Editorial

Forward to the special issue on cybersecurity assurance

Foreword

This special issue on cybersecurity assurance has six papers. Two are conceptual papers and four are experimental papers. Readers of this special issue should benefit from the conceptual papers, as each provides a perspective on the assurance process. The experimental papers provide readers with insights into specific questions about cybersecurity behaviors and processes within firms.

In the paper by Charika Channuntapipat entitled "Assurance for service organisations: contextualising accountability and trust", the issue of service organizations is addressed. For cybersecurity, this is a critical concern, as the firm's data are being held and processed outside the organizational boundaries. This presents a number of problems that must be addressed in the assurance process. First is the risk associated with opening up channels to the service organization to provide and/or obtain the firm's information. While firms usually transmit their own data from within their infrastructure, the reliance on an external party requires a different level of assurance. Second, and perhaps of more concern, is the storage of what could be critical information outside the firm. In the USA, firms would require a SOC 1 report of the service organization. In other jurisdictions, other types of reports would be required. This paper goes through the various requirements for the assurance process and the reports those results.

The second conceptual paper by Sezer Bozkus Kahyaoglu and Kiymet Tunca Çaliyurt, "The cybersecurity assurance process from the internal audit perspective", focuses on assurance from within the firm. A good deal of previous studies conclude that internal audit plays a critical role in the firm's cybersecurity processes. While internal audit must consider a multitude of stakeholders in their role as overall assurance providers, for cybersecurity assurance, they must be able to interact with the information security group. This includes determining the risks and the quality of the processes to address these risks. Thus, there is a critical interaction between these groups, as cybersecurity assurance covers a multitude of processes within the firm. The Kahyaoglu and Çaliyurt paper considers this interaction by examining some of the more accepted frameworks for cybersecurity and audit processes.

The third paper by Shariful Islam, Nusrat Farah and Thomas Stafford entitled "Factors associated with security/cybersecurity audit by internal audit function: an international study" makes a connection with the Kahyaoglu and Çaliyurt paper by examining how internal audit impacts the practice of cybersecurity assurance. The authors review different firm characteristics and their impact on the cybersecurity audit process. Their findings are consistent with other work that shows that the board of directors' governance activities and competence of internal audit are important for this process. Some of their other findings are very interesting, as they find some variables that are presumed to be important but are not.

In a continuation of the stream of research, which shows the importance of internal audit in cybersecurity assurance, is the Islam *et al.* paper. Their paper confirms this from a slightly different perspective. Yaojie Li, George Deitz and Thomas Stafford look at information security policy compliance. Their paper, "The role of internal audit and user training in information security policy compliance" examines a very crucial and yet unresolved issue – how can firms ensure compliance. Some compliance concerns arise when a person within the firm deliberately attempts to thwart information security policies. This paper addresses noncompliance by employees who are not aware that their actions are

Managerial Auditing Journal
Vol. 33 No. 4, 2018
pp. 338-339

0268-6902
DOI 10.1108/MAJ-04-2018-014

against firm policies. Noncompliance of this type can be a rather serious problem for firms, as even the best training can't ensure 100 per cent compliance. The authors examine the potential for internal audits to improve awareness and reduce complacency.

The first four papers have looked at the assurance process, while the final two examine the consequences of a cybersecurity breach. While firms would like to believe they have excellent cybersecurity policies and procedures, the truth is that there will always be attacks on their IT infrastructure, and some will get through. The paper entitled "Consumer security behaviors and trust following a data breach", by Shelby Curtis, Jessica Rose Carré and Daniel Jones looks at the reactions of consumers. As firms see more of their sales from online purchases, it is critical for them to consider and to prepare for the eventuality of a data breach. Among their findings is the indication that statements firms make about the security of their online business may lead consumers to rely on the firm's security policies and relax their own personal security measures.

In a second paper which uses an experimental approach to focus on the outcomes of security breaches, Jessica Rose Carré, Shelby Curtis and Daniel Jones examine how individuals determine responsibility for a data breach. In their article "Ascribing responsibility for online security and data breaches" the authors examine the psychological contract a consumer has with a firm. Under this view, the failure to protect the consumer's data is seen by consumers as a breach of contract. In their study, individuals view firms as being more responsible for data breaches and therefore reduce their trust in the company even if the breach did not impact their data.

This special issue has papers that examined cybersecurity and assurance by using both conceptual and experimental approaches. Readers of this issue should come away with an appreciation of both the review of assurance practices and the practices that can be improved in firms. In the conceptual papers by Channuntapipat and Kahyaoglu and Çaliyurt, the importance of considering organizational issues is presented. The role of the internal audit function is suggested and confirmed in the Yaojie Li *et al.* and Islam *et al.* papers. Taken together, these two papers, as well as other studies, make the case that increased reliance on internal audit is critical and that training of internal audit is necessary to make this increased reliance effective. Finally, the last two papers consider an eventuality that clearly must be considered. All the policies and cybersecurity assurance practices can't eliminate all breaches; therefore, firms must have some idea of how to handle these situations. The Curtis *et al.* and the Carré *et al.* papers consumers trust in the organization after a breach is examined. In each case, the communication between the firm and the consumer is important to the outcome after a breach is disclosed.

Graham Gal
Department of Accounting, University of Massachusetts, Amherst, Massachusetts, USA