Managerial Auditing Journal

Factors associated with security/cybersecurity audit by internal audit function: An international study

Md. Shariful Islam, Nusrat Farah, Thomas F. Stafford,

Factors associated with security/cybersecurity audit by internal audit function

An international study

Md. Shariful Islam
Louisiana Tech University, Ruston, Louisiana, USA

Nusrat Farah
Oregon State University, Corvallis, Oregon, USA, and

Thomas F. Stafford
Department of Computer Information Systems, Louisiana Tech University, Ruston, Louisiana, USA

Abstract

Purpose – The purpose of the study is to explore the factors associated with the extent of security/cybersecurity audit by the internal audit function (IAF) of the firm. Specifically, the authors focused on whether IAF/CAE (certified audit executive [CAE]) characteristics, board involvement related to governance, role of the audit committee (or equivalent) and the chief risk officer (CRO) and IAF tasked with enterprise risk management (ERM) are associated with the extent to which the firm engages in security/cybersecurity audit.

Design/methodology/approach – For analysis, the paper uses responses of 970 CAEs as compiled in the Common Body of Knowledge database (CBOK, 2015) developed by the Institute of Internal Auditors Research Foundation (IIARF).

Findings – The results of the study suggest that the extent of security/cybersecurity audit by IAF is significantly and positively associated with IAF competence related to governance, risk and control. Board support regarding governance is also significant and positive. However, the Audit Committee (AC) or equivalent and the CRO role are not significant across the regions studied. Comprehensive risk assessment done by IAF and IAF quality have a significant and positive effect on security/cybersecurity audit. Unexpectedly, CAEs with security certification and IAFs tasked with ERM do not have a significant effect on security/cybersecurity audit; however, other certifications such as CISA or CPA have a marginal or mixed effect on the extent of security/cybersecurity audit.

Originality/value – This study is the first to describe IAF involvement in security/cybersecurity audit. It provides insights into the specific IAF/CAE characteristics and corporate governance characteristics that can lead IAF to contribute significantly to security/cybersecurity audit. The findings add to the results of prior studies on the IAF involvement in different IT-related aspects such as IT audit and XBRL implementation and on the role of the board and the audit committee (or its equivalent) in ERM and the detection and correction of security breaches.

Keywords Internal audit, Cybersecurity, Board governance

Paper type Research paper

JEL classification – M42

The Common Body of Knowledge in Internal Auditing (CBOK, 2015) database was used for this study. One of the authors of this study is permitted to use the data by the Institute of Internal Auditors Research Foundation (IIARF). We gratefully acknowledge the support of IIARF.

Managerial Auditing Journal

0268-6902
DOI 10.1108/MAJ-07-2017-1595

Introduction

Cyberattacks have been unprecedented in the recent years; of the ten top technology risks identified by the Institute of Internal Auditors (IIA), both cybersecurity and information security rank as the top two technology risk concerns facing firms (IIA, 2015a, 2015b). The Heritage Foundation (2015) reported an average of 160 successful cyberattacks per week in 2014, which was more than three times the 2010 average. The costs of cyberattacks are tremendous (Ponemon Institute, 2015), averaging $15.4 million for a company operating in the USA, This figure has more than doubled since 2010, and the number of data breaches is expected to continue to increase (DiPietro, 2013). It is estimated that cybercrime could cost businesses over $2 trillion by 2019 (Juniper Research, 2015), which is nearly four times the estimated 2015 expense. In view of these findings, we see that cybersecurity risk management is of paramount importance, and we can confidently assert as a generality that higher-quality cybersecurity is in the interests of firms everywhere.

Cybersecurity research has investigated behavioral aspects of technology users (Bulgurcu *et al.*, 2013; D'Arcy *et al.*, 2009; Johnston and Warkentin, 2010; Siponen and Vance, 2010; Spear and Barki, 2010). Researchers have also investigated security awareness (Herath and Rao, 2009; Puhakainen and Siponen, 2010; Willison and Warkentin, 2013) and market reactions to information security initiatives (Gordon *et al.*, 2010). The relationship between the makeup of board technology committees in the context of security breaches has been studied (Higgs *et al.*, 2016), similar to the effects of security incidents on firms and their reputations (Campbell *et al.*, 2003; Cavusoglu *et al.*, 2004; Goldstein *et al.*, 2011; Wang *et al.*, 2013). The relationship between security programs (Cavusoglu *et al.*, 2009; Iheagwara, 2004; Kumar *et al.*, 2008; Straub, 1990) and the optimal investment in security (Gordon and Loeb, 2002; Wang *et al.*, 2008) has been studied as well. Less research has focused on information security governance (Dhillon *et al.*, 2007; Hong *et al.*, 2003; Mishar and Dhillon, 2006; Steinbart *et al.*, 2016) and the important relationship between information security management and the internal audit function (IAF) (Steinbart *et al.*, 2014a; 2014b; 2013; 2012).

Importance of security/cybersecurity audit

Even though the security risks to organizations have steadily increased, less empirical research has investigated various types of information systems (IS) security, in particular the nature and scope of system security implementations (Dhillon *et al.*, 2007). There is also a limited understanding of how organizations manage the various IS security dimensions and the potential problems involved in doing so (Dhillon and Backhouse, 2001).

Security/cybersecurity audit is a new dimension of security practice intended to support the protection of critical information assets of the firm. An auditing process will seek to obtain evidence of organizational information security policies and their efficacy for the protection of asset integrity, data confidentiality, and data access and availability (Pereira and Santos, 2010). Essentially, the audit serves to assess the effectiveness of an organization's ability to protect its valued or critical assets (Onwubiko, 2009). Managing IS security is increasingly important for companies due to the growing dependence of the firm on technology for conducting business, creating competitive advantage and achieving a higher ROI (Pereira and Santos, 2010).

There are no specific theories guiding the investigation of cybersecurity audit, although there are plentiful frameworks about the process, including COBIT 5, the ISO 2700 Series and the NIST SP 800 Series (Pereira and Santos, 2010). To the extent that those investigate the process and quality of audit in the firm as it impacts cybersecurity, familiar governance theories such as agency theory (Herath and Herath, 2014) or agency-related implications for the overall theory of the firm (e.g. Watts and Zimmerman, 1983) are most prevalent. It is

more common, however, to see authors simply affirm the importance of critical guiding frameworks from auditor-certifying organizations such as ISACA (Almadhoob and Valverde, 2014) in establishing the importance of auditing and board-level governance in influencing cybersecurity practices.

Although useful, such general frameworks may be in guiding research and practice; there is a degree of overlap in general security concepts among them. The choice of a framework depends on many factors, including industry, compliance requirements and factors idiosyncratic to the company itself. Therefore, the areas of information security that will be audited are totally dependent on the organizations' needs and circumstances (Lo and Marchand, 2004). Since this research is based on The Common Body of Knowledge in Internal Auditing database developed by the Institute of Internal Audit Research Foundation (CBOK, 2015), our focus here on security/cybersecurity audit is confined for purposes of the study to those areas for which adequate responses were available in the database to which we had access.

Notwithstanding, the CBOK is the world's largest ongoing study of the internal audit profession (IIA, 2015a, 2015b). Many academic researchers have utilized the CBOK databases to study the IAF (Abdolmohammadi, 2013; 2012; 2009; DeSimone and Abdolmohammadi, 2016; Abdolmohammadi *et al.*, 2017; Abdolmohammadi and Boss, 2010; Sarens *et al.*, 2012). Hence, the responses on security/cybersecurity audit variables in the CBOK can be expected to be representative of typical IAF security/cybersecurity audit factors. These factors include areas of security such as general IT risks, audits of cybersecurity of electronically held information, physical security of major data centers, audits of mobile devices, audits of procedures for employee social media use and audits of Internet security of company websites. While it may be guided by more practical frameworks on the practice of auditing, such research can contribute to the eventual development of an emergent theory describing the influence of board governance on cybersecurity audit processes, such that the theory of the firm might eventually be restated to include not only assets and resources leading to profitability but also risks and threats that might impede it, of which cybersecurity threats are increasingly potent and visible. Championed as it is by the certifying agency of IT audit certification, ISACA, we believe that the COBIT framework has a particularly high degree of relevance (Almadhoob and Valverde, 2014).

Motivation for the study

This study is motivated by the realization that many audit committees and boards have increasing expectations for internal auditors to understand and assess the organization's capabilities in managing the risks associated with cybersecurity (Deloitte, 2017) and have relevant and direct expectations for increased levels of auditor professionalism and training (Patton, 2005). This expectation spans to the regulatory environment, with the US Securities and Exchange Commission (SEC) (2011) noting that:

> Registrants should address cybersecurity risks and cyber incidents in their Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A), Risk Factors, Description of Business, Legal Proceedings and Financial Statement Disclosures.

Security programs are important to accountants and auditors because security issues can result in harmful problems such as fraud (Ngai *et al.*, 2011), can lead to inaccurate managerial forecasts (Li *et al.*, 2012) and can result in poor corporate performance (Carter *et al.*, 2012; Steinbart *et al.*, 2016). A prominent consultancy reports that 70 per cent of investors are interested in reviewing firms' cybersecurity practices and that nearly 80

per cent would not likely consider investing in firms with a history of cyber-attacks (HBGary Inc, 2013). Furthermore, in April 2017, the AICPA (2017) introduced a market-driven, flexible, and voluntary "cybersecurity risk management reporting framework", which highlights the importance of security/cybersecurity attestation in organizations.

To that end, many companies consider the IAF as a critical line of cyber-defense, providing for independent review of security measures and their performance. Internal Audit should help by identifying vulnerabilities and assessing the adequacy of controls, policies and procedures in place. IAF also helps ensure that regulatory cybersecurity guidelines, such as SEC disclosures, Sarbanes Oxley requirements and HIPAA requirements are being met. In general, the IAF can independently review and aid in assuring the effectiveness of the organizational cybersecurity risk management programs.

Purpose of the study

The purpose of this paper is to explore the factors associated with the extent to which organizations utilize IAF for security/cybersecurity audit. Specifically, we focused on how IAF or chief audit executive (CAE) characteristics and board involvement related to governance are associated with the extent of security/cybersecurity audit. Security/cybersecurity audit is an IT governance process (Heroux and Fortin, 2013) intended to formally define and update IT strategy, inform regular self-assessments and supplement independent assurance activities on the governance and control of IT, including IT investments and projects, IT performance measurement, IT governance and control frameworks and IT budget control and reporting (De Haes and Grembergen, 2009). In light of recent endeavors by different important stakeholders to mitigate the effects of cyberattacks, these questions are critical and urgent.

The paper proceeds as follows: first, background literature is reviewed in support of the development of research questions, followed by specification of explanatory variables and expected controls. Then, methodology is described, including the sample and measurement of variables in the model. Finally, results of testing the model are reported along with discussion of implications for research and practice.

Background and research questions

Security/cybersecurity audit and professional certification

The auditing literature requires that internal auditors possess knowledge, skills and other competencies needed to perform their individual responsibilities (IIA, 2017). Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as certified internal auditor (CIA) designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations (IIA, 2017).

Security/cybersecurity audit requires sophisticated information technology (IT) knowledge. Internal auditors must have sufficient knowledge of key IT risks and controls the and available technology-based audit techniques to perform their work (IIA, 2017), and studies have noted the importance of auditor professional development such as training and certification (Patton, 2005), although the sense is that more work on this factor is required. In addition, the IT Governance Institute emphasizes that individuals responsible for assessing information security should have knowledge about both IS audit techniques and information security standards (ITGI, 2012), suggesting a certain value for professional certifications in these areas. Steinbart *et al.* (2013) noted that an internal auditor's level of knowledge about information security (which we construe specifically as the skillset of the CAE) is an important determinant of its ability to successfully fulfill the role of an

independent monitor and assessor of an organization's information security program. When internal auditors possess detailed technical expertise about information security, they are able to develop deeper relationships with the IS security functions, thus contributing to building a more effective security management program (Steinbart *et al.*, 2012). Moreover, auditor knowledge about IT and control systems is directly related to the quality of IT audits (Stoel *et al.*, 2012). Therefore, for high-quality security/cybersecurity audit, it seems reasonable to conclude that internal auditors will possess specialized IT knowledge and that the IAF will feature CAEs with appropriate security certifications such as CISM, CISSP, CSP, CDP and CISRCP. Hence, it is expected that an IAF staffed with CAEs carrying security certifications is positively and significantly associated with the security/cybersecurity audit. Moreover, IS audit certification (such as CISA, QiCA and CRISC) is considered a security certification (Abdolmohammadi and Boss, 2010; Burning Glass Technologies, 2015). Hence, it is expected that an IAF staffed with CAEs carrying IS audit certifications is positively and significantly associated with the extent of security/cybersecurity audit.

Public accounting firms employ individuals with CPA credentials as well as other varied qualifications specifically related to IT and security (Center for Audit Quality, 2017). To that end, an IAF featuring CAEs with CPA or CIA certification and possessing appropriate training on security is expected to be positively and significantly associated with excellent security/cybersecurity audit (IIA, 2017). Hence, the following research questions are suggested:

RQ_{1a}. Is security certification (such as CISM, CISSP, CSP, CDP and CISRCP) of the chief audit executive (CAE) positively and significantly associated with the extent of security/cybersecurity audits by the internal audit function (IAF)?

RQ_{1b}. Is information systems auditing certification (such as CISA, QiCA and CRISC) of the CAE positively and significantly associated with the extent of security/cybersecurity audits by IAF?

RQ_{1b}. Is the certified internal auditor (CIA) certification held by CAE positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

RQ_{1d}. Is the CPA certification held by the CAE positively and significantly associated with the extent of security/cybersecurity audits by IAF?

Security/cybersecurity audit, risk assessment, enterprise risk management and the internal audit function

Organizations face numerous risks, with the threat landscape changing every day. Not so long ago, cybersecurity was not seen a pressing issue by business, but over a short period of time cybersecurity has become a top concern of American companies, financial institutions, law enforcement and many regulators (Aguilar, 2014). The importance of cybersecurity risk management is also evident by the issuance of a new framework for cybersecurity risk management by the American Institute of CPAs to help businesses meet the growing challenge (AICPA, 2017). It is clear that security/cybersecurity challenges demand an effective risk management on the part of organizations.

Enterprise risk management (ERM) has emerged as the new watchword in the climate of ever-increasing corporate uncertainty and financial scandal (Walker *et al.*, 2003). The Committee of Sponsoring Organizations (COSO, 2004) defines ERM as:

> [. . .] a process, effected by an entity's Board of directors, management and other personnel, applied in strategy settings and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

There are eight components of ERM: internal environment, setting objectives, event identification, assessment of risk, risk response, control activities, information and communication and monitoring. Internal environment involves setting the basis for how risk and control are viewed and addressed by the top management. In this respect, board oversight, commitment to competence and risk appetite are most important for cybersecurity risks. An effective oversight by a competent board toward cybersecurity risk is the most important prerequisite to form an effective cybersecurity risk management program. Objectives must be set before management identifies events affecting the achievement. Setting objectives implies that organizations should prepare themselves for a different aspects of cybersecurity emergencies, such as those which might be outlined in a disaster recovery plan. Event identification implies that risk factors that might have an impact on organizations must be identified, and security/cybersecurity audit helps identify different kinds of vulnerabilities and suggest remedial measures. Identified risks are analyzed in relation to their likelihood and their severity; risk assessment needs to be done continuously and a well-formed security/cybersecurity audit assesses the likelihood of risk from the identified vulnerabilities. Risk response involves selecting a set of actions to align risks with the entity's risk tolerances and appetite. Security/cybersecurity audit can help evaluate alternatives and select the best courses of action to address cybersecurity threats. Control activities are those processes that involve establishing and executing policies and procedures to help ensure that risk responses are effectively carried out. In terms of control activities, security/cybersecurity audit can help in two ways: it can assess whether existing control activities are being executed effectively, or it can recommend new and improved control activities to address new and sophisticated forms of security risks. Information and communication include the identification, capture and communication of information throughout the organization in an effective manner. Finally, monitoring is undertaken to manage risks. In this way, it can react dynamically, changing as conditions warrant.

The COSO ERM framework calls on the IAF to assist management and the board of directors and its audit committee by examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of the entity's ERM process (COSO, 2004). Internal auditors play a key role in providing both assurance and consulting services with respect to the management of risk within their organizations (Sarens and De Beelde, 2006), and researchers increasingly acknowledge the fact that the IAF significantly facilitates and supports ERM (Walker *et al.*, 2002). The CAE is also seen to play a significant ERM leadership role. There is evidence of close interaction between internal audit and the chief risk officer (CRO), as well as evidence of internal audit focus on coordinating ERM efforts by assisting with risk identification, suggesting control activities, and monitoring the ERM process (Beasley *et al.*, 2005). Given the internal audit's natural focus on governance, risk and compliance, it plays a vital role in overseeing all eight components of the ERM framework. Hence, ERM has the greatest impact on internal audit's activities when the organization's ERM process is completely in place (Beasley *et al.*, 2006).

Walker *et al.* (2003) found that the IAF received several major benefits from its involvement in ERM processes. First, audits were more effective because ERM enabled the departments to marshal extensive information about their companies' risk profile and gauge the extent to which those risks were being managed. Second, the CAEs were able to operate their departments more efficiently by leveraging ERM resources. Internal auditors consider

the risk analyses developed through their companies' ERM efforts and applies this information to their own audit planning and execution process. Finally, when IAF is involved in ERM, auditors begin thinking like managers and focusing on business objectives rather than solely on audit objectives. The IAF, by performing a comprehensive cyber risk assessment, can present objective perspectives and findings to the audit committee and board members and use those findings to develop a broad internal audit plan that addresses the areas of cyber-risk that the organization faces over a single or multi-year audit period (Deloitte, 2017). This all indicates that IAFs are well positioned to perform security/cybersecurity audits as they become more experienced with ERM processes. Based on the preceding discussion, we formulate the following research questions:

RQ$_2$. Is a comprehensive risk assessment done by the IAF positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

RQ$_3$. When the responsibility for enterprise risk management (ERM) resides with the IAF, is this positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

RQ$_4$. Are IAF competencies related to governance, risk, and compliance positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

Security/cybersecurity audit and corporate governance

The risk of security breaches (and the harm that these breaches pose) is of increasing concern for most companies; hence, it rises to a heightened degree of focus for the board (Gregogry and Austin LLP, 2014). A recent survey of more than 250 board members indicated that cybersecurity is a rising concern, even surpassing compliance risk. Approximately 74 per cent of board directors indicated that their CEOs have a strong understanding of regulatory compliance challenges, while only half (51 per cent) said their CEOs possess a strong understanding of cybersecurity topics (Tysiac, 2014). In considering whether executive roles and compensation schemes are associated with security breach occurrences, it was noted that security breaches are less common when IT executives are more involved in the leadership team and when they are compensated based on behaviors rather than outcomes (Kwon *et al.*, 2013). Hence, it is reasonable to expect that cybersecurity management involvement at the board level has an impact on the cybersecurity component of IT risk (Higgs *et al.*, 2016; Steinbart *et al.*, 2013).

A corporate board engaged with cybersecurity issues is the key to more robust cybersecurity measures. The common denominator among entities with strong cybersecurity frameworks is an engaged board of directors that genuinely understands security and privacy issues, according to a recent survey (Protiviti, 2015). It was found that 77 per cent of organizations with boards demonstrating a high or medium level of engagement with and understanding for security risks generally had all "core" information security policies in place (Protiviti, 2015). To that end, a board with security expertise would seem to be a prerequisite for an effective cybersecurity management program. Although many organizations task the cybersecurity issue directly to the audit committee, companies for which technology forms the backbone of their business often have a dedicated cyber-risk committee that focuses exclusively on cybersecurity and other risk management issues. Even so, these sorts of risk committees are relatively rare outside of the financial sector (KPMG, 2014).

The audit committee (or its equivalent) has an enormous influence on the IAF as CAEs report to the audit committee and because internal auditor areas of work are bound by the committee's responsibilities (Barua *et al.*, 2010). Internal audit should play a central role in helping the audit committee oversee cybersecurity, as an internal auditor is expected to develop a road map for the future that deals with various cybersecurity risk issues (Deloitte, 2015). Regulators emphasize on frequent audit committee meetings to allow for better communication between audit committee members and auditors, because these meetings reflect due diligence [National Commission on Fraudulent Financial Reporting (Treadway Commission), 1987; PCAOB, 2012; Blue Ribbon Committee, 1999]. Previous studies suggest that frequent auditor meetings with the audit committee reduce the likelihood of problems such as fraud and financial reporting restatements (Beasley *et al.*, 1999; Abbott *et al.*, 2004). Following these guidelines, we expect that frequent audit committee meetings with the CAE will tend to increase the extent of security/cybersecurity audit by IAF.

As discussed, security/cybersecurity risk management is a part of ERM. Hence, an enterprise with effective ERM is expected to have more security/cybersecurity audit activity. In an examination of the factors associated with stage of ERM implementation at a variety of US and international organizations, it was found that the stage of ERM implementation is positively related to the presence of a CRO, to board independence, and to the appearance of CEO and CFO support for ERM; other factors included the presence of Big Four auditors, company size and business sector membership (Beasley *et al.*, 2005). Moreover, firms employing a CRO include larger firms, firms with a greater risk of financial distress or high volatility of share prices and firms with CEOs who have a high propensity to take risk (Pagach and Warr, 2011). To that end, it is expected that the presence of a CRO or the equivalent is associated with the security/cybersecurity audit process in organizations. Hence, the following are suggested:

RQ_5. Is support received by the IAF from the board of directors to review the organization's governance policies and procedures positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

RQ_6. Do audit committee (or equivalent) meetings with the CAE positively and significantly associate with the extent of security/cybersecurity audits by the IAF?

RQ_7. Is a formal ERM process with a chief risk officer (CRO) or the equivalent positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

Security/cybersecurity audit and high-quality IAFs

Managerial audit literature confirms that high-quality IAFs are associated with many benefits such as improved corporate governance and financial reporting quality (Christ *et al.*, 2015), effective internal controls (Lin *et al.*, 2011), better risk assessments (Asare *et al.*, 2008; Sarens and De Beelde, 2006), the prevention of management misconduct (Ege, 2015; Prawitt *et al.*, 2012), and greater external audit efficiency (Pizzini *et al.*, 2014). However, surveys indicate that many stakeholders (including board members, regulators, senior managers and CAEs) feel that internal auditors are still under-performing [PriceWaterhouseCoopers (PWC), 2017]. Regarding security/cybersecurity, the IAF can present an objective perspective to the audit committee and other board members and then use those findings to develop a broad internal audit plan that addresses the areas of cyber-risk for the organization (Deloitte, 2017). Thus, by performing a comprehensive cyber risk assessment, the IAF can play a critical role in the ongoing battle of managing cyber threats.

However, studies confirm that the IAF lacks necessary qualities such as security training/knowledge, communication skills, and the appropriate attitude requisite to build up an effective security/cybersecurity risk management program (Steinbart *et al.*, 2012; 2013; 2014b). The Quality Assurance and Improvement Program (QAIP) of IAFs represents a quality assessment benchmark, such that high-quality IAFs are expected to be significantly and positively associated with the security/cybersecurity audit process (DeSimone and Abdolmohammadi, 2016). Internal auditing standards also require that CAEs develop and maintain a QAIP (IIA, 2017), and hence, the following is suggested:

RQ_8. Is a well-defined Quality Assurance and Improvement Program (QAIP) at organizations positively and significantly associated with the extent of security/cybersecurity audits by the IAF?

Expected control variables

In addition to the explanatory variables outlined in the research questions given above, several control variables are included. The data set for this study includes CAE personal demographic variables such as education level, academic degree major, training hours and job experience. CAEs with higher education (graduate versus undergraduate) are expected to be more likely to conduct more security/cybersecurity audits as CAEs with graduate degrees are significantly more associated with the extent of IT audit than those with only an undergraduate degree (Abdolmohammadi and Boss, 2010). However, a similar relationship between CAE education level and use of XBRL (eXtensible Business Reporting Language) has not been seen (Abdolmohammadi *et al.*, 2017). As security/cybersecurity audit is IT intensive, it is expected that CAEs with computer science or IT majors will tend to do more audit work in this area (Abdolmohammadi and Boss, 2010); yet the academic major of the CAE is significantly and positively associated with XBRL implementation in public companies (Abdolmohammadi *et al.*, 2017). CAE training hours are also expected to have a positive association with security/cybersecurity audit because training will help CAEs to gain more hands-on experience with security/cybersecurity risks. To that end, a significant positive association between training hours and IT audit has been noted (Abdolmohammadi and Boss, 2010), and the amount of CAE continuous professional education (CPE), which is equivalent to training, is also significantly associated with XBRL implementation in public companies (Abdolmohammadi *et al.*, 2017). The experience level of a CAE is also expected to have an effect on the extent of security/cybersecurity audit, but the direction of the effect is not clear; more experienced CAEs might prefer either to do more security/cybersecurity audits to mitigate the organization's exposure towards risk or spending time on more traditional audits (Abdolmohammadi and Boss, 2010).

As with the CAE personal demographic variables, IAF characteristics are found to have an effect on IT governance (Heroux and Fortin, 2013). Hence, we focused on IAF age, number of employees dedicated to IAF and the budget allocated to IAF in organizations. Prior studies suggest that the longevity of the IAF (we refer to this as "age") is an indicator of its maturity (Heroux and Fortin, 2013; Abdolmohammadi *et al.*, 2017), with the provision that a mature IAF is expected to be more involved with emerging areas such as security/cybersecurity audit and XBRL implementation. The number of employees assigned to the IAF reflects the capabilities of the process, and it is generally expected that an IAF with a greater number of employees can provide organizations with more value (Heroux and Fortin, 2013). The IAF budget is also considered a valuable resource, as it helps IAF to get involved with IT governance. To that end, different IAF characteristics influence IAF

involvement in IT governance structure, process and relational capabilities (Heroux and Fortin, 2013).

Organizational variables such as size and industry are also included as control variables. Some organizations are far more susceptible to cyberattack due to the very nature of their business. For example, attacks on government organizations also rose sharply in 2016 to 14 per cent of all attacks, compared to 7 per cent in 2015. Meanwhile, the finance industry saw a significant rise in its share of recent attacks, growing from 3 per cent of all attacks in 2015 to 14 per cent in 2016 (Dimension Data, 2017). Among the top three most attacked industries, the finance industry was the only industry consistently represented in all the geographic regions that were analyzed (Dimension Data, 2017). Security/cybersecurity audit demands more resources; therefore, large organizations tend to be associated with a greater extent of security/cybersecurity audit than are smaller organizations.

Research method

Sample

Data for the study were collected from the Common Body of Knowledge in Internal Auditing (CBOK, 2015), a database that includes the world's largest ongoing study of the internal audit profession including studies of internal audit practitioners and their stakeholders. CBOK builds on two previous global surveys of internal audit practitioners conducted by the IIA Research Foundation in 2006 and 2010. The number of respondents is 14,518 internal auditors from 166 countries, with CAEs representing about 26 per cent of total respondents. For the current study, CAE responses were the focus owing to the knowledge and experience characteristic of that level of responsivity in the auditing process (Abdolmohammadi and Boss, 2010). After filtering the data (Table I), our sample size was 970 observations, although this varied in some analyses because of the missing data. As was the case with Abdolmohammadi *et al.* (2017), the data sample is limited to countries with at least 10 CAE observations, except for Israel (n = 9), Ireland (n = 4) and the UK (n = 8); the observations of the UK and Ireland were merged in one case, as per Abdolmohammadi and Boss (2010) and Abdolmohammadi (2013). Tables I to IV provide a visual representation of the sample composition.

We analyzed the data across different geographical regions because security issues are generally concentrated in neither any one industry nor any specific region of the world; instead, security problems are generally pervasive around the world (Dimension Data, 2017). Many studies that use CBOK database either focus solely on Anglo-culture countries (Abdolmohammadi, 2013) or analyze data across Anglo-culture and non-Anglo culture

Table I. Total observations used

Total respondent	14518
Less: Director or Senior manager	1630
Less: Manager	2098
Less: Staff	5644
Less: Missing value for respondents' position	182
Less: Academic staff or retired	1620
Chief audit executives (CAEs)	3344
Less: Missing values for dependent variable	953
Less: Missing values for other independent variables	1421
Total observations used	970

countries (Abdolmohammadi and Boss, 2010; DeSimone and Abdolmohammadi, 2016; Abdolmohammadi, 2012).

Different specific aspects or symptoms of cybersecurity problems might also contribute in varying fashion in the security/cybersecurity audits of different global regions. Hence, analysis of the data across regions will highlight the importance of these different factors in their respective regions. It also bears notice that many studies that used the CBOK database (Abdolmohammadi, 2013; Abdolmohammadi *et al.*, 2017; Abdolmohammadi and Boss, 2010; DeSimone and Abdolmohammadi, 2016; Abdolmohammadi, 2012) analyzed the data across different regions. In that light, it seems a reasonable approach to take; we further compared responses across Anglo-culture and non-Anglo culture countries because a significant portion of respondents of our sample (about 35 per cent) are from Anglo-culture countries. Thus, this analysis will tend to highlight any potential regional biases in our results.

Variable measurement and empirical model

The dependent variable of the study is the extent of security/cybersecurity audit by the IAF, which is represented by the variable *securityaudit*. Questions 92-1 through 92 -7 from the CBOK (2015) measure the extent of security/cybersecurity audit by the IAF, with 1 being none and 4 being extensive. For the purpose of ensuring proper dimensionality, it was decided to further evaluate *securityaudit* by factor analysis, which is elaborated below.

For RQ_{1a}, security certification of the CAE is measured by *certification_Security*, which is a categorical variable (1 representing security certification, 0 otherwise). Similarly, the variables *certification_IS*, *cpa* and *cia* represent RQ_{1b}, RQ_{1c} and RQ_{1d}, respectively. The details of these variable definitions are provided in Table V. The IAF reliance on comprehensive risk assessment is measured using the variable *riskassessmentscope* (RQ_2). The variable *ERM_IA* (RQ_3) measures if the IAF is responsible for the organization's ERM functions, and *governance_Boardsupport* (RQ_5) measures whether the IAF has complete board support regarding the organization's governance and policies and procedures. The variable *acmeeting_cae* (RQ_6) represents due diligence on the part of the audit committee (or equivalent) by measuring the number of audit committee meetings in which the CAE was invited to attend. If the organizations have a CRO or the equivalent, the appropriate variables would be *riskmagt_officer* (RQ_7). The quality of the IAF is measured by *qaip* (RQ_8), with 1 representing the presence of a QAIP and 0 otherwise. The variable *ACCountries* represents the respondents from Anglo countries. With the operational measures defined for analysis, the model of the study is as follows:

No.	Region	Frequency	(%)	Cumulative
1	Africa	73	7.67	7.67
2	Asia	158	16.6	24.26
3	Pacific	35	3.68	27.94
4	Europe	223	23.42	51.37
5	Middle East	53	5.57	56.93
6	North America	300	31.51	88.45
7	South America	110	11.55	100
	Total	952	100	

Table II. Regional representation

No.	Countries by region	Frequency	(%)	Cumulative
	Africa			
1	South Africa	29	39.73	39.73
2	Tanzania	20	27.4	67.12
3	Uganda	11	15.07	82.19
4	Zimbabwe	13	17.81	100
	Total	73	100	
	Asia			
1	China	34	21.52	21.52
2	India	27	17.09	38.61
3	Indonesia	17	10.76	49.37
4	Japan	18	11.39	60.76
5	Malaysia	28	17.72	78.48
6	Singapore	10	6.33	84.81
7	Taiwan	24	15.19	100
	Total	158	100	
	Pacific			
1	Australia	26	74.29	74.29
2	New Zealand	9	25.71	100
	Total	35	100	
	Europe			
1	Denmark	10	4.48	4.48
2	France	33	14.8	19.28
3	Germany	25	11.21	30.49
4	Greece	13	5.83	36.32
5	Ireland	4	1.79	38.12
6	Italy	16	7.17	45.29
7	Slovenia	11	4.93	50.22
8	Spain	28	12.56	62.78
9	Sweden	10	4.48	67.26
10	Switzerland	51	22.87	90.13
11	Turkey	14	6.28	96.41
12	United Kingdom	8	3.59	100
	Total	223	100	
	Middle East			
1	Israel	9	16.98	16.98
2	Saudi Arabia	15	28.3	45.28
3	UAE	29	54.72	100
	Total	53	100	
	North America			
1	Canada	45	15	15
2	United States	255	85	100
	Total	300	100	

Table III. Countries represented

(*continued*)

No.	Countries by region	Frequency	(%)	Cumulative
	South America			
1	Argentina	10	9.09	9.09
2	Brazil	16	14.55	23.64
3	Chile	22	20	43.64
4	Colombia	17	15.45	59.09
5	El Salvador	12	10.91	70
6	Mexico	10	9.09	79.09
7	Panama	11	10	89.09
8	Peru	12	10.91	100
	Total	110	100	

Table III.

No.	Types of organizations	Frequency	(%)	Cumulative
1	Privately held	316	33.19	33.19
2	Publicly traded	390	40.97	74.16
3	Public sector (Government)	159	16.70	90.86
4	Not-for-profit	60	6.30	97.16
5	Others	27	2.84	100.00
	Total	952	100	

Table IV.
Organization type

$$securityaudit = \beta_0 + \beta_1 certification\_Security + \beta_2 certification\_IS + \beta_3 cpa + \beta_4 cia + \beta_5 riskassessmentscope + \beta_6 ERM\_IA + \beta_7 iacompetence\_grc + \beta_8 governance\_Boardsupport + \beta_9 acmeeting\_cae + \beta_{10} riskmagt\_officer + \beta_{11} qaip + \beta_{12} ACCountries + \sum \beta_i control\ variables + \varepsilon$$

Results

Descriptive statistics and univariate analysis

Table VI and VII presents the descriptive statistics and univariate analysis of the data; the analysis was performed based on differing geographical regions. The CBOK's global regions are derived from World Bank categories, and we excluded one region owing to lack of observations (The Caribbean). Depending on the nature of variable (discrete or continuous), either *F*-tests or χ^2 tests of independence were utilized. In the analysis presented in Table VI and VII, significant results appear in italics. The means for dependent variable *securityaudit* vary across different regions, with significant p values. This finding indicates that the extent of security/cybersecurity audit is not uniform across all regions surveyed, which was not unexpected as security/cybersecurity is an emerging risk area for the IAF in different parts of the world. Not only does the IAF struggle with security/cybersecurity risk, but other stakeholders including policymakers are struggling to formulate well-defined policy to mitigate this emerging area of risk. In terms of the variable,

Variables	CBOK (2015) Questions	Definition
Dependent variable		
securityaudit	Q 92-1 through Q 92-7	Sum of the responses of the extent of security audit; 1 = None and 4 = Extensive
Independent variables		
certification_Security (RQ_{1a})	Q13	1 if CAE has security certification such as CISM, CISSP, CSP, CDP, CISRCP; 0 otherwise
certification_IS (RQ_{1b})	Q13	1 if CAE has IS auditing certification such as CISA, QiCA, CRISC; 0 otherwise
cpa (RQ_{1c})	Q13	1 If CAE has public accounting certification such as CA, CPA, ACCA, ACA; 0 otherwise
cia (RQ_{1d})	Q12	1 if CAE has internal auditing certification such as CIA; 0 otherwise
riskassessmentscope (RQ_2)	Q41	1 if IAF relies on "Comprehensive risk assessment done by IAF"; 0 otherwise
ERM_IA (RQ_3)	Q59	1 if IAF is responsible for the organization's ERM function; 0 otherwise
iacompetence_grc (RQ_4)	Q 81-1 through Q 81-5	Sum of the responses related to governance, risk, and compliance; 1 = Novice; 5 = Expert
governance_Boardsupport (RQ_5)	Q67	1 if IAF has complete Board support regarding organization's governance and policies and procedures; 0 otherwise
acmeeting_cae (RQ_6)	Q78b	Number of Audit Committee or equivalent Meetings in which CAE was invited to attend
riskmagt_officer (RQ_7)	Q58	1 if Organizations have Chief Risk Officer or Equivalent
qaip (RQ_8)	Q47	1 if organizations have well defined QAIP; 0 otherwise
Control Variables		
education_cae	Q5	1 If CAE has graduate or higher degree; 0 otherwise
experience	Q10	Years of experience of as CAE
training_hours	Q14	Hours of formal training related to the internal audit profession
major_cs_it	Q5a	1 if CAE has computer science/IT as academic major; 0 otherwise
IAFage	Q23	Number of years IAF has been in the organizations
IAFempLN	Q24	Natural log of the number of Full Time Employees (FTE) in IAF
IAFbudget	Q28	1 if IAF has completely sufficient budget, 0 otherwise
industry_combined	Q18	1 If the organization belongs to finance or insurance industry; 0 otherwise
employees_organization	Q19	Natural log of the number of Full Time Employees (FTE) in organizations
ACCountries		1 if respondents are from UK/Ireland; USA; Canada; Australia; New Zealand; or South Africa, 0 otherwise

Table V. Measurement of variables

Table VI.
Descriptive statistics – mean "univariate analysis *(standard deviation)*" and univariate analysis

Variables	Full dataset	Africa	Asia	Pacific	Europe	Middle east	NorthAmerica	SouthAmerica	*F*-statistic/χ^2(Sig)
securityaudit	18.55 (5.26)	17.58 (4.82)	18.16 (5.55)	18.17 (4.62)	18.59 (5.60)	20.30 (5.09)	18.28 (4.76)	19.81 (5.80)	2.78 *(0.011)*
certification_Security	0.03 (0.17)	0.03 (0.16)	0.03 (0.18)	0.00 (0.00)	0.02 (0.15)	0.02 (0.14)	0.03 (0.18)	0.05 (0.23)	4.10 (0.66)
certification_IS	0.15 (0.36)	0.11 (0.32)	0.14 (0.35)	0.11 (0.32)	0.08 (0.27)	0.23 (0.42)	0.21 (0.41)	0.12 (0.32)	22.77 *(0.00)*
cpa	0.45 (0.50)	0.55 (0.50)	0.34 (0.48)	0.69 (0.47)	0.29 (0.46)	0.57 (0.50)	0.63 (0.48)	0.25 (0.44)	99.86 *(0.00)*
cia	0.41 (0.49)	0.36 (0.48)	0.40 (0.49)	0.40 (0.50)	0.32 (0.47)	0.40 (0.49)	0.54 (0.50)	0.25 (0.44)	41.11 *(0.00)*
riskassessmentscope	0.56 (0.50)	0.47 (0.50)	0.34 (0.48)	0.40 (0.50)	0.61 (0.49)	0.77 (0.42)	0.70 (0.46)	0.46 (0.50)	75.46 *(0.00)*
ERM_IA	0.17 (0.37)	0.21 (0.41)	0.13 (0.33)	0.17 (0.38)	0.17 (0.37)	0.17 (0.38)	0.19 (0.40)	0.14 (0.35)	4.85 (0.56)
iacompetence_grc	19.77 (3.91)	18.42 (3.70)	17.54 (4.08)	20.37 (3.40)	21.23 (3.34)	20.64 (3.98)	19.92 (3.63)	19.97 (4.19)	17.42 *(0.00)*
governance_Boardsupport	0.67 (0.47)	0.68 (0.47)	0.68 (0.47)	0.60 (0.50)	0.65 (0.48)	0.68 (0.47)	0.69 (0.46)	0.65 (0.48)	2.36 (0.88)
acmeeting_cae	5.68 (4.13)	5.04 (5.49)	4.99 (3.75)	4.91 (1.82)	4.81 (2.98)	5.57 (2.89)	5.87 (3.86)	8.70 (5.64)	13.90 (0.00)
riskmagt_officer	0.35 (0.48)	0.36 (0.48)	0.26 (0.44)	0.43 (0.50)	0.40 (0.49)	0.21 (0.41)	0.38 (0.49)	0.31 (0.46)	16.49 *(0.01)*
qaip	0.17 (0.37)	0.12 (0.33)	0.19 (0.39)	0.17 (0.38)	0.18 (0.39)	0.19 (0.40)	0.14 (0.35)	0.19 (0.40)	3.69 (0.72)
education_cae	0.56 (0.50)	0.71 (0.46)	0.46 (0.50)	0.60 (0.50)	0.69 (0.47)	0.62 (0.49)	0.45 (0.50)	0.62 (0.49)	44.71 *(0.00)*
experience	7.35 (6.12)	6.81 (5.19)	6.23 (5.81)	8.57 (6.01)	6.88 (5.50)	6.92 (5.70)	8.52 (6.70)	6.45 (5.60)	3.88 *(0.00)*
training_hours	46.50 (33.77)	41.22 (21.20)	40.94 (27.15)	34.80 (16.06)	45.05 (27.83)	51.15 (32.42)	46.84 (19.71)	61.63 (71.02)	5.78 *(0.00)*
major_cs_it	0.12 (0.32)	0.21 (0.41)	0.11 (0.31)	0.14 (0.36)	0.11 (0.31)	0.17 (0.38)	0.08 (0.27)	0.15 (0.36)	13.87 *(0.03)*
IAFage	17.69 (16.33)	13.18 (8.63)	14.68 (11.22)	16.30 (17.72)	18.71 (19.24)	12.18 (8.48)	20.70 (16.32)	19.08 (20.82)	4.44 *(0.00)*
IAFempLN	2.01 (1.35)	1.94 (1.45)	2.19 (1.68)	1.51 (1.18)	1.90 (1.36)	2.02 (1.03)	2.02 (1.23)	2.16 (1.31)	1.74 (0.11)
IAFbudget	0.37 (0.48)	0.15 (0.36)	0.34 (0.48)	0.23 (0.43)	0.41 (0.49)	0.42 (0.50)	0.44 (0.50)	0.32 (0.47)	28.72 *(0.00)*
industry_combined	0.28 (0.45)	0.23 (0.43)	0.20 (0.40)	0.20 (0.41)	0.35 (0.48)	0.19 (0.40)	0.27 (0.44)	0.40 (0.49)	22.48 *(0.00)*
employees_organization	7.01 (2.54)	6.30 (2.75)	6.66 (2.23)	7.14 (2.44)	7.34 (2.95)	6.78 (2.27)	7.26 (2.33)	6.68 (2.39)	3.05 *(0.00)*
N	970.00	73.00	158.00	35.00	223.00	53.00	300.00	110.00	

Table VII. Descriptive statistics – mean "univariate analysis *(standard deviation)*" and univariate analysis of Anglo Culture (AC) countries and Non-Anglo culture countries

Variables	Full dataset	Anglo culture (AC) countries	Non-AC countries	*F*-statistic/χ^2 (Sig)
securityaudit	18.55 (5.26)	18.19 (4.68)	18.79 (5.59)	3.00 *(0.08)*
certification_Security	0.03 (0.17)	0.03 (0.18)	0.03 (0.17)	0.09 (0.77)
certification_IS	0.15 (0.36)	0.20 (0.40)	0.11 (0.32)	13.23 *(0.00)*
cpa	0.45 (0.50)	0.61 (0.49)	0.35 (0.48)	60.67 *(0.00)*
cia	0.41 (0.49)	0.52 (0.50)	0.33 (0.47)	35.95 *(0.00)*
riskassessmentscope	0.56 (0.50)	0.64 (0.48)	0.52 (0.50)	13.58 *(0.00)*
ERM_IA	0.17 (0.37)	0.18 (0.39)	0.16 (0.36)	1.20 (0.27)
iacompetence_grc	19.77 (3.91)	19.89 (3.59)	19.69 (4.10)	0.63 (0.43)
governance_Boardsupport	0.67 (0.47)	0.68 (0.47)	0.66 (0.47)	0.43 (0.51)
acmeeting_cae	5.68 (4.13)	5.74 (4.22)	5.65 (4.07)	0.12 (0.73)
riskmagt_officer	0.35 (0.48)	0.39 (0.49)	0.32 (0.47)	3.74 *(0.05)*
qaip	0.17 (0.37)	0.15 (0.35)	0.18 (0.38)	1.72 (0.19)
education_cae	0.56 (0.50)	0.49 (0.50)	0.61 (0.49)	13.70 *(0.00)*
experience	7.35 (6.12)	8.50 (6.61)	6.63 (5.68)	21.92 *(0.00)*
training_hours	46.50 (33.77)	44.82 (19.73)	47.57 (40.19)	1.52 (0.22)
major_cs_it	0.12 (0.32)	0.09 (0.29)	0.13 (0.34)	3.27 *(0.07)*
IAFage	17.69 (16.33)	19.29 (15.88)	16.79 (16.53)	4.73 *(0.03)*
IAFempLN	2.01 (1.35)	2.01 (1.26)	2.01 (1.41)	0.00 (0.96)
IAFbudget	0.37 (0.48)	0.40 (0.49)	0.36 (0.48)	1.77 (0.18)
industry_combined	0.28 (0.45)	0.24 (0.43)	0.30 (0.46)	3.26 *(0.07)*
employees_organization	7.01 (2.54)	7.30 (2.37)	6.82 (2.63)	8.19 (0.00)
N	970.00	376.00	594.00	

certification_Security, only about 3 per cent CAEs in the sample had security certification, and this result does not vary across regions. This suggests that IAFs in all assessed regions lack CAEs with sufficient security skills. Compared to other certifications such as *certification_IS* (15 per cent), *cpa* (45 per cent), and *cia* (41 per cent), this percentage is unusually low.

The percentage of comprehensive risk assessment done by the IAF also varies across global regions, and the difference is statistically significant; this implies the involvement of CAEs or IAFs in the comprehensive risk assessment of the firm is not uniform between each region. The same finding is also true for IAF competence regrading governance, risk and control. Notwithstanding, across the regions of the world, there were no statistical differences in the involvement of the IAF with the ERM process. The implication is that while differences are not found in regard to involvement of the IAF with ERM, there are differences across regions in terms of risk assessment and risk competence of the IAF.

There were no differences found for board of directors' support for governance, but there were statistically significant differences noted in the number of audit committee meetings with CAEs and the existence of a CRO (or the equivalent) in the organizations. For IAF quality, there were no differences regarding the existence of a well-defined QAIP in the organizations; at the same time, the percentage of organizations having a well-defined QAIP is very low (mean = 17 per cent).

In assessing control variables, 56 per cent of CAEs have graduate degrees (or higher), and this percentage is statistically significant across different regions. CAEs also differ significantly in terms of experience, with the average years of experience in the job role being 7.35 years. Furthermore, the average percentage of CAEs with Computer Science (CS) or Information Technology (IT) majors is 12 per cent, which does differ across different regions. The average number of training hours for CAEs is 46.50, with statistically

significant difference across regions. The average IAF age is 17.69 years, which also varies significantly across regions. Although IAFs do not differ in terms of employees, they do differ in terms of budget, with 37 per cent of CAEs reporting that they have sufficient budget.

As mentioned earlier, many studies that used the CBOK database focused on either Anglo-culture countries only (Abdolmohammadi and Boss, 2010; Abdolmohammadi, 2013) or both Anglo and Non-Anglo countries (Abdolmohammadi *et al.*, 2017); hence, we regrouped our data based on the Anglo/Non-Anglo classification. Table VII presents the descriptive statistics and univariate analysis of this classification.

For the variable *securityaudit*, it is found that Anglo countries differ marginally from Non-Anglo, although they do not vary for the *certification_Security* variable. However, they do vary for *certification_IS, cpa* and *cia*. Furthermore, they vary for *riskassessmentscope*, but not for *ERM_IA* or *iacompetence_grc*. These findings suggest that although the IAF is responsible for ERM and that they share similar competencies regarding risks and control, they do differ in risk assessment scope. No differences were found between Anglo and Non-Anglo countries for *governance_Boardsupport* and *acmeeting_cae*, but they differ marginally in terms of having a CRO or the equivalent. For *qaip*, there is no difference, but for the control variables, *education_cae*, *experience*, *major_cs_it* and *IAFage*, responses do vary across the two groups of countries. Other control variables that differ between these two groups of countries include *industry_combined* and *employees_organization*.

Multivariate analysis

Table VIII presents the correlation matrix of the variables studied in this research, and, as can be seen, none of the correlation is greater than 0.50 and most are below 0.30, with four exceptions. The correlation between *certification_IS* and *certification_Security* is 0.347, indicating that CAEs with IS certifications are also likely to have security certifications, and the correlation between *iacompetence_grc* and *securityaudit* is 0.335, indicating that IAF competence related to risk, governance, and control are highly associated with the extent of security/cybersecurity audit. The correlation between *IAFage* and *IAFempLN* is 0.356, indicating that as the IAF matures, more employees are hired. Finally, *IAFempLN* and *employees_organization* are highly correlated (0.424); this result makes sense as the larger the organizations, the larger the IAF.

Different certifications seem to have very low correlations with the extent of security/cybersecurity audit, with the CIA certification demonstrating a negative relationship. These findings suggest that professional accountants are likely to focus more on traditional audit functions than on audit activities in emerging risk areas such as security/cybersecurity. Other factors such as lack of knowledge and shortage of skills might also contribute to this trend. *ERM_IA* and *securityaudit* also have negative correlations; this finding is unexpected, as the expectation was that if internal auditors are responsible for ERM, they are likely to conduct more security/cybersecurity audits. One possible reason for this unusual outcome could be that security/cybersecurity risk is completely different from the rest of the risks that the internal auditors deal with, such that many internal auditors do not possess the training and skills required in sophisticated security/cybersecurity audit activities.

Regression analysis

Table IX (Panel A) presents the results of a regression analysis on the full data set, analyzing across regions. Stepwise regression was selected owing to the large number of variables for analysis, and our analysis generally focused on the factors predictive of the degree of security/cybersecurity audit in the internal audit process as a function of a varied

Table VIII.
Correlation matrix

Variables	security audit	certification _Security	certification _IS	cpa	cia	riskassess mentscope	ERM _IA	iacompetence _grc	governance _boardsupport	acmeeting _cae	riskmagt _officer	qaip
security audit	1											
certification_Security	0.0535	1										
certification_IS	0.0876*	0.347***	1									
cpa	0.0395	−0.00769	0.0568	1								
cia	−0.0114	0.0639	0.230***	−0.0153	1							
riskassessmentscope	0.109**	0.0365	−0.00724	0.0474	0.0404	1						
ERM_IA	−0.120***	0.0827*	0.0727*	0.0349	0.0247	0.0565	1					
iacompetence_grc	0.335***	0.0241	0.0680*	0.0305	0.0438	0.0903**	−0.0138	1				
governance_boardsupport	0.176***	0.00851	0.0276	0.00243	−0.0345	−0.0125	−0.0341	0.188***	1			
acmeeting_cae	0.107**	−0.00520	0.0590	0.0181	−0.0448	−0.0142	−0.116***	0.0204	0.0676*	1		
riskmagt_officer	0.200***	0.0588	0.0238	0.0931**	0.0371	0.0220	−0.0776*	0.177***	0.164***	0.0485	1	
qaip	0.228***	−0.00810	0.00249	0.0475	−0.0264	−0.0190	−0.0482	0.148***	0.0924**	0.0859*	0.246***	1
education_cae	0.0943**	0.0547	0.0834*	0.00824	−0.0237	−0.0479	−0.00607	0.103**	−0.0146	−0.00238	0.0629	0.0637
experience	0.134***	0.0233	0.0617	0.0867*	0.116***	0.0303	−0.0431	0.177***	0.120***	−0.0156	0.0825*	0.0346
training_hours	0.136***	0.0480	0.0688*	0.0389	0.125***	0.0313	0.00207	0.159***	0.0368	0.0614	0.0220	0.0432
major_cs_it	0.123***	0.106**	0.228***	−0.0297	0.0473	−0.0342	−0.0188	0.0336	−0.0180	0.0429	0.0389	0.0592
IAF age	0.223***	0.00983	−0.00639	0.0263	−0.0316	0.0785*	−0.161***	0.0914**	0.0740*	0.130***	0.178***	0.137***
IAF empLN	0.267***	0.0733*	0.0533	0.0771*	−0.00431	0.0166	−0.164***	0.109**	0.0601	0.155***	0.172***	0.253***
IAF budget	0.188***	0.0217	0.0393	0.0228	−0.00446	0.0713*	−0.0380	0.197***	0.214***	0.0631	0.124***	0.138***
industry_combined	0.235***	0.0121	0.0355	0.0399	−0.0227	0.0864*	−0.204***	0.0602	0.0594	0.126***	0.191***	0.0687*
employees_organization	0.0826*	0.0110	0.0147	0.0249	0.0503	0.00222	−0.0495	0.136***	0.0448	0.0738*	0.120***	0.130***
AC Countries	−0.0521	0.00880	0.111**	0.252***	0.187***	0.0895**	0.0435	0.0378	0.0315	0.0324	0.0569	−0.0347

Notes: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

(*continued*)

Table VIII.

Variables	education_cae	experience	training _hours	major _cs_it	IAF age	IAF empLN	IAF bud get	industry _combined	employees _organization	AC countries
security audit										
certification_Security										
certification_IS										
cpa										
cia										
riskassessmentscope										
ERM_IA										
iacompetence_grc										
governance_boardsupport										
acmeeting_cae										
riskmagt_officer										
qaip										
education_cae	1									
experience	0.0301	1								
training_hours	0.0560	0.124***	1							
major_cs_it	0.124***	−0.0328	0.00543	1						
IAF age	0.0428	0.131***	0.108**	0.0243	1					
IAF empLN	0.0505	0.0998**	0.0414	0.0258	0.356***	1				
IAF budget	0.00539	0.0486	0.0776*	0.0452	0.140***	0.176***	1			
industry_combined	0.0370	−0.0186	−0.0177	0.0375	0.127***	0.125***	0.106**	1		
employees_organization	0.0251	0.0351	0.0204	0.0241	0.199***	0.424***	0.0629	−0.104**	1	
AC Countries	−0.105**	0.157***	−0.0381	−0.0514	0.0730*	0.00737	0.0332	−0.0483	0.0912**	1

Table IX.
Multivariate analysis: Panel A

Variables	*RQ*	Full dataset (1) securityaudit	Africa (2) securityaudit	Asia (3) securityaudit	Pacific (4) securityaudit
ACCountries		−0.7421** (0.0265)			
experience		0.05010* (0.0630)			
IAFage		0.02862*** (0.0062)		0.08927** (0.0293)	
industry_combined		1.9648**** (0.0000)	4.0940**** (0.0002)	2.0053* (0.0906)	3.7308* (0.0610)
riskassessmentscope	RQ_2	0.7683** (0.0165)			
training_hours		0.009687** (0.0352)			
iacompetence_grc	RQ_4	0.3288**** (0.0000)	0.4605**** (0.0003)	0.2751** (0.0280)	0.7254*** (0.0028)
governance_Boardsupport	RQ_5	1.0209*** (0.0029)			
IAFempLN		0.5445**** (0.0000)			1.8954*** (0.0066)
major_cs_it		1.6124*** (0.0011)			
qaip	RQ_8	1.5850**** (0.0003)	2.9561** (0.0374)	2.0700* (0.0819)	−4.1478* (0.0515)
certification_IS	RQ_{1b}		2.9353** (0.0475)		
education_cae				1.8629* (0.0554)	
cpa	RQ_{1d}			−2.1847** (0.0238)	3.3702** (0.0451)
riskmagt_officer	RQ_7				
ERM_IA	RQ_3				
acmeeting_cae	RQ_6				
_cons		7.7585**** (0.0000)	7.3567*** (0.0014)	10.911**** (0.0000)	−1.3374 (0.7804)
N		848	70	133	31
adj. *R*-sq		0.250	0.380	0.174	0.382

Notes: *p*-values, in parentheses $^{*}p < 0.10$; $^{**}p < 0.05$; $^{***}p < 0.01$; $^{****}p < 0.001$

(*continued*)

Table IX.

Variables	Europe (5) securityaudit	Middle east (6) securityaudit	North america (7) securityaudit	South america (8) securityaudit
ACCountries				
experience	0.1438** (0.0273)	0.2736** (0.0264)		
IAFage	0.04070** (0.0486)	0.1757** (0.0191)		
industry_combined	2.3546*** (0.0020)		1.7042*** (0.0038)	
riskassessmentscope			0.9642* (0.0811)	
training_hours		−0.03770* (0.0794)		0.01605*** (0.0095)
iacompetence_grc	0.1999* (0.0665)	0.5585**** (0.0007)	0.3738**** (0.0000)	0.4791**** (0.0001)
governance_Boardsupport			1.5033*** (0.0086)	
IAFempLN	0.8023*** (0.0046)		1.1571**** (0.0000)	0.7094* (0.0551)
major_cs_it		4.3851** (0.0117)		
qaip				2.5308** (0.0374)
certification_IS				
education_cae				2.0294** (0.0227)
cpa				
riskmagt_officer	1.2994* (0.0825)			
ERM_IA			−1.5248** (0.0181)	−3.9926*** (0.0044)
acmeeting_cae				0.1491* (0.0565)
_cons	9.7151**** (0.0000)	5.7854* (0.0908)	6.5828**** (0.0000)	5.2485** (0.0333)
N	207	50	238	104
adj. *R*-sq	0.221	0.397	0.295	0.420

set of predictors specified in the research questions. RQ_1 posits, in general, that various professional certifications tend to increase the extent of security/cybersecurity audit by the IAF, on the principle that specialized certifications tend to be indicative of increased professional experience and knowledge. We reason that more experienced and knowledgeable auditors largely will bring a greater focus on cybersecurity issues in audits, all things being equal.

Even so, in assessing RQ_1 (directly referencing security certifications, systems auditing certification, internal auditing certification or public accounting certifications), we find that *no* certification is significant in its effect on the extent of security/cybersecurity audit by IAF, overall (in testing the model with pooled data with no regional consideration). Breaking the data set into regions for additional consideration, however, gives a slightly different picture. We do find some region-specific outcomes: certification for IS auditing (variable *certification_IS*) *is* significant in the African region, and public accounting certification (variable *cpa certification*) has mixed and provocative results in the Asia region, where CPA certifications tended to be *less* indicative of the extent of security/cybersecurity audit while in the Pacific region the same certification is *positively* correlated with the security focus on an audit. These results are somewhat unanticipated and provide the basis for interesting interpretations, which we offer in the discussion section.

Asking about the degree to which risk assessment activities by the IAF impact the extent of cybersecurity focus in the auditing process (RQ_2), *riskassessmentscope* is positively and significantly associated with the extent of security/cybersecurity audits. However, we see that this result is based entirely upon the strongly significant effect for the variable found in the North American region of the dataset. This was not conceptualized as a cross-cultural study, but we are noticing some interesting regional effects in analysis. Risk assessment is likely far more impactful in this region owing to legislative efforts targeting accountability and quality of management in firms (Sarbanes Oxley, most significantly) relative to other quarters of the world.

Research Question three (RQ_3), as operationalized, asks about the degree of integration between ERM processes and the IAF, as to its impact on the extent of cybersecurity focus in the auditing process. The answer to this question is a resounding "no", which is interesting and worth consideration. Our results indicate that *ERM_IA* (RQ_3) is *negatively* associated with security/cybersecurity audit in both North American and South American regions. The literature supports the supposition that responsibility of ERM residing with the IAF will lead to *more* extensive security/cybersecurity audit activity because security/cybersecurity risk also demands efficient risk management. The results run counter to this. Given the limitations of generality arising from analyzing a pre-structured database, we can speculate with limitation. One notion is that risk management sophistication implicitly includes detailed knowledge of cybersecurity concerns, in which case sophisticated ERM in the IAF covers cybersecurity risk without the need for additional focus on the matter as a separate element of the audit process. We might alternatively suppose that this mirrors Steinbart *et al.* (2012, 2013) indication that a general lack of knowledge exists about the importance of security expertise in the internal audit process (i.e. ERM sophistication is not a broadly impressive preparation for cybersecurity audit expertise). We will consider this point in further detail in our discussion section.

RQ4 considers the degree to which IAF governance skills (governance, risk and compliance) impact the extent of security/cybersecurity in the audit process. In the broad data set, that is, in all analyzed regions, *iacompetence_grc* (RQ_4) is positively and significantly associated with the extent of security/cybersecurity audit. This finding again confirms Steinbart's indication that security expertise of IAF contributes to information

security effectiveness (Steinbart *et al.*, 2012; 2013). By contrast, asking whether the board authorizes the IAF to review governance policies (*RQ5*, variable *governance_Boardsupport*) leads to a positive relation *only* in the North America region. This outcome might arise from strong corporate governance and robust regulatory enforcement in North America, especially from factors such as Sarbanes Oxley and HIPPA, and to that extent, perhaps this finding should have been expected to exhibit regional difference.

We did not find that frequent audit committee meetings with the CAE led to a greater extent of security/cybersecurity audit processes (RQ_6). This might be due to the fact that audit committees have not focused on security issues or that boards are taking care of this issue instead. However, recent anecdotal evidence suggests that in many cases, internal auditors are expected to play a role on behalf of the audit committee to formulate an effective cybersecurity risk management (Deloitte, 2015). As such, we expect that there is a need for further research about this lack of involvement on the part of the audit committee or its equivalent in interactions with the CAE on cybersecurity matters.

The notion that the risk management function being led by a specific risk management officer (CRO) would result in a greater extent of cybersecurity audit activities (RQ_7) was only significant in Europe, which suggests to us a differential emphasis on the degree and type of risks companies face on each side of the Atlantic. This finding also suggests that the role of the CRO has not matured enough to address security/cybersecurity risks. This might be the case due to the fact that security issues are emergent in many areas, and hence CROs have not yet taken them into account, or that management has decided to tolerate the risks of certain security issues given the cost/benefits associated solving such problems. At the same time, the impact of robust QAIPs in a firm (RQ_8, as assessed by the variable *qaip*) is positive and significant for companies reporting from the regions of Africa, Asia, and South America, and negatively associated with the extent of security/cybersecurity audit in the Pacific region (characterized by Australia and New Zealand). This finding suggests that the quality of IAF has an effect on the extent of security/cybersecurity audit. These qualities of IAF might arise from the competence related to governance, risk and compliance. However, we think further research should delve into how the quality of IAF is associated with the extent of security/cybersecurity audit. For control variables, we have obtained expected results. However, it is found that Anglo countries are negatively associated with the extent of security/cybersecurity audit.

As discussed earlier, we analyzed data between Anglo and Non-Anglo countries since a large portion of our data are from Anglo countries. In panel B of Table X, *iacompetence_grc* and *governance_Boardsupport* are significantly and positively associated with security/cybersecurity audit in both Anglo and Non-Anglo countries; this result is different from when the analysis is run *across* different regions. Regional analysis might balance results of one region against another. Nevertheless, we found only the North American region significant. We consider that this analysis reflects the true nature of the association, as each country in its respective group shares similar characteristics. These findings again confirm that IAF competence and board support regarding governance is associated with security/cybersecurity audit. In addition, *riskassessmentscope* and *qaip* are significantly and positively associated with security/cybersecurity audit in Non-Anglo countries, thus confirming that comprehensive risk assessment and quality of IAF are positively and significantly associated with security/cybersecurity audit. Even so, *ERM_IA* is negatively associated with security/cybersecurity audit only in Anglo nations. This finding might be due to the fact that the IAF in Anglo nations is overwhelmed with traditional risks or that they lack competencies as suggested by Steinbart *et al.* (2012, 2013). Overall, these findings are not very much different from those of regional analysis. Both analyses confirm that IAF

Variables	*RQ*	Full data set (1) securityaudit	AC countries (2) securityaudit	Non-AC countries (3) securityaudit
ACCountries		−0.7421** (0.0265)		
experience		0.05010* (0.0630)		0.08210** (0.0326)
IAFage		0.02862*** (0.0062)		0.04109*** (0.0024)
industry_combined		1.9648***** (0.0000)	1.9366***** (0.0003)	1.9395***** (0.0000)
riskassessmentscope	RQ_2	0.7683** (0.0165)		0.9062** (0.0332)
training_hours		0.009687** (0.0352)		0.01103** (0.0338)
iacompetence_grc	RQ_4	0.3288***** (0.0000)	0.3515***** (0.0000)	0.3278***** (0.0000)
governance_Boardsupport	RQ_5	1.0209*** (0.0029)	1.3563*** (0.0072)	0.8685* (0.0542)
IAFempLN		0.5445***** (0.0000)	1.0245***** (0.0000)	0.3523** (0.0288)
major_cs_it		1.6124*** (0.0011)		1.6554*** (0.0081)
qaip	RQ_8	1.5850***** (0.0003)		2.1857***** (0.0001)
ERM_IA	RQ_3		−1.6232*** (0.0060)	
_cons		7.7585***** (0.0000)	7.9718***** (0.0000)	7.5943***** (0.0000)
N		848	306	542
adj. *R*-sq		0.250	0.261	0.257

Notes: *p*-values in parentheses; *$p < 0.10$; **$p < 0.05$; ***$p < 0.01$; ****$p < 0.001$

Table X. Multivariate analysis: panel B

competencies, comprehensive risk assessment, and board support are associated with the extent of security/cybersecurity audit. The only unexpected results arise in cases where the IAF is tasked with ERM and the role of the CRO has not grown enough to address security/cybersecurity risks.

These findings are in line with Abdolmohammadi and Boss (2010), wherein they find that IS certification, IAF age and training are significantly and positively associated with IT audit by IAF. As in their study, we also find that CPA and CIA certification and education of CAE are not significantly associated with security/cybersecurity audit. However, unlike the Abdolmohammadi and Boss study, we find that CAE experience and CAE academic major does have a significant association with the extent of security/cybersecurity audit.

Sensitivity analysis

The dependent variable *securityaudit* is measured by summing the responses of the questions 92-1 through 92-7 for the models discussed above, that is, a summed-score composite was used. These security questions (Q92-1 through Q92-7) cover the following areas of security/cybersecurity: general IT security, cybersecurity, physical security of data centers, security of mobile devices, social media security, intranet security and website security. It is possible from a standpoint of internal validity that the questions might measure a construct conceptually related to but qualitatively different from security/cybersecurity audit, as is examined in our work. Hence, to examine the dimensionality of these questions for the *securityaudit* variable in our model, factor analysis was conducted (principle components with varimax rotation) as recommended by Schroeder and Hogan (2013). Bartlett's test of sphericity also supported the wisdom of conducting a factor analysis. Results from the factor analysis confirmed that the criterion questions do, indeed, perform in a unidimensional manner. A single factor was found with an eigenvalue of 4.52, accounting for 64.64 per cent of variance, and all factor loadings were above recommended thresholds (Hair *et al.*, 1998). As such, this analysis confirms that these questions measure the dependent variable – *securityaudit* – quite well. We used the Bartlett's method to produce

individual respondent factor scores, which we later use for regressions analysis to test the sensitivity of our results. We did not document any significant changes in the results, thus confirming that the summed score dependent variable does not bias the result.

Discussion and conclusion

The purpose of the study is to explore the factors associated with the extent of security/cybersecurity audits by the IAF. Using responses from 970 CAEs across different regions represented in CBOK (2015) database, it was determined that the extent of security/cybersecurity audit by the IAF in firms is not uniform across different regions and countries. Different factors play different roles across the regions and countries with regard to the prevalence of security/cybersecurity audit. Descriptive statistics and univariate analysis of data suggest that IAFs across different regions significantly differ in their involvement with security/cybersecurity risks. For example, the number of CAEs with security certification is far lower in our sample when compared to traditional certifications such as CPA or CIA. This result is both expected and to a degree unexpected. It is expected in the sense that security is not direct area of responsibility for CAEs to deal with; however, in view of the rising tide of cyberattacks, IAFs are expected by stakeholders to play a leading role in cybersecurity risk management programs in organizations. Nevertheless, the data indicate that CAEs are not still well prepared to lead this role, as reflected by the low percentage of CAEs with pertinent security certifications. This finding mirrors that of Steinbart *et al.* (2012, 2013), in which they documented that when internal auditors possess detailed technical expertise about information security, they are able to develop deeper relationships with the IS security function. However, certification remains significantly and positively associated with IT audit (Abdolmohammadi and Boss, 2010).

In addition, the competencies related to risk – governance and compliance by IAF – have an impact on the security/cybersecurity risk management. The IAF's lack of security expertise was first documented by Steinbart *et al.*'s (2012) qualitative study, in which they documented that the IAF's lack of technical skills and communication skills affects information security effectiveness. Later, Steinbart *et al.* (2013) empirically found that the frequency of IAF review of different aspects of security impacts the security effectiveness of organizations. Our results thus confirm the findings of Steinbart *et al.* (2012, 2013) and reiterate the importance of improving IAF competencies to form an effective security/cybersecurity risk management program. In a similar fashion, we have found that comprehensive risk assessment affects the security/cybersecurity audit. Risk assessment is one of the eight components of ERM (COSO, 2004). Although the literature suggests that different kinds of risk assessment models are used by IAF (Allegrini and D'Onza, 2003), a comprehensive risk management process is vital for security risk management. The fraud literature also supports the use of comprehensive risk assessment in fraud risk management (Lister, 2007). Unexpectedly, IAF being tasked with ERM in an organization does not impact security well as it is not found to be significantly associated with the extent of security/cybersecurity audit.

The literature suggests mixed results when IAF is tasked with ERM of an organization (Walker *et al.*, 2003; Beasley *et al.*, 2005; de Zwaan *et al.*, 2011). In our case, we suspect that IAF tasked with ERM either focuses on traditional risk areas, overlooking cybersecurity risks, or that it lacks the required skills to perform security/cybersecurity audits. We recommend future research exploring this lack of association.

The findings of the study also suggest that board support related to governance is significant even though the role of the audit committee is not, which highlights the importance of good governance in mitigating security risks. Studies confirm that good

corporate governance is associated with mitigating many kinds of risks (Klein, 2002; Armstrong *et al.*, 2014; Armstrong *et al.*, 2015; Beasley, 1996); however, very little is known about the role of corporate governance in mitigating security risks in organizations (Higgs *et al.*, 2016; Haislip *et al.*, 2017; Islam and Stafford, 2017). This scarcity emphasizes the need for more research on the role of good corporate governance in mitigating security risks. Like the audit committee, the CRO's role in mitigating security risk does not perform as expected, although the role of the CRO in mitigating risks and reaping the subsequent benefits is well documented (Aabo *et al.*, 2005). Finally, the quality of the internal audit process plays a role in mitigating security/cybersecurity risks. This finding is in line with the literature on IAF quality (Prawitt *et al.*, 2009; Ege, 2015; Pizzini *et al.*, 2014).

In sum, IAF competencies, comprehensive risk assessment, board support, and quality of internal audits are associated with the extent of security/cybersecurity audit; however, IAF being tasked with ERM and the role of CRO are not significantly associated with the extent of security/cybersecurity audit.

Key contributions

To the best of our knowledge, this study is the first to describe IAF involvement in security/cybersecurity audit, which is an increasingly important IT governance dimension. It provides insights into the specific IAF/CAE characteristics and corporate governance characteristics that can lead the IAF to contribute to security/cybersecurity audit outcomes. Moreover, given the issuance of the "cybersecurity risk management framework" by AICPA, the findings of the study will help auditors to plan for and perform effectively this new attestation service. Furthermore, the study makes important contributions to the internal audit literature, IT governance literature and ERM literature. The findings add to the results of prior studies on the IAF involvement in different IT-related aspects such as IT audit and XBRL implementation (Abdolmohammadi *et al.*, 2017; Abdolmohammadi and Boss, 2010) and as regards the role of the board and the audit committee in ERM (Beasley *et al.*, 2005). The findings of the study are useful for boards, policymakers, and auditors in formulating an effective cyber security risk management program.

Practical implications

The findings of the study have several practical implications. First, identification of IAF characteristics that contribute to the support of security/cybersecurity audit will help management to make effective resource allocation decisions and aid in the development of policies related to competencies required for IAF functions or the operation of CAEs. Second, the findings are of interest to boards of directors who are going to delegate risk management and governance issues to an audit committee or a CRO. The results indicate the role of an audit committee or a CRO in impacting security/cybersecurity audit and highlights the importance of factors that have significant effects on the extent of security/cybersecurity audit. Third, the IAF tasked with ERM function of an organization should focus on security risks besides traditional risks; alternatively, the responsibility can be delegated. Finally, policymakers will have interest in the findings because they highlight the factors that have an influential role in cybersecurity risk management in the private sector. Policymakers can require new skills or competencies, or issue new governance guidelines that will help mitigate the incidence of cyberattacks in the corporate world.

Limitations and directions for future research

The research has some limitations. First, as the CBOK database is generated from surveys of CAEs and other internal auditors, it is subject to survey research limitations

especially in regard to the differential perceptions of individuals in their subjective views of reality and also in regard to the level of measurement chosen by the owners of the dataset we accessed and subsequent assumptions for statistical tests (particularly in terms of nominal variables which we were forced to include as dummy variables in our testing). Second, this research focuses on associational analysis and cannot be taken as providing direct evidence of causality. Third, as our sample includes respondents from organizations in which audit committees might be present, caution should be taken before interpreting and generalizing the results to situations beyond that context. Fourth, we acknowledge that security/cybersecurity audit might be performed by parties other than the IAF, including the IT department of the organization or outside consultants from professional organizations such as Big Four audit firms. In those cases, results should be interpreted cautiously.

Finally, an endogeneity problem can occur when an explanatory variable is correlated with the error term, which is a serious limitation in non-experimental research (Hamilton and Nickerson, 2016). Unfortunately, solving the problem is often more challenging than its basic nature suggests, in accord with Tukey's (1986) sage observation that there are limits to the sorts of analysis that can be objectively derived from data and modeling, in line with the assumptions most statistical models presume in order to support such analysis. It is a weak point to fall back on model assumptions and *ceteris paribus* limitations, certainly, but this is the typical response to the point. Accordingly, our results are limited by the potential for endogeneity.

Additional research opportunities are suggested by these limitations. For example, future studies could seek to understand the reasons why the IAF tasked with ERM or CRO has not manifested the expected results with security/cybersecurity audit, as noted above. Furthermore, future research could focus on the reasons for low involvement of the audit committee with the extent of security/cybersecurity audit. Finally, further clarity must be sought in understanding the role of security certifications which could lead to effective cybersecurity risk management programs on the part of the IAF.

References

Aabo, T., Fraser, J. and Simkins, B. (2005), "The rise and evolution of the chief risk officer: enterprise risk management at hydro one", *Journal of Applied Corporate Finance*, Vol. 17 No. 3, pp. 62-75.

Abbott, L., Parker, S. and Peters, F. (2004), "Audit committee characteristics and restatements", *Auditing: A Journal of Practice & Theory*, Vol. 23 No. 1, pp. 69-87.

Abdolmohammadi, M. (2009), "Factors associated with the use of and compliance with the IIA standards: a study of Ango-culture CAEs", *International Journal of Auditing*, Vol. 13 No. 1, pp. 27-42.

Abdolmohammadi, M. (2012), "Chief Audit Executives' assessment of internal auditors' performance attributes by professional rank and cultural cluster", *Behavioral Research in Accounting*, Vol. 24 No. 1, pp. 1-23.

Abdolmohammadi, M. (2013), "Correlates of co-sourcing/outsourcing of internal audit activities", *Auditing: A Journal of Practice & Theory*, Vol. 32 No. 3, pp. 69-85.

Abdolmohammadi, M. and Boss, S. (2010), "Factors associated with IT audits by the internal audit function", *International Journal of Accounting Information Systems*, Vol. 11 No. 3, pp. 140-151.

Abdolmohammadi, M., DeSimone, S. and Hsieh, T. (2017), "Factors associated with Internal Audit Function involvement with XBRL implementation in public companies: an international study", *International Journal of Accounting Information Systems*, Vol. 25, pp. 45-56.

Aguilar, L. (2014), "Boards of directors, corporate governance and cyber-risks: sharpening the focus", Retrieved from US Securities and Exchange Commission, avaialble at: www.sec.gov/news/speech/2014-spch061014laa

AICPA (2017), *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*, American Institute of Certified Public Accountants, New York, NY.

Allegrini, M. and D'Onza, G. (2003), "Internal auditing and risk assessment in large Italian companies: an empirical survey", *International Journal of Auditing*, Vol. 7 No. 3, pp. 191-208.

Almadhoob, A. and Valverde, R. (2014), "Cybercrime prevention in the kingdom of Bahrain via IT security audit plans", *Journal of Theoretical and Applied Information Technology*, Vol. 65 No. 1, pp. 274-292.

Armstrong, C., Core, J. and Wayne, G. (2014), "Do independent directors cause improvements in firm transparency?", *Journal of Financial Economics*, Vol. 113 No. 3, pp. 383-403.

Armstrong, C., Blouin, J., Jagolinzer, A. and Larcker, D. (2015), "Corporate governance, incentives, and tax avoidance", *Journal of Accounting and Economics*, Vol. 60 No. 1, pp. 1-17.

Asare, S., Davidson, R. and Gramling, A. (2008), "Internal auditors' evaluation of fraud factors in planning an audit: the importance of audit committee quality and management incentives", *International Journal of Auditing*, Vol. 12 No. 3, pp. 181-203.

Barua, A., Rama, D.V. and Sharma, V. (2010), "Audit committee characteristics and investment in internal auditing", *Journal of Accounting and Public Policy*, Vol. 29 No. 5, pp. 503-513.

Beasley, M. (1996), "An empirical analysis of the relation between the board of director composition and financial statement fraud", *The Accounting Review*, Vol. 71 No. 4, pp. 443-465.

Beasley, M., Carcello, J. and Hermanson, D. (1999), "Fraudulent financial reporting: 1987-1997, an analysis of US public companies", *The Auditor's Report*, Vol. 22 No. 3, pp. 15-17.

Beasley, M., Carcello, J. and Hermanson, D. (2005), "ERM: a status report", *Internal Auditor*, Vol. 62 No. 1, pp. 67-72.

Beasley, M., Clune, R. and Hermanson, D. (2005), "Enterprise Risk Management: an empirical analysis of factors associated with the extent of implementation", *Journal of Accounting and Public Policy*, Vol. 24 No. 6, pp. 521-531.

Beasley, M., Clune, R. and Hermanson, D. (2006), *The Impact of Enterprise Risk Management on the Internal Audit Function, Kennesaw*, Kennesaw State University, GA.

Blue Ribbon Committee (1999), *Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees*, NYSE, New York, NY.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2013), "Information security compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Burning Glass Technologies (2015), "Job market intelligence: cybersecurity jobs, 2015", avaiable at: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

Campbell, K., Gordon, L., Loeb, M. and Zhou, I. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, Vol. 11 No. 3, pp. 431-448.

Carter, L., Millington, P. and Philips, B. (2012), "The impact of information technology internal controls on firm performance", *Journal of Organizational and End User Computing*, Vol. 24 No. 2, pp. 39-49.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), "The effect of Internet security breach announcements on market value of breached firms and Internet security developers", *International Journal of Electronic Commerce*, Vol. 9 No. 1, pp. 69-105.

Cavusoglu, H., Raghunathan, S. and Cavusoglu, H. (2009), "Configuration of and interactions between security technologies: the case of firewalls and intrusion detection systems", *Information Systems Research*, Vol. 20 No. 2, pp. 198-217.

CBOK (2015), *Common Body of Knowledge in Internal Auditing*, The Institute of Internal Auditors Research Foundation, Altamonte Springs.

Center for Audit Quality (2017), *How the Auditing Profession Promotes Cybersecurity Resilience*, Center for Audit Quality.

Christ, M., Masli, N., Sharip, N. and Wood, D. (2015), "Rotational internal audit programs and financial reporting quality: Do compensating controls help?", *Accounting, Organizations and Society*, Vol. 44, pp. 37-59.

Committee of Sponsoring Organizations (COSO) (2004), "Enterprise Risk Management – Integrated framework executive summary", avaialble at: www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

D'Arcy, J., Hovav, A. and Galleta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 201 No. 1, pp. 79-98.

De Haes, S. and Grembergen, W. (2009), "An exploratory study into IT governance implementation and its impact on business/IT alignment", *Information Systems Management*, Vol. 26 No. 2, pp. 123-137.

De Zwaan, L., Stewart, J. and Subramaniam, N. (2011), "Internal audit involvement in Enterprise Risk Management", *Managerial Auditing Journal*, Vol. 26 No. 7, pp. 586-604.

Deloitte (2015), "Cybersecurity: the changing role of audit committee and internal audit", available at: www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

Deloitte (2017), "Cybersecurity and the role of internal audit: an urgent call to action", available at: www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html

DeSimone, S. and Abdolmohammadi, M. (2016), "Correlates of external quality assessment and improvement program in internal auditing: a study of 68 countries", *Journal of International Accounting Research*, Vol. 15 No. 2, pp. 53-71.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizations perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Dhillon, G., Tejay, G. and Hong, W. (2007), "Identifying governance dimensions to evaluate information systems security in organizations", *Proceedings of the 40th Hawaii International Conference on Systems Sciences*.

Dimension Data (2017), "The executive's guide to the 2017 Global Threat Intelligence Report", avaialble at: www2.dimensiondata.com/en/microsites/global-threat-intelligence-report

DiPietro, B. (2013), "Cybercrime 2014: More attacks, more boardroom scrutiny", avaialble at: http://blogs.wsj.com/cfo/2013/12/03/cybercrime-2014-more-attacks-moreBoardroom-

Ege, M. (2015), "Does Internal Audit Function quality deter management miscoduct?", *The Accounting Review*, Vol. 90 No. 2, pp. 495-497.

Goldstein, J., Chernobai, A. and Benaroch, M. (2011), "An event study analysis of the economic impact of IT operational risk and its subcategories", *Journal of the Association for Information Systems*, Vol. 12 No. 9, pp. 606-631.

Gordon, L. and Loeb, M. (2002), "The economics of information security investment", *ACM Transactions on Information Systems Security*, Vol. 5 No. 4, pp. 438-457.

Gordon, L., Loeb, M. and Sohail, T. (2010), "Market value of voluntary disclosures concerning information security", *MIS Quarterly*, Vol. 34, pp. 567-594.

Gregogry and Austin LLP (2014), "Board oversight of cybersecurity risks", avaialble at: https://content.next.westlaw.com/5-558-2825?transitionType=Default&contextData=(sc.Default)&__lrTS=20170609212306243&firstPage=true&bhcp=1

Haislip, J., Lim, J. and Pinsker, R. (2017), "Do the roles of the CEO and CFO differ when it comes to data security breaches", *Proceedings of the 2017 Americas Conference for Information Systems, Association for Information Systems, Boston, MA*.

Hair, J., Anderson, R., Tatham, R. and Black, W. (1998), *Multivariate Data Analysis*, 5th ed., Prentice Hall, Upper Saddle River, NJ.

Hamilton, B.H. and Nickerson, J.A. (2016), "Correcting for endogeneity in strategic management research", *Strategic Organization*, Vol. 1 No. 1, pp. 51-78.

HBGary Inc (2013), "Cybersecurity directly affects investor attitudes, new HBGary survey finds", available from PR Newswire A Cision Company: www.prnewswire.com/news-releases/cybersecurity-directly-affects-investor-attitudes-new-hbgary-survey-finds-193105951.html

Herath, H. and Herath, T. (2014), "IT security auditing: a performance evaluation decision model", *Decision Support Systems*, Vol. 57, pp. 54-63.

Herath, T. and Rao, R. (2009), "Protection motivation and deterrence: a framework for security compliance in organizations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Heroux, S. and Fortin, A. (2013), "The internal audit function in information technology governance: a holistic perspective", *Journal of Information Systems*, Vol. 27 No. 1, pp. 189-217.

Higgs, J., Pinsker, R., Smith, T. and Young, G. (2016), "The relationship between board-level technology committees and reported security breaches", *Journal of Information Systems*, Vol. 30 No. 3, pp. 79-98.

Hong, K., Chi, Y., Chao, L. and Tang, J. (2003), "An integrated system theory of information security management", *Information Management and Computer Security*, Vol. 11 No. 5, pp. 243-248.

Iheagwara, C. (2004), "The effect of intrusion detection management methods on the return on investment", *Computer Security*, Vol. 23, pp. 213-228.

Islam, M.S. and Stafford, T. (2017), "Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors", *Proceedings of the 2017 Americas Conference for Information Systems, Association for Information Systems, Boston, MA*.

ITGI (2012), *COBIT5 for Information Security*, IT Governance Institute, Rolling Meadows, IL.

Johnston, A. and Warkentin, M. (2010), "Fear appeals and information security behavior: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Juniper Research (2015), "Cybercrime will cost businesses over $2 trillion by 2019", avaialble at: www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Klein, A. (2002), "Audit committee, board of director characteristics, and earnings management", *Journal of Accounting and Economics*, Vol. 33 No. 3, pp. 375-400.

KPMG (2014), "Global boardroom insights", avaialble at: https://home.kpmg.com/xx/en/home/insights/2015/04/global-Boardroom-insights-series.html

Kumar, R., Park, S. and Subramaniam, C. (2008), "Understanding the value of countermeasure portfolios in information systems security", *Journal of Management Information Systems*, Vol. 25, pp. 241-279.

Kwon, J., Ulmer, J. and Wang, T. (2013), "The association between top management involvement and compensation and information security breaches", *Journal of Information Systems*, Vol. 27 No. 1, pp. 219-236.

Li, C., Peters, G., Richardson, V. and Weidenmier-Watson, M. (2012), "The consequences of information technology control weaknesses on management information systems", *MIS Quarterly*, Vol. 36 No. 1, pp. 179-204.

Lin, S., Pizzini, M., Vargus, M. and Bardhan, I. (2011), "The role of the Internal Audit Function in the disclosure of material weaknesses", *The Accounting Review*, Vol. 86 No. 1, pp. 287-323.

Lister, L. (2007), "A practical approach to fraud risk", *Internal Auditor*, pp. 61-65.

Lo, E. and Marchand, M. (2004), "Security audit: a case study", *Proceedings of the CCECE, Niagara Falls*.

Mishar, S. and Dhillon, G. (2006), "Information systems security governance research: a behavioral perspective", *Proceedings of the 1st Annual Symposium on Information Assurance*, New York, NY.

National Commission on Fraudulent Financial Reporting (Treadway Commission) (1987), *Report of the National Commission on Fraudulent Financial Reporting*, AICPA, New York, NY.

Ngai, E.H., Wong, Y. and Sun, X. (2011), "The application of data mining techniques in financial fraud detection: a classification framework and an academic review of literature", *Decision Support Systems*, Vol. 50 No. 3, pp. 559-569.

Onwubiko, C. (2009), "A security audit framework for security management in the Enterprise", *Proceedings of 5th International Conference ICGS3, London*.

Pagach, D. and Warr, R. (2011), "The characteristics of firms that hire Chief Risk Officer", *The Journal of Risk and Insurance*, Vol. 78 No. 1, pp. 185-211.

Patton, D.M. (2005), "An analysis of the impact of locus-of-control on internal auditor job performance and satisfaction", *Managerial Auditing Journal*, Vol. 20 Nos 8/9, pp. 1016-1029.

Pereira, T. and Santos, H. (2010), "A security framework for audit and manage information systems security", *Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*.

Pizzini, M., Lin, S. and Ziegenfuss, D. (2014), "The impact of Internal Audit Function quality and contribution on audit delay", *Auditing: A Journal of Practice & Theory*, Vol. 34 No. 1, pp. 25-58.

Ponemon Institute (2015), "Cost of Cyber Crime Study: United States", avaialble at: http://img.delivery.net/cm50content/hp/hosted-files/2015_US_CCC_FINAL_4.pdf

Prawitt, D., Sharp, N. and Wood, D. (2012), "Internal audit outsourcing and the risk of misleading or fraudulent financial reporting: did Sarbanes-Oxley get it wrong", *Contemporary Accounting Research*, Vol. 29 No. 4, pp. 1109-1136.

Prawitt, D., Smith, J. and Wood, D. (2009), "Internal audit quality and earnings management", *The Accounting Review*, Vol. 84 No. 4, pp. 1255-1280.

PriceWaterhouseCoopers (PWC) (2017), *Staying the Course toward True North: Navigating Disruption*, PWC.

Protiviti (2015), "*The Battle Continues – Working to Bridge the Data Security Chasm*", avaialble at: www.protiviti.com/sites/default/files/united_states/insights/2015-it-security-privacy-survey-protiviti.pdf

Public Company Accounting Oversight Board (PCAOB) (2012), "AS1301: Communications with Audit Committees", available at: https://pcaobus.org/Standards/Auditing/Pages/AS1301.aspx

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Sarens, G. and De Beelde, I. (2006), "Internal auditors' perception about their role in risk management: a comparison between US and Belgian companies", *Managerial Auditing Journal*, Vol. 21 No. 1, pp. 63-80.

Sarens, G., Abdolmohammadi, M. and Lenz, R. (2012), "Factors associated with the Internal Audit Function's role in corporate governance", *Journal of Applied Accounting Research*, Vol. 13 No. 2, pp. 191-204.

Schroeder, J. and Hogan, C. (2013), "The impact of PCAOB AS5 and the economic recession on client portfolio characteristics of the Big 4 audit firms", *Auditing: A Journal of Practice & Theory*, Vol. 32 No. 4, pp. 95-127.

Siponen, M. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Spear, J. and Barki, H. (2010), "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

Steinbart, P., Raschke, R., Gal, G. and Dilla, W. (2012), "The relationship between internal audit and information security: an exploratory investigation", *International Journal of Accounting Information Systems*, pp. 228-243.

Steinbart, P., Raschke, R., Gal, G. and Dilla, W. (2013), "Information security professionals' perceptions about the relationship between the Information Security and Internal Audit Functions", *Journal of Information Systems*, Vol. 27 No. 2, pp. 65-86.

Steinbart, P., Raschke, R., Gal, G. and Dilla, W. (2016), "SECURQUAL: an instrument for evaluating the effectiveness of Enterprise Information Security programs", *Journal of Information Systems*, Vol. 30 No. 1, pp. 71-92.

Steinbart, P., Raschke, R., Graham, G. and Dilla, W. (2014a), "Internal audit's contribution to the effectiveness of information security (part 1): perceptions of information security professionals", *ISACA Journal*, Vol. 2, pp. 42-47.

Steinbart, P., Raschke, R., Graham, G. and Dilla, W. (2014b), "Internal audit's contribution to the effectiveness of information security (part 2): perceptions of internal auditors", *ISACA Journal*, Vol. 3, pp. 51-55.

Stoel, D., Havelka, D. and Merhout, J. (2012), "An analysis of attributes that impact information technology audit quality: a study of IT and financial audit practitioners", *International Journal of Accounting Information Systems*, Vol. 13, pp. 60-69.

Straub, D. (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276.

The Heritage Foundation (2015), "Cyber attacks on US companies since November 2014", avaialble at: http://report.heritage.org/ib4487

The Institute of Internal Auditors (IIA) (2015a), "Common Body of Knowledge (CBOK) Resource Exchange", avaialble at: https://global.theiia.org/iiarf/pages/common-body-of-knowledge-cbok.aspx

The Institute of Internal Auditors (IIA) (2015b), "Navigating Technology's Top 10 risks: Internal Audit's Role", avaialble at: http://theiia.mkt5790.com/Navigating_Technologys_Top_10_Risks/?webSyncID=ad198d79-

The Institute of Internal Auditors (IIA) (2017), "International standards for the professional practice of internal auditing", avaialble at: https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf

Tukey, J.W. (1986), "Sunset Salvo", *The American Statistician*, Vol. 40 No. 1, pp. 72-76.

Tysiac, K. (2014), "Technology plays a role in board members' top two concerns", available at: www.cgma.org/magazine/2014/jul/201410602.html

US Securities and Exchange Commission (SEC) (2011), "CF disclosure guidance: Topic No. 2", available at: www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Walker, P., Shenkir, W. and Barton, T. (2003), "ERM in practice", *Internal Auditor*, pp. 51-55.

Walker, P., Shenkir, W. and Barton, T. (2002), *Enterprise Risk Management: Putting it all Together*, Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

Wang, J., Chaudhury, A. and Rao, H. (2008), "A value-at-risk approach to Information Security investment", *Information Systems Research*, Vol. 19 No. 1, pp. 106-120.

Wang, T., Kannan, K. and Ulmer, J. (2013), "The association between the disclosure and the realization of information security risk factors", *Information Systems Research*, Vol. 24 No. 2, pp. 201-218.

Watts, R. and Zimmerman, J. (1983), "Agency problems, auditing, and the theory of the firm: some evidence", *Journal of Law and Economics*, Vol. 26 No. 3, pp. 613-633.

Willison, R. and Warkentin, M. (2013), "Beyond deterrence: an expanded view of employee computer abuse", *MIS Quarterly*, Vol. 37 No. 1, pp. 1-20.

About the authors

Md. Shariful Islam is a Doctoral Student in the Louisiana Tech University. He earned MBA from the Eastern Illinois University and BBA from the University of Dhaka. He is a certified CPA in Illinois and holds CMA license in Bangladesh. He is a Faculty Member (on study leave) in the Accounting & Information Systems department in the University of Dhaka. His research interests include the internal auditors' role in cybersecurity and accounting information systems.

Nusrat Farah is a Doctoral Student in the Oregon State University. She has completed her Master of Arts in Economics at Eastern Illinois University and both BBA and MBA from University of Dhaka. She is a Faculty Member (on study leave) in the Accounting & Information Systems Department in University of Dhaka. Her research interests include entrepreneurial creativity, merger and acquisitions and the internal auditors' role in IT audit.

Thomas F. Stafford is J.E. Barnes Professor of Computer Information Systems in the College of Business, Louisiana Tech University. Stafford holds PhD in Marketing from the University of Georgia and Ph.D. in Management Information Systems from the University of Texas – Arlington. Stafford is Editor of ACM's Data Base for Advances in Information Systems and is Conference Co-Chair of the 2018 Americas Conference for Information Systems. Stafford is an international authority on the topic of malware, and his research spans behavioral and neurocognitive aspects of information systems security and information assurance. Thomas F. Stafford is the corresponding author and can be contacted at: stafford@latech.edu