SEC updates cybersecurity guidance as it struggles to stay ahead of threats

By Amy Leisinger, J.D.

From WannaCry to Equifax, from Uber to the SEC, cyber attacks are becoming an increasingly vexing problem for consumers, businesses, investors, and capital markets alike. With digital technology at the heart of today's commerce, the economy depends on the security of information and communications, as well as the systems and networks that maintain and transfer that data. As companies' reliance on technology increases by the day, the threat of attacks and frequency of incidents (unintentional and/or deliberate) rise exponentially. Whether an attack is directed at disrupting the operations of a public company or merely misappropriating information, victims pay the price.

In response to recent increases in cyber risks and incidents, the SEC has issued new interpretive guidance relating to public companies' cybersecurity disclosure obligations under the federal securities laws. The guidance updates an interpretive release on cybersecurity issued in October 2011, elevates its authority from staff- to Commission-level, and includes new topics about the importance of cybersecurity policies and procedures designed to ensure more timely disclosure, stress the importance of board-level risk oversight, and clarify the application of insider trading prohibitions during the period between discovery of a cybersecurity threat or attack and its disclosure to the public.

"I believe that providing the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors," said SEC Chairman Jay Clayton.

As the Commission continues its consideration of cybersecurity issues, the Division of Enforcement and Office of Compliance Inspections and Examinations continue to target industry risks and incidents and address evolving technological solutions. However, the agency itself recently learned first-hand about cybersecurity preparation, threats, and attacks: in 2017, SEC Chairman Jay Clayton disclosed a 2016 cyberattack on the SEC's EDGAR test filing system that enabled a hacker to gain access to nonpublic information. Like many other governmental and private entities, the SEC is subject to attempts by bad actors to disrupt access, steal information, or cause damage to its technology infrastructure. As the Commission has advised registrants, the agency plans to periodically test its systems, regularly review its internal policies and procedures and controls to ensure information security, and ensure that officials and employees are trained to deal with and/or escalate cybersecurity risks and incidents.
Cybersecurity Guidance

In 2011, the Division of Corporation Finance issued guidance providing the division’s views on disclosure obligations relating to cybersecurity risks and incidents. Noting that although no disclosure requirement explicitly refers to cybersecurity risks, incidents, or attacks, the guidance advised that a company still may be obligated to disclose information regarding these issues under existing federal law and SEC regulations and reporting requirements. After the guidance was issued, many companies began to additional cybersecurity disclosures, particularly in connection with reported risk factors.

In light of the increasing frequency and significance of cybersecurity risk and incidents, the Commission determined it was necessary to provide further guidance and issued an interpretive release on the subject applicable to public companies (separate guidance and information is provided for investment companies and investment advisers and broker-dealers, and Regulation SCI sets forth obligations for self-regulatory organizations). The guidance, adopted unanimously by the Commission seriatim on February 20, 2018, reinforces and builds on the 2011 guidance and expands on its suggested considerations with respect to the technological developments and cyber attacks seen in recent years. It is critical that a company to take all required actions to timely inform investors about material cybersecurity risks and attacks, the SEC explained.

Chairman Jay Clayton issued a statement in which he urged public companies to examine their controls and procedures, not only with their securities law requirements in mind, but also with regard to reputational considerations around the sales of securities by executives. Commissioner Robert Jackson expressed his hope that the guidance is just the first step in countering those who use technology to threaten the economy and raised concerns about potential underreporting as a result of differing interpretations. Commissioner Kara Stein echoed these concerns, questioning whether the guidance will actually help a registrant provide investors with “comprehensive, particularized, and meaningful disclosure about cybersecurity risks and incidents.” In recent remarks, she had urged companies to view cyber threats as a business risk rather than a technology problem. Cybersecurity is one of the biggest challenges that corporations face and much of current disclosure is boilerplate; it is unclear why companies are not doing more to implement robust cybersecurity frameworks and to provide more meaningful disclosures about the risk of data loss, Stein said.

In addition to elaborating on CorpFin’s 2011 statements, the 2018 guidance adds the Commission’s position that the most crucial component of a company’s effort to manage cybersecurity concerns involves disclosure controls and procedures that provide a method of discerning how cyber risks and incidents will affect the company’s business and financial condition and determining the materiality of issues. Further, the SEC explained that to ensure proper and effective controls and procedures, executives and directors must be kept informed problems and potential risks. Additionally, a company should have policies and procedures in place to prevent insiders from trading in a public company’s securities while in possession of material, nonpublic information, which may include knowledge regarding a significant cybersecurity incident or risk, the SEC stated. In the process, a company must be mindful of selective disclosure and Regulation FD limitations, according to the Commission.
## General Disclosure Obligations

<table>
<thead>
<tr>
<th><strong>2018 Cybersecurity Guidance</strong></th>
<th><strong>2011 Cybersecurity Guidance</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Factors</strong></td>
<td><strong>Risk Factors</strong></td>
</tr>
</tbody>
</table>
| Companies should assess cybersecurity risks and incidents and the probability and magnitude of future incidents. A broader discussion of risk may need to discuss the occurrence of a specific attack and its known and potential consequences. | CorpFin suggested that material disclosures may include, among other things:  
- Business aspects giving rise to risks;  
- Measures to address risk in outsourced functions;  
- Risks of incidents that remain undetected for an extended period |
| **MD&A**                      | **MD&A**                       |
| To fully discuss changes in financial condition and results of operations, companies should consider the cost of cybersecurity efforts, fallout from incidents, and risks of future incidents. | CorpFin noted that, if intellectual property is stolen in an attack and the theft is likely to be material, the company should describe the property lost and the effect on its results of operations and financial condition. |
| **Business Description**      | **Business Description**       |
| A company should disclose a cyber risk or incident that materially affects its products, services, or relationships with customers or vendors. | A registrant with a product in development that learns of a cyber incident that could impair its viability should discuss the incident and the potential impact, if material. |
| **Legal Proceedings**         | **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 the litigation. | 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 the litigation. |
| **Financial Statements**      | **Financial Statements**       |
| Information regarding the financial effects of a cybersecurity risk or incident should be incorporated into a registrant’s financial statements as it becomes available. | CorpFin recommended that a registrant consult the Accounting Standards Codifications to inform its accounting and analysis. If an issue is discovered after the balance sheet date but before financial statements issuance, the company should consider the necessity of disclosing a recognized or non-recognized subsequent event. |
| **Board Oversight**           | **Board Oversight**            |
| Disclosure of information regarding a company’s cybersecurity risk management program and the board’s interaction with management on cybersecurity issues. | This issue was not addressed in the 2011 guidance. |
Risk factors. Item 503 of Regulation S-K and Item 3.D of Form 20-F require a company to disclose significant factors that make investment in the company risky; according to the SEC, this requirement should involve cybersecurity risks and incidents as appropriate. The Commission advises a company to consider disclosure of occurrences of cybersecurity risks and incidents (as well as severity and frequency) and the probability and potential quantitative and qualitative magnitude of future incidents, particularly with regard to existing preventative measures or limitations and aspects of its business that could give rise to material threats, and to specify how each risk affects the registrant. In meeting its disclosure obligations, a company may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of risk in the appropriate context. For example, if a company previously experienced a material incident, it likely would not be sufficient to disclose a “risk” that an attack may occur. The guidance suggests that as part of a broader discussion of attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential consequences. Context is necessary to effectively communicate with investors, the guidance explains.

In 2011, CorpFin suggested that, depending on a company’s particular circumstances, appropriate material disclosures may include:

• Business aspects that give rise to material cybersecurity risks;
• Means by which the company addresses risks attendant to outsourced functions;
• Risks related to cyber incidents that may remain undetected for an extended period; and
• Descriptions of relevant insurance coverage.

MD&A of Financial Condition and Results of Operations. Regulation S-K and Form 20-F also require a company to discuss changes in financial condition and results of operations, including events, trends, or uncertainties that are reasonably likely to have a material effect on results or financial condition. In this context, the cost of ongoing cybersecurity efforts, consequences of cybersecurity incidents, and risks of potential incidents could inform a full analysis, the guidance notes. A company should consider all costs associated with cybersecurity issues, not just immediate costs but also the costs of property loss and resources necessary to implement preventative measures, acquire insurance, and respond to potential litigation and/or regulatory investigations.

In 2011, CorpFin provided an example noting that, if intellectual property is stolen in an attack and the theft is likely to be material, the company should describe the property lost and the effect on its results of operations and financial condition. If it is reasonably likely that the incident will lead to reduced revenues and increased protection expenditures, these problems should be discussed, CorpFin found.

Business description. According to the guidance, if a cyber risk or incident materially affects a company’s products, services, or relationships with customers or vendors, it should disclose the issue in its “Description of Business” after considering the impact on each of its reportable segments.
Legal proceedings. The guidance further notes that Item 103 of Regulation S-K requires a company to disclose information relating to material pending legal proceedings to which the company or a subsidiary is a party, and this requirement includes proceedings involving cybersecurity issues. A registrant may need to disclose certain information regarding pending litigation in its “Legal Proceedings” disclosure, including the court in which a proceeding is taking place, the date it was instituted, the principal parties involved in the matter, and the relief sought, as well as a description of the alleged facts underlying the litigation.

Financial statements. The Commission also notes that cybersecurity risks and incidents may have an impact on a company’s financial statements, particularly in the form of breach notification, investigation, and remediation costs, as well as revenue loss, weakened cash flows, and potential legal fees. According to the guidance, the SEC expects a company’s financial reporting and control systems to be designed to provide reasonable assurance that information regarding the range and magnitude of the financial effects of a cybersecurity risk or incident would be incorporated into the registrant’s financial statements as it becomes available.

In 2011, CorpFin recommended that a registrant consult the Accounting Standards Codifications to inform its accounting and analysis. To the extent a cyber risk or incident is discovered after the balance sheet date but before financial statements are issued, the division continued, the company should consider whether disclosure of a recognized or non-recognized subsequent event is necessary.

Board risk oversight. Under Item 407(h) of Regulation S-K and Item 7 of Schedule 14A, a company must disclose the extent of its board’s involvement in the risk oversight of the company, and the Commission has stated that disclosure should provide information with regard to how a company perceives the board’s role and how it relates to senior management in managing material risks, including cybersecurity risks. Thus, in the 2018 guidance, the Commission urged each registrant to focus on these particular issues when making disclosures. Information about a company’s cybersecurity risk management program and the board’s interaction with management on cybersecurity issues will allow investors to assess how directors are meeting their oversight responsibilities, the guidance explains.
### New Subjects in 2018 Guidance

<table>
<thead>
<tr>
<th>2018 Cybersecurity Guidance</th>
<th>2011 Cybersecurity Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Materiality</strong></td>
<td><strong>Materiality</strong></td>
</tr>
<tr>
<td>A company must disclose all material facts necessary to make statements in the disclosure not misleading, and this reporting should involve timely information regarding cybersecurity issues, as appropriate. In determining materiality of a cybersecurity risk or incident, a company should consider its nature, extent, and potential magnitude in relation to its business and operations and the potential harm that could arise. A company is not expected to make detailed disclosures that could compromise its cybersecurity efforts, but it must disclose risks and incidents that are material to investors, including the potential financial, legal, or reputational consequences. The Commission expects companies to provide cybersecurity disclosures tailored to their unique circumstances and urges them to disseminate relevant and useful material information while avoiding generic statements and boilerplate language.</td>
<td>This issue was not addressed in the 2011 guidance.</td>
</tr>
</tbody>
</table>

| **Disclosure Controls and Procedures** | **Disclosure Controls** |
| Disclosure controls and procedures should provide a method for determining the effect of a cyber event on a company’s business, financial condition, and results of operations. A company should consider whether they will enable the company to identify cybersecurity risks and incidents, assess their impact, and lead to appropriate recording, processing, and reporting of issues required to be disclosed in filings. A company should also regularly assess the effectiveness of disclosure controls and procedures in relation to cybersecurity disclosure. | This issue was not addressed in the 2011 guidance. |

| **Insider Trading** | **Insider Trading** |
| A company should adopt and maintain policies and procedures designed to prevent insiders from taking advantage of the time between discovery of a cybersecurity risk or incident and public disclosure. A company should consider existing preventative measures designed to address the appearance of improper trading in the context of a cyber event and develop policies and procedures designed to ensure that they make timely and appropriate disclosure of material, nonpublic information. | This issue was not addressed in the 2011 guidance. |

| **Regulation FD** | **Regulation FD** |
| A company should adopt and maintain policies and procedures to ensure that any disclosures of material, nonpublic information related to cybersecurity issues are not made selectively and otherwise comply with the requirements of Regulation FD. A company should consider omitted information material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or if the disclosure would significantly alter the total mix of information available, the guidance explains. | This issue was not addressed in the 2011 guidance. |
Materiality

While preparing disclosures and reports under the federal securities laws and the SEC’s regulations, a company should consider the materiality of cybersecurity threats and events, the guidance states. Although Regulations S-K and S-X do not specifically refer to “cybersecurity,” several of their requirements impose obligations to disclose risks and incidents in certain circumstances. For example, Form 10-K requires a company to disclose information about its operations, risk factors, legal proceedings, financial statements, disclosure controls and procedures, and corporate governance. These items require disclosure of all material facts necessary to make statements in the disclosure not misleading, and this reporting should involve timely information regarding cybersecurity issues, according to the guidance. The Commission reminds companies that omitted information is material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or would be viewed by the reasonable investor as significantly altering the total mix of available information.

In determining materiality of a cybersecurity risk or incident, a company should consider its nature, extent, and potential magnitude in relation to its business and operations and the potential harm that could arise, including with respect to financial losses and performance, reputation damage, and the possibility of legal or regulatory actions.

A company is not expected to make detailed disclosures that could compromise its cybersecurity efforts, but it must disclose risks and incidents that are material to investors, including the potential financial, legal, or reputational consequences, the guidance explains. The SEC recognizes that it may take some time to determine the full implications of an incident and that it may be necessary to cooperate with law enforcement, which could affect the scope of the disclosure. The guidance adds, however, that an ongoing internal or external investigation would not on its own provide a basis for avoiding disclosure of a material cybersecurity incident. Companies also are obligated to correct any disclosures subsequently determined to have been untrue at the time they were made, the guidance notes, so firms should consider revisiting previous disclosures while investigating cyber risks or incidents.

The Commission expects companies to provide cybersecurity disclosures tailored to their unique circumstances and urges them to disseminate relevant and useful material information while avoiding generic statements and boilerplate language.

Speaking about cyber issues at a conference on March 15, 2018, Commissioner Jackson noted that, of 81 cybersecurity incidents uncovered in 2017, only two public companies chose to file an 8-K disclosing the breach to their investors. Hiding attacks from the board and investors can prove very costly in the form of lawsuit settlements and future risks that may not be addressed, he said. In addition, Jackson said that he has called upon his SEC colleagues to consider new 8-K requirements for cyber events and urged companies to adopt internal controls to channel the relevant information about cyber risks and incidents up the corporate ladder.
Policies and Procedures

The 2018 guidance adds recommendations concerning certain policies and procedures a public company should adopt with regard to cybersecurity issues. According to the Commission, cybersecurity concerns are a key element of risk management, and the guidance encourages adoption of comprehensive policies and procedures related to cybersecurity. The guidance advises that disclosure controls and procedures should provide a method for determining the impact of cyber events on a company's business, financial condition, and results of operations. In addition, companies should adopt and maintain policies and procedures designed to prevent insider trading on material, nonpublic information regarding cybersecurity risks and incidents. Finally, in adopting cybersecurity policies and procedures, companies should address the potential application of Regulation FD and its limitations on selective disclosure.

Disclosure controls and procedures. The guidance advocates regular assessment of the effectiveness of disclosure controls and procedures in relation to cybersecurity disclosure by public companies. In addition, a registrant should ensure that a process is in place to get information about risks and incident to the appropriate personnel, including information not currently but potentially subject to required disclosure. A company should consider whether the disclosure controls and procedures in place will enable it to identify cybersecurity risks and incidents, assess their impact, and lead to appropriate recording, processing, and reporting of issues required to be disclosed in filings.

To the extent cybersecurity incidents or risks may affect a company's ability to process and report information required to be disclosed, management should consider whether deficiencies exist within the firm's disclosure controls and procedures that would render them ineffective, according to the guidance.

Insider trading. The guidance warns that officers, directors, and other corporate insiders must not trade a public company's securities while in possession of material, nonpublic information, which may include knowledge about significant cybersecurity risks and incidents, including known vulnerabilities and actual breaches. A registrant should have policies and procedures in place to guard against insiders taking advantage of the time between discovery of a cybersecurity incident or risk and public disclosure to trade on inside material, nonpublic information about the issue—conduct that would violate the antifraud provisions.

The guidance encourages firms to take existing preventative measures designed to address the appearance of improper trading and consider them in the context of a cyber event, then develop policies and procedures designed to ensure that they make timely and appropriate disclosure of material, nonpublic information. The Commission also encourages companies to consider how their codes of ethics prevent trading on the basis of material, nonpublic information regarding cybersecurity issues.

Regulation FD and selective disclosure. The guidance also notes that a company 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.” The SEC reminds companies to refrain from making selective disclosure of material, nonpublic information about cybersecurity incidents or risks before disclosing that same information to the public.
A company should consider omitted information material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or if the disclosure would significantly alter the total mix of information available, the guidance explains. The Commission expects each registrant to adopt and maintain policies and procedures to ensure that any disclosures of material, nonpublic information related to cybersecurity issues are not made selectively and otherwise comply with the requirements of Regulation FD.

Other SEC Cyber Efforts

Cyber Unit

Last fall, the SEC created a Cyber Unit in the Division of Enforcement to target cyber-related misconduct. In recent years, the Enforcement Division has focused on developing substantial cyber-related expertise and dedicating resources to the detection of fraudulent conduct in an increasingly technological and data-driven industry. According to the Commission, the unit is designed to complement Chairman Clayton’s initiative to implement an internal cybersecurity risk profile and create a cybersecurity working group to coordinate the agency’s risk monitoring and response efforts throughout the agency.

“Cyber-related threats and misconduct are among the greatest risks facing investors and the securities industry,” said Enforcement Co-Director Stephanie Avakian.

The Cyber Unit will focus on cyber-related misconduct, such as:

- Market manipulation schemes using false information spread through electronic media;
- Hacks designed to obtain material, nonpublic information or to intrude on retail brokerage accounts;
- Violations involving distributed ledger technology and initial coin offerings;
- Cyber threats to trading platforms and market infrastructure

In recent comments at the 2018 SEC Speaks conference, Cybersecurity Unit Chief Robert Cohen said the group is currently focused on initial coin offerings and digital assets; trading cases such as hacking, account takeovers, and electronic platform manipulations; and issues involving cybersecurity controls. To illustrate the unit’s efforts, he referred to the ongoing BitFunder case in which an unregistered securities exchange was charged with defrauding users, making false and misleading statements in connection with an unregistered offering of securities, and also failing to disclose a cyberattack that resulted in the theft of more than 6,000 bitcoins.
Recent Cyber Enforcement Actions

Regulation SCI. Earlier this month, the New York Stock Exchange LLC and affiliated exchanges agreed to settle the first-ever charged violations of Regulation SCI, the agency’s cybersecurity and business resiliency rules for market-facing entities. The SEC alleged that, in one instance, NYSE and NYSE American LLC issued quotations labeled as “automated” when, in fact, they were not automated due to connectivity issues during a 47-minute period before a trading shutdown in July 2015. The SEC alleged that the mislabeled quotes amounted to negligent misrepresentations or omissions of material facts. In addition to finding other improper disruptions, the SEC claimed that NYSE lacked business continuity and disaster recovery plans because, for a one-year period after Regulation SCI became effective, NYSE would have had to rely on NYSE Arca, Inc.’s backup systems.

Without admitting or denying the Commission's findings, NYSE and the other named exchanges agreed to be censured and to cease and desist from further violations. In addition to paying a $14 million civil penalty, the exchanges, for a total of three years, must have their principal executive officers certify in writing that the exchanges have taken reasonable steps to comply with portions of Exchange Act Section 19. Moreover, the exchanges’ respective senior management teams must meet in person with Commission staff on an annual basis for three years to further discuss the exchanges' compliance with federal securities laws.

Insider Trading. In another action, the SEC filed a complaint in Georgia federal court charging a former Equifax executive with insider trading ahead of the company’s announcement of a massive data breach. In late July 2017, Equifax’s security department determined that there was a possibility the company had been the victim of a cybersecurity breach, and the executive was warned of the possible attack. Within an hour after learning that a competitor’s stock price fell following a breach in that company’s systems, the SEC alleged, the executive accessed his company-sponsored stock plan account, exercised all of his vested options to buy Equifax shares, and then immediately sold the shares for proceeds of over $950,000. Equifax publicly announced the massive data breach in September 2017, after which its stock price dropped by nearly 14 percent. According to the Commission, the executive avoided more than $117,000 in losses that he would have suffered had he not sold until after the news of the breach became public. Following an internal investigation, Equifax concluded that the executive had violated Equifax’s insider trading policy, and he agreed to resign.

The Commission asks the court to order an injunction and payment of disgorgement, interest, and penalties.

OCIE on Data Protection and Corporate Policies

In August 2017, OCIE released a summary of its observations following cybersecurity examinations of 75 broker-dealers, investment advisers, and investment companies. The staff assessed compliance with cybersecurity preparedness and included more validation and testing of procedures and controls than in previous examinations. The staff noted an improvement in firms’ awareness of cyber-related risks and in the implementation of cybersecurity practices since OCIE’s first cybersecurity examination initiative undertaken in 2014.
The staff found that all of the broker-dealers and funds and most the advisers had written policies and procedures to address the protection of customer or shareholder records and information. Most of the registrants conducted periodic risk assessments, penetration tests, and vulnerability scans of critical systems, according to OCIE. All of the firms had methods for detecting data loss relating to personally identifiable information, and all of the broker-dealers and most of the funds and advisers had maintenance systems, including software patches to address security vulnerabilities. Most of the broker-dealers had plans for data breach incidents and for notifying customers of material events, but less than two-thirds of the funds and advisers had these types of plans, the staff noted. The staff also found that almost all of the firms conducted vendor risk assessments or required vendors to provide their risk management and performance reports and security reviews or certification reports.

OCIE also reported on a number of elements found during the review that reflected robust controls, including the maintenance of inventories of data, information, and vendors, as well as detailed cybersecurity-related instructions on conducting penetration tests, security monitoring and system auditing, access rights, and reporting of incidents. Some firms had prescriptive schedules and processes for testing data integrity and vulnerabilities, established and enforced controls to access data and systems, mandatory employee training, and policies and procedures that were vetted and approved by senior management, according to the report.

However, OCIE concluded that firms could improve in a number of areas, including the adoption of more tailored policies and procedures in place of general or vague guidance. The staff also recommended enforcement of policies regarding required annual customer protection reviews, cybersecurity awareness training, and adequate system maintenance.

Cybersecurity remains a top compliance risk for financial firms, and the staff will continue to examine for compliance procedures and controls, OCIE advised.

**Internal SEC Cybersecurity**

In 2016, the SEC discovered a software vulnerability in the test filing component of the EDGAR system that allowed an intrusion and access to nonpublic information. After announcing the breach in September 2017, based on forensic data analysis, the SEC announced that the test filing accessed contained personal information pertaining to two individuals. According to the SEC, the intrusion did not jeopardize agency operations or result in systemic risk. Clayton issued a statement in which he pledged to regularly assess whether regulatory protections were appropriate in light of the risks of unauthorized access. He directed the staff to focus first on strengthening EDGAR’s cybersecurity risk profile given the substantial amounts of data, including sensitive, nonpublic data, stored on the system.

Finding that the improvements to EDGAR could affect its ability to validate and accept certain filings, the SEC postponed for nine months a final requirement that large registered investment companies begin filing information about their monthly portfolio holdings in order to provide more time for the EDGAR, requiring them instead to maintain in their records the information required to be Form N-PORT, in lieu of filing reports with the Commission, until April 2019.
In his statement about the EDGAR breach, Clayton noted that the Commission would continue its investigation into the matter and focus on evaluating potential cybersecurity issues affecting the agency in general. Like many other governmental agencies, financial market participants, and other private sector entities, the SEC is the subject of frequent attempts by unauthorized actors to disrupt access or cause damage to the agency’s technological infrastructure, Clayton stated.

The SEC receives, stores, and transmits data under three broad categories, Clayton explained. For example, it collects and makes publicly available information filed by issuers and other registrants through its EDGAR system. The second category includes nonpublic information related to its supervisory and enforcement functions, and the third category relates to internal operations, such as personnel records. In the second category, Clayton noted that the consolidated audit trail, once launched, will contain significant, nonpublic, market sensitive data and personally identifiable information, so cybersecurity is a key element in its development.

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, and independent assessments and verification and validation, according to the chairman. The Commission also maintains a number of internal policies and procedures related to cybersecurity delineating the responsibilities of various agency employees and committees in carrying out the SEC’s information security objectives and training efforts, he explained.

“When determining when and how to collect data, it is important that we regularly review whether our related data protections are appropriate in light of the sensitivity of the data and the associated risks of unauthorized access,” Clayton asserted.

The SEC’s cybersecurity program is subject to review by internal and external independent auditors, including the Government Accountability Office. In November 2017, for the third year in a row, the SEC received a clean GAO audit report with no found material weaknesses or significant deficiencies in the Commission’s internal controls over financial reporting. The GAO highlighted the proactive steps taken by the SEC to enhance its information security related to the deficiencies identified as a result of the 2016 cyber intrusion of its EDGAR system and stated that it would monitor the SEC’s actions in response to the intrusion as a separate matter.

Like many other governmental agencies, financial market participants, and other private sector entities, the SEC is the subject of frequent attempts by unauthorized actors to disrupt access or cause damage to the agency’s technological infrastructure, Clayton stated.
In March 16, 2018, remarks at the Investment Adviser Association’s annual compliance conference, Commissioner Hester Peirce reiterated that cybersecurity has been and will remain a top priority for the Commission and that it is one of Chairman Clayton’s main concerns. The cybersecurity issue is important not just for registrants, but also for the SEC itself, she said. “If we can’t promise to protect data, we shouldn’t be collecting it,” Peirce proclaimed.

**Conclusion**

Cyberattacks on U.S. business and government entities continue to increase in frequency and cunning, with data breaches and attendant costs rising exponentially from year to year. As such, Chairman Clayton has provided assurances that the Commission will continue to prioritize effective cybersecurity practices with respect to the markets and individual registrants, as well as within the Commission itself.

“By promoting effective practices in connection with both external oversight and internal operations, it is our objective to contribute substantively to a financial market system that recognizes and addresses cybersecurity risks and, in circumstances in which these risks materialize, exhibits strong mitigation and resiliency.”