The Role of Accounting and Professional Associations in IT Security Auditing

Panel

Sharif Islam and Randi Jiang, Moderators
Louisiana Tech
sharif10.ais.du2004@gmail.com, rjiang05@gmail.com

Robin S. Poston, Ph.D.
University of Memphis
rposton@memphis.edu

Graham Gal, Ph.D.
University of Massachusetts - Amherst
gfgal@isenberg.umass.edu

Mr. Paul Phillips
ISACA
pphillips@isaca.org

Thomas F. Stafford, Ph.D.
Louisiana Tech
Stafford@LaTech.edu

ABSTRACT

Information Systems Security is a critical area of inquiry and scholarship in our field, yet relatively little is known about the process by which scholars and professionals become certified as security experts for purposes of assessing the quality of information security implementations. The Information Systems Audit and Control Association (ISACA.org) is the professional association that serves as a bridge between the expertise area from which auditing skills are delivered and assessed and the areas in which information systems security is developed and delivered, effectively bridging the practices of accounting and IT Security. Individuals skilled in accounting, such as graduates from combined Accounting/Information Systems departments in business schools are naturally oriented to such industry groups and certifications, but the mainstream IT practice and literature is not. This panel will serve to brief IT Security researchers interested in the process of auditing on the values and procedures of the certification process with implications for understanding corporate IT Security performance as a function of auditing expertise represented at the highest levels of organizational decision making.

Keywords

IT Security, IT Security Auditing, Accounting and IT, Professional Certifications

INTRODUCTION: OVERVIEW AND OBJECTIVE

Cybersecurity is a concept that has only recently become a part of mainstream awareness in terms of corporate governance (Lanz, 2014). The risk of cybersecurity breaches (and the harm that these breaches pose) is one of increasing significance for most companies and therefore an area for heightened board focus (Gregory and Pollack, 2002). Research demonstrates the value of a robust interaction between internal audit and information security skillsets (Steinbart et al., 2013), with strong implications for involvement at the highest levels of the firm. The problem that we see is that academicians interested in IT Security will not be fully aware of the procedures and mechanisms by which IT Security Audit becomes inculcated at the C-level of the firm. This implies a need for consideration of specialized training and certifications programs offered by organizations such as ISACA.org (formerly, the Information Systems Audit and Control Association) which have as a primary mission the promulgation, education, and certification of IT Security Auditing skills. To that end, our panel introduces information systems researchers with security interests to the notion of IT Security Audit and the Auditor Certification Process produced, maintained and administered by ISACA.org, the leading industry consultancy on IT Security Auditing.

ACOUNTING AND INFORMATION SYSTEMS AT THE IT SECURITY INTERSECTION

Internal audit is a uniquely accounting-oriented skill, but is likewise an essential skill for the practice of IT Security assurance (Steinbart et al, 2013). Accountants have always been aware of the need for auditing capabilities and skills in the firm, and at

increasingly higher levels of corporate decision making, but IT professionals and educators are not as well schooled in the role or process of auditing in assuring the effective functioning of the IT Security programs of businesses.

Security Audit Involvement at the Board Level

In years past, the term 'cybersecurity' was not typically addressed in the boardroom, with its management residing with the chief information or technology officer. Yet, the Commissioner of New York Stock Exchange (NYSE) has noted that cybersecurity has become a top concern of American companies, financial institutions, law enforcement and regulators (Auguilar, 2014). To that end, the need to closely manage confidentiality, integrity, and availability of information has driven the management of cybersecurity/security threats and risks into boardroom (Lanz, 2014), which is strategically sensible since poor security management can adversely impact firm value in the marketplace (Schatz and Bashroush, 2016).

A recent survey of more than 250 corporate board members indicates that cybersecurity is a rising concern of the board, surpassing compliance risk (Tysiac, 2014) and while 74% of directors said their CEOs have a strong understanding of regulatory compliance challenges, barely half (51%) said their CEOs possess a strong understanding of cybersecurity topics. Hence, it seems clear that board-level governance has an impact on the cybersecurity component of IT risk (Higgs et al., 2016). At the same time, the task of developing and managing proper relationships between the technology audit function and auditees at the board level involves a host of complex behavioral issues (Dittenhofer et al. 2010).

CPA for Accountants, CISA/CISM for Information Technologists

The CPA certification is well understood as a signal of excellence when companies seek executives who might be skilled in the auditing process. At the same time, the need for similar auditing skills and certifications is strongly implied by the growing need for and presence of IT Security skills at the highest corporate levels. To that end, certifications offered by industry trade associations such as ISACA are particularly useful analogs to the CPA for purposes of assuring well-developed and robust IT Security Auditing skills. Certifications such as CISA (Certified Information Security Auditor) and CISM (Certified Information Security Manager) provide reassurance to companies seeking executive talent in the increasingly important IT Security area with attendant audit responsibilities at the Board level.

Panel Members

Dr. Robin S. Poston, Executive Director
Center for the Advancement of Security and Testing
FedEx Institute for Technology
University of Memphis
Memphis TN

Doctor Poston administers an industry training group in cybersecurity, but also does research on the role of IT Audit and Cybersecurity. Poston holds the Ph.D. from Michigan State University, is a CPA, and has industry experience with the KPMG consultancy.

Robin's topics: IT Audit in the real world, bringing industry cybersecurity training knowledge to the research program. IT Security in the Boardroom.

Dr. Graham Gal
Associate Professor of Accounting
University of Massachusetts Amherst

Dr. Gal is a graduate of the Michigan State University and has extensive experience in IT Audit and Security. His research covers the role of accounting and auditing in IT Security, and his industry experience was with RSA Securities.

Graham's topics: Accounting has an important role in security audit; professional associations have an important role to play. IT Security in the Boardroom.

Mr. Paul Phillips
Technical Research Manager, ISACA

Mr. Phillips is a top executive with ISACA, the Information Systems Audit and Control Association, which is the industry certification and training organization that provides important information security auditing certifications, which are regarded in the practice much like the CPA certification is regarded in mainstream accounting as a certification of excellence and skill.

ISACA provides training and certification testing for Certified Information Security Auditor, Certified Information Security Manger and several other important IT security certifications.

Paul's topics: the role of ISACA certification in the assurance of information security audit expertise. The paths to certification; training and certification programs available for security researchers and practitioners to follow.

Dr. Tom Stafford
J.E. Barnes Professor of Computer Information Systems
Louisiana Tech

Tom is resident at a NSA/DHS certified Academic Center of Excellence in Information Assurance Research and Education. His focus on IT Security as an aspect of his industry interactions with IT Security constituents with a strong Department of Defense focus on cybersecurity has extended to the step of seeking ISACA certification as an auditor.

Tom's topics: CISA certification and preparation for the certification exam. IT Security Audit in the Classified Cybersecurity environment.

CONCLUSION

This panel brings together an optimal mixture of professional experience, academic expertise, research visibility and applied IT Security Auditing skills for purposes of demonstrating the importance of IT Security Audit and the avenues for obtaining training and enrichment in the process, such that attendees can then provide richer experiences to their students, clients, and research colleagues on the matter. IT Security researchers and teachers who attend will come away with a new perspective on the role of IT Security at the highest levels of cooperate decision making, and the critical aspect of IT Security Audit as part of that process.

REFERENCES

1. Aguilar, L.A. (2014). Boards of directors, corporate governance and cyber-risks: Sharpening the focus." New York Stock Exchange Cyber Risk and the Boardroom Conference, June 2014.
2. Dittenhofer, M.A., Ramamoorti, S., Ziegenfuss, D.E. and Evans, L.E. (2010). Behavioral dimensions of internal auditing. Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.
3. Gregory, H. and Pollack, J.G. (2002) Corporate Social Responsibility, Global Counsel, March, 41-55.
4. Higgs, J.L., Pinsker, R.E., Smith, T.J., and Young, G.R. (2016) The relationship between board-level technology committees and reported security breaches. Journal of Information Systems, 30, 3, 79-98.
5. Kwon, J., Ulmer, J.R., and Wang, T. (2013) The association between top management involvement and compensation and information security breaches. Journal of Information Systems, 27, 1, 219-236.
6. Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. The CPA Journal, 84, 11, 6-10.
7. Schatz, D., and Bashroush, R. (2016). The impact of repeated data breach events on organizations' market value. Information & Computer Security, 24, 1, 73 – 92.
8. Steinbart, P.J., Raschke, R., Gal, G., and 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.
9. Tysiac, K. (2014). Audit regulators see positive signs. Journal of Accountancy, 218, 3, 38-40, 42-43.