CURRENT ISSUES IN AUDITING
Vol. 13, No. 2
Fall 2019
pp. C1–C9

American Accounting Association
DOI: 10.2308/ciia-52419

COMMENTARY

Accounting and Cybersecurity Risk Management

Tim V. Eaton
Jonathan H. Grenier
David Layman
Miami University

SUMMARY: As the number of cybersecurity incidents continue to rise and stakeholders are becoming increasingly concerned, companies are devoting considerable resources to their cybersecurity risk management efforts and related cybersecurity disclosures. This paper describes how accountants are uniquely positioned to assist companies with these efforts in advisory and assurance capacities. We present a model of effective cybersecurity risk management and discuss how accountants' core competencies can add significant value in each of the model's five stages. In addition, we use several recent high-profile cybersecurity incidents as illustrative examples in each of the five stages. We conclude by discussing implications for accountants.

Keywords: cybersecurity; risk management; controls; assurance.

I. INTRODUCTION

According to an FBI director, "There are only two types of companies: those that have been hacked, and those that will be" (Cowley 2012). As such, managing and reporting cybersecurity risks are high priorities for the management and board of almost every company—particularly as proprietary financial and non-financial information, including information related to customers and suppliers, is increasingly stored on networks and in the Cloud. By 2020, over one third of data is projected to live in or pass through the Cloud; within five years, there will be over 50 billion smart connected devices (Marr 2015). These trends provide ample opportunity for cybercriminals looking to compromise an organization's sensitive data. In fact, 4,500 data breaches have been publicly disclosed since 2005 in the United States alone (Lord 2018),

We thank Michele Frank, Corrine Kidd, and Jon Pyzoha for constructive feedback. Tim Eaton and David Layman appreciate the financial support of the EY Foundation. Jonathan Grenier is grateful for the financial support of Miami University's Committee on Faculty Research and of the Farmer School of Business.

Editor's note: Accepted by Lisa Milici Gaynor.

Submitted: September 2018
Accepted: March 2019
Published Online: March 2019

including recent attacks at well-known companies such as Equifax, Uber, Yahoo, Target, and Home Depot. Stakeholders (e.g., investors, customers, suppliers) are also demanding more information about cybersecurity. As a result, the AICPA, in conjunction with the Auditing Standards Board, recently issued a voluntary reporting and assurance framework as a means for companies to communicate their cybersecurity risk management efforts to interested stakeholders (AICPA 2017a). In sum, it is projected that companies will spend over $1 trillion on cybersecurity efforts in the five-year period from 2017 to 2021 (Morgan 2016).

Beyond the need to protect organizational data, recent academic research suggests numerous benefits of cybersecurity disclosures for client firms. Two of the key benefits are that cybersecurity disclosures can be informative to investors (e.g., Ettredge and Richardson 2003; Gordon, Loeb and Sohail 2010; Frank, Grenier, and Pyzoha 2019) and can help mitigate the negative impacts of a subsequent breach (e.g., Wang, Kannan, and Ulmer 2013).[1] However, despite the recommendations of regulatory bodies and the findings of recent research, firms often fail to provide disclosures regarding cyber issues (Amir, Levi, and Livne 2018; Rubin 2019).

In a time when data breaches are common headlines and companies are making massive investments in cybersecurity risk management and reporting, we posit that accounting firms are in a unique position to help. Specifically, we discuss the role of accountants in all stages of effective cybersecurity risk management: risk identification and measurement, control system design and testing, external reporting, and independent assurance. We illustrate the importance of these roles by discussing their applicability to three recent data breaches. This analysis of recent major data breaches creates an opportunity to learn how companies' security systems are compromised and to demonstrate how public accounting firms can assist in those areas. We close with implications for companies in managing their cybersecurity risk and for public accounting firms in the design and marketing of their cybersecurity services.

II. ACCOUNTING AND CYBERSECURITY RISK MANAGEMENT

As an organizing framework for our discussion of how accountants can enhance cybersecurity, we integrate general concepts from enterprise risk management with recent cybersecurity reporting and assurance guidance from the AICPA (2017a, 2017b, 2017c). The result, presented in Table 1, can be characterized as the stages of an effective cybersecurity risk management program.[2] Although Table 1 represents these stages as discrete steps, they should be performed continuously and repeatedly as new cybersecurity risks continually arise. The first three stages are foundational to any effective risk management program, where the organization (1) identifies and prioritizes its risks/exposures, (2) designs and implements relevant controls to mitigate the risks/exposures, and (3) monitors the operating effectiveness of the controls in mitigating the risks/exposures. The final two stages represent the AICPA's (2017a, 2017b) recent guidance on cybersecurity reporting and assurance, which is designed to address external stakeholders' concerns with the reporting organization's cybersecurity risk management. In the reporting stage, the AICPA (2017a) has issued description and control criteria to facilitate

[1] See Wang et al. (2013) for a review of other academic studies on cybersecurity disclosure.

[2] Table 1 is simply a cybersecurity adaption of general enterprise risk management (ERM) principles that are embedded in frameworks such as the COSO Framework for Internal Control (COSO 2013) along with cybersecurity reporting and assurance criteria from the AICPA. As such, Table 1 is not intended to be a key takeaway or contribution. As interested parties likely already have a general understanding and appreciation of general ERM principles, the stages in Table 1 are only intended to be an organizing framework for our discussion of how accountants can benefit cybersecurity risk management.

TABLE 1

Stages of Effective Cybersecurity Risk Management

1. Cybersecurity risk/exposure identification and prioritization	Accounting firms can help companies identify and prioritize cybersecurity risks/exposures by leveraging their IT expertise and knowledge of current cybersecurity threats.
2. Cybersecurity control system design	Accounting firms can help companies design cybersecurity controls to address the risks/exposures identified in Stage 1. Accounting firms possess considerable IT control system expertise, including current industry best practices and control standards (e.g., AICPA's Cybersecurity Control Criteria).
3. Testing the operating effectiveness of cybersecurity controls	Accounting firms can test the operating effectiveness of companies' cybersecurity controls in either advisory or assurance capacities. Accounting firms have extensive experience in testing IT controls in conjunction with their financial statement audits and IT advisory services. If not part of externally reported assurance, this advisory service would be considered internal auditing.
4. External cybersecurity reporting	Accounting firms can help companies prepare external cybersecurity reports in accordance with external criteria (e.g., the AICPA's entity-level cybersecurity reporting framework).
5. Assurance on external cybersecurity reporting	Advisory: Accounting firms can help companies prepare for and assess their readiness for a formal assurance engagement regarding the effectiveness of a company's cybersecurity risk management program. Readiness assessments should be based on successful completion of Stages #1–4. Assurance: Accounting firms can provide a formal assurance engagement regarding the effectiveness of a company's cybersecurity risk management program. Assurance reports may or may not be shared publicly. If shared publicly, the accounting firm should not have provided any advisory services in Stages 1–4, for independence purposes.

management's preparation of consistent external cybersecurity reporting. In the assurance stage, reporting organizations can foster the credibility of their cybersecurity reporting by procuring independent assurance of their description and control criteria. To facilitate the provision of this assurance service, the AICPA (2017b) has issued cybersecurity attestation criteria. In the following section, we describe how accountants can, in their advisory and/or assurance capacities, enhance cybersecurity efforts within each stage. Before doing so, it is important to note that accounting firms utilize multidisciplinary teams comprising traditional accountants who are also trained in IT/cybersecurity, working alongside IT/cybersecurity specialists who may not have an accounting background.

Cybersecurity Risk/Exposure Identification and Prioritization

Risk identification and prioritization is essential for effective risk management. If a company fails to identify certain risks or prioritizes the wrong risks, risk management is bound to fail and result in significant adverse consequences. This is especially true in cybersecurity, where there are

countless and ever-changing cybersecurity threats devised by hackers. As keeping current on cybersecurity threats is challenging for companies, accounting firms' advisory practices are dedicated to keeping abreast of new and emerging cybersecurity threats and communicating them to their clients (i.e., collective intelligence; Mahidhar, Shatsky, and Bissell 2013). In addition, accountants with auditing backgrounds have significant expertise in risk assessment, making them well-positioned to assess the likelihood and magnitude of the various threats for risk prioritization purposes based on the exposures and vulnerabilities within their client's business. High-quality IT risk assessments are critical in identifying the areas in the system that may be vulnerable to data breaches. Accounting firms also employ sophisticated technologies to identify these vulnerabilities in a process known as vulnerability scanning (MPA 2018). Vulnerability scanning involves using software (e.g., Nessus, OpenVAS), or other technologies, to test company networks for unknown open ports or systems that cybercriminals may exploit in a cyberattack (MPA 2018).

The importance of effective risk identification and prioritization can be seen in the Target incident (see Edwards [2013] for more details), in which intruders gained access to proprietary information (e.g., credit/debit card information) of over 70 million customers through malware (i.e., software designed to disrupt, damage, or gain unauthorized access to a system) on store point-of-sale systems. To do so, a Target employee either intentionally or unintentionally (e.g., by clicking on a link in an email) installed the malware. Although the federal government had warned Target that point-of-sale systems were being targeted with malware by cybercriminals, Target may not have been aware of the specific risk of collusion with an insider or that malware could be installed unintentionally by an employee. Even if Target were aware of this specific risk, the incident illustrates the importance of effective risk prioritization in that Target was made aware of the general risk of malware on their point-of-sale systems and did not prioritize mitigation of this risk.

Cybersecurity Control System Design

After identifying cybersecurity risks, the next stage is to design effective controls to mitigate the risks. Accountants have a significant competitive advantage in this stage due to their expertise in internal control. Although most cybersecurity controls do not fall under the audit requirements of SOX 404, auditors have significant experience identifying and evaluating internal controls that have financial reporting implications, including IT controls over the accounting-related systems and general controls over the IT function.[3] Beyond the SOX 404 requirement to opine on the operating

[3] Under Section 404 of Sarbanes-Oxley and PCAOB Auditing Standard No. 2201 (PCAOB 2007; formerly AS5), auditors are required to opine on the operating effectiveness of internal control over financial reporting (ICFR). Only the subset of cybersecurity controls that have potential to materially affect financial reporting and general controls over information technology fall under the purview of ICFR. Other cybersecurity controls over specific systems in the company's enterprise-wide control system (e.g., controls over the privacy of customer information) are not required to be audited under SOX 404 since they have limited, if any, potential to materially affect financial reporting and are not general controls over IT. The Center for Audit Quality (2016b) discusses these and auditors' other responsibilities with respect to cybersecurity, which include: (1) considering the audit client's IT systems and controls when assessing the risk of material misstatement of the financial statements under PCAOB Auditing Standard No. 2010 (PCAOB 2010, formerly AS12), (2) discussing the overall audit approach regarding IT with the audit committee under PCAOB Auditing Standard No. 1301 (PCAOB 2012, formerly AS16), (3) determining if the financial statements and related disclosures properly account for any identified material cybersecurity incidents, and (4) assuring that there are no material inconsistencies between the audited financial statements and any cybersecurity disclosures not included in the financial statements (e.g., disclosures in the 10-K, annual report) under PCAOB Auditing Standard No. 2701 (PCAOB 2013, formerly AU Section 550).

effectiveness of internal control over financial reporting (ICFR), auditors also assess business process controls under the business risk auditing methodology that is commonly used at most large firms. Large accounting firms also stay current on the latest technologies, including those that can enhance cybersecurity controls, such as Blockchain, cloud computing and security, advanced authentication, and built-in encryption. Due to the inherent complexity and rapid rate of innovation, it is challenging for companies to keep up with these innovations and ensure that they are utilizing the full capabilities of the technology, whereas accounting firms have advisory practices dedicated to this very task. In sum, accountants are well-positioned to develop a plan to design cybersecurity controls based on the exposures identified in the cybersecurity risk assessment stage.

The importance of designing effective controls can be seen in the Home Depot incident (see Ragan [2014] for more details). In the incident, cybercriminals compromised over 56 million credit/debit card accounts through store point-of-sale systems. Intruders used a vendor's username and password to enter the perimeter of Home Depot's network, but the stolen credentials alone did not provide direct access to the company's point-of-sale devices. For that, they had to turn to a vulnerability in Microsoft Windows that was patched only after the breach occurred.

In sum, Home Depot's controls were insufficient to prevent the incident, creating valuable lessons for other companies about the importance of cybersecurity controls. For instance, the use of multifactor authentication for vendors would have greatly minimized the possibility that an intruder could access the system with a stolen username and password. Standardizing remote access methodologies for vendors would also have been beneficial. As vendors typically use different devices to access a given network, it is difficult to ensure network security (Granneman 2016). Thus, a control system should define a few remote access methodologies with sufficient security controls and block any unauthorized remote access technologies. It is also important to segregate vendor remote access into firewalled zones (Granneman 2016), allowing a vendor access to only a fraction of the network to protect other network assets (e.g., point-of sale systems).

Test Operating Effectiveness of Cybersecurity Controls

Once controls are in place, they must be regularly tested to ensure they are operating effectively. As alluded to above, accountants have significant expertise in control testing, as auditors opine on the operating effectiveness of public companies' ICFR. In addition to testing ICFR, auditors test any additional controls that they believe reduce the risk of material misstatement in the financial statements. Many ICFR controls are IT-related. In fact, most firms have designated IT auditors to test the IT-related controls, and many firms require that these IT auditors be used on every audit. Thus, accountants are well-positioned to help their clients develop and execute audit programs to test the operating effectiveness of cybersecurity controls. As an example, to evaluate organizations' security systems, Ernst & Young has developed a Cybersecurity Program Management Framework (CPM) that involves a meaningful analysis of how information security shapes and fits into an organization's overall risk management structure (Ernst & Young 2014). Similar to identifying vulnerabilities in the client's IT system, large accounting firms have sophisticated technologies for testing the operating effectiveness of cybersecurity controls. Firms have technologies that analyze large data sets (e.g., access attempts) and simulate cybersecurity threats to see if the controls adequately thwart them.

The importance of testing the operating effectiveness can be seen in the Anthem incident (see Palermo [2014]), as well as the aforementioned Target and Home Depot incidents. In the Anthem incident, the personal information of 80 million people was compromised (Palermo 2014), wherein

hackers likely sent a phishing message to Anthem's IT team. By either opening an attachment or clicking on a web link in one of the emails, one of Anthem's own employees may have allowed the installation of malicious software. One of the key controls that failed to detect the incident at its initial stages was insufficient monitoring of unusual flows of data out of the company computer systems. If the company had tested the operating effectiveness of this monitoring control, they would have found it to be ineffective, allowing the company to strengthen the control or add a compensating control. Testing would have also likely revealed that the data outflows were not encrypted, another key control that would have minimized the impact of the attack. In the Target and Home Depot incidents, effective control testing over the point-of-sale systems could have revealed the vulnerabilities in the system. Home Depot could have also tested the new Microsoft software during rollout for any vulnerabilities.

External Cybersecurity Reporting

As mentioned above, in response to stakeholders' demand for more information from companies on cybersecurity, the AICPA recently issued a voluntary reporting and assurance framework as a means for companies to communicate their cybersecurity risk management efforts to interested stakeholders (AICPA 2017a, 2017b). This reporting is indeed voluntary as it goes beyond the SEC requirements to report material cybersecurity risks, incidents, and related controls.[4] The reporting entails a narrative description of the company's cybersecurity risk management program, management's assertions as to the description's compliance with the guidelines set forth by the AICPA, and whether the cybersecurity controls were operating effectively during the reporting period. As accountants' core competency is external reporting, they have the skills to help companies prepare the narrative description. In addition, as previously discussed, their expertise in control testing can inform management's assessment of the operating effectiveness of cybersecurity controls. It is important to note that if external accountants assist in either of these tasks, they would not be able to perform an independent assessment of the resulting cybersecurity risk management report (see next section).

With respect to companies who have experienced cybersecurity incidents, recent research suggests that external cybersecurity reporting can help restore investor confidence when coupled with assurance (see next section; Frank et al. 2019). Thus, companies like Target, Home Depot, and the countless others that have experienced prior cybersecurity incidents should consider external cybersecurity reporting such as the AICPA Framework. In fact, Frank et al. (2019) find that external cybersecurity reporting also promotes investor confidence for firms that have not experienced cybersecurity incidents. These results demonstrate the value of external cyberse-

[4] See SEC (2018) for recent interpretative guidance on required SEC disclosures regarding cybersecurity risk management. The guidance discusses how companies are required to disclose, on a timely basis, any material cybersecurity risks and/or incidents along with the related controls used to manage the risk. This disclosure is typically done in the risk reporting section of Form 10-K or 8-K, but any method that is "reasonably designed to effect broad, non-exclusionary distribution" is acceptable (SEC 2018, 24). Prior research finds that many firms fail to disclosure cybersecurity risks and incidents, claiming they are immaterial (Amir, Levi, and Livne 2018). A recent study of the SEC reveals a similar pervasive lack of disclosure with 90% of all cybersecurity incidents at public companies not being disclosed (Rubin 2019). The SEC is currently considering what further guidance is needed to address this issue (Rubin 2019). The AICPA Framework represents a far more robust and holistic reporting on cybersecurity risk management that is not constrained to particular material cybersecurity risks. Although consultation with accountants regarding compliance with SEC reporting requirements is not discouraged, our discussion focuses on how accountants can assist companies with voluntary cybersecurity reporting.

curity reporting as a means to address investors' significant cybersecurity concerns across all public companies, not just those that have experienced incidents (cf. Center for Audit Quality 2016a).

Assurance on External Cybersecurity Reporting

In tandem with the reporting guidance, the AICPA also issued an attestation guide for companies that desire to have their cybersecurity report independently assured. Such assurance over cybersecurity risk management is broader than the traditional SOC assurance engagements, which cover narrower aspects of IT controls for service organizations. Of course, assurance is another core competency of accountants. In fact, beyond financial statement auditing, accounting firms have been providing other forms of assurance, including assurance over CSR/sustainability reports and SOC reports over IT controls. Thus, accountants not only have assurance expertise but also the subject matter expertise to effectively evaluate the effectiveness of companies' cybersecurity risk management.

As mentioned above, when a firm has experienced a prior cybersecurity incident, research indicates that independent assurance is necessary for external cybersecurity reporting to improve investor confidence (Frank et al. 2019). Thus, firms that have experienced cybersecurity incidents should be cautious of investing in external cybersecurity reporting without the enhanced credibility from independent assurance.

III. IMPLICATIONS FOR ACCOUNTANTS

As discussed in the preceding section and illustrated in Table 1, accountants can be involved in all five stages of cybersecurity risk management, either in an advisory or assurance capacity. This represents a tremendous opportunity for accountants to earn some of the aforementioned $5 trillion that is expected to be spent on cybersecurity between 2017 and 2021. Accounting firms have recognized these trends and have developed advisory practices that include a wide range of services to help companies of all sizes stay ahead of cyber threats and externally report their cybersecurity risk management efforts to their investors and other stakeholders. Accounting firms are bringing over their knowledge of internal controls, external reporting, and assurance to their cybersecurity practice. This creates an advantage over non-accounting cybersecurity consulting firms. Accountants' expertise in the cybersecurity space is being recognized. Cybersecurity Ventures (2018), a research and market intelligence firm, lists 500 innovative companies known as the Cybersecurity 500 and all of the Big 4 accounting firms are ranked in the top 50.

Accounting firms offer an array of cybersecurity risk management services. For example, cybersecurity is a core service offered in Deloitte's Enterprise Risk Services (ERS) business. Deloitte's ERS practice assists clients when they face the "most complex risk issues by delivering end-to-end integrated risk solutions" (Deloitte 2014). KPMG Cyber helps companies to transform "their security, privacy, and continuity controls into business-enabling platforms" (KPMG 2017). Other firms, including Crowe Horwath, Grant Thornton, RSM, and BKD, offer services that help organizations manage business and cybersecurity risks. Public accounting firms are now equipped to help companies secure their networks and work alongside companies to improve their current security systems. These practices are growing rapidly as more companies seek help in protecting their information. Market demand should also increase as companies start externally reporting on their cybersecurity risk management efforts and obtaining assurance for the reporting (e.g., using the AICPA Framework).

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2017a. *SOC for Cybersecurity: A Backgrounder*. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2017b. *Illustrative Cybersecurity Risk Management Report*. New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). 2017c. *AICPA Unveils Cybersecurity Risk Management Reporting Framework*. Available at: https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies* 23 (3): 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Center for Audit Quality. 2016a. *2016 Main Street Investor Survey*. Available at: https://www.thecaq.org/2016-main-street-investor-survey

Center for Audit Quality. 2016b. *Understanding cybersecurity and the external audit: A resource for audit committees, investors, management, and others*. Available at: https://www.thecaq.org/wp-content/uploads/2019/03/cybersecurity_and_external_audit_final.pdf

Committee of Sponsoring Organizations (COSO). 2013. *Internal Control—Integrated Framework*. New York, NY: COSO.

Cowley, S. 2012. *FBI Director: Cybercrime Will Eclipse Terrorism*. Available at: https://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/

Cybersecurity Ventures. 2018. *Cybersecurity 500*. Available at: https://cybersecurityventures.com/cybersecurity-500/

Deloitte. 2014. *Leading Cyber Risk Management in a Smaller, More Perilous World*. Available at: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/gr14-cyber-security.html# (last accessed August 29, 2018).

Edwards, J. 2013. The incredibly clever way thieves stole 40 million credit cards from 2,000 Target stores in a 'Black Friday' sting. *Business Insider* (December 19). Available at: https://www.businessinsider.com/target-credit-card-hackers-2013-12

Ettredge, M. L., and V. J. Richardson. 2003. Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems* 17 (2): 71–82. https://doi.org/10.2308/jis.2003.17.2.71

Ernst & Young. 2014. *EY Cybersecurity—Cyber Program Management*. Available at: www.ey.com/gl/en/services/advisory/ey-cybersecurity-cyber-program-management

Frank, M. L., J. H. Grenier, and J. S. Pyzoha. 2019. How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*. https://doi.org/10.2308/isys-52374

Gordon, L. A., M. P. Loeb, and T. Sohail. 2010. Market value of voluntary disclosures concerning information security. *Management Information Systems Quarterly* 34 (3): 567–594. https://doi.org/10.2307/25750692

Granneman, J. 2016. Third-party vendor management security best practices. *TechTarget* (September 21). Available at: https://searchsecurity.techtarget.com/tip/Third-party-vendor-management-security-best-practices

KPMG. 2017. *KPMG Cyber Security Overview*. Available at: https://home.kpmg.com/zm/en/home/insights/2017/08/kpmg-cyber-security-overview.html

Lord, N. 2018. The history of data breaches. *Digital Guardian* (April 6). Available at: https://digitalguardian.com/blog/history-data-breaches

Mahidhar, V., D. Shatsky, and K. Bissell. 2013. *Cyber Crime Fighting*. Available at: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/cyber-crime-fighting.html

Marr, B. 2015. Big data: 20 mind-boggling facts everyone must read. *Forbes Magazine* (September 30). Available at: *www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#27cc2e9817b1*

McGowan Program Administrators (MPA). 2018. *A CPA's Guide to Vulnerability Scans*. Available at: http://mcgowanprograms.com/blog/a-cpas-guide-to-vulnerability-scans/

Morgan, S. 2016. *Cybersecurity Spending Outlook: $1 Trillion from 2017 to 2021*. Available at: www.csoonline.com/article/3083798/security/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html

Palermo, E. 2014. *10 Worst Data Breaches of All Time. Privacy Risk Advisors*. Available at: https://www.privacyrisksadvisors.com/news/a10-worst-data-breaches-of-all-time-by-elizabeth-palermo/

Public Company Accounting Oversight Board (PCAOB). 2007. *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements. PCAOB Auditing Standard No. 2201*. Available at: https://pcaobus.org/Standards/Auditing/Pages/default.aspx

Public Company Accounting Oversight Board (PCAOB). 2010. *Identifying and Assessing Risks of Material Misstatement. PCAOB Auditing Standard No. 2110*. Available at: https://pcaobus.org/Standards/Auditing/Pages/default.aspx

Public Company Accounting Oversight Board (PCAOB). 2012. *Communications with Audit Committees. PCAOB Auditing Standard No.1301*. Available at: https://pcaobus.org/Standards/Auditing/Pages/default.aspx

Public Company Accounting Oversight Board (PCAOB). 2013. *Auditing Supplemental Information Accompanying Audited Financial Statements. PCAOB Auditing Standard No. 2701*. Available at: https://pcaobus.org/Standards/Auditing/Pages/default.aspx

Ragan, S. 2014. *What You Need to Know About the Home Depot Data Breach*. Available at: https://www.csoonline.com/article/2604320/data-protection/what-you-need-to-know-about-the-home-depot-data-breach.html

Rubin, G. 2019. Many company hacks go undisclosed to SEC despite regulator efforts. *Wall Street Journal* (February 26).

Securities and Exchange Commission (SEC). 2018. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures Release Nos. 33-10459; 34-82746*. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

Wang, T., K. N. Kannan, and J. R. Ulmer. 2013. The association between the disclosure and the realization of information security risk factors. *Information Systems Research* 24 (2): 201–218. https://doi.org/10.1287/isre.1120.0437