Building a better working world

EY Center for Board Matters

SEC reporting update

Spotlight on cybersecurity disclosures

What you need to know

- With the increase in cyber threats and attacks, SEC Chairman Jay Clayton has signaled that the SEC staff will increase its scrutiny of companies' disclosures about cyber incidents and their cybersecurity programs.
- The SEC staff's guidance states that companies need to consider disclosing the risks associated with cyber attacks and breaches in registration statements and periodic reports. The SEC staff has said that it expects the SEC to update and expand that cybersecurity guidance very soon.
- The type of disclosure and the level of detail depend on a registrant's facts and circumstances, including the probability of an incident occurring and the potential magnitude of its effects on the company.
- This publication outlines factors that companies can consider in making these disclosures and examples of what some companies have disclosed.

Overview

After the U.S. Securities and Exchange Commission (SEC or Commission) said its EDGAR filing system had been compromised, SEC Chairman Jay Clayton issued a statement about the importance of cybersecurity to the Commission and registrants. While he acknowledged that "even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face," Chairman Clayton said "that reality does not make adequate disclosure less important."

Chairman Clayton said companies "should consider whether their publicly filed reports adequately disclose information about their risk management governance and cybersecurity risks, in light of developments in their operations and the nature of current and evolving cyber threats."

He also signaled that the SEC staff will increase its scrutiny of cybersecurity risk factor disclosures and disclosures in management's discussion and analysis (MD&A), especially those that use boilerplate language or appear incomplete. "We are continuing to examine whether public companies are taking appropriate actions to inform investors, including after a breach has occurred, and we will investigate issuers that mislead investors," Clayton said.

The statement reflects the dramatic increase in the severity and frequency of cyber attacks and concerns that many companies continue to understate the risk of a cyber incident in their disclosures.[1]

Common cyber threats include intrusions into companies' operating systems, the theft of personal or other sensitive data and the disruption of a company's operations. For example, ransomware attacks quadrupled to 4,000 per day from 2015 to 2016, according to the U.S. Department of Justice.[2]

In this publication, we outline how public companies should approach their cybersecurity disclosures and provide examples of disclosures that some companies have made. In the appendix, we provide excerpts from Chairman Clayton's statement as an example of cybersecurity disclosures a registrant could consider emulating.

What to disclose about cybersecurity and cyber incidents

While there are no specific SEC disclosure rules that refer to cybersecurity risks or cyber incidents, the SEC's Division of Corporation Finance issued CF Disclosure Guidance: Topic No. 2 — *Cybersecurity* in 2011, which clarified that Regulation S-K disclosure requirements apply to cybersecurity risks and incidents that could have a material effect on a registrant.

In it, the SEC staff said registrants should consider disclosing both the direct and indirect effects of cyber incidents, such as:

- Costs for remediation, protection and litigation
- Implications of the disruption of operations
- Possible theft of intellectual property, customer information or other sensitive data such as personal information
- Reputational damage with customers and investors
- Potential for lost revenues

Registrants should consider this guidance when evaluating the information they disclose in this area. The SEC staff has said that it expects the SEC to update and expand the staff's 2011 cybersecurity guidance very soon. The SEC's updates are expected to address internal escalation policies, disclosure controls and procedures regarding cyber incidents and internal pre-disclosure securities trading policies for those aware of the incident.

> "Cybersecurity is critical to the operations of our markets and the risks are significant and, in many cases, systemic."
>
> **— SEC Chairman Jay Clayton**

Risk factor disclosures

As part of their registration statements and annual and quarterly reports, registrants are required to disclose significant factors that would make an investment in their securities speculative or risky and the potential effects of each of the risks and any changes in those risks during the period. Registrants need to consider whether to include the risks associated with cybersecurity or cyber incidents in their risk factor disclosures. This evaluation should include the likelihood of incidents occurring and the potential magnitude of the consequences of such incidents.

These disclosures should be sufficiently detailed to allow investors to appreciate the nature of the risks, but do not need to include details that would compromise a registrant's security. This may be challenging for registrants because disclosing information about potential vulnerabilities could increase their exposure to attacks.

Chairman Clayton's statement provides a road map for risk factor disclosures. He cited the following potential risks:

- Risks to operational performance due to denial-of-service attacks or the destruction of systems
- Loss or exposure of consumer data or theft or exposure of intellectual property
- Losses resulting from the theft of funds or market value declines from cyber attacks
- Risks related to intrusions of critical infrastructure such as the power grid or communications systems
- Risks related to vendors that may have a weakness that could be exploited and used to attack the company's systems

Depending on the circumstances, risk factor disclosures may include a discussion of aspects of the registrant's business that create cybersecurity exposures and the potential costs and consequences of breaches. Disclosures also may include a description of specific incidents that are individually, or in the aggregate, material, including a description of the known or potential costs and other consequences and the extent to which the company is vulnerable to breaches or disruptions.

Companies that haven't yet had or discovered a significant cyber incident tend to provide generic disclosures about cyber risks, including those related to confidential information they maintain or possess. Companies that store or process personal information such as email addresses, credit card information, social security numbers or medical records should consider discussing the risks associated with this information.

Illustration 1

A detailed disclosure of risks associated with personal information

"The payment methods that we offer also subject us to potential fraud and theft by criminals, who are becoming increasingly more sophisticated, seeking to obtain unauthorized access to or exploit weaknesses that may exist in the payment systems. If we fail to comply with applicable rules or requirements for the payment methods we accept, or if payment-related data is compromised due to a breach or misuse of data, we may be liable for costs incurred by payment card issuing banks and other third parties or subject to fines and higher transaction fees, or our ability to accept or facilitate certain types of payments may be impaired. In addition, our customers could lose confidence in certain payment types, which may result in a shift to other payment types or potential changes to our payment systems that may result in higher costs."

Chairman Clayton also said companies should consider providing details about the measures they have implemented to enhance cybersecurity. These might include training or education programs for employees to prevent and raise awareness about phishing or social engineering.

Illustration 2

A disclosure that highlights employee training

"The company is continuously working to install new, and upgrade its existing, information technology systems and provide employee awareness training around phishing, malware and other cyber risks to ensure that the company is protected, to the greatest extent possible, against cyber risks and security breaches."

Some companies acknowledge in their risk factor disclosures that attacks are increasing and that they have been a target. "While we have been subject to security breaches or cyber attacks, these did not result in a material adverse effect on our operations," one company said.

Illustration 3

A disclosure of "regular" attacks

"We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours."

Some companies acknowledge that they also face cybersecurity risks in connection with their suppliers of goods and services, including those that provide software or hardware security products and those that may have access to a company's critical systems.

Illustration 4

A disclosure about risks related to suppliers

"While the company selects these third-party vendors carefully, it does not control their actions. Any problems caused by these third parties, including those resulting from breakdowns or other disruptions in communication services provided by a vendor, failure of a vendor to handle current or higher volumes, cyber attacks and security breaches at a vendor could adversely affect the company's ability to deliver products and services to its customers and otherwise conduct its business."

Registrants that have been targeted by attacks that are widely reported or that have been materially affected by an attack generally expand their risk factor disclosures to include some details about the incident and the company's response. Their observations about the consequences of these incidents provide investors with insights about the current and potential future effects of cyber incidents such as reputational risks and risks to relationships with vendors or customers.

Illustration 5

A company provided more detail in risk factor disclosures after an attack

Before the attack, a company provided a generic risk factor disclosure that said: "An unauthorized disclosure of sensitive or confidential member information could have an adverse effect on our business, reputation and profitability."

After a cyber attack, the company revised its risk factor disclosure to say: "An unauthorized disclosure of sensitive or confidential member or employee information, including by cyber attacks or other security breach, could cause a loss of data, give rise to remediation or other expenses, expose us to liability under federal and state laws, and subject us to litigation and investigations, which could have an adverse effect on our business, cash flows, financial condition and results of operations."

In another example, a company added this detail after an incident: "We cannot assure that all potential causes of the incident have been identified and remediated and will not occur again."

How we see it

We expect the SEC staff to increase its scrutiny of cybersecurity risk disclosures. In particular, the staff may question boilerplate disclosures or the completeness of risk factor disclosures if information included elsewhere in the filing or other public information indicates that material cybersecurity risks exist.

Management's discussion and analysis

Registrants should also discuss cybersecurity incidents, prevention and consequences in their MD&A when one or more incidents (or the risk of a potential incident) represent a material event, trend or uncertainty that has had or is reasonably likely to have a material effect on their results of operations, liquidity or financial condition.

Registrants should discuss any material effect on operating results from one or more cyber incidents. They also should disclose whether the incident(s) might cause reported financial information to not be indicative of the company's future operating results or financial condition. A registrant should discuss the reasonably possible outcomes of the incident(s) (e.g., the amount and duration of the expected costs).

Companies generally provide MD&A disclosure when a breach involving customers' personal information or other sensitive data is widely reported or a disruption of operations directly affects customers. Few companies have disclosed disruptions of industrial processes, the corruption of strategic data or the theft of intellectual property. Minor incidents that have no material effect on operations, customer data or future earnings do not need to be disclosed in the MD&A.

Illustration 6

A disclosure of disruption of operations

"We (recently) announced that our operations were significantly affected by the cyber attack known as …, which involved the spread of an information technology virus through a software product. We use the software that was compromised, which allowed the virus to infiltrate our operating systems and encrypt their data. While our operations and communications were significantly affected, no data breach or data loss to third parties is known to have occurred as of the date of this filing."

MD&A disclosures generally focus on:

- The expenses a company incurred in connection with the incident and how the current period is affected by contingency plans and the cost of restoring operations
- How the incident likely will affect the company's business, cash flows and financial condition or results of operations in the future
- The status of any litigation, investigations by law enforcement agencies and insurance claims arising from the incidents
- The loss of revenue, if any, arising from the disruption of operations

Illustration 7

A disclosure about costs incurred and how the incident affected its business

"We recorded expenses of $XX million related to the cyber incident in the year ended December 31, 201X, of which $XX million was associated with the ongoing forensic investigation and remediation activities and $XX million was associated with nonrecurring legal costs. The cyber incident did not have a material adverse impact on our business, cash flows, financial condition, or results of operations for the year ended December 31, 201X. However, we have subsequently incurred additional expenses to investigate and take remedial actions to notify and protect our users and systems, and expect to continue to incur investigation, remediation, legal, and other expenses associated with the cyber incident in the foreseeable future. We will recognize and include these expenses as part of our operating expenses as they are incurred."

Illustration 8

A disclosure about costs incurred, insurance proceeds and potential losses resulting from claims

"The company recorded $XX million of pretax expenses related to the cyber incident, partially offset by $XX million of expected insurance proceeds for costs the company believes are reimbursable and probable of recovery under its insurance coverage, for pretax net expenses of $XX million. Expenses include costs to investigate the cyber incident; provide identity protection services, including credit monitoring, to impacted customers; increase call center staffing; and pay legal and other professional services, all of which were expensed as incurred.

"The company believes it is probable that (third parties) will make claims against the company. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses that the (third parties) have incurred."

Financial statement implications

Cybersecurity risks and incidents could have a material effect on a registrant's financial statements, depending on the nature and severity of the potential or actual incident. For example:

- Registrants may incur substantial costs to prevent cyber incidents. If these costs involve internal use software, registrants would need to consider whether to capitalize them in accordance with Accounting Standards Codification (ASC) 350-40, *Intangibles — Goodwill and Other — Internal-Use Software*.
- Registrants may face losses resulting from claims (asserted and unasserted), including those related to warranties, breach of contract, product recall and replacement and indemnification of counterparty losses. They should refer to ASC 450-20, *Contingencies — Loss Contingencies*, to determine when to recognize losses that are probable and reasonably estimable, when to disclose losses that are reasonably possible and when to recognize insurance proceeds, if any.
- Because cyber incidents may reduce future cash flows because of expenditures or loss of revenues, registrants may also need to evaluate assets for impairment, including goodwill, customer-related intangible assets, trademarks, patents, inventory, capitalized software or other long-lived assets such as technology assets or software.
- Registrants may be required to make various estimates of the effects of a cyber incident if they are not immediately known and should subsequently reassess the assumptions that underlie these estimates. Examples of estimates that may be affected are warranty liability, allowances for product returns, inventory reserves, litigation expenses and deferred revenue.

If a cyber incident is discovered after the balance sheet date but before the financial statements are issued, the registrant should consider whether to account for it as a recognized event that occurred before the balance sheet date or disclose it as a nonrecognized subsequent event. If the incident is deemed to be a material nonrecognized subsequent event, the registrant should disclose the nature of the incident and an estimate of its financial effect or a statement that such an estimate cannot be made in the financial statements.

Disclosure controls and procedures

Companies also need to consider cyber risks in their assessment of the effectiveness of disclosure controls and procedures. If cyber incidents could pose a risk to a registrant's ability to record, process, summarize and report information that is required to be disclosed in SEC filings in a timely manner, management should consider whether there are any deficiencies in disclosure controls and procedures that would cause them to be ineffective. For example, management may conclude that disclosure controls and procedures are ineffective if it is reasonably possible that timely disclosure would not be made about a material cyber incident.

After a cyber incident that calls into question the effectiveness of disclosure controls and procedures, companies might describe the remedial actions they undertook to address any deficiencies identified as part of the post-incident investigation and to prevent future occurrences.

Appendix

Excerpts from Chairman Clayton's statement on cybersecurity

The following excerpts from Chairman Clayton's statement provide an example of a disclosure a company might make:

"Data collection, storage, analysis, availability and protection (including security, validation and recovery) have become fundamental to the function and performance of the U.S. Securities and Exchange Commission ('Commission' or 'SEC'). As a result of these and other developments, the scope and severity of risks that cyber threats present have increased dramatically, and constant vigilance is required to protect against intrusions. The Commission is focused on identifying and managing cybersecurity risks … .

Malicious attacks and intrusion efforts are continuous and evolving, and in certain cases they have been successful at the most robust institutions and at the SEC itself. Cyber security efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery.

In today's environment, cyberattacks are perpetrated by identity thieves, unscrupulous contractors and vendors, malicious employees, business competitors, prospective insider traders and market manipulators, so-called 'hacktivists,' terrorists, state-sponsored actors and others.

Cyber intrusions can create significant risks … (in) the form of denials of service and the destruction of systems, potentially resulting in impediments to account access and transaction execution, and disruption of other important … functionalities. The risks associated with cyber intrusions may also include loss or exposure of consumer data, theft or exposure of intellectual property, and investor losses resulting from the theft of funds or market value declines among others. (We) face regulatory, reputational and litigation risks resulting from cyber incidents, as well as the potential of incurring significant remediation costs.

Cybersecurity risks extend beyond data storage and transmission systems. Maintaining reliability of data operations also depends on the continued functioning of other services that themselves face significant cyber risks, including, most notably, critical infrastructure such as electric power and communications grids … .

In support of its mission, the Commission receives, stores and transmits data falling under three broad categories.

The first category of data includes public-facing data that is transmitted to and accessed through Commission systems. In 1984 the Commission began collecting, and making publicly available, disclosure documents through its EDGAR system. In 2017, on a typical day, investors and other market participants access more than 50 million pages of disclosure documents through the EDGAR system, which receives and processes over 1.7 million electronic filings per year.

The second category of data the Commission receives, stores and transmits includes nonpublic information, including personally identifiable information, generally related to our supervisory and enforcement functions. This data, which relates to the operations of issuers, broker-dealers, investment advisers, investment companies, self-regulatory organizations (SROs), alternative trading systems (ATSs), clearing agencies, credit rating agencies, municipal advisors and other market participants, may be sensitive to individuals, organizations and our markets generally.

The third category of data includes nonpublic data, including personally identifiable information, related to the Commission's internal operations. This includes, for example, personnel records, records relating to internal investigations, and data relating to our risk management and internal control processes. This category also includes materials that Commission staff generate in connection with their daily roles and responsibilities, including work papers and internal memoranda.

The Commission receives, stores and transmits substantial amounts of data, including sensitive and nonpublic data. Like many others, we are the subject of frequent attempts by unauthorized actors to disrupt access to our public-facing systems, access our data, or otherwise cause damage to our technology infrastructure, including through the use of phishing, malware and other attack vectors. For example, with respect to our EDGAR system, we face the risks of cyber threat actors attempting to compromise the credentials of authorized users, gain unauthorized access to filings data, place fraudulent filings on the system, and prevent the public from accessing our system through denial of service attacks. We also face the risks of actors attempting to access nonpublic data relating to our oversight of, or enforcement actions against, market participants, which could then be used to obtain illicit trading profits.

Notwithstanding our efforts to protect our systems and manage cybersecurity risk, in certain cases cyber threat actors have managed to access or misuse our systems. In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of our EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information. We believe the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk. Our investigation of this matter is ongoing, however, and we are coordinating with appropriate authorities … .

In addition, like other organizations, we are subject to the risk of unauthorized actions or disclosures by Commission personnel. For example, a 2014 internal review found that certain SEC laptops that may have contained nonpublic information could not be located. We also have found instances in which SEC personnel have transmitted nonpublic information through non-secure personal email accounts. We seek to mitigate this risk by requiring all personnel to complete privacy and security training and we have other relevant risk mitigation controls in place.

Similarly, we are subject to cybersecurity risk in connection with vendors we utilize. For example, a weakness in vendor systems or software products may provide a mechanism for a cyber threat actor to access SEC systems or information through trusted paths. Recent global supply chain security incidents such as compromises of reputable software update services are illustrative of this type of occurrence.

In light of the nature of the data at risk and the cyber-related threats faced by the SEC, the Commission employs an agency-wide cybersecurity detection, protection and prevention program for the protection of agency operations and assets. This program includes cybersecurity protocols and controls, network protections, system monitoring and detection processes, vendor risk management processes, and regular cybersecurity and privacy training for employees. That said, we recognize that cybersecurity is an evolving landscape, and we are constantly learning from our own experiences as well as the experiences of others. To aid in this effort, and notwithstanding limitations on our hiring generally, we expect to hire additional expertise in this area.

The SEC periodically assesses the effectiveness of its cybersecurity efforts, including through penetration testing of internal and public-facing systems, ongoing monitoring by the Department of Homeland Security, independent verification and validation, and security assessments conducted by impartial third parties."

Endnotes

1 Path to cyber resilience: Sense, resist, react – EY's 19th Global Information Security Survey 2016-17 (SCORE EYG No. 04260-163GBL)

2 How to protect your networks from ransomware – Government interagency technical guidance – 2017