis Fortune 1000 Cyber Disclosure Report (Aug. 2013), available at http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf. In 2015, over 88% of Russell 3000 companies disclosed cybersecurity as a risk. See Audit Analytics, "Cybersecurity Disclosure in Risk Factors," (Jan. 14, 2016), available at http://www.auditanalytics.com/blog/cybersecurity-disclosures-in-risk-factors/.

[13] This release does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations. For example, in 2014 the Commission adopted Regulation Systems Compliance and Integrity, applicable to certain self-regulatory organizations, to strengthen the technology infrastructure of the U.S. securities markets. Final Rule: Regulation Systems Compliance and Integrity, Release No. 34-73639 (Nov. 19, 2014) [79 FR. 72252 (Dec. 5, 2014)], available at https://www.sec.gov/rules/final/2014/34-73639.pdf. For additional cybersecurity regulations and resources, see the Commission's website page devoted to cybersecurity issues, available at https://www.sec.gov/spotlight/cybersecurity; see also Cybersecurity Guidance; IM Guidance Update (April 2015), available at https://www.sec.gov/investment/im-guidance-2015-02.pdf (staff guidance on cybersecurity measures for registered investment companies and investment advisers).

accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws.

Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.[14]

The Commission, and the staff through its filing review process, continues to monitor cybersecurity disclosures carefully.

II. Commission Guidance

A. Overview of Rules Requiring Disclosure of Cybersecurity Issues

1. Disclosure Obligations Generally; Materiality

Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act"), and periodic and current reports under the Exchange Act.[15] When a company is required to file a disclosure

---

[14] See Final Rule: Selective Disclosure and Insider Trading, Release No. 33-7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)], available at https://www.sec.gov/rules/final/33-7881.htm.

[15] Listed companies also should consider any obligations that may be imposed by exchange listing requirements. For example, the NYSE requires listed companies to "release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities." See NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments. In addition, in 2015, the NYSE, in partnership with Palo Alto Networks, published a summary of information about legal and regulatory aspects of cybersecurity governance for directors and officers of public companies. See Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc., 2015, available at https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf. Similarly, Nasdaq requires listed companies to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions." See Nasdaq Listing Rule 5250(b)(1).

document with the Commission, the requisite form generally refers to the disclosure requirements of Regulation S-K[16] and Regulation S-X.[17] Although these disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to disclose such risks and incidents depending on a company's particular circumstances. For example:

- Periodic Reports: Companies are required to file periodic reports[18] to disclose specified information on a regular and ongoing basis.[19] These periodic reports include annual reports on Form 10-K,[20] which require companies to make disclosure regarding their business and operations, risk factors, legal proceedings, management's discussion and analysis of financial condition and results of operations ("MD&A"), financial statements, disclosure controls and procedures, and corporate governance.[21] Periodic reports also include quarterly reports on Form 10-Q,[22] which require companies to make disclosure regarding their

[16] 17 CFR part 229.

[17] 17 CFR part 210.

[18] An issuer with a class of securities registered under Section 12 or subject to Section 15(d) of the Exchange Act is subject to the periodic and current reporting requirements of Section 13 and 15(d), respectively, of the Exchange Act.

[19] "Congress recognized that the ongoing dissemination of accurate information by companies about themselves and their securities is essential to effective operation of the trading markets. The Exchange Act rules require public companies to make periodic disclosures at annual and quarterly intervals, with other important information reported on a more current basis. The Exchange Act specifically provides for current disclosure to maintain the currency and adequacy of information disclosed by companies." Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, Release No. 33-8106, 3-4 (Jun. 17, 2002) [67 FR 42914 (Jun. 25, 2002)].

[20] 17 CFR 249.310.

[21] See Part I, Items 1, 1A and 3 of Form 10-K; Part II, Items 7, 8 and 9A of Form 10-K; and Part III, Item 10 of Form 10-K [17 CFR 249.310].

[22] 17 CFR 249.308a.

financial statements, MD&A, and updated risk factors.[23] Likewise, foreign private issuers are required to make many of these same disclosures in their periodic reports on Form 20-F.[24] Companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.

- Securities Act and Exchange Act Obligations: Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.[25]
- Current Reports: In order to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents,[26] companies can provide current reports on Form 8-K[27] or Form 6-K.[28] Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity

[23] See Part I, Items 1 and 2 of Form 10-Q; Part II, Item 1A of Form 10-Q [17 CFR 249.308a].

[24] See Part I, Items 3.D, 4, 5 and 8 of Form 20-F; Part II, Items 15 and 16G of Form 20-F; Part III, Items 17 and 18 of Form 20-F [17 CFR 249.220f].

[25] 15 U.S.C. 77k; 15 U.S.C. 77l; 15 U.S.C. 77q; 15 U.S.C 78j(b); 17 CFR 240.10b-5.

[26] See Item 11(a) of Form S-3 [17 CFR 239.13] and Item 5(a) of Form F-3 [17 CFR 239.33].

[27] 17 CFR 249.308.

[28] 17 CFR 249.306.

incidents.[29] The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur.[30]

In addition to the information expressly required by Commission regulation, a company is required to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading."[31] The Commission considers omitted information to be material 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.[32]

In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact

---

[29] "The registrant may, at its option, disclose under this Item 8.01 [of Form 8-K] any events, with respect to which information is not otherwise called for by this form, that the registrant deems of importance to security holders." 17 CFR 308.

[30] See Sections II.B.2 and II.B.3 below for further discussion of insider trading and Regulation FD.

[31] Rule 408 of the Securities Act [17 CFR 230.408]; Rule 12b-20 of the Exchange Act [17 CFR 240.12b-20]; and Rule 14a-9 of the Exchange Act [17 CFR 240.14a-9].

[32] This approach is consistent with the standard of materiality articulated by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (a fact is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" to the shareholder).

of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations.[33] The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause.[34] This includes 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.

This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts – for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale

---

[33] For example, the compromised information might include personally identifiable information, trade secrets or other confidential business information, the materiality of which may depend on the nature of the company's business, as well as the scope of the compromised information.

[34] 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. Basic v. Levinson, 485 U.S. 224, 238 (1988) (citing SEC v. Texas Gulf Sulphur Co., 401 F. 2d 833, 849 (2d Cir. 1968)). Moreover, no "single fact or occurrence" is determinative as to materiality, which requires an inherently fact-specific inquiry. Basic, 485 U.S. at 236.

of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.[35]

Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

We remind companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made[36] (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made[37] (for example, when the original statement is still being relied on by reasonable investors). Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

---

[35] See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15. U.S.C. 78o(d); 17 CFR 240.10b-5].

[36] See Backman v. Polaroid Corp., 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies "if a disclosure is in fact misleading when made, and the speaker thereafter learns of this.").

[37] See id. at 17 (describing the duty to update as potentially applying "if a prior disclosure 'becomes materially misleading in light of subsequent events'" (quoting Greenfield v. Heublein, Inc., 742 F.2d 751, 758 (3d Cir. 1984))). But see Higginbotham v. Baxter Intern., Inc., 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); Gallagher v. Abbott Laboratories, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).

We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we "emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies."[38] Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

2. Risk Factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company's securities speculative or risky.[39] Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.[40]

It would be helpful for companies to consider the following issues, among others, in evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;

---

[38] See Business and Financial Disclosure Required by Regulation S-K, Release No. 33-10064 (Apr. 13, 2016) [81 FR 23915 (Apr. 22, 2016)]. See also Plain English Disclosure, Release No. 33-7497 (Jan. 28, 1998) [63 FR 6370 (Feb. 6, 1998)]; and Updated Staff Legal Bulletin No. 7: Plain English Disclosure (Jun. 7, 1999) available at https://www.sec.gov/interps/legal/cfslb7a.htm.

[39] 17 CFR 229.503(c); 17 CFR 249.220f.

[40] See Final Rule: Business Combination Transactions, Release No. 33-6578 (Apr. 23, 1985) [50 FR 18990 (May 6, 1985)].

- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose

particular risks to the company's business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

3. MD&A of Financial Condition and Results of Operations

Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations.[41] In this context, the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation,

[41] 17 CFR 229.303; 17 CFR 249.220f.

and the loss of competitive advantage that may result.[42] Finally, the Commission expects companies to consider the impact of such incidents on each of their reportable segments.[43]

4. Description of Business

Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions.[44] If cybersecurity incidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure.

5. Legal Proceedings

Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party.[45] Companies should note that this requirement includes any such proceedings that relate to cybersecurity issues. For example, if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

---

[42] A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056 (Dec. 29, 2003)]; Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746 (Jan. 25, 2002)]; Management's Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427 (May 24, 1989)].

[43] 17 CFR 229.303(a).

[44] 17 CFR 229.101; 17 CFR 249.220f.

[45] 17 CFR 229.103.

6. Financial Statement Disclosures

Cybersecurity incidents and the risks that result therefrom may affect a company's financial statements. For example, cybersecurity incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
- loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases; and
- diminished future cash flows, impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

The Commission expects that a company's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.[46]

7. Board Risk Oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to 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.[47] The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to

[46] See Section 13(b)(2)(B) of the Exchange Act [15 U.S.C.78m(b)(2)(B)].

[47] 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.

investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[48] A company must include a description of how the board administers its risk oversight function.[49] To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk.

In addition, we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

B. Policies and Procedures

1. Disclosure Controls and Procedures

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and

[48] Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (Dec. 16, 2009) [74 FR 68334 (Dec. 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.

[49] See Item 407(h) of Regulation S-K [17 CFR 229.407(h)].

other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.[50]

Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness.[51] These rules define "disclosure controls and procedures" as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) "recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms," and (2) "accumulated and communicated to the company's management … as appropriate to allow timely decisions regarding required disclosure."[52]

A company's disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses.[53] Information also must be

---

[50] See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that, to assist principal executive and financial officers in the discharge of their responsibilities in making the required certifications, as well as to discharge their responsibilities in providing accurate and complete information to security holders, it is necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner."); see also Section 10(b) of the Exchange Act and Rule 10b-5 thereunder [15 U.S.C. 78j(b); 17 CFR 240.10b-5].

[51] 17 CFR 240.13a-15; 17 CFR 240.15d-15.

[52] Id.

[53] See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that the new rules will help to ensure that an issuer's systems grow and evolve with its business and are capable of producing Exchange Act reports that are timely, accurate and reliable.").

evaluated in the context of the disclosure requirement of Exchange Act Rule 12b-20.[54] When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

Exchange Act Rules 13a-14 and 15d-14[55] require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures,[56] and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures.[57] These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

---

[54] 17 CFR 240.12b-20.

[55] 17 CFR 240.13a-14; 17 CFR 240.15d-14.

[56] Section 302 of the Sarbanes-Oxley Act of 2002 required the Commission to adopt final rules under which the principal executive officer or officers and the principal financial officer or officers, or persons providing similar functions, of an issuer each must certify the information contained in the issuer's quarterly and annual reports. Pub. L. 107-204, 116 Stat. 745 (2002).

[57] 17 CFR 229.307; 17 CFR 249.220f.

2. Insider Trading

Companies and their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches.[58] It is illegal to trade a security "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information."[59] As noted above, information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.[60]

Beyond the antifraud provisions of the federal securities laws, companies and their directors, officers, and other corporate insiders must comply with all other applicable insider trading related rules. Many exchanges require listed companies to adopt codes of conduct and policies that promote compliance with applicable laws, rules, and regulations, including those prohibiting insider trading.[61] We encourage companies to consider how their codes of ethics[62]

---

[58] In addition to promoting full and fair disclosure, the antifraud provisions of the federal securities laws prohibit insider trading, which harms not only individual investors but also the very foundations of our markets by undermining investor confidence in the integrity of those markets. 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

[59] Rule 10b5-1(a) of the Exchange Act [17 CFR 240.10b-5-1(a)].

[60] This would not preclude directors, officers, and other corporate insiders from relying on Exchange Act Rule 10b5-1 if all conditions of that rule are met.

[61] See e.g., NYSE Listed Company Manual Section 303A.10, which states in relevant part that every NYSE "listed company should proactively promote compliance with rules and regulations, including insider trading laws.

and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. The Commission believes that it is important to have well designed policies and procedures to prevent trading on the basis of all types of material non-public information, including information relating to cybersecurity risks and incidents.

In addition, while companies are investigating and assessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents, they should consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. Company insider trading policies and procedures that include prophylactic measures can protect against directors, officers, and other corporate insiders trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident. As noted above, we believe that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.

3. Regulation FD and Selective Disclosure

Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Under Regulation FD, "when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information."[63] The Commission adopted Regulation FD owing to concerns

---

Insider trading is both unethical and illegal, and should be dealt with decisively." See also NASDAQ Listing Rule 5610 and Section 406(c) of the Sarbanes-Oxley Act of 2002.

[62] Item 406 of Regulation S-K [17 CFR 229.406].

[63] 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

about companies making selective disclosure of material nonpublic information to certain persons before making full disclosure of that same information to the general public.[64]

In cases of selective disclosure of material nonpublic information related to cybersecurity, companies should ensure compliance with Regulation FD. Companies and persons acting on their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons[65] before disclosing that same information to the public.[66] We expect companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to

---

[64] Id.

[65] Regulation FD applies generally to selective disclosures made to persons outside the issuer who are (1) a broker or dealer or persons associated with a broker or dealer; (2) an investment advisor or persons associated with an investment advisor; (3) an investment company or persons affiliated with an investment company; or (4) a holder of the issuer's securities under circumstances in which it is reasonably foreseeable that the person will trade in the issuer's securities on the basis of the information. 17 CFR 243.100(b)(1).

[66] Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made simultaneously (in the case of an intentional disclosure as defined in the rule) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation.[67]

By the Commission.

Dated: February 21, 2018

Brent J. Fields
Secretary

---

[67] "Under the regulation, the required public disclosure may be made by filing or furnishing a Form 8-K, or by another method or combination of methods that is reasonably designed to effect broad, non-exclusionary distribution of the information to the public." Id. at 3.