Academic Research on the Role of Corporate Governance and IT Expertise in Addressing Cybersecurity Breaches: Implications for Practice, Policy, and Research

Caroline C. Hartmann  
*Texas A&M University–Commerce*

Jimmy Carmenate  
*Florida International University*

**SUMMARY:** Frequent cyber-attacks on organizations in the last decade have caught the attention of practitioners and governance bodies, who have called for boards to take a more active role in managing and preventing future cyber risks. Governance surveys, however, find that boards are not sufficiently prepared to address cybersecurity risks due to a lack of IT expertise. Firms have begun appointing technology experts, creating board-level technology (IT) committees and delegating responsibilities to the audit committee as a means of managing cybersecurity risk. With the aim of understanding the current and future role of governance mechanisms in managing cybersecurity risks, this paper reviews the existing cybersecurity guidelines and regulations, and summarizes the empirical research related to corporate governance, security breaches, and IT expertise in overseeing cyber risks. Finally, we discuss implications for practice, policy, and researchers.

**Keywords:** cybersecurity; security breaches; information technology; corporate governance; board of directors; board IT expertise; CEO IT expertise; audit committee.

Caroline C. Hartmann, Texas A&M University–Commerce, Department of Accounting, Commerce, TX, USA; Jimmy Carmenate, Florida International University, College of Business, School of Accounting, Miami, FL, USA.

Editor’s note: Accepted by Denise Dickins.

Submitted: November 2020  
Accepted: April 2021  
Published Online: April 2021
I. INTRODUCTION

Cyber-attacks have been a concern for organizations since the early 21st century when Commissioner Luis Aguilar of the Securities and Exchange Commission (SEC) raised public awareness about the consequences of cyber-attacks. In a speech at the Cyber Risk and Boardroom Conference on June 10, 2014 (Aguilar 2014), he stressed the importance of cybersecurity being a critical part of the board of directors’ risk oversight responsibilities and the risks associated with not being adequately prepared to address them. Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company’s cybersecurity measures needs to be a critical part of a board of director’s risk oversight responsibilities. (Aguilar 2014, 3)

In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and lasting reputational harm, there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats. Thus, boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril. (Aguilar 2014, 4)

Since Commissioner Aguilar’s speech, major breaches of proprietary information have become increasingly common, with companies falling victim to theft of financial assets and intellectual property and, in some cases, sabotage. In 2019, the number of data breaches reached 1,473, with over 164.68 million sensitive records exposed (Clement 2020), while the financial impact to businesses has been substantial. On average, $17,700 is lost every minute due to phishing attacks, and data breaches cost businesses an average of $3.92 million (CSO 2020), with the cost of cyber-crime expected to grow to more than $6 trillion annually by 2021 (Herjavec Group 2017).

The increased cyber-attacks and security risks have caught the attention of stakeholders, practitioners, and governance bodies, who have called for boards to take a more active role in providing comprehensive oversight of these cyber risks (NACD 2020; SEC 2018). In a meeting on March 13, 2019, the National Association of Corporate Directors (NACD) Risk Oversight Advisory Council recommended organizations assess their cybersecurity strategy and evaluate whether they have the necessary IT expertise and talent to fulfill their risk oversight responsibilities (NACD 2019).

Governance surveys, however, find that boards are not sufficiently prepared to address cybersecurity risks or still have dated views about what cybersecurity is. A panel discussion by the NACD cited an “IT confidence gap,” indicating that most directors are in their 60s, grew up in a pre-digital environment, and become overwhelmed by the technical jargon used in the digital era today (NACD 2012). Recently, 77 percent of organizations surveyed operate with limited cybersecurity, and 87 percent do not have sufficient resources or a plan in place to provide the level of cybersecurity needed to prevent a cyber breach (EY 2018).

In order to address the risks and costs associated with security breaches, and recognizing the importance of having IT expertise in the boardroom, companies have begun appointing technology experts to the board or creating board-level technology committees to help oversee cybersecurity, digital disruptions, and complex technology issues (Higgs, Pinsker, Smith, and Young 2016). In other situations, cybersecurity oversight and IT responsibilities have been assigned to the audit...
committee or a separate risk committee (EY 2020). Moreover, organizations are taking a good look at their governance structure to ensure they have skilled senior management (i.e., CEO and CFO with IT expertise, CIO) that prioritize information security and risk management as part of the organization’s strategic agenda (Lipton, Neff, and Brownstein 2019).

To date, cyber-attacks continue to increase and the success of governing bodies in addressing cybersecurity risks and security breaches is relatively unknown.¹ Although there are studies related to cybersecurity that provide research summaries in the areas of (1) cybersecurity disclosures, (2) cybersecurity investment, (3) economic consequences to cybersecurity incidents, and (4) manager and auditor responses to cybersecurity risks (Haapamäki and Sihvonen 2019; Richardson, Smith, and Weidenmier Watson 2019; Walton, Wheeler, Zhang, and Zhao 2021; Wilkin and Chenhall 2020), the role of IT as a governance tool to combat cyber-attacks has not been fully explored. With the aim of understanding the current and future role of governance mechanisms in managing cybersecurity risks, this paper reviews the existing cybersecurity guidelines and regulations, and summarizes the empirical research related to corporate governance, security breaches, and IT expertise in overseeing cyber risks, using a combination of words to search for relevant studies published in top peer-reviewed journals.² Finally, we discuss implications for practice, policy, and researchers.

II. BACKGROUND ON DATA PRIVACY AND CYBERSECURITY

Cybersecurity and data privacy are ranked third among key strategic risks cited by more than 60 institutional investors representing more than $35 trillion assets under management (EY 2020). The rapid growth in cyber-crime has led regulators worldwide to introduce legislation to protect consumer data and privacy. The General Data Protection Regulation (GDPR) of 2016 is the most comprehensive data privacy law in the European Union (EU) that regulates the protection of personal data of EU consumers as well as companies outside of the EU who serve EU residents. The law addresses how data are collected, processed, and stored and requires businesses to report data security breaches to national authorities within 72 hours of a breach if it has a material effect on user privacy (Sebastian 2019). Fines and penalties for not complying with this regulation can be quite costly. This directive has served as a model for similar laws passed in foreign countries and the 2018 California Consumer Privacy Act (CCPA) that took effect on January 1, 2020.

¹ Research on cybersecurity has mainly focused on information sharing, investments in cybersecurity, the role of internal audit, disclosure of cybersecurity activities, and effects of security breaches. Please refer to Haapamäki and Sihvonen (2019), Richardson et al. (2019), Walton et al. (2021), and Wilkin and Chenhall (2020) for a comprehensive review of these topics.

² Words used to search for relevant studies included cybersecurity, information security, cyber-attack, information breach, security breach, cyber threats, board of directors, audit committee, management, Chief Information Officer/CIO, Chief Financial Officer/CFO, and Chief Executive Officer/CEO. A search was performed using Google Scholar and ABI/Inform Global as well as manually examining peer-reviewed journals related to corporate governance and information systems in the accounting, finance, MIS, and business fields from 2000 to 2021. Among the many outlets reviewed for articles were the following journals: The Accounting Review; Journal of Accounting Research; Journal of Accounting and Economics; Review of Accounting Studies; Contemporary Accounting Research; Accounting, Organizations and Society; Accounting Horizons; Auditing: A Journal of Practice and Theory; Current Issues in Auditing; Journal of Accounting & Public Policy; Managerial Auditing Journal; International Journal of Accounting Information Systems; Journal of Information Systems; and Information Systems Research. The majority of articles identified were published in the Journal of Information Systems, International Journal of Accounting Information Systems, and Managerial Auditing Journal.
2020, in the U.S. Similar to the GDPR, the CCPA’s main focus is to allow California residents more control over the collection and disclosure of personal information and requires businesses to disclose security breaches related to stolen personal information (Becerra 2020).

In the U.S., a few federal regulations requiring disclosure of cybersecurity risks have been introduced; however, none of these rulings offer guidance on how organizations should address the risk associated with security breaches. Three bills introduced between 1996 and 2002 control the protection of systems and information in the healthcare industry, financial institutions, and federal agencies (CSO 2021).3 Four additional bills have successfully passed both chambers of Congress but unfortunately only address the sharing of information about cybersecurity threats between the U.S. government, technology companies, and health insurance providers (Coranet 2018).4

In 2011, the SEC issued guidance to public companies regarding disclosure of cybersecurity risks (SEC 2011); however, since it was simply a guidance and did not require companies to comply, the effort had little impact. Subsequently in 2018, the SEC passed additional interpretive guidance emphasizing companies’ obligations to disclose cybersecurity risks, material breaches, and the potential impact of these breaches on business, finance, and operations. It prompts companies to disclose cybersecurity procedures and the board’s role and engagement in cyber-risk oversight (SEC 2018).

Of late, policymakers have introduced the Cybersecurity Disclosure Act of 2019. This proposal was approved by the House Financial Services Committee in December 2019 and is currently pending in Congress (CBO 2020, H.R. 1731). This bill would direct the SEC to issue final rulings requiring registered public companies to disclose on their annual report or proxy statement whether any board member has expertise or experience in cybersecurity. If no member has such expertise or experience, public companies would need to discuss what other cybersecurity aspects or plans were considered in evaluating director qualifications. The main reason for this bill is the lack of IT expertise among directors to effectively oversee cybersecurity risks (EY 2018).

In summary, the regulations and guidelines proffered by policymakers have focused primarily on making organizations accountable for disclosing cyber-attacks and the consequences of these attacks, with very little guidance on how firms can address current and future cybersecurity breaches and be prepared to confront the ever-changing technological landscape.

III. CORPORATE GOVERNANCE AND CYBERSECURITY RESEARCH

The Role of the Board in Cybersecurity Risk Oversight

The SEC considers risk oversight to be a primary responsibility of the board and requires organizations to disclose their role in overseeing risks that could disrupt and materially impact an organization’s business strategy (SEC 2009). Disclosures include whether the entire board is involved in risk oversight, whether certain board committees are involved, and whether employees responsible for risk management report to the board. Boards generally oversee the risk

---

3 The initial three bills introduced were the 1996 Health Insurance Portability and Accountability Act, the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act.

4 These four bills include the Cybersecurity Enhancement Act of 2014, Cybersecurity Information Sharing Act of 2015, Federal Exchange Data Breach Notification Act of 2015, and the National Cybersecurity Protection Advancement Act of 2015.
management process by assigning risk responsibilities to various board committees and the audit
committee (Bujno et al. 2018).

Similarly, organizations have changed their approach to better address the risks and costs associated with security breaches. In some companies, cybersecurity is managed at the board level and is not delegated to a separate committee. This approach is beneficial when board members have knowledge in the areas of IT, systems implementation, and technology transformation (KPMG 2016). Firms have begun appointing technology experts and creating board-level technology (IT) committees to help the board manage its IT and cybersecurity risk oversight responsibilities. The benefit of this committee is that IT experts can educate the rest of the board on cybersecurity risks (Kickenweiz, Sedlock, and Daum 2016). This practice has resulted in the number of technology board committees among public companies having grown from 10 to 17 percent between 2010 and 2016 and it continues to increase each year (Kark, Lewis, and Brown 2017). In other situations, the board may delegate oversight of cyber risks to the audit committee or a separate risk committee. Regardless of whether the board or a specific committee is responsible for overseeing cybersecurity risks, the main objective is for an organization to have an integrated approach to preparing, protecting, detecting, and responding to cyber incidents (KPMG 2016).

A recent examination performed on 76 Fortune 100 companies’ cybersecurity disclosures in proxy statements and 10-K filings between 2018 and May 31, 2020 (EY 2020), reveals that most companies are enhancing their cybersecurity disclosures in their 10-K filings (as required by the SEC [2018] guidelines) and that they vary in their choice of selecting the committee that is assigned cybersecurity oversight responsibilities. The study finds that 87 percent of the companies surveyed assigned oversight of cybersecurity to a board-level IT committee while 67 percent assigned it to the audit committee. Only 26 percent of the companies assigned cybersecurity oversight to IT or risk committees. Interestingly, very few companies provided information on the Form 10-K as to their cyber-readiness practices (simulations and use of third-party advisors) and 37 percent of companies are increasingly seeking to retain directors with IT and cybersecurity expertise (EY 2020).

We identified three studies investigating the relationship between board of directors’ characteristics, board-level IT committees and cybersecurity, and one study that examined board IT expertise and IT risk management practices. As presented in Table 1, Hsu and Wang (2014) examine the composition of the board and find that larger boards, boards with older directors, and longer tenure are associated with a lower likelihood of security breaches, while boards with a greater percentage of independent directors are positively associated with breaches. They reason that outside directors may not have enough internal knowledge of the company to contribute to a reduction in the likelihood of breaches.

Higgs et al. (2016) are the first to examine the relation between board-level IT committees and the likelihood of firms reporting security breaches. They find that firms with a board IT committee are more likely to report breaches than firms without these committees. Additionally, firms with more mature IT committees are less likely to report a breach, implying that more established technology committees help mitigate or prevent security breaches. When examining the type of breach, the authors find IT board committees are positively associated with disclosure of external breaches while risk and compliance committees are positively associated with the disclosure of internal breaches.

A third study by Lending, Minnick, and Schorno (2018) finds that firms that have experienced a breach have larger boards with less financial expertise, and subsequently make governance changes to mitigate future breaches. These include decreasing the size of the board to reduce
| Article                      | Type of Board Characteristic | Sample Period/Number of Participants | Measure               | Results                                                                                       |
|-----------------------------|------------------------------|--------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------|
| Hsu and Wang 2014           | • Board size                 | 1997–2009 32,470 executive year event observations | Security breach       | • Larger boards are negatively associated with breaches                                       |
|                             | • Percentage of independent directors |                             |                       | • Percentage of independent directors is positively associated with breaches                   |
|                             | • Average age of directors   |                             |                       | • The older the director, the less likelihood of a breach                                       |
|                             | • Tenure of directors        |                             |                       | • The greater the tenure of the director, the less likelihood of a breach                      |
| Higgs et al. 2016           | • Board IT Committee         | 2005–2014 281 breach year observations | Internal breaches     | • Firms with IT committees are more likely to disclose breaches than firms without IT committees |
|                             | • Compliance Committee       |                             | External breaches     | • External breaches occur more frequently for firms with IT board committees                  |
|                             | • Risk Committee             |                             |                       | • Internal breaches occur for firms with risk and compliance committees                        |
|                             |                              |                             |                       | • More mature IT committees are less likely to report a breach                                |
| Lending et al. 2018         | • Changes in Board Composition | 2004–2012 271 breaches        | Security breach       | • Firms that have experienced a breach have larger boards with less financial expertise       |
|                             | • Financial Expertise        |                             |                       | • These firms subsequently decrease the size of the board to reduce entrenchment, and replace the CEO and Chief Technology Officer |
|                             | • Size of the Board          |                             |                       |                                                                                               |
| Vincent et al. 2019         | • Board IT Involvement       | 215 IT professionals          | Maturity of IT risk management practices | • Board involvement is positively associated with maturity of IT risk practices                |
|                             | • Board IT Expertise         |                             |                       | • Board IT expertise is positively associated with maturity of risk practices                  |
|                             | • Management Risk Attitude   |                             |                       | • Management risk-taking behavior is negatively associated with the level of maturity of IT risk practices |
entrenchment and replacing the CEO and Chief Technology Officer. A recent study by Vincent, Higgs, and Pinsker (2019) examines how board involvement, board IT expertise, and management’s risk attitude affect the maturity of IT risk management practices. They find that management’s risk-taking behavior is negatively associated with the maturity of IT systems, indicating that risky behavior could have negative consequences on an organization’s ability to manage IT risks. Additionally, board involvement and board IT expertise seem to enhance the level of maturity of an organization’s risk management practices, thereby mitigating management’s risk-taking behavior.

Audit Committee Involvement in Cybersecurity Oversight

While the board is primarily responsible for risk oversight, the New York Stock Exchange (NYSE) Final Corporate Governance Rules call for the audit committee to discuss guidelines and policies with respect to risk assessment and risk management, and to discuss an entity’s major financial risk exposures (NYSE 2003, §303A.07d). In that capacity, the audit committee is responsible for reviewing the guidelines and policies that govern the process by which risk assessment is undertaken. As cybersecurity risks have increased in the last decade, audit committees have extended their risk disclosure activities to being more involved in managing cybersecurity risks, as evidenced by the fact that 67 percent of organizations surveyed in 2020 have assigned this risk responsibility to the audit committee (EY 2020). This move is not surprising since audit committees are already responsible for overseeing the effectiveness of the organization’s IT function and internal controls system, and cybersecurity risk is one component of the IT function.

Our literature review identified two studies examining the audit committee’s IT responsibilities and one study exploring the role of the audit committee when breach incidents occur. As presented in Table 2, Hadden and Hermanson (2003) initially explore whether the audit committee should have a role in addressing IT risks as part of their focus on organizational risks given the important risks associated with reliance on IT systems. They find that 55 percent of the companies surveyed formally charged the audit committee with overseeing both IT risks and management’s action plans related to IT. A subsequent study by Hadden, Hermanson, and DeZoort (2003) further explored the IT activities audit committees were involved in. Using a survey approach, they find that audit committees’ involvement with oversight of IT risks was very limited; in the cases where the audit committee was involved, the directors had auditing experience or familiarity with the COBIT model for assessing IT risks, suggesting IT literacy was important.

A more recent study by Lankton, Price, and Karim (2020) is the first to examine the oversight role of the audit committee in relation to cybersecurity breaches. Using a sample of 189 Fortune 500 firms that had breach incidents from 2005 to 2017, they review the audit committee charters in proxy statements to identify the types of cybersecurity responsibilities assigned to the audit committee. They find a negative association between prior breaches and the inclusion of IT governance roles in the audit committee charter, suggesting that audit committees do not assume primary responsibility for cybersecurity oversight. When organizations have a board-level IT committee in place and a breach occurs, they find firms subsequently assign IT risk responsibilities to the audit committee as another layer of oversight. Last, firms with few or no data breaches were

---

5 Financial companies and certain nonbank financial companies are required to have dedicated risk committees as required by the Dodd-Frank Act of 2010. Other industries may choose to have separate risk committees, the board, or the audit committee oversee risk management.
| Article | Audit Committee (AC)/Other Variables | Sample Period/Number of Participants | Measure | Results |
|---------|-------------------------------------|-------------------------------------|---------|---------|
| Hadden and Hermanson 2003 | Audit committee members | 50 responses | AC involvement in IT risk oversight | • 55 percent of organizations surveyed charge the audit committee with overseeing IT risks <br> • 8 percent of organizations surveyed make other board committees accountable for IT risk oversight |
| Hadden et al. 2003 | Audit committee members | 39 audit committee members | Types of IT risk oversight | • Limited involvement of audit committee in IT risk oversight <br> • Directors involved in IT risk oversight had previous auditing experience and familiarity with COBIT risk model |
| Lankton et al. 2020 | • Audit committee charters<br> • Board IT committees | 2005–2017 189 firms with security breaches | Security breach | • There is a negative association between the occurrence of a prior breach and the inclusion of IT risk responsibilities in the AC charter <br> • When an organization has a board-level IT committee and a breach occurs, the organization subsequently assigns IT risk responsibilities to the AC <br> • Firms with few or no security breaches were more likely to have assigned IT risk responsibilities in the AC charter |
more likely to have disclosed IT responsibilities in the audit committee charter, implying that audit committees may be more involved in the prevention of cybersecurity risks.

### Management Involvement in Cybersecurity Risks

The CEO and senior management (CFO and CIO) are responsible for overseeing firm-wide IT policies and strategies that include assessing and mitigating security breaches (Haislip, Lim, and Pinsker 2017). Research on the role of senior management in IT governance and information security management has mostly focused on the importance of top management and managerial perceptions on the effectiveness of security systems (Kankanhalli, Teo, Tan, and Wei 2003), CIO characteristics (Feeny and Wilcocks 1998), and the role of internal audit in improving IT effectiveness (Islam, Farah, and Stafford 2018), with very little information on the role management plays in addressing cybersecurity risks. There are a limited number of studies on the CIO, CEO, and CFO’s role in assuming cybersecurity responsibilities.

As presented in Table 3, Kwon, Ulmer, and Wang (2013) and Zafar, Ko, and Osei-Bryson (2016) examine the association between the existence of IT executives (CIO, Chief Security Officer, VP of IT) within the top management team and the occurrence of security breaches. Kwon et al. (2013) find that the existence of an IT executive among the management team is associated with a reduction in the likelihood of a security breach and that behavior-based compensation (salary) is negatively related to the possibility of a breach by motivating IT executives to increase security management. In contrast, outcome-based compensation (bonuses, stock awards, and stock options) has the opposite effect. Zafar et al. (2016) further support this viewpoint as they find that the presence of a CIO within the top management team is positively associated with firms being better prepared to respond to security breaches, which impacts firm performance.

Feng and Wang (2019) subsequently examine whether the risk appetite of the CIO affects the likelihood of a security breach and find when the CIO is risk averse, organizations are less likely to experience a security breach. Interestingly, the CEO’s level of risk aversion moderates this relationship, such that risk-averse CIOs are able to minimize the probability of a breach only when the CEO is also risk averse. When investigating the type of breach, CIOs were more likely to deter internal and non-hack incidents but faced a challenge in handling threats and breaches that occurred from outside the firm. Last, Banker and Feng (2019) examine the relationship between security breaches, the type of breach, and CIO turnover since a security breach is a visible sign of IT performance failure for which CIOs are directly responsible. They find that firms with a system deficiency security breach tend to experience more CIO turnovers and may also lead to CEO turnover.

Research on CEOs with IT expertise suggest that a CEO with IT knowledge is more likely to be involved in procuring IT systems and ensuring they align with the firm’s strategic objectives (Armstrong and Sambamurthy 1999; Bassellier, Benbasat, and Reich 2003; Jarvenpaa and Ives 1991). Furthermore, Haislip and Richardson (2018) find that CEOs with IT expertise enhance the information environment resulting in more accurate earnings forecasts, while Haislip, Karim, Lin, and Pinsker (2020) find that CEOs with IT expertise disclose more timely filings. In line with the positive findings related to CEO IT expertise, our review identified a recent study by Haislip et al. (2017), which is the first to examine the role of IT expertise among senior management (CFO and CEO) with regards to security breaches. Using a sample of 127 firms with reported breaches over the period 2005 to 2013, they find that CEOs with IT expertise are positively associated with breaches, suggesting they are more likely to detect and report security breaches. CFOs with IT expertise are negatively associated with security breaches, implying that they are more likely to
| Article                          | Type of IT Expertise/Other Variables | Measure       | Sample Period | Sample Size | Results                                                                                                                                                                                                 |
|---------------------------------|--------------------------------------|---------------|---------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kwon et al. 2013                | IT Executive involvement             | Security breach | 2003–2008     | 242 firms with breaches | - Existence of IT executive on management team is associated with a reduction in the likelihood of a breach  
- Behavior-based (salary) compensation of IT executive is associated with a reduction in the likelihood of a breach  
- Outcome-based (bonus, stock awards, stock options) compensation is associated with a greater likelihood of a breach |
| Zafar et al. 2016               | CIO in Top Management Team           | Firm performance | 2000–2010     | 439 breached firms with IT executive | - A firm is better prepared to respond to a security breach when the CIO is part of the top management team  
- Confidentiality type breaches are impacted the most by the presence of a CIO on the top management team |
| Haislip et al. 2017             | CEO IT Expertise, CFO IT Expertise, Presence of CIO | Security breach | 2005–2014     | 265 breached firms and non-breached firms | - CEOs with IT expertise are positively associated with breaches  
- CFOs with IT expertise are negatively associated with security breaches  
- Firms who have an IT board committee are more likely to detect and report security breaches even when the firm has a CEO or CFO with IT expertise |
| Article                  | Type of IT Expertise/Other Variables                                                                 | Sample Period          | Measure        | Results                                                                                                                                 |
|-------------------------|-----------------------------------------------------------------------------------------------------|------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Banker and Feng 2019    | • System deficiency breaches<br>• Human error breaches<br>• Criminal fraud breaches                  | 2008–2016<br>348 firms with 314 turnovers | CIO turnover   | • Firms with system deficiency breaches experience more CIO turnovers<br>• Results for human error and criminal fraud related breaches and CIO turnover were not statistically significant |
| Feng and Wang 2019      | • CIO risk aversion<br>• CEO risk aversion                                                          | 2003–2015<br>360 firms with 1,142 firm-year observations | Security breach | • CIO risk aversion is negatively associated with the likelihood of security breaches<br>• CIO risk aversion is negatively related to internal breaches<br>• CIO risk aversion is positively related to external breaches |
prevent security breaches. Last, they find that firms that have an IT board committee are more likely to detect and report security breaches, even when the firm has a CEO or CFO with IT expertise.

IV. IMPLICATIONS FOR PRACTICE, POLICY, AND RESEARCH

Implications for Practice and Policy

Our review of academic studies related to the board and various committees reveals that boards continue to struggle with having the necessary IT expertise to oversee security breaches. The creation of board-level IT committees seems to improve IT oversight by the board as they serve as a link between the board and management and relieve some of the pressure faced by boards (Kark et al. 2017). Firms with an IT board committee are more likely to disclose the occurrence of cyber-attacks while more mature IT committees may have the ability to mitigate these incidents due to their experience and expertise (Higgs et al. 2016).Audit committees are becoming more involved by serving as an additional layer of protection/oversight when a breach has occurred, and an IT committee is already in place. They also seem to be more adept at managing cybersecurity risks due to their existing IT oversight role (Lankton et al. 2020). These findings have implications for practice as they suggest that IT boards and audit committees have different objectives. The IT committees seem to fulfill the role of disclosing breaches while the audit committee of mitigating or preventing cyber breaches. Organizations should therefore carefully consider their cybersecurity environment and specific needs in deciding which committee should assume responsibility of cybersecurity risks.

Our examination of studies related to the CIO and CEO reveal that senior management continues to be held accountable for the daily oversight of internal controls, IT systems, as well as ensuring strategic technology-related goals are met. When security breaches occur that are related to system deficiencies, CIOs suffer the consequences by experiencing turnover (Banker and Feng 2019). Firms need to hire CIOs who are knowledgeable and conservative in their approach to adapting to technological changes while ensuring they have the most up-to-date IT systems to curb security breaches. Since the CEO’s risk appetite has the ability to influence the CIO’s behavior (Feng and Wang 2019), it is important that the CIO and CEO be properly aligned in their view of fighting cybersecurity if they are to be effective.

Our summary also highlights that IT expertise is a necessary characteristic for the board to perform its fiduciary IT oversight responsibilities, especially those related to cybersecurity risks. Firms continue to seek directors with IT and cybersecurity expertise to help create cyber defense strategies that will permit firms to manage the occurrence of cybersecurity breaches and quickly and successfully adapt to technological disruptions (EY 2020). Ultimately, organizations may want to consider retaining younger and more tech savvy directors with IT or cybersecurity experience on the board as a means to ensure that the board is well prepared to manage its IT related fiduciary responsibilities.

From a policy perspective, regulatory bodies need to consider whether IT expertise, and perhaps even cybersecurity expertise on the board, or as a separate IT committee, should be required as a means to manage cybersecurity risks. Currently, the SEC requires public companies to have at least one financial expert on the audit committee but is silent as to other types of expertise. Policymakers have already signaled that cybersecurity expertise/experience is needed as reflected by passage of the Cybersecurity Act of 2019; however, this ruling only applies to disclosure of members with this type of expertise and does not require public companies to hire
cybersecurity experts to the board. Requiring IT and/or cybersecurity experts may thereby help strengthen the IT environment within organizations and provide directors with the necessary tools to manage cybersecurity strategies and prevent future breaches.

**Implications for Researchers**

Research on cybersecurity and the role of corporate governance is in its infancy. Although recent studies have appeared on cybersecurity disclosures, impact of security breaches, and auditor responses to security breaches, the role of corporate governance and IT expertise to combat cyber-attacks has not been fully explored. Our literature review provides evidence that board IT committees, management teams with IT expertise, and audit committees can play an active role in mitigating security breaches. A recent survey reveals that 67 percent of organizations delegate cybersecurity matters to the audit committee (EY 2020); however, their involvement and impact in mitigating security breaches may not be salient since these responsibilities may not be documented in the charter. We encourage researchers to further explore the role of the audit committee in the cybersecurity arena, especially since they are already responsible for oversight of IT risks.

Findings related to the type of security breach (external and internal) reveal that various mechanisms are at play in attempting to manage the variety of breaches. Results show that IT board committees are positively associated with the disclosure of external breaches while risk committees with disclosure of internal breaches (Higgs et al. 2016). At the management level, CIOs are able to respond to internal and non-hack breaches but have a difficult time addressing external breaches (Feng and Wang 2019). Further research is needed to understand how firms can better address and prevent the various types of breaches that affect organizations.

Last, given that many boards have a scarce pool of IT and cybersecurity experts, and the creation of IT committees is voluntary, we encourage future scholars to continue to examine how IT expertise and cybersecurity expertise at the board level and audit committee level can assist organizations in addressing future cybersecurity risks.

**REFERENCES**

Aguilar, L.A. 2014. *Board of Directors Corporate Governance and Cyber-Risks: Sharpening the Focus*. Cyber Risks in the Boardroom Conference, New York Stock Exchange (June 10). New York, NY: SEC. Available at: https://www.sec.gov/news/speech/2014-spch061014laa

Armstrong, C., and V. Sambamurthy. 1999. Information technology assimilation in firms: The influence of senior leadership and IT infrastructure. *Information Systems Research* 10 (4): 304–327. https://doi.org/10.1287/isre.10.4.304

Banker, R. D., and C. Feng. 2019. The impact of information security breach incidents on CIO turnover. *Journal of Information Systems* 33 (3): 309–329. https://doi.org/10.2308/isys-52532

Bassellier, G., I. Benbasat, and H. Reich. 2003. The influence of business managers’ IT competence on championing IT. *Information Systems Research* 14 (4): 317–336. https://doi.org/10.1287/isre.14.4.317.24899

Becerra, X. 2020. *California Consumer Privacy Act (CCPA)*. Xavier Becerra Attorney General. Sacramento, CA: California Department of Justice. Available at: https://oag.ca.gov/privacy/ccpa

Bujno, M., C. Hitchcock, K. Parson, B. Lamm, D. DeHass, and H. Phillips. 2018. Risk oversight and the role of the board. *Deloitte* (October 2). Available at: https://deloitte.wsj.com/riskandcompliance/2018/10/02/risk-oversight-and-the-role-of-the-board/

Clement, J. 2020. *Cyber crime: Number of breaches and records exposed 2005–2019* (March 10). Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
Congressional Budget Office (CBO). 2020. *H.R. 1731, Cybersecurity Act of 2019* (February 20). Washington, DC: CBO. Available at: https://www.cbo.gov/publication/56181

Coranet. 2018. *Federal cybersecurity regulations* (July 10). New York, NY: Coranet. Available at: https://www.coranet.com/federal-cybersecurity-regulations/

CBO. 2020. *Top cybersecurity facts, figures, and statistics for 2020*. Available at: https://www.cbo.gov/publication/53157

CSO. 2020. *Top cybersecurity facts, figures, and statistics for 2020*. Available at: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

CSO. 2021. *The Security laws, regulations and guidelines directory* (December 19). Available at: https://www.csoonline.com/article/2126072/compliance-the-security-laws-regulations-and-guidelines-directory.html

EY. 2018. *Global Information Security Survey: Five key health-sector findings* (January 24). Available at: https://www.ey.com/en_gl/giss

EY. 2020. *What companies are disclosing about cybersecurity risk and oversight in 2020*. EY Center for Board Matters. Available at: https://ey.com/us/boardmatters

Feeny, D., and L. Wilcocks. 1998. Core IS capabilities for exploiting information technology. *Sloan Management Review* 39 (3): 9–21.

Feng, C., and T. Wang. 2019. Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems* 32: 59–75. https://doi.org/10.1016/j.accinf.2018.11.001

Haapamäki, E., and J. Silvonen. 2019. Cybersecurity in accounting research. *Managerial Auditing Journal* 34 (7): 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Hadden, L. B., and D. R. Hermanson. 2003. Is your audit committee watching IT risks? *Journal of Corporate Accounting & Finance*. https://doi.org/10.1002/jcaf.10181

Hadden, L. B., D. R. Hermanson, and F. T. DeZoort. 2003. Audit committee’s oversight of information technology risk. *Review of Business Information Systems*. 7 (4): 1–12. https://doi.org/10.19030/rbis.v7i4.4509

Haislip, J. Z., and V. J. Richardson. 2018. The effect of CEO IT expertise on the information environment: Evidence from earnings forecasts and announcements. *Journal of Information Systems* 32 (2): 71–94. https://doi.org/10.2038/isys-51796

Haislip, J., J. Lim, and R. Pinsker. 2017. *Do the Roles of the CEO and CFO Differ When It Comes to Data Security Breaches?* 23rd Americas Conference on Information Systems, Boston, MA, August 10–12.

Haislip, J. Z., K. E. Karim, K. Lin, and R. E. Pinsker. 2020. The influences of CEO IT expertise and board-level technology committees on Form 8-K disclosure timeliness. *Journal of Information Systems* 34 (2): 167–185. https://doi.org/10.2308/isys-52530

Herjavec Group. 2017. *2017 Cybercrime Report*. Available at: https://www.wlrk.com/docs/2017CCybercimereport.pdf (last accessed May 30, 2020).

Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems* 30 (3): 79–98. https://doi.org/10.2308/isys-51402

Hsu, C., and T. Wang. 2014. Exploring the association between board structure and information security breaches. *Asia Pacific Journal of Information Systems*. 24 (4): 531–557. https://dx.doi.org/10.14329/apjis.2014.24.4.531

Islam, M. S., N. Farah, and T. S. Stafford. 2018. Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal* 33 (4): 377–409. https://doi.org/10.1108/MAJ-07-2017-1595

Jarvenpaa, S., and B. Ives. 1991. Executive involvement and participation in the management of information technology. *Management Information Systems Quarterly* 15 (2): 205–227. https://doi.org/10.2307/249382

Kankanhalli, A., H. H. Teo, B. C. Tan, and K.-K. Wei. 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management* 23 (2): 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kark, K., J. Lewis, and C. Brown. 2017. Bridging the boardroom’s technology gap. *CIO Insider*. New York, NY: Deloitte University Press. Available at: https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/bridging-boardroom-technology-gap.html

Kickenweiz, B., G. Sedlock, and J.H. Daum. 2016. *Technology in the boardroom: Five things directors should be thinking about* (March). New York, NY: SpencerStuart. Available at: https://www.spencerstuart.com/research-and-insight/technology-in-the-boardroom-five-things-directors-should-be-thinking-about

KPMG. 2016. *Audit point of view. Cyber security is a critical audit committee issue*. Amstelveen, The Netherlands: KPMG. Available at: https://assets.kpmg/content/dam/kpmg/ca/pdf/2016/08/ca-cyber-security-is-a-critical-audit.pdf
Kwon, J., J. R. Ulmer, and T. Wang. 2013. The association between top management involvement and compensation and information security breaches. *Journal of Information Systems* 27 (1): 219–236. https://doi.org/10.2308/isys-50339

Lankton, N., J. B. Price, and M. Karim. 2020. Cybersecurity breaches and information technology governance roles in audit committee charters. *Journal of Information Systems* 35 (1): 101–119. https://doi.org/10.2308/isys-18-071

Lending, C., K. Minnick, and P. J. Schorno. 2018. Corporate governance, social responsibility, and data breaches. *Financial Review* 53 (2): 413–455. https://doi.org/10.1111/fire.12160

Lipton, M., D.A. Neff, and A.R. Brownstein. 2019. Risk management and the board of directors. *Harvard Law School Forum on Corporate Governance* (November 20). Cambridge, MA: Harvard Law School. Available at: https://corpgov.law.harvard.edu/2019/11/20/risk-management-and-the-board-of-directors-7/

National Association of Corporate Directors (NACD). 2012. Cybersecurity and the Board. *NACD Board Leadership Conference* (October 15). Arlington, VA: NACD.

National Association of Corporate Directors (NACD). 2019. 2019–2020 NACD Public Company Governance Survey. *The Current State of the American Boardroom*. Arlington, VA: NACD. Available at: https://www.nacdonline.org/analytics/survey.cfm?ItemNumber=66753

National Association of Corporate Directors (NACD). 2020. Cyber-Risk Oversight 2020. Key Principles and Practical Guidance for Corporate Boards. Arlington, VA: NACD. Available at: https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298

New York Stock Exchange (NYSE). 2003. *Final NYSE corporate governance rules*. Section 3030A. New York, NY: NYSE. Available at: https://ecgi.global/code/final-nyse-corporate-governance-rules

Richardson, V., R. E. Smith, and M. Weidenmier Watson. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems* 33 (3): 227–265. https://doi.org/10.2308/isys-52379

Sebastian, F. 2019. *GDPR in the US: Requirements for US companies* (June 21). Available at: https://termly.io/resources/articles/gdpr-in-the-us/

Securities and Exchange Commission (SEC). 2009. *Proxy disclosure enhancements*. 17 CFR PARTS 229, 239, 240, 249 and 274. Release Nos. 33-9089; 34-61175; IC-29092; File No. S7-13-09. RIN 3235-AK28. Available at: https://www.sec.gov/rules/final/2009/33-9089.pdf

Securities and Exchange Commission (SEC). 2011. *CF Disclosure Guidance: Topic No. 2. Cybersecurity* (October 13). Washington, DC: SEC. Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities and Exchange Commission (SEC). 2018. *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. Release Nos. 33-10459, 34-87246 (February 26). Washington, DC: SEC. Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

Vincent, N. E., J. L. Higgs, and R. E. Pinsker. 2019. Board and management-level factors affecting the maturity of IT risk management practices. *Journal of Information Systems* 33 (3): 117–135. https://doi.org/10.2308/isys-52229

Walton, S., P. Wheeler, Y. Zhang, and X. Zhao. 2021. An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems* 35 (1): 155–186.

Wilkin, C. L., and R. H. Chenhall. 2020. Information technology governance: Reflections on the past and future directions. *Journal of Information Systems* 34 (2): 257–292. https://doi.org/10.2308/isys-52632

Zafar, H., M. S. Ko, and K. Osei-Bryson. 2016. The value of the CIO on the top management team on performance in the case of information security breaches. *Information Systems Frontiers* 18: 1205–1215. https://doi.org/10.1007/s10796-015-9562-5