Communications of the Association for Information Systems

Volume 43 Article 27

9-2018

The Role of Accounting and Professional Associations in IT Security Auditing: An AMCIS Panel Report

Thomas Stafford
Louisiana Tech University, stafford@latech.edu

Graham Gal
University of Massachusetts – Amherst

Robin Poston
University of Memphis

Robert E. Crossler
Washington State University

Randi Jiang
Louisiana Tech University

See next page for additional authors

Recommended Citation
Stafford, Thomas; Gal, Graham; Poston, Robin; Crossler, Robert E.; Jiang, Randi; and Lyons, Robin (2018) "The Role of Accounting and Professional Associations in IT Security Auditing: An AMCIS Panel Report," *Communications of the Association for Information Systems*: Vol. 43 , Article 27.
DOI: 10.17705/1CAIS.04327
Available at: https://aisel.aisnet.org/cais/vol43/iss1/27

The Role of Accounting and Professional Associations in IT Security Auditing: An AMCIS Panel Report

Authors
Thomas Stafford, Graham Gal, Robin Poston, Robert E. Crossler, Randi Jiang, and Robin Lyons

Communications of the Association for Information Systems

Panel Report DOI: 10.17705/1CAIS.04327 ISSN: 1529-3181

The Role of Accounting and Professional Associations in IT Security Auditing: An AMCIS Panel Report

Thomas F. Stafford
Department of Computer Information Systems
Louisiana Tech University
stafford@latech.edu

Graham Gal
Department of Accounting
University of Massachusetts – Amherst

Robin Poston
Management Information Systems
University of Memphis

Robert E. Crossler
Management, Information Systems, & Entrepreneurship
Washington State University

Randi Jiang
Department of Computer Information Systems
Louisiana Tech University

Robin Lyons
Information Systems Audit and Control Association (ISACA)

Abstract:

Information systems security is a critical area of inquiry and closely allied with IT audit skills from the accounting discipline. While accounting scholars are well informed about IT audits, information systems scholars interested in the security aspects of IT audits sometimes lack knowledge about the process through which scholars and professionals become security and audit experts in order to assess the quality of information-security implementations. IT audit knowledge enriches cybersecurity professors for both teaching and research. Individuals skilled in accounting, such as graduates from combined accounting/information systems departments in business schools, are naturally oriented to industry certification groups and their professional certifications, but mainstream IT academics are not. In this paper, we report on a panel discussion at AMCIS 2017 that focused on how researchers and educators who seek professional certifications offered by organizations such as the Information Systems Audit and Control Association (ISACA) can gain much richer knowledge of and insights into IT security assurance, which they can use for both teaching and research purposes. Such certifications provide valuable perspectives for the classroom and for research and are useful for IT professors interested in all aspects of security.

Keywords: IT Security, IT Security Auditing, Accounting and IT, Professional Certifications.

This manuscript underwent peer review. It was received 10/30/2017 and was with the authors for 4 months for 2 revisions. Christoph Peters served as Associate Editor.

1 Introduction: Overview of the Cybersecurity Interface with Accounting

As a concept, cybersecurity has only recently become a part of mainstream training and awareness in terms of corporate governance (Lanz, 2014). Cybersecurity breaches (and the harm that these breaches pose) pose an increasingly significant risk for most companies, and, as such, corporate boards have come to focus on them more (Larcker, Reiss, & Tayan, 2017; Malhotra, 2017). Research demonstrates that a robust interaction between internal audit and information-security skillsets has beneficial outcomes for cybersecurity practice and management (Steinbart, Raschke, Gal, & Dilla, 2013). However, internal audit skills accrue largely to those trained in accounting; as such, mainstream information systems scholars interested in cybersecurity may not fully understand a number of the beneficial security procedures and mechanisms that arise from an auditing persecptive. In this paper, we report on a panel discussion at AMCIS 2017 that focused on how researchers and educators who seek professional certifications offered by organizations such as the Information Systems Audit and Control Association (ISACA) can gain much richer knowledge of and insights into IT security assurance, which they can use for both teaching and research purposes. To that end, the panel promoted IT security audits and the professional training and certification process one needs to undergo to conduct them as an avenue to consider for personal and professional enrichment.

2 Accounting and Information Systems at the IT Security Intersection (by Tom Stafford and Randi Jiang)

While a uniquely accounting-oriented skill, knowing how to conduct internal audits also constitutes an essential skill for the IT security and information assurance researcher (Steinbart et al., 2013). Accountants have always recognized the need for auditing capabilities in firms and at increasingly higher corporate levels. However, IT professionals and educators often lack knowledge about the auditing process in order to ensure IT security programs function effectively.

2.1 Cybersecurity Involvement at the Board Level

In the past, corporate boardrooms typically have not addressed “cybersecurity”. Rather, its management resided with the chief information officer (CIO) or chief technology officer (CTO). Yet, the commissioner of New York Stock Exchange (NYSE) has noted that cybersecurity has become a top concern for American companies, financial institutions, law enforcement agencies, and regulators (Auguilar, 2014). To that end, the need to closely manage information’s confidentiality, integrity, and availability has driven cybersecurity/security threats and risks into the boardroom (Lanz, 2014)—a strategically sensible development since poor security management can adversely impact a firm’s value in the marketplace (Schatz & Bashroush, 2016). As the American Institute of Certified Public Accountings (2016) has noted, firms need to effectively conduct IT audits in order to ensure proper cybersecurity coverage. We believe that top management that has sufficient interest in and concern for its firm’s cybersecurity greatly enhances the effectiveness of security implimentations in the firm.

A recent survey of more than 250 corporate board members found that cybersecurity represents a rising concern for boards and has come to surpasses concern about compliance risks (Tysiac, 2014). However, while 74 percent of directors said their CEOs strongly understood regulatory compliance challenges, barely half (51%) said their CEOs strongly understood cybersecurity topics. Hence, board-level governance clearly seems to have an impact on the cybersecurity component of IT risk (Higgs, Pinsker, Smith, & Young, 2016). At the same time, developing and managing proper relationships between the technology audit function and auditees at the board level involves a host of complex behavioral issues (Dittenhofer, Ramamoorti, Ziegenfuss, & Evans, 2010).

2.2 Accounting-oriented Certifications for Information Technologists

Accounting certifications represent a signal of excellence when companies seek executives who might be skilled in the auditing process. At the same time, auditing skills and certifications also synergize with IT security skills, which firms have come to increasingly demand. To that end, certifications that industry trade associations such as ISACA offer represent particularly useful analogs to the various certifications that accounting organizations around the world offer. Executives who have certifications such as certified

information-security auditor (CISA) and certified information-security manager (CISM) provide reassurance to companies who seek executive talent in the increasingly important IT security area.

3 Cybersecurity Assurance (by Graham Gal)

The Sarbanes-Oxley legislation (SOX) requires firms to disclose information about their internal controls that relate to their financial reporting systems. Independent auditors must review this report as it becomes part of their financial statements. Other types of potentially relevant reports include disclosures about a firm's social responsibility activities. Some evidence suggests that social responsibility and sustainability actions can impact a firm's financial success. As such, some have called for firms to disclose and review this information. Integrated reporting (International Integrated Reporting Council, 2013) seeks to document all value-creation activities in firms. Further, information about securing cyberinfrastructure has also begun to enter the disclosure discussions under SOX. This discourse ultimately focuses on firms' security over data. There are as many types of data as there are types of security. Firms may already disclose customer information in some form to credit bureaus and distributions centers, and they may transmit employee data to the federal government, health insurance firms, and pension providers. Basically, two types of assurance exist: the assurance that an independent assurance provider provides and the assurance that a group internal to the firm provides.

3.1 Independent Assurance of Cybersecurity

The American Institute of Certified Public Accountants (2016) has promulgated advice concerning cybersecurity audits for small to medium sized enterprises, with Deloitte (2018) providing more generally relevant guidance for larger firms. This cybersecurity guidance, which is reported in more detail in the auditing literature (Tysiac, 2016), specifies that company management is responsible for assertions about the firm's cybersecurity risk management program. Auditors, in contrast, are tasked with assessments of the effectiveness of the controls devised by management for achieving cybersecurity objectives. While accounting associations as well as the literature indicate growing demand for cybersecurity assurance audits, the practicing independent auditor only "makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria" (American Institute of Certified Public Accountants, 2016, p. 4). Therefore, the auditor's assurance is only provided in regard to managerial assertions about cybersecurity controls, and not the firm's entire cybersecurity program, itself. Certainly, stakeholders would prefer audits which indicate that a firm is completely secure, but under the current state of business information systems this is probably not possible.

Hence, an auditor reviews a management statement about the state of cybersecurity controls in their firm, they are not aiming to provide an evaluation of the overall state of cybersecurity at the company but rather an evaluation of the quality of managerial assurances on the matter. This is critical for stakeholders to understand: it is management's statements on the matter of cybersecurity controls which are generally examined in the audit. To provide a global assessment of a firm's cybersecurity program would require an auditor to consider additional criteria. Since the basic purpose of any audit is to provide "assurance" on factors which could impact a company's financial position, auditors are generally concerned with defining what is known as a "materiality threshold". The materiality threshold relates to the magnitude of differences between any "true" value of an audited category and a given set of disclosed values; this materiality, particularly when involving financial statements, is generally defined in terms of a specific dollar amount. For assurance of cybersecurity, it is not nearly as clear in dollar value terms when a materiality threshold has been crossed, owing to the multiple factors that could render a cybersecurity program insufficient and the difficulty in expressing these evaluative factors in objective cost terms.

Perhaps the most prominent factor that makes cybersecurity assurance problematic relates to the various points of entry and access to a firm's technological infrastructure. For instance, many firms' airconditioning systems are connected in such a way as to perform remote monitoring and control, and as has been seen, this is a potential entry point to corporate networks and systems that can be exploited by malicious attackers. In fact, there are so many of these insidious entry points that, in 2013, President Obama issued an executive order concerning the need to improve critical infrastructure with regards to cybersecurity (The White House, 2013).

This brings up the related issue of audit scope. When an auditor looks at internal controls, they generally restrict their evaluation to the controls that impact financial reporting. However, because of the potential impact of any cyber-attack on a company's infrastructure, the auditing scope of any assurance of

cybersecurity effectiveness could potentially be limitless. For instance, a cyber-attack on a nuclear power plant run by a utility firm could be devastating; should or could an independent auditor examine all the potential weaknesses in the nuclear reactor as part of his/her examination of internal managerial controls typically evaluated for financial consistency? Would this be "in scope" for a cybersecurity assurance program? Still another factor concerns the adequacy of training for a firm's employees. Ransomware cyber-attacks are typically initiated through infected email attachments. Even if a firm provides training to all its employees concerning policies regarding email attachments it only takes a single person to make the mistake of opening the wrong attachment for the company to suffer a devastating exploit. In this context, it is hard to imagine a training program that would be 100 percent effective, with related issues involving security audits intended to assure the effectiveness of cybersecurity programs. Firms have so many entry points to their sensitive systems and data, including those managed by third parties, that to provide audit assurance that all of these entry points are secure would be extremely difficult for any team of auditors.

Still another issue that needs to be considered is the liability that providing assurance of IT security would create for an independent audit firm. When a breach of the IT infrastructure occurs, the financial impact (not to mention other potential impacts), can be extremely large. It is probably not within the risk profile of an audit firm to provide assurances of a company protections against such liabilities. It is for this reason that independent audit firms are more inclined to simply review management's reported approaches to and plans for cybersecurity, as opposed to the security plans, themselves. Given what auditors are able and willing to examine and provide assurances on, the question becomes which approach can be taken by independent auditors to review and provide assurance to company management their stakeholders that corporate cybersecurity efforts are appropriate. Recent research seems to suggest that a vibrant and forward thinking internal audit group is a great place to start (Steinbart, Raschke, Gal, & Dilla, 2015).

3.2 Internal Audit's Role in Cybersecurity Assurance

Several studies have examined the relationship between internal audits (IA) and the information-security departments (infosec) in firms (Steinbart et al., 2013; Steinbart, Raschke, Gal, & Dilla, 2014a, 2014b, 2016). These studies have found that a synergistic relationship between the auditor (IA) and the auditee (infosec) enhances information-security outcomes. This research stream examines both outcome measures (number of incidents causing harm) and performance measures (number of incidents stopped prior to causing harm). It has shown that IA can provide assurance about the adequacy of processes that control financial-statement disclosures. The research provides support for an IA's role in providing internal assurance to information systems-security processes. This finding concurs with the Institute of Internal Auditors' (2013) conceptualization of an IA's role in the "three lines of defense" against exploits. The measures these studies used relate to the relationship between IA and Infosec, and the studies found factors that either facilitated or improved this relationship.

The two groups perceived their relationship in either an adversarial or supportive way. Steinbart, Raschke, Gal, and Dilla (2012) found that, in some organizations, infosec felt that IA tried to catch infosec at being non-compliant. In other organizations, infosec felt that IA's role involved assisting infosec in providing strong information-security programs. In these organizations, infosec saw IA as an ally in obtaining necessary support for cybersecurity initiatives. In addition to IA's perceived role as supporting the information-security processes, IA's knowledge level also had an impact on the relationship. The results show that, when the IA had more knowledge of information-security processes and issues than infosec, the relationship improved. Finally, these studies clearly found that top management played a critical role in creating a good relationship between infosec and IA.

This research does indicate that IA may be the appropriate group to provide assurance for cybersecurity. If top management considers its role to be important and commits to creating knowledgeable and well-supported internal auditors, firms at least have a fighting chance to create quality information-security processes.

3.3 Disclosure of Assurance Information

If a firm has a perfect system, then cybersecurity may not be an issue. However, investors may like to know whether a firm has fallen behind in upgrading its IT infrastructure and processes. Other individuals may also find this information to be quite interesting. Even knowledge about different vendors that supply components to a firm may sufficiently provide a potential entry point for an attacker. Certainly, stakeholders may find all information about potential exploits or security vulnerabilities to be relevant, but such disclosure may also be detrimental to the firm's success. This consideration of how much information to audit and disclose is

similar in concept to rule 3.1 in the Australian Stock Exchange (2016) that requires Australian firms to continuously disclose information that stockholders would consider relevant in evluatintg soundness of oocpmany operation, except under certain conditions. Investors are sensitive to the implicaitons of poor cybersecurity, but research shows (Wang, Kannan, & Ulmer, 2013) that there may be no significant influence on investor reactions to security breach disclosures that follow financial report releases which include details of prior security breaches. In essence, it appears that disclosing risk-mitigating information does not result in subsequent investment downgrades following security incidents (Wang et al., 2013, p. 215).

4 The Information-security Value of Audit Certification (by Robert Crossler)

The certified information systems auditor (CISA) certification from the information systems audit and control association (ISACA) gives cybersecurity researchers among the readership at *CAIS* important perspectives useful for their work given the valuable perspective that audit expertise brings to understanding security matters. ISACA functions as the knowledge bridge between scholars and practitioners. In order for researchers to certify for CISA with ISACA, they need to understand the certification exam and success strategies for passing it.

Individuals who successfully pass the CISA exam generally say that, when preparing for it, receiving some sort of CISA training is extremely helpful. Much training material exists (http://www.isaca.org/Education/Pages/default.aspx). Depending on where one lives, going to live training probably constitutes the best (though also most expensive) alternative. With that said, many online training opportunities exist as well (http://www.isaca.org/Education/on-demand-learning/Pages/cisa-online-review-course.aspx). To find them, one can search on the Internet for “CISA training”. This training helps the information-security researcher to begin to learn to think like an auditor.

The CISA study guide book and the practice exams that ISACA offers also serve as other valuable resources that one can use to prepare for training (see https://www.isaca.org/bookstore/Pages/CISA-Exam-Resources.aspx). One can purchase these resources through ISACA’s website directly or often find them on Amazon.com. One approach to prepare for the exam that works well involves combining online training and the CISA sample quizzes. After reviewing weak areas, one can revisit quizzes to assess study efficacy. Repeating this process regularly helps one to focus one’s study time on the CISA material.

4.1 Insights Regarding the CISA Exam

ISACA generally offers the CISA exam three times per year in centralized testing centers. One takes the exam on a computer in a secure environment to prevent cheating. Students cannot bring cellphones, pencil cases, written notes, or water bottles into the testing venue. One should consider carefully whether to bring a water bottle: the exam lasts for four hours, and the proctor only allows one person to use the restroom at a time.

4.2 CISA Success Points

Candidates who have successfully passed the CISA exam have provided guidance for future aspiring candidates. Specifically, they have suggested that one needs to:

1. Learn to think like an auditor
2. Realize many auditing steps are similar, and
3. Try to relate the audit process to IS processes you are familiar with.

To successfully obtain CISA certification as an information-security researcher, one needs not to memorize study details but to try to *think like an auditor*. By doing so, regardless of what type of audit one completes, one can correctly answer a multiple choice question through understanding the thought processes auditors go through. In the process of doing so, perspective candidates will realize that every audit has similar steps.

Finally, one may find it useful to relate the steps in an audit to IS processes that one may be familiar with. For example, systems analysis and design has the systems development lifecycle. While this lifecycle helps developers to ensure that a systems project successfully moves from inception to completion, it is

conceptually similar to the audit process. As one realizes these similarities, one needs to expend less cognitive effort to learn to think like an auditor.

5 The Role of Accounting and Professional Associations in IT Security Auditing (by Robin Lyons)

ISACA helps individuals and enterprises realize technology's positive potential. As such, ISACA provides a centralized source of information and guidance in the field of auditing controls for computer systems. The COBIT framework, which ISACA created, provides organizations with guidance for technology governance and information, and professional IS auditors in industry widely use it.

5.1 Education

As Robert Crossler indicates in regard to preparation for CISA certification through ISACA in Section 4, conferences, training seminars, and online events keep IT professionals and professors updated on the latest topics and techniques. These training opportunities represent valuable tools for researchers and educators who seek CISA certification in order to strengthen their IT audit and cybersecurity credentials. Such seminars also provide an excellent way for already-certified colleagues to maintain their certification status through continuing professional education (CPE), which is a component of maintaining important certifications once gained.

5.2 Certifications

ISACA also sponsors several important certifications. Certifications serve as a way for IT professionals to demonstrate a command of IT principles and skills to employers (current and potential). Table 1 lists the certifications that ISACA offers.

Table 1. ISACA Certifications

Certification	Description
CISM	Certified information systems manager
CRISC	Certified in risk and information systems control
CGEIT	Certified in the governance of enterprise IT
CISA	Certified information systems auditor
CSX	Cybersecurity nexus fundamentals
CSXP	Cybersecurity nexus practitioner

The CISA designation is designed for information-security audit, security, cybersecurity, control, and assurance professionals. In addition to a passing score on the examination, eligibility for the CISA certification requires five years of work experience in IS audit, control, assurance, or security. Currently, over 129,000 professionals hold the CISA certification. Individuals who hold the CISA designation may have positions performing audits and risk assessments and providing advisory services. Such individuals can also often have positions in which they perform all three of these responsibilities.

5.3 Career Advancement

ISACA's CSX certification (cybersecurity nexus) focuses even more on cybersecurity expertise in contrast to the CISA certification, which combines IT audit and cybersecurity issues under a single certification. ISACA provides both a fundamentals certification (CSX) and a practitioner-oriented certification (CSXP). The CSX fundamentals certificate represents a useful starting point for the cybersecurity researcher interested in certification because one can obtain it from earning a passing score of 65 percent on an online, closed-book, remotely proctored exam. The exam covers:

- Cybersecurity concepts
- Cybersecurity architecture principles
- Security of networks, systems, applications, and data
- Incident response, and
- Security implications and adoption of emerging technologies.

CSXP certification depends on performance. In a virtual lab environment, those who pursue the CSXP designation need to demonstrate the abilities to:

- Use vulnerability-assessment processes and scanning tool sets to identify and document vulnerabilities based on defined asset criticality and technical impacts.
- Obtain and aggregate information from multiple sources (e.g., logs, event data) for use in threat intelligence, metrics, and incident detection.
- Implement specified cybersecurity controls (for network, application, endpoint, server, and more) and validate that controls operate as required.
- Conduct ongoing control tests and validations to verify effectiveness of controls and identify deficiencies and vulnerabilities.
- Implement and document changes to cybersecurity controls (e.g., antivirus signatures, firewall rule changes) in compliance with change-management procedures.
- Identify anomalous activity and potential internal, external, and third-party threats to network resources using network-traffic monitors or intrusion-detection and -prevention systems, and ensure timely detection of compromise indicators.
- Perform initial-attack analysis to determine the attack vectors, targets and scope, and potential impact.
- Execute defined response plans to contain damage on affected assets.

Given the projected shortage of cybersecurity professionals, the CSX or CSXP designation coupled with the CISA certification represents an excellent option for an IT security auditor or IT security research to demonstrate expertise. A background in cybersecurity and IT audit would allow cybersecurity scholars to have informed and in-depth discussions with IT practitioners with whom they interact with for their research.

5.4 Summary

ISACA certifications constitute a helpful tool for IT and cybersecurity research. In the face of the growing cybersecurity threat landscape, ISACA is an important partner for security and audit researchers as they grow their IT audit, management, risk, and cybersecurity skills.

6 Role of Universities in Accounting/IT Security Workforce Development (by Robin Poston)

Today's executive accounting and IT security management teams must strategically leverage their company's resources by managing their workforce's skills and competencies. As cybercriminals continuously improve their capabilities and attacks become more common and sophisticated, the corporate workforce must match pace in their capabilities. Corporate agility enables ever-changing operating environments to take advantage of ever-changing threat situations. In today's world, two factors combine to enable organizations and the managers responsible for IT security to rapidly respond to the increasingly volatile security threat landscape: 1) the ever-increasing pervasiveness of data and information systems in virtually all activities and 2) the rapid escalation in technology speed and capability. Universities that pursue cutting-edge research and scholarly advancements must disseminate the latest knowledge via classroom, online, textbook, and publication mechanisms. Indeed, advancing the latest knowledge and technologies represents a major focal point of many universities because it positions them to help colleges to assist corporate executives to train their workforce to quickly respond to the latest technology developments and threats across cloud computing, cybersecurity, virtualization, new database techniques, and so on.

6.1 Managing Based on a Bundle of Skillsets in this Space

To manage an agile workforce, managers must first understand an organization's underlying skills and competency profile (Poston & Dhaliwal, 2015). Academic researchers, while not always the most knowledgeable about state-of-the-art professional practice, have skills in analyzing organizational processes and can help firms achieve the professional outcomes they desire. Specifically, managers first analyze the skills and competency an organization's workforce and uncover the current skills and competency profile that comprises its accounting and IT security core knowledge areas. They can then customize the knowledge through site visits with the organizational leadership team. Based on this

consultation, academics can then create and administer a survey to assess the current bundle of skillsets of the accounting and IT security workforce.

6.2 How to Ensure that the Workforce Capabilities are Strong

A skills and competency analysis also can yield interesting findings about the extent to which a company's accounting and IT security workforce has modernized to maintain a comparative advantage given industry performance levels. Analyzing demographic data across skillsets can highlight how employee skill levels, educational backgrounds, certifications, and/or years of experience might interact with workforce skills and competencies. For example, a company may find that individuals with master's degrees report higher skill levels than those with only bachelor's degrees but that individuals with only associate's degrees who have over 20 years of experience have the highest skill levels. Another example, individuals with IT degrees may report the highest skill levels, while individuals with 10 or more years of experience may report higher skill levels than those with under 10 years of experience. Regardless of overall findings, the data then allows the management team to drill down into the areas in which their employees have expert-level skills and those in which they do not. They can then focus on raising the latter via appropriate methods. Managing the workforces based on annually assessing their accounting and IT security capabilities allows firms to enable the processes that ensure the workforce capabilities remain strong and increase over time.

Based on a skills profile analysis, firms can take actions to shore up key shortfalls. To do so, they can adopt academic-led customized curriculum development. University courses typically include a balanced mix of theory, research, and practical application-based examples obtained from a focal company. Furthermore, firms should incorporate the skills and competencies survey into employees' normal work processes (i.e., as part of an annual skills-gap analysis). Discussions about each employee's skills and competencies should factor into annual evaluations. This annual analysis should then drive managerial decisions about training, hiring, and other organizational development decisions.

7 Conclusion and Takeaways: The Interface between Cybersecurity and Internal Audit (by Tom Stafford and Randi Jiang)

Organizations and IS researchers alike understand the significance of cybersecurity. With an increase in data breaches, individuals at the highest levels in firms have started to participate in managing and monitoring cybersecurity issues. While top management must consider their role as the facilitator between the internal auditor's knowledge and the firm's commitment to quality information-security processes, security researchers must become more aware of these dynamics as well. Corporations have begun to see the value of maintaining high levels of communication between their information-security and internal-audit departments. Researchers with similar interests have begun to investigate the juncture between accounting and IT knowledge of the security and auditing processes. To that end, researchers in the security field have begun to bridge the gap between accounting certification processes and IT security audits and to pursue audit certifications useful to their IT security audit interests. Along that vein, our panel focused on making security researchers aware of the rich sources of information and training available from accounting-oriented certification organizations such as ISACA. While one can also gain the knowledge about IT auditing inherent in a CISA certification via an affiliation with such organizations, our panel (including a CISA-certified IT security researcher) felt that certification leads to a fuller and more lasting learning experience. At the same time, CISA certification might provide one with connections and introductions to research contexts and data opportunities that colleagues with more tenuous connections to the certifying organization might not have access to.

The internal audit function and its impact on IT security benefits these audit certifications. ISACA's training and certifications only strengthen an IS researcher's knowledge about corporate IT security processes. Auditors could learn several cybersecurity skills through reviewing IT audits in more detail just as IT security experts could also benefit from more detailed knowledge of audit processes. Cybersecurity defenses rely heavily on technology, but companies and researchers alike need to know how to handle protective technologies effectively and efficiently.

Accountants who specialize in auditing have typically earned the certified public accountant certification. IS security researchers who are interested in IT audits as yet have no formal professional certification available to them. However, the accounting organization ISACA can certify any individual who can successfully pass the associated exam for the role as an IT auditor. This certification gives IT security researchers the common knowledge that accountants with interests in IT security can regularly access.

With this paper, we hope we encourage security researchers to engage with the accounting discipline in order to access and appreciate the extensive set of skills already available to accountants in IT audits and other security-related matters. We believe that IS security research can benefit from more frequent and detailed interactions with IT auditors and accounting IS scholars, which one can frequently find in the accounting field. One can often find the practical nexus of these two skill and research areas in the CISA certification, which explains why the AMCIS panel and this paper that reports on it specifically focus on promoting visibility of and knowledge about this important option.

References

Aguilar, L. A. (2014). Boards of directors, corporate governance and cyber-risks: Sharpening the focus. In *Proceedings of the New York Stock Exchange Cyber Risk and the Boardroom Conference*.

American Institute of Certified Public Accountants. (2015). *Comment letter to NIST on NISTIR 7621 rev.1.* Durham, NC.

American Institute of Certified Public Accountings. (2016). *Proposed description criteria for management's description of an entity's cybersecurity risk management program*. Durham, NC.

Australian Stock Exchange. (2016). *Continuous disclosure: An abridged guide*. Sydney, Australia. Retrieved from https://www.asx.com.au/documents/rules/gn08_continuous_disclosure.pdf

Deloitte. (2018). *AICPA proposed revision of trust services criteria for security.* Retrieved from https://www.iasplus.com/en-ca/projects/regulations/completed-projects/aicpa-proposed-revision-of-trust-services-criteria-for-security-availability-processing-integrity-confidentiality-and-privacy-ed

Dittenhofer, M. A., Ramamoorti, S., Ziegenfuss, D. E., & Evans, L. E. (2010). *Behavioral dimensions of internal auditing.* Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79-98.

Institute of Internal Auditors. (2013). The three lines of defense in effective risk management and control. The Institute of Internal Auditors, Altamonte Springs, FL.

International Integrated Reporting Council. (2013). *The international framework.* London, UK.

Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. *The CPA Journal*, *84*(11), 6-10.

Larcker, D. F., Reiss, P. C., & Tayan, B. (2017). *Critical update needed: Cybersecurity expertise in the boardroom.* Graduate School of Stanford Business. Retrieved from https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/cgri-closer-look-69-cybersecurity-experise-boardroom.pdf

Malhotra, Y. (2017). Toward "cyber-finance" cyber risk management frameworks of practice: Bridging networks, systems, and, controls frameworks. *Journal of Operational Risk*.

Poston, R., & Dhaliwal, J. (2015). IS human capital: Assessing gaps to strengthen skill and competency sourcing. *Communications of the Association for Information Systems*, *36*, 669-695.

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organizations' market value. *Information & Computer Security*, *24*(1), 73-92.

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228-243.

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems*, *27*(2), 65-86.

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2014a). Internal audit's contribution to the effectiveness of information security: Perceptions of information security professionals. *ISACA Journal, 2*,1-6.

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2014b). Internal audit's contribution to the effectiveness of information security: Perceptions of information security professionals. *ISACA Journal, 3*, 1-5.

Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectives of enterprise information security programs. *Journal of Information Systems*, *30*(1), 71-92.

Steinbart, P. J., Raschke, R., Gal, G., Dilla, W. N. (2015). The influence of internal audit on information security effectiveness: Perceptions of Internal Auditors.

The White House. (2013). *Executive Order 1336 on improving critical infrastructure cybersecurity*. Washington, DC: Office of the Press Secretary.

Tysiac, K. (2014). Technology plays a role in board members' top two concerns. *Financial Management.* Retrieved from https://www.fm-magazine.com/news/2014/jul/201410602.html

Tysiac, K. (2016). New path for CPAs in cyber risk management. *Journal of Accountancy*, *222*(5), 1-2.

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218.

About the Authors

Tom Stafford is the J. E. Barnes Professor of CIS at Louisiana Tech University and is affiliated with their DHS/NSA certified Center of Excellence in Information Assurance.

Graham Gal is an Associate Professor in Accounting at the University of Massachusetts at Amherst. Gal is an internationally recognized expert in internal audit and is currently editing a special of *Managerial Auditing Journal* on cybersecurity.

Robin Poston is the Papasan Family Professor for Exemplary Leadership and Chair of the Business Information & Technology Department at the University of Memphis. She is affiliated with the FedEx Institute of Technology Cluster for the Advancement of Testing and Security.

Robert E. Crossler is an Assistant Professor of Management Information Systems at Washington State University. He is a prominent security researcher and carries the CISA certification from ISACA.

Randi Jiang is a doctoral student in Computer Information Systems at Louisiana Tech University. Jiang is a certified internal auditor with extensive research experience in Information Security.

Robin Lyons is a Technical Research Manager with ISACA, the Information Systems Audit and Control Association.