PCAOB
Public Company Accounting Oversight Board

1666 K Street, NW
Washington, D.C. 20006
Telephone: (202) 207-9100
Facsimile: (202)862-8430

STANDING ADVISORY GROUP MEETING

PANEL DISCUSSION – CYBERSECURITY

JUNE 5-6, 2018

Introduction

At the June 2018 Standing Advisory Group ("SAG") meeting, a panel will discuss cybersecurity issues and the potential implications for financial reporting and auditing. The panelists will provide brief remarks, and the SAG will have an opportunity to ask questions and provide input.

Background

Cybersecurity continues to be a topic of growing concern among public companies, investors, audit committees, regulators, auditors, and others.

Recent Cyber Events

Since the discussion of cybersecurity at the June 2014 SAG meeting, a number of high-profile events have occurred. Retailers have paid millions of dollars in settlements over credit card data breaches.[1] A leading health insurer announced

[1] *See* HBC, *HBC Provides Information about Data Security Issue in Certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor Stores in North America*, Apr. 1, 2018; *see also* Nicole Hong, *Target to Pay $18.5 Million to Settle Massive 2013 Data Breach*, Wall Street Journal, May 23, 2017; and Jonathan Stempel, *Home Depot Settles Consumer Lawsuit Over Big 2014 Data Breach*, Reuters, Mar. 8, 2016.

multiple data breaches that affected more than 90 million individuals,[2] including one breach that resulted from a phishing scam.[3] The data breach of one credit reporting agency led to the exposure of personally identifiable information of over 143 million individuals.[4]

Government agencies have also reported data breaches. In 2015, the Office of Personnel Management ("OPM") announced two cybersecurity incidents that impacted the data of federal government employees, contractors, and others. In both incidents, personally identifiable information was stolen.[5] The Securities and Exchange Commission ("SEC") also disclosed information about the 2016 intrusion on EDGAR and the SEC's efforts going forward in response.[6]

Additionally, accounting firms of various sizes, including a large multinational firm, have reported data breaches, some of which exposed personally identifiable information of employees and clients.[7]

In addition to data breaches, other types of cybersecurity threats are also viewed as posing risks to businesses. Recent reports have described a range of cyber threats, including malware, ransomware, and denial of service attacks.[8] The World Economic Forum observed that ransomware attacks accounted for 64% of all malicious emails sent between July and September 2017, and affected twice the number of businesses

---

[2] *See* CareFirst BlueCross BlueShield, *CareFirst BlueCross BlueShield Has Been the Target of a Cyberattack*, available at http://carefirstanswers.com/home.html.

[3] *See* CareFirst BlueCross BlueShield, *CareFirst Announces "Phishing" Email Incident; 6,800 Members Offered Protection*, Mar. 30, 2018.

[4] *See* Seena Gressin, *The Equifax Data Breach: What to Do,* Federal Trade Commission, Sept. 8, 2017.

[5] *See* OPM, *Cybersecurity Resource Center: Cybersecurity Incidents*, available at https://www.opm.gov/cybersecurity/cybersecurity-incidents/.

[6] *See* SEC, *Chairman Clayton Provides Update on Review of 2016 Cyber Intrusion Involving EDGAR System*, Press Release No. 2017-186 (Oct. 2, 2017).

[7] *See, e.g.*, Roman H. Kepczyk, *CPA Firm Security Briefing*, AICPA; Michael Cohn, *California CPA Firm Reports Data Breach*, Accounting Today, Aug. 25, 2017; and Deloitte, *Deloitte Statement on Cyber-Incident*, Sept. 25, 2017.

[8] *See* European Union Agency for Network and Information Security (ENISA), *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* (Jan. 2018).

compared to 2016.[9] It also described the rising costs of cybersecurity, and noted the near doubling of cyber breaches in the past five years from 68 per business in 2012 to 130 per business in 2017.[10] Others have observed that, for some cyber attackers, "the prize isn't ransom, but the destruction of systems and data."[11] These risks could escalate due to the growing use of cloud services and the expansion of the Internet of Things.[12]

Recent Governmental and Audit Industry Guidance

Regulators and audit industry organizations have taken actions in response to continued cybersecurity threats to their regulated or member organizations. In February 2018, the SEC published guidance to help public companies prepare disclosures about cybersecurity risks and incidents.[13] This release stressed the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Further, in April 2018, the SEC announced that an issuer agreed to settle charges that it misled investors by failing to disclose a data breach affecting hundreds of millions of user accounts. That settlement resulted in a penalty of $35 million.[14]

In April 2018, the U.S. Commerce Department's National Institute of Standards and Technology ("NIST") released a revised version of its widely-used Framework for Improving Critical Infrastructure Cybersecurity, a voluntary framework for reducing cyber risks to critical infrastructure.[15] The Framework provides an approach to prioritize cybersecurity resources, make risk decisions, and take action to reduce risk. It is used to enhance cybersecurity communication within an organization and with other

---

9 *See* World Economic Forum, *The Global Risks Report 2018*, at 15 (citing Proofpoint, *Quarterly Threat Report Q3 2017*).

10 *Id.* at 14.

11 Cisco Systems, Inc., *Annual Cybersecurity Report* (2018), at 6.

12 World Economic Forum, *The Global Risks Report 2018*, at 14-15.

13 SEC, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Securities Act Release No. 10459 (Feb. 21, 2018), 83 FR 8166 (Feb. 26, 2018).

14 *See Altaba Inc., f/d/b/a Yahoo! Inc.*, SEC Accounting and Auditing Enforcement Release No. 3937 (Apr. 24, 2018).

15 *See* NIST, *NIST Releases Version 1.1 of Its Popular Cybersecurity Framework*, Apr. 16, 2018.

organizations (such as partners, suppliers, regulators, and auditors) and help organizations identify, manage, and assess cybersecurity risks.[16]

The American Institute of Certified Public Accountants ("AICPA") and the Center for Audit Quality ("CAQ") have published resources for audit committees and auditors. An AICPA cybersecurity resource center provides resources to help organizations and businesses, including CPA firms, assess cybersecurity risks.[17] The AICPA also published a voluntary cybersecurity risk management framework to help companies and auditors communicate cyber risk readiness.[18] Additionally, the AICPA published a new attest guide and resource page to assist CPAs engaged to examine and report on an entity's cybersecurity risk management program.[19] In April 2018, the CAQ published a tool to assist board members in their oversight of enterprise-wide cybersecurity risk management.[20] The tool provides questions board members can use as they discuss cybersecurity risks and disclosures with management and CPA firms.

PCAOB Oversight of Auditors and Audits

The PCAOB staff monitor developments related to cybersecurity and considers auditor responsibilities in an audit of the financial statements and internal control over financial reporting ("ICFR"), including the response by an auditor to a cyber incident. PCAOB Inspections staff also continue to review and develop an understanding of how firms evaluate the risks of material misstatement associated with cybersecurity and any impact to the related ICFR and financial statements.[21] For the issuers that were

---

16 *Id*.

17 *See* AICPA, *Cybersecurity Resource Center*, available at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cyber-security-resource-center.html.

18 *See* AICPA, *AICPA Unveils Cybersecurity Risk Management Reporting Framework*, Apr. 26, 2017.

19 AICPA, *SOC for Cybersecurity: Information for CPAs*, available at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html.

20 *See* Center for Audit Quality, *CAQ Tool Helps Boards Oversee Cybersecurity Risk Management of Public Companies*, Apr. 12, 2018.

21 *See* PCAOB, *Staff Inspection Brief: Preview of Observations from 2016 Inspections of Auditors of Issuers* (Nov. 2017), at 13. PCAOB standards provide that an auditor, while obtaining an understanding of the company's information system related to financial reporting, should obtain an understanding of how the company uses information technology ("IT") and how IT affects the financial statements. The auditor

identified as having experienced a cybersecurity incident and whose audits were reviewed by Inspections staff during 2016, it appears that these cybersecurity incidents have not been related to the risks of material misstatement of financial statements, including disclosures, or led to the identification of material weaknesses in ICFR.[22] Risks remain, however, that future cyber attacks may affect issuer financial statement reporting, and as a result, Inspections staff view this as an evolving risk area that requires ongoing focus.[23]

Panel Discussion

Panelists will include:

- A SAG member who serves on audit committees, who will address: how boards and their audit committees consider cybersecurity at public companies; the audit committee's role in oversight of management's response to cyber risk at public companies; and questions asked of auditors regarding their procedures in considering cybersecurity risks as part of the audits of the financial statements and ICFR;

- A SAG member from a public accounting firm, who will address: the auditor's responsibilities when considering cybersecurity risk as part of the audits of internal control over financial reporting and the financial statements; audit responses to known cyber attacks; and what firms are doing to safeguard client data received as part of the audit;

- A representative from the SEC staff, who will address: the implications of cyber risks and cyber incidents for financial reporting, including the issuer's disclosure obligations in filings with the SEC; and

- A representative from the PCAOB's Division of Registration and Inspections, who will address: auditor responsibilities related to cyber risks

---

also should obtain an understanding of the specific risks to a company's internal control over financial reporting resulting from IT, including unauthorized changes to systems, programs, or data in master files and potential loss of data or inability to access data as required. *See* Appendix B of AS 2110, *Identifying and Assessing Risks of Material Misstatement*.

[22] *See* PCAOB, *Staff Inspection Brief: Preview of Observations from 2016 Inspections of Auditors of Issuers*, at 13.

[23] *Id*.

and cyber incidents; and PCAOB staff observations regarding cybersecurity in audits of issuers and audit firm responses.

SAG members will have the opportunity to discuss the following topics, among others:

- Perspectives of audit committee members on cyber risks;
- How companies evaluate, manage, and respond to cyber risks and cyber incidents;
- Implications of cyber risks and cyber incidents for financial reporting, including disclosure obligations in filings with the SEC;
- Auditor responsibilities as part of an audit of financial statements or ICFR related to cyber risks and cyber incidents; and
- How audit firms evaluate, manage, and respond to their own cyber risks and cyber incidents.

* * *

The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public companies in order to protect investors and the public interest by promoting informative, accurate, and independent audit reports. The PCAOB also oversees the audits of broker-dealers, including compliance reports filed pursuant to federal securities laws, to promote investor protection.