



Vaasan yliopisto
UNIVERSITY OF VAASA

OSUVA Open
Science

This is a self-archived – parallel published version of this article in the publication archive of the University of Vaasa. It might differ from the original.

Cybersecurity in Accounting Research

Author(s): Haapamäki, Elina; Sihvonen, Jukka

Title: Cybersecurity in Accounting Research

Year: 2022

Version: Accepted manuscript

Copyright ©2022 Routledge. This is an Accepted Manuscript of a book chapter published by Routledge in *Artificial Intelligence in Accounting: Organisational and Ethical Implications* on 5 August 2022, available online: <https://doi.org/10.4324/9781003198123>

Please cite the original version:

Haapamäki, E. & Sihvonen, J. (2022). Cybersecurity in Accounting Research. In: Lehner, O. M. & Knoll, C. (eds.) *Artificial Intelligence in Accounting: Organisational and Ethical Implications*, 182-214. Routledge Studies in Accounting. Oxon: Routledge.
<https://doi.org/10.4324/9781003198123-10>

Abstract: This chapter aims to update the cybersecurity-related accounting literature by synthesising 39 recent theoretical and empirical studies on the topic. Furthermore, the chapter provides a set of categories into which the studies fit. It is a synthesis chapter that summarises the research literature on cybersecurity, introducing knowledge from the extant research and revealing areas requiring further examination. This synthesis identifies a research framework that consists of the following research themes: cybersecurity and information sharing; cybersecurity investments; internal auditing and controls related to cybersecurity; disclosure of cybersecurity activities; and security threats and security breaches. Academics, practitioners, and the public would benefit from a research framework that categorises the research topics related to cybersecurity in the accounting field. This type of analysis is vital to enhance the understanding of the academic research on cybersecurity and can be used to support the identification of new lines for future research. This analysis has significant implications for research and practice by detailing, for example, the benefits of and obstacles to information sharing. This synthesis also highlights the importance of the model for cybersecurity investments. Further, the review emphasises the role of internal auditing and controls to improve cybersecurity.

Keywords: Cybersecurity, Risk Management, Accounting, Auditing, Digitalisation

8

Cybersecurity in Accounting Research

Elina Haapamäki and Jukka Sihvonen

Introduction

The increasing use of digital technologies among companies has emphasised the importance and role of cybersecurity as a new risk management dimension, not least because cyber threats and risks have attracted significant attention from the public (e.g., Amir, Levi, & Livne, 2018; Li, No, & Wang, 2018). Furthermore, firms hit by cyber-attacks tend to suffer long-lasting economic and reputational losses (Agrafiotis et al., 2018; Kamiya et al., 2018). Recent studies suggest that, over the course of just a few years, cybersecurity has grown into one of the most significant risk challenges facing every type of organisation and society (e.g., IIA, 2018; Islam, Farah, & Stafford, 2018; Kahyaoglu & Caliyurt, 2018). For instance, Gordon, Loeb, Lucyshyn, and Zhou (2015b) argued that it is possible that a cybersecurity breach could shut down an entire critical infrastructure industry and threaten a nation's entire economy and national defence.

Cybersecurity is more often acknowledged as a severe organisational concern best addressed by integrating it as a part of managerial control system (Gordon, Loeb, Sohail, Tseng, & Zhou, 2008). This development is partly due to enforcement and supervision by regulatory authorities (SEC, 2018a, 2018b) and partly due to increased guidance from the Big 4 accounting firms and audit industry organisations (e.g. AICPA, 2018a, 2018b); market discipline also plays a part (Gordon, Loeb, & Sohail, 2010; Gordon, Loeb, & Zhou, 2011; Berkman, Jona, Lee, & Soderstrom, 2018; Amir et al., 2018). As a part of a managerial control system, cybersecurity has

also become very much a managerial accounting and auditing matter, subject to cost-benefit analysis, internal control assessment, and disclosure policy considerations. According to [Gordon and Loeb \(2006\)](#), the objectives of cybersecurity can be divided into three broad categories. First, cybersecurity protects the confidentiality of private information; second, it ensures that authorised users can access information on a timely basis; and third, cybersecurity protects the accuracy, reliability, and validity of information. The purpose of this chapter is to advance the research on cybersecurity in the accounting domain by investigating how well recent literature addresses the accounting implications of those objectives. We synthesise cybersecurity research in the accounting context into different categories intending to inform the reader of the learning available from the prior literature and which avenues of research require further investigation.

This literature synthesis has three primary objectives. The first is to provide a comprehensive overview of the current academic knowledge on cybersecurity in accounting and auditing research and to provide a set of categories into which these studies fit. The second objective is to identify key topics and issues that have appeared in the previous literature. Finally, the third objective is to identify gaps in the literature and suggest fruitful future research opportunities. This literature analysis has significant implications for research and practice by detailing, for example, the benefits of and obstacles to information sharing. This synthesis also highlights the importance of the model for information-security (cybersecurity) investments by [Gordon and Loeb \(2002\)](#). Their model has received a significant amount of attention in the literature and is known as the Gordon–Loeb model. By providing an economic model that determines the optimal amount to invest in protecting a given set of information, it contributes to scientific research and practice.

Moreover, this synthesis highlights the role of internal auditing and controls to improve cybersecurity. It emphasises that the cooperation between internal auditing and information-security functions should be uncomplicated and smooth. Finally, given the significance of cybersecurity to the field of accounting in today's interconnected digital environment, a synthesis chapter that focuses on cybersecurity from an accounting perspective could help to

stimulate much-needed cybersecurity research by accounting academics and practitioners. Furthermore, this chapter conducts citation analysis, which is essential for analysing the most-cited articles in the specific research field (e.g., [Guffey & Harp, 2017](#)). The remainder of the chapter is organised as follows. Section 2 presents the relevant background information on the topic. Section 3 explains the method used to conceptualise the synthesis. Section 4 presents the examination of the theoretical and empirical literature and a comprehensive list of topics examined in prior cybersecurity studies in the accounting field. Section 5 provides the citation analysis. Finally, in Section 6, the conclusions are summarised and avenues for future studies are suggested.

Background

Cybersecurity Risk Management Reporting

The [American Institute of Certified Public Accountants \(AICPA\) \(2018a\)](#), p. 1) stated that “Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world – large and small, public and private”. Therefore, it is extremely important that every organisation at least considers a cybersecurity risk management program. In addition, certain organisations and their stakeholders need timely, useful information about organisations’ cybersecurity risk management efforts. Therefore, it is vital that the [AICPA \(2018\)](#) has a goal to establish a common, underlying language for cybersecurity risk management reporting (for the US GAAP and/or the IFRS). Accordingly, the [AICPA \(2018a\)](#) highlighted that cybersecurity is not just an Information Technology (IT) problem; it is an enterprise risk management problem that requires a global solution. The [AICPA \(2018b\)](#) also emphasised the importance of the entity-level cybersecurity reporting framework. It explicitly stated that the goal of the reporting framework is to provide a means by which organisations can communicate useful information regarding their cybersecurity risk management programs to stakeholders. Hence, the reporting

framework is used to perform an examination-level attestation engagement. The framework is a key component of a new system and organisation control (SOC) for cybersecurity engagement. The cybersecurity report includes the following three key sets of information: i) the management's description, ii) the management's assertion, and iii) the practitioner's opinion. To conclude, the [AICPA \(2018b\)](#) emphasised that its cybersecurity risk management reporting framework is a crucial first step toward enabling a consistent, market-based, business-based solution for companies to communicate successfully with key stakeholders on how they are managing cybersecurity risk.

In addition, the [Securities and Exchange Commission \(SEC\) \(2013\)](#), p. 4) argued that it is essential that "public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack". The increasing significance of cybersecurity incidents persuaded the SEC that it should provide further guidance, and in 2011 it released its first guidelines on cybersecurity. The SEC continues to consider other means of promoting appropriate disclosure of cyber incidents and is reinforcing and expanding that 2011 guidance. Specifically, the SEC is addressing two topics that were not developed earlier, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

Motivation

An effective review creates a basis for advancing knowledge ([Webster & Watson, 2002](#)). Similarly, why synthesise studies related to cybersecurity in the accounting and auditing field? The number and severity of cyber threats have been unprecedented in recent years, and successful cyber-attacks have been reported regularly (e.g., [Islam et al., 2018](#)). Moreover, the costs of cyber-attacks are tremendous; therefore, cybersecurity risk management is argued to be extremely important for organisations (e.g., [Islam et al., 2018](#)). In relation to this, [Hausken](#)

(2006, p. 630) asserted that “the intensity of cyber war has increased through the internet revolution”. Relatedly, [Gordon, Loeb, and Luevshyn \(2003\)](#) suggested that the Internet revolution has dramatically changed the way in which individuals, firms, and the government communicate and conduct business. The authors argued that the telecommunications, banking and finance, energy, and transportation industries, as well as the military and other essential government services, all depend on the Internet. Moreover, they concluded that this widespread interconnectivity has increased the vulnerability of computer systems. The same research also highlights how the links between public policy and information security are clear. For instance, the threat of cyber terrorism, aimed at shutting down critical infrastructure industries, has brought cybersecurity to the forefront of the public policy agenda.

In addition, [Gansler and Luevshyn \(2005\)](#) stated that the growing dependence of both public and private sectors on web-based technologies and networks for their financial management systems does not come without a price, and this price is increased vulnerability. Hence, according to [the World Bank \(2018\)](#), the financial service sector was attacked more than any other industry in 2016. However, [Lainhart \(2000\)](#) had already claimed that, for many organisations, information and the technology that supports it represent their most valuable assets. [Lainhart \(2000\)](#) argued that, in this global information society, in which information travels through cyberspace, its effective management is critical. Effective management is in turn related to the awareness of increasing vulnerabilities, such as cyber threats and information warfare. Organisations’ incentives to invest in security technology are influenced by regulation. For instance, the Sarbanes-Oxley Act of 2002 (SOX) placed strict requirements on firms (e.g., [Hausken, 2006](#)). The SOX highlights the significance of information system controls by requiring the management and auditors to report on the effectiveness of internal controls over the financial reporting component of the firm’s management information systems (e.g., [Li, Peters, Richardson, & Watson, 2012](#)). For example, [Gordon, Loeb, Luevshyn, and Sohail \(2006\)](#) empirically examined the impact of the SOX on the voluntary disclosure of information-security activities by corporations. The empirical evidence provided clearly indicated that the SOX is

having a positive impact on voluntary disclosure. [Gordon et al. \(2006\)](#) offered strong indirect evidence that corporate information-security activities have attracted more attention since the passage of the SOX than before it was enacted. Indeed, they supported the widely held view that cybersecurity is an implicit requirement of the internal control structure. Overall, they argued that the information content of information-security activities is higher in some industries than in others. Firms in industries like banks, business services, insurance, telecommunications, financial services, transportation, and health care appear to be more proactive in providing voluntary disclosure of security-related activities ([Gordon et al., 2006](#)). In addition, [Gordon and Loeb \(2006\)](#) suggested guidelines for the efficient management of cybersecurity. Their cost-benefit analysis compared the costs of an activity with its benefits and the authors argued that, as long as the benefits of an additional information-security activity exceed its costs, it is valuable to engage in that activity. Further, they asserted that, while more cybersecurity does not always benefit an organisation, cyber-attacks are one of the main risks that organisations must control ([Amir et al., 2018](#)).

Based on the previous arguments, it is vital to synthesise the previous literature related to cybersecurity and identify the research streams of the articles under review. To the authors' knowledge, this is the first study to describe and synthesise the cybersecurity-related accounting and auditing studies. For instance, earlier review studies related to the topic have discussed research opportunities in IT and internal auditing (e.g., [Weidenmier & Ramamoorti, 2006](#)) and the impact of information-security events on the stock market (e.g., [Spanos & Angelis, 2016](#)).

Terminology and Methodology

Cybersecurity

Cybersecurity is often used as an analogous term for information security. However, cybersecurity is not necessarily only the protection of cyberspace itself but also the protection of

those who function in cyberspace and any of their assets that can be reached via cyberspace (von Solms & van Niekerk, 2013). Cybersecurity comprises technologies, processes, and controls that are designed to protect systems, networks, and data from cyber-attacks. Effective cybersecurity reduces the risk of cyber-attacks and protects societies, organisations, and individuals from the unauthorised exploitation of systems, networks, and technologies. Cybersecurity is an umbrella concept that encompasses information security and information assurance (Gyun No & Vasarhelyi, 2017). Thus, cybersecurity involves the protection of information that is assessed and transmitted via any computer network (Gordon & Loeb, 2006).

Method

To introduce, summarise, and analyse the extent of the research on cybersecurity in the accounting field, a list of published studies was collected using the following methods. The articles collected were identified through a systematic process that combined electronic and manual research. The combinations of keywords used to search for relevant studies included *cybersecurity*, *cyber*, *information security*, *security threats*, and *cyber threats*. An electronic search was performed using Scopus and Google Scholar. A manual search was also conducted by tracking down references in the collected studies to guarantee that all the relevant papers were included in the analysis. This chapter reviews 39 studies related to cybersecurity; the majority of the studies were published in high-quality, prominent, peer-reviewed, accounting and auditing journals between 2000 and 2018. Table 8.1. provides a count of the studies reviewed, grouped by source journal, while Table 8.2. presents the topics, the types of articles, and the key research findings related to cybersecurity. It should be noted that there is considerable variation among the methodologies of the papers under review. For instance, the articles consist of analytical, conceptual, and exploratory studies. However, the most common are empirical studies using regression analysis. As shown in Table 8.1., the collected articles come from high-quality accounting and auditing journals, including, for instance, *Accounting, Organization and Society*,

Review of Accounting Studies, International Journal of Accounting & Information Management, Journal of Information Systems, International Journal of Accounting Information Systems, Journal of Accounting and Public Policy, European Accounting Review, and Managerial Auditing Journal. The prevalence of cybersecurity-related studies in major accounting and auditing journals emphasises the topic's significance to the literature. Other journals are also included in the review, because articles in them clearly have an accounting perspective. These journals are mainly related to information management. The search included publications up to October 1, 2018. [Figure 8.1](#) presents the trends of cybersecurity-related studies in the accounting and auditing literature over the period 2000–2018. To conclude, 39 studies fulfilled the selection criteria. After the selection of the studies, the articles were carefully read and analysed in a rather inductive manner. The overall purpose was to introduce, summarise and analyse the extent of research on cybersecurity, and there were no predispositions regarding the topics that would be covered. Rather, based on an initial review of each selected paper, notes were made on various aspects, such as research questions, hypotheses, and results.

After analysing the papers, a set of categories into which these 39 studies fit could be constructed. Hence, these categories are the result of a critical and constructive analysis of the studies under review through summary, analysis, and comparison. To clarify, this synthesis identified five research streams that are related to cybersecurity.

Furthermore, it is essential to categorise the research streams related to cybersecurity in the accounting field to provide data on the level of activity in a particular research field, allowing the outcomes to be used to evaluate the performance of research streams, researchers, and journals. Methodologically, this study builds on the previous literature to deepen the understanding of cybersecurity research.

To clarify, the chapter is not directed at a specific cybersecurity-related question or issue or restricted to a specific geography. It is more comprehensive and provides relatively broad coverage of cybersecurity (in accounting) research topics. Hence, the article provides a cohesive picture of the theoretical and empirical archival literature related to cybersecurity. In terms of

8 Cybersecurity in Accounting Research

structure, it is divided into sections based on the topics covered. Therefore, academics or practitioners working on specific cybersecurity-related topics should be able to benefit from reading even a limited part of this chapter. Furthermore, [Figure 8.2.](#) illustrates the research streams and factors related to cybersecurity stemming from the studies under review. Hence, [Figure 8.2.](#) incorporates the research categories – identified by section number – and presents the interrelations between the sections. It appears to show that the studies surveyed are concentrated in the left-most elements (text boxes). However, accounting journals publish a broad variety of research, hence, there might be opportunities to investigate and publish topics related to the right-most elements in the future. Future research ideas are discussed in more detail in the concluding section.

Table 8.1 Breakdown of studies reviewed
--

8 Cybersecurity in Accounting Research

<i>Accounting, Organizations and Society</i>					1
<i>ACM Transactions on Information and System Security (TISSEC)</i>					1
<i>European Accounting Review</i>					1
<i>Information Systems Research</i>					1
<i>International Journal of Accounting & Information Management</i>					1
<i>International Journal of Accounting Information Systems</i>					3
<i>Journal of Accounting and Public Policy</i>					7
<i>Journal of Emerging Technologies in Accounting</i>					1
<i>Journal of Information Security</i>					3
<i>Journal of Information Systems</i>					11
<i>Managerial Auditing Journal</i>					6
<i>MIS Quarterly</i>					2
<i>Review of Accounting Studies</i>					1
Total					39

Source: Authors

Table 8.2 Studies on cybersecurity. The number of articles within each stream is presented in parentheses

8 Cybersecurity in Accounting Research

<i>Author(s)</i>	<i>Research topic</i>	<i>Type of the paper/conclusions that are related to cybersecurity</i>	
Panel A. Information sharing and cybersecurity (4)			
Gordon et al. (2003)	Sharing information on computer systems security: An economic analysis.		Analytical study. Gordon et al., suggested that information sharing concerning security breaches can lead to an increased level of information security.

8 Cybersecurity in Accounting Research

<p>Gansler and Lucyshyn (2005)</p>	<p>Improving the security of financial management systems: What are we to do?</p>		<p>Research note. Gansler and Lucyshyn suggested that to avoid cyber-attacks every organisation should implement a cybersecurity program, but this is often done with limited success, because it is challenging to estimate risk and the security landscape is constantly changing.</p>	
<p>Hausken (2007)</p>	<p>Information sharing among firms and cyber-attacks.</p>		<p>Analytical study. Hausken suggested that assessing costs and benefits of information sharing and security investment are interlinked with other strategies to gain</p>	

8 Cybersecurity in Accounting Research

<p>Gordon, Loeb, Lucvshyn, and Zhou (2015a)</p>	<p>The impact of information sharing on cybersecurity underinvestment: A real options perspective.</p>		<p>Empirical study using real options perspective. Gordon et al. suggested that maintaining adequate cybersecurity is crucial for a firm to maintain the integrity of its external and internal financial reports, as well as to protect the firm's strategic proprietary information.</p>	
<p>Panel B. Cybersecurity investments (8)</p>				

8 Cybersecurity in Accounting Research

<p>Gordon and Loeb (2002)</p>	<p>The economics of information-security investment.</p>		<p>Analytical study.</p> <p>Gordon and Loeb aimed to derive an economic model that determines the optimal amount to invest in information security.</p> <p>Based on the Gordon–Loeb model, the findings indicate that the amount a firm should spend to protect information sets should generally be only a small fraction of the expected loss.</p>	
---	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Tanaka, Matsuura, and Sudoh (2005)</p>	<p>Vulnerability and information-security investment: An empirical analysis of E-local government in Japan.</p>		<p>Empirical study using regression analysis. The authors utilised the Gordon–Loeb model and suggested that the decision related to the information-security investments depends on vulnerability. Their findings supported the insights of the Gordon and Loeb (2002)</p>	
<p>Hausken (2006)</p>	<p>Income, interdependence, and substitution effects affecting incentives for security investment.</p>		<p>Analytical study. Hausken concluded that each firm invests in security technology when the required rate of return from security investment exceeds the average attack level, or when the formal control requirements dictate investment.</p>	

8 Cybersecurity in Accounting Research

<p>Gordon et al. (2008)</p>	<p>Cybersecurity, capital allocations and management control systems.</p>		<p>Analytical study. Gordon et al., argued that the design and use of management control systems can play a key role in dealing with cybersecurity issues.</p>	
<p>Bose and Luo (2014)</p>	<p>Investigating security investment impact on firm performance.</p>		<p>Conceptual study. Their study proposes a comprehensive conceptual framework where non-IT-related and IT-related security investment factors are posited to influence a firm's performance.</p>	

8 Cybersecurity in Accounting Research

<p>Gordon et al. (2015b)</p>	<p>Externalities and the magnitude of cybersecurity underinvestment by private sector firms: A modification of the Gordon–Loeb model.</p>		<p>Analytical study. The authors continue to extend the Gordon–Loeb model to incorporate externalities in deciding on the appropriate level of cybersecurity investment. The authors show that the firm’s social optimal investment in cybersecurity increases by no more than 37% of the expected</p>	
--	---	--	--	--

8 Cybersecurity in Accounting Research

<p>Gordon, Loeb, and Zhou (2016)</p>	<p>Investing in cybersecurity: Insights from the Gordon–Loeb model.</p>		<p>Conceptual study. This paper explains how organisations could use, based on four simple steps, the Gordon and Loeb (2002). Thus, this paper has provided a conceptual explanation, accompanied by an illustrative example, of how organisations can use the Gordon–Loeb model to derive their appropriate level of cybersecurity investment.</p>	
--	---	--	---	--

8 Cybersecurity in Accounting Research

<p>Gordon, Loeb, Lucvshyn, and Zhou (2018)</p>	<p>Empirical evidence on the determinants of cybersecurity investments in private sector firms.</p>		<p>Empirical study using instrument survey and regression analysis. Gordon et al., indicate that there is a significant positive association between firms' spending on cybersecurity activities and their treatment of cybersecurity as an important component of the firm's internal controls over financial reporting.</p>	
<p>Panel C. Internal audit, controls, and cybersecurity (13)</p>				

8 Cybersecurity in Accounting Research

<p>Lainhart (2000)</p>	<p>COBIT™: A methodology for managing and controlling information and Information Technology risks and vulnerabilities.</p>		<p>Research note. Lainhart (2000) argued that in this global information society where information travels through cyberspace the effective management of information is very</p>	
<p>Pathak (2005)</p>	<p>Risk management, internal controls, and organisational vulnerabilities.</p>		<p>Research note. Pathak (2005) argued that cyber-attacks followed by physical attacks against critical infrastructure are a real threat; however, little is being done to provide a comprehensive defence against such a</p>	

8 Cybersecurity in Accounting Research

<p>Wallace, Ling and Cefaratti (2011)</p>	<p>Information security and Sarbanes-Oxley compliance.</p>		<p>Exploratory study. The results reveal that organisations differ in their implementation of certain IT controls based on different attributes.</p>	
---	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Li et al. (2012).</p>	<p>The consequences of Information Technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports.</p>		<p>Empirical study using regression analysis. The authors examined three dimensions of Information Technology material weaknesses: data processing integrity, system access and security, and system structure and usage. The authors find that the association with forecast accuracy appears to be strongest for IT control weaknesses most directly related to data processing integrity.</p>	
--	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Steinbart, Raschke, Gal, and Dilla (2012)</p>	<p>The relationship between internal audit and information security.</p>		<p>Exploratory study. Steinbart et al., stated that the internal audit and information-security functions should co-operate synergistically.</p>	
--	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Steinbart, Raschke, Gal, and Dilla (2013)</p>	<p>Information-security professionals' perceptions about the relationship between the information security and IAFs.</p>		<p>Empirical study using survey instrument and Partial Least Squares (PLS). Steinbart et al., suggest that information-security professionals' perceptions about the level of technical expertise possessed by internal auditors and the extent of internal audit review of information security are positively associated with the assessment about the quality of the relationship between</p>	
--	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Steinbart, Raschke, Gal, and Dilla (2016)</p>	<p>SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs.</p>		<p>Empirical study using survey data and factor analysis. The authors emphasise that SECURQUAL scores reliably predict objective measures of information-security program effectiveness.</p>	
<p>Rahimian, Bajaj, and Bradley (2016)</p>	<p>Estimation of deficiency risk and prioritisation of information-security controls.</p>		<p>Empirical study using design science approach. The results indicate that the operational, public image, legal (OPL) model can be used to create a detailed risk assessment of all corporate data.</p>	

8 Cybersecurity in Accounting Research

Gyun No and Vasarhelvi (2017)	Cybersecurity and continuous assurance.		Research note. The authors addressed the most pressing topics in cybersecurity: the need for new approaches for its assurance.	
---	---	--	--	--

8 Cybersecurity in Accounting Research

<p>Islam et al. (2018)</p>	<p>Factors associated with security/cybersecurity audit by IAF: An international study.</p>		<p>Empirical analysis using regression analysis. Islam et al. (2018) examined the factors associated with the extent of cybersecurity audit by the internal audit function (IAF) of the firm. The authors suggested that the extent of cybersecurity audit by IAF is significantly and positively associated with IAF competence related to governance, risk, and control.</p>
--	---	--	--

8 Cybersecurity in Accounting Research

<p>Kalyaoglu and Caliyurt (2018)</p>	<p>Cyber security assurance process from the internal audit perspective.</p>		<p>Conceptual study. The authors concluded that cyber-risk must be managed and stated that it is very important to maintain formal documentation on related cyber controls and internal audit should be an integral part of cybersecurity assurance process, as internal audits have a unique capacity to look</p>	
--	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Stafford, Deitz, and Li (2018)</p>	<p>The role of internal audit and user training in information-security policy compliance.</p>		<p>Qualitative case analysis. Stafford et al., examined the role of information-security policy compliance and the role of information systems auditing in identifying non-compliance in the workplace. The study is a qualitative case analysis of technology user security perceptions combined with interpretive analysis of depth interviews with auditors. The findings indicate that enterprise risk management benefits from audits.</p>	
---	--	--	---	--

<p>Steinbart, Raschke, Gal, and Dilla (2018)</p>	<p>The influence of a good relationship between the internal audit and information-security functions on information-security outcomes.</p>		<p>Empirical study using survey data and PLS. The authors investigate how the quality of the relationship between the internal audit and the information-security functions affects objective measures of the overall effectiveness of an organisation's information-security efforts. The quality of this relationship has a positive effect on the number of reported internal control weaknesses and incidents of non-compliance, as well as on the numbers of security incidents detected both before and after they caused material harm to the organisation.</p>
--	---	--	--

Panel D. Disclosure of cybersecurity activities (5)			
Gordon et al. (2006)	The impact of the Sarbanes-Oxley Act on the corporate disclosures of information-security activities.		Empirical study. The results reveal that SOX is having a positive impact on voluntary disclosure. Gordon et al. provide strong indirect evidence that corporate information-security activities are receiving more focus since the passage of SOX than before SOX was enacted.

8 Cybersecurity in Accounting Research

<p>Gordon et al. (2010)</p>	<p>Market value of voluntary disclosures concerning information security.</p>		<p>Empirical study using regression analysis. This article aims to examine market value of voluntary disclosures of items pertaining to information security. The findings provide strong evidence that voluntarily disclosing items concerning information security is associated positively with the market value</p>	
---	---	--	---	--

8 Cybersecurity in Accounting Research

<p>Wang, Kannan, and Ulmer (2013)</p>	<p>The association between the disclosure and the realisation of information security risk.</p>		<p>Mixed methods. Wang et al. evaluated how the nature of the disclosed security risk factors is associated with future breach announcements reported in the media. Their model is able to accurately associate disclosure characteristics with breach announcements about 77% of the time.</p>	
---	---	--	---	--

8 Cybersecurity in Accounting Research

Li et al. (2018)	SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors.		Empirical study using regression analysis. Li et al. investigate whether cybersecurity risk disclosure is informative for future cybersecurity incidents. The authors suggest that the presence in the pre-guidance period and length of cybersecurity risk disclosure are positively associated with subsequent cybersecurity	
----------------------------------	---	--	--	--

8 Cybersecurity in Accounting Research

<p>Ettredge, Guo, and Li (2018)</p>	<p>Trade secrets and cybersecurity breaches.</p>		<p>Empirical study using regression analysis. The authors find that firms mentioning the existence of trade secrets have a significantly higher subsequent probability of being breached relative to firms that do not do so.</p>	
<p>Panel E. Security threats and security breaches (9)</p>				

8 Cybersecurity in Accounting Research

<p>Ettredge and Richardson (2003)</p>	<p>Information transfer among internet firms: The case of hacker attacks</p>		<p>Empirical study using regression analysis. The authors showed negative mean abnormal returns among internet firms that have not actually been attacked. Further, they suggested that investors believed that firms would respond to the hacker attacks with higher spending on IT security.</p>
---	--	--	--

8 Cybersecurity in Accounting Research

<p>Boritz and Ne 2005</p>	<p>Security in XML-based financial reporting services on the Internet.</p>		<p>Conceptual study. The authors presented security threats and limitations of current security technologies. The authors also identified security requirements that should be considered to ensure reliable, trustworthy XBRL and XARL services.</p>	
---	--	--	---	--

8 Cybersecurity in Accounting Research

<p>Abu-Musa (2006)</p>	<p>Perceived security threats of computerised accounting information systems in the Egyptian banking industry.</p>		<p>Empirical study using survey data. Abu-Musa (2006) suggested that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and human-made disasters, employees' sharing of passwords, and misdirecting prints and distributing information to unauthorised people are the most serious</p>	
--	--	--	--	--

8 Cybersecurity in Accounting Research

<p>Kwon, Ulmer, and Wang (2013)</p>	<p>The association between top management involvement and compensation and information security breaches.</p>		<p>Empirical study using regression analysis. The findings present how an IT executive's status in the top management team and the composition of his/her compensation can be related to a firm's IT governance mechanisms.</p>	
<p>Higgs, Pinsker, Smith, and Young (2016)</p>	<p>The relationship between board-level technology committees and reported security breaches.</p>		<p>Empirical study using regression analysis. Using reported security breaches during the period 2005–2014, results reveal that firms with technology committees are more likely to have reported breaches in a given year than are firms without the</p>	

8 Cybersecurity in Accounting Research

<p>Carré, Curtis, and Jones (2018)</p>	<p>Ascribing responsibility for online security and data breaches.</p>		<p>Exploratory study. The authors reveal that individuals held companies more responsible for protecting private data and held companies even more responsible following a data breach.</p>	
<p>Curtis, Carré, and Jones (2018)</p>	<p>Consumer security behaviours and trust following a data breach.</p>		<p>Exploratory study. The authors' summary is that online security is of great concern and companies that have had a breach face reputational damage.</p>	

8 Cybersecurity in Accounting Research

<p>Smith, Higgs, and Pinski (2018)</p>	<p>Do auditors price breach risk in their audit fees?</p>		<p>Empirical study using regression analysis. The authors suggest that breaches are associated with an increase in fees, but the result is driven by external breaches. Further, the study reveals the presence of board-level risk committees and more active audit committees may help mitigate the breach risk audit fee premium.</p>	
--	---	--	--	--

<p>Amir et al. (2018)</p>	<p>Do firms underreport information on cyber-attacks? Evidence from capital markets.</p>		<p>Empirical study using regression analysis. The findings reveal that the market reaction to disclosed cyber-attacks is indeed small, but the market reaction to withheld attacks is negative and significant.</p>	

Source: Authors

[Insert 15032-5311-008_Figure_001 Here]

Figure 8.1 Trends of cybersecurity-related studies over the period of 2000–2018

[Insert 15032-5311-008_Figure_002 Here]

Figure 8.2 Framework of research streams and factors related to cybersecurity

Source: Authors

Previous Theoretical and Empirical Literature

Information Sharing and Cybersecurity

The first research stream identified in this synthesis examines information sharing and its role in cybersecurity. The prior literature has suggested that information sharing in cybersecurity has

become extremely important for accounting and public policy. [Gordon et al. \(2003\)](#) examined information sharing in relation to computer system security. Their findings indicated that sharing information about threats and breaches of computer security lowers the overall costs of achieving any particular level of cybersecurity. Therefore, they suggested (p. 481) that sharing information “has been promoted as an important tool in enhancing social welfare”. However, while their analysis showed that information sharing does indeed offer the potential to reduce overall security costs and raise social welfare, some pitfalls exist that may well prevent the realisation of the full potential benefits. These pitfalls concern the need to create economic incentives to facilitate effective information sharing related to cybersecurity. In other words, [Gordon et al. \(2003\)](#) suggested that companies and society could benefit from sharing information concerning security breaches. However, without appropriate economic incentives, firms may try to exploit the security expenditure of others. Similarly, [Gansler and Lucyshyn \(2005\)](#) suggested that the vulnerabilities associated with cyber-attacks are often exploited by a variety of threats: hackers, insiders, criminals, terrorists, or possibly a combination of those. The authors argued that, to avoid cyber-attacks, every organisation should implement a cybersecurity program, but this might often achieve only limited success, because it is challenging to estimate risk, and the security landscape is constantly changing. [Gansler and Lucyshyn \(2005\)](#) stated that the current cyber threats are fairly well understood, but firms are not always proactive enough. They also claimed that it has been generally assumed that a key element required to improve cybersecurity is the sharing of information, because “having information on threats and on actual incidents experienced by others can help an organization better understand the risks faced and determine what preventive measures should be implemented” ([Gansler & Lucyshyn, 2005](#), p. 6). They concluded that the importance of financial management systems in a cybersecurity process should be highlighted. In addition, they argued that the US is already the nation most dependent on information systems. Therefore, the consequences of the vulnerability of information systems should be considered extremely carefully ([Gansler & Lucyshyn, 2005](#)).

In contrast, [Hausken \(2007\)](#) suggested that assessing the costs and benefits of information sharing and security investment is interlinked with other strategies to gain a competitive advantage. [Hausken \(2007\)](#), p. 641) argued that

the security of an interlinked information system depends on the strategies about information sharing and security investment chosen by all actors, including those that are players in it, those that attempt to regulate and reshape it and those that attempt to shut it down, which opens a role for public policy.

[Hausken \(2007\)](#) considered two firms that are subject to cyber-attacks. The firms defend themselves by sharing information with each other and investing in security. Each firm chooses to receive information about the other firm's security breaches. [Hausken \(2007\)](#) analysed the incentives to voluntarily provide information to another firm and the trade-offs that each firm makes between sharing information and investing in security. The same research introduced the classic free-rider problem to explain why information sharing often does not occur and also highlighted that the classic free-rider was also identified by [Gordon et al. \(2003\)](#). [Hausken \(2007\)](#), p. 674) indicated that "information sharing increases linearly in the interdependence between firms, and is zero with negative or no interdependence". To conclude, [Hausken \(2007\)](#), p. 647) suggested that "it is the interdependence between firms that is the key determinant of information sharing and not the competitiveness".

On a related note, [Gordon et al. \(2015a\)](#) suggested that academics, government officials, and corporate executives have recommended information sharing related to cybersecurity, explaining that "the argument for sharing information is based on the belief that firms can reduce their cybersecurity threats, vulnerabilities and, in turn, cyber incidences, based on the experiences of other (especially similar) firms" (p. 518). Based on a real options perspective, they demonstrated that "information sharing, with its ability to reduce the uncertainty associated with cybersecurity investments, may well result in reducing the tendency by private-sector firms to underinvest in cybersecurity activities" ([Gordon et al., 2015a](#), p. 518). Furthermore, the study

suggested that the benefit gained from information sharing could provide a vital incentive to overcome firms' unwillingness to share their private information actively.

Cybersecurity Investments

The second research stream identified concentrates on cybersecurity investments. Given the significance of cybersecurity to organisations, a fundamental economics-based question has been brought up regularly in prior studies: How much should be invested in cybersecurity-related activities? [Gordon and Loeb \(2002\)](#) presented a model to address this research question, and this model has received considerable attention in the literature, in which it is known as the Gordon–Loeb model. The originators argued that, owing to the information-intensive characteristics of a modern economy (e.g., the Internet and the World Wide Web), information security is a growing spending priority for most companies around the world, which prompted them to create an economic model that determines the optimal amount to invest in information security. To be more specific, they stated that the term information security in their model can be interpreted broadly. The Gordon–Loeb model is applicable to investments related to various information-security goals, for instance protecting the confidentiality, availability, and integrity of information. Hence, the model is also applicable to cybersecurity investments.

To summarise, their findings indicated that the optimal amount to spend on protecting information sets does not always increase with the level of vulnerability of such information. The Gordon–Loeb model can be interpreted as suggesting that the amount that a firm should spend on protecting information sets should generally be only a small fraction of the expected loss, and, accordingly, the findings showed that “managers allocating an information-security budget should normally focus on information that falls into the midrange of vulnerability to security breaches” ([Gordon & Loeb, 2002](#), p. 453). “Since extremely vulnerable information sets may be inordinately expensive to protect, a firm may be better off concentrating its efforts on information sets with midrange vulnerabilities” ([Gordon & Loeb, 2002](#), p. 438). Moreover,

[Gordon et al. \(2016\)](#) discussed the Gordon–Loeb model with a focus on providing insights to aid the model’s use in a practical setting. They highlighted that, despite its mathematical underpinnings:

the Gordon–Loeb Model provides an intuitive framework that lends itself to an easily understood set of steps for deriving an organization’s cybersecurity investment level. These four steps are: (i) to estimate the value, and thus the potential loss, for each information set in the organization; (ii) to estimate the probability that an information set will be breached based on the information set’s vulnerability; (iii) to create a grid of all possible combinations of steps 1 and 2 above; and finally (iv) to derive the level of cybersecurity investment by allocating funds to protect the information sets, subject to the constraint that the incremental benefits from additional investments exceed (or are at least equal to) the incremental costs of the investment.

([Gordon et al., 2016](#), pp. 57–58)

Similarly, [Tanaka et al. \(2005\)](#) studied the relationship between vulnerability and information-security investment using data on Japanese municipal authorities. They exploited the Gordon–Loeb model and suggested that the decision related to information-security investments depends on vulnerability. Their findings revealed that the municipal authorities examined did not commit higher than usual expenditures on information security if the vulnerability levels were low or extremely high while, in contrast, they invested more than usual if the vulnerability levels were medium-high. Therefore, Tanaka et al.’s findings supported the insights provided by [Gordon and Loeb’s \(2002\)](#) model.

Moreover, [Gordon et al. \(2015b\)](#) extended the Gordon–Loeb model to derive the optimal level of investment in cybersecurity activities. They investigated how the existence of well-recognised externalities changes the maximum that a firm should, from a social welfare perspective, invest in cybersecurity activities. They showed that a firm’s social optimal investment in cybersecurity increases by no more than 37% of the expected externality loss.

[Gordon et al.'s \(2015b\)](#) results have important implications for practice because they indicate that, unless private-sector firms consider the costs of breaches associated with externalities, in addition to the private costs resulting from breaches, underinvestment in cybersecurity activities is essentially a given. Therefore, the authors concluded that cybersecurity underinvestment might pose a serious threat to national security and to the economic prosperity of a jurisdiction. In relation to this, they suggested that “governments around the world are justified in considering regulations and/or incentives designed to increase cybersecurity investments by private sector firms” ([Gordon et al., 2015b](#), p. 29). The latest study by [Gordon et al. \(2018\)](#) found a significant positive association between the importance that firms attach to cybersecurity for internal control purposes and the percentage of their IT budget spent on cybersecurity activities; accordingly the study ([2018](#), p. 133) suggests that “treating cybersecurity as an important component of a firm’s internal control system serves as an incentive for private firms to invest in cybersecurity activities”.

The prior literature has also discussed other approaches to evaluating cybersecurity investments. For instance, [Hausken \(2006\)](#) argued that firms are threatened with cyber-attacks and invest increasingly in security technology. A variety of principles are applied to determine the size of the investment. However, firms’ incentives to invest in security technology are also influenced by law. As mentioned earlier, the SOX imposed strict requirements. [Hausken \(2006\)](#) stated that firms invest maximally in security when the average attack level is 25% of the firm’s required rate of return. [Hausken \(2006\)](#), p. 629) emphasised that “each firm invests in security technology when the required rate of return from security investment exceeds the average attack level, or when the formal control requirements dictate investment”.

Similarly, [Bose and Luo \(2014\)](#) argued that today’s organisations are challenged by the threats of cybersecurity, It is therefore essential for organisations of different sizes and types to understand the potential impacts of cybersecurity on organisational performance. [Bose and Luo \(2014\)](#), p. 204) highlighted that “security investments need to be made by organizations to help secure their tangible and intangible or physical and intellectual assets”. Moreover, they argued

that understanding organisational cybersecurity now involves drawing from a holistic view of not only technical but also financial, legal, and policy aspects. In conclusion, the study proposed a comprehensive conceptual framework in which non-IT-related and IT-related security investment factors are posited to influence a firm's performance. The authors put forward 14 propositions^[^1] to understand the relationship between security investments and firm performance.

Finally, [Gordon et al. \(2008\)](#) stated that cybersecurity breaches represent an important component of the enterprise risk confronting organisations. They therefore argued that security audits are simultaneously gaining in popularity. [Gordon et al. \(2008\)](#), p. 216) concluded that “the information security audit component of a management control system is useful in mitigating an agent's empire building preferences in addressing cybersecurity threats”. By implication, the broader objective of their paper was to make the case that accounting researchers who are concerned with management control systems can – and should – play a dominant role in addressing issues related to cybersecurity. To be more specific, [Gordon et al. \(2008\)](#) analysed the role of security auditing in controlling the natural tendency of a chief information security officer (CISO) to overinvest in cybersecurity activities; in essence, they argued that firms can use an information-security audit to reduce a CISO's power.

Internal Auditing, Controls, and Cybersecurity

The third research stream concentrates on internal auditing, controls, and cybersecurity. For instance, [Pathak \(2005\)](#) demonstrated the impact of technology convergence on the internal control mechanism of a firm and suggested that it is important for an auditor to be aware of the security hazards faced by the financial or even the entire organisational information system.

[Pathak \(2005\)](#) attempted to place the security system design and the organisational vulnerabilities in the context of the convergence of communication and networking technologies with the complex IT in business processes. [Pathak \(2005\)](#) also highlighted that auditors should

be aware of technology risk management and its impact on the enterprise's internal controls and organisational vulnerabilities.

However, [Lainhart \(2000\)](#) suggested that management needs generally applicable and accepted IT governance and control practices to benchmark the existing and planned IT environment. [Lainhart \(2000\)](#), p. 22) stated that “Cobit™ is a tool that allows managers to communicate and bridge the gap with respect to control requirements, technical issues and business risks”. Moreover, he suggested that Cobit™ enables the development of clear policy and good practices for IT control throughout firms. Finally, [Lainhart \(2000\)](#) concluded that Cobit™ is intended to be the breakthrough IT governance tool that helps understand and manage the risks associated with cybersecurity and information.

[Steinbart et al. \(2016\)](#), p. 71) stated that “the ever-increasing number of security incidents underscores the need to understand the key determinants of an effective information security program”. Therefore, they examined the use of the COBIT Version 4.1 Maturity Model Rubrics to develop an instrument (SECURQUAL) that can obtain an objective measure of the effectiveness of enterprise information-security programs. They argued that scores for various rubrics predict four separate types of outcomes, thereby providing a multidimensional picture of information-security effectiveness. Finally, [Steinbart et al. \(2016\)](#), p. 88) concluded that “researchers can, therefore, use the SECURQUAL instrument to reliably measure the effectiveness of an organization's information-security activities, without asking them to divulge sensitive details that most organizations are unwilling to disclose”.

Because the SOX created a resurgence of the organisational focus on internal controls, [Wallace et al. \(2011\)](#) studied the extent to which the IT controls suggested by the ISO 17799 security framework have been integrated into organisations' internal control environments. By surveying the members of the IIA on the usage of IT controls in their organisations, their results revealed the ten most commonly implemented controls and the ten least commonly implemented. The findings indicated that organisations may differ in their implementation of certain IT controls based on the size of the company, whether they are a public or private organisation, the

industry to which they belong, and the level of training given to IT and audit personnel. Moreover, [Li et al. \(2012\)](#), p. 180) stated that “SOX guidance and auditing standards also emphasize the unique benefits that accompany the use of IT-related controls, including enhancing the usefulness of information produced by the system”.

Hence, using a design science approach, [Rahimian et al. \(2016\)](#) developed the operational, public image, legal (OPL) multidimensional risk specification model to quantitatively estimate the contribution of security controls in place as well as the control deficiency risk due to missing controls. They contributed to the literature by indicating that the OPL model can be used to create a detailed risk assessment of all corporate data. This finding was important because it is often difficult for the internal audit function (IAF) to assess control deficiency risk (CDR) in the area of information security.

In addition to the important topics discussed earlier, a vital subject within this research stream is the cooperation between internal auditing and information-security functions. In many companies, both the information systems and the IAFs are involved with information security and cybersecurity. [Steinbart et al. \(2012\)](#), p. 228) argued that these functions should work together synergistically, because “the information security staff designs, implements, and operates various procedures and technologies to protect the organization’s information resources, and internal audit provides periodic feedback concerning effectiveness of those activities along with suggestions for improvement”. The main contribution of their study was to develop an exploratory model of the factors that influence the nature of the relationship between the IAF and the information-security function. These factors are, for instance, the internal auditor’s level of IT knowledge, the internal auditor’s communication skills, and the internal auditor’s attitude (i.e., role perception).

In contrast, [Steinbart et al. \(2013\)](#) examined the relationship between the information-security function and the IAF from the perspective of information security professionals. The study in question surveyed information-security professionals’ perceptions, and the findings revealed that “information security professionals’ perceptions about the level of technical

expertise possessed by internal auditors and the extent of internal audit review of information security are positively related to their assessment about the quality of the relationship between the two functions” (Steinbart et al., 2013, p. 65). Most importantly, the study argued that the quality of the relationship is positively associated with perceptions of the value provided by internal auditing and with measures of the overall effectiveness of the organisation’s information-security endeavours. The latest study examining the cooperation between the IAF and the information-security function was also conducted by Steinbart et al. (2018). This latter study investigated the influence of a good relationship on information-security outcomes. In other words, using a unique dataset, Steinbart et al. (2018) investigated how the quality of the relationship objectively measures the overall effectiveness of an organisation’s information-security efforts. The findings highlighted that the quality of the relationship has a positive effect on the number of reported internal control weaknesses and incidents of non-compliance as well as on the number of security incidents detected, both before and after they caused material harm to the organisation. Finally, Steinbart et al. (2018, p. 1) emphasised that “higher levels of management support for information security and having the chief information security officer (CISO) report independently of the IT function have a positive effect on the quality of the relationship between the internal audit and information security functions”.

Instead, Stafford et al. (2018) examined the role of information-security policy compliance and information system auditing in identifying non-compliance in working environments. They concentrated on the role of non-malicious insiders who unknowingly or innocuously thwart corporate cybersecurity directives by engaging in unsafe computing practices. Hence, they conducted a qualitative case analysis of technology user security perceptions, combined with an interpretive analysis of in-depth interviews with auditors, to examine and explain user behaviours in violation of cybersecurity directives. Thus, they determined the ways in which auditors can best assist management in overcoming the problems associated with security complacency among users. Their findings indicated that enterprise risk management (ERM) benefits from audits that identify technology users who might feel

invulnerable to cyber threats. Moreover, [Stafford et al. \(2018\)](#), p. 420) argued that “the IT auditor is likely the most valuable objective consultant and critic of the process that is designed to manage and enforce security compliance in the firm”. Nevertheless, the same report also stated that “the function of an audit is to consult, to improve and to guide; it is the role of corporate management to seek and embrace auditing guidance in the matter of improving cybersecurity” ([2018](#), p. 420).

Similarly, [Islam et al. \(2018\)](#) stated that cybersecurity auditing is a relatively new dimension of security practice intended to support the protection of critical information assets. The authors added that an auditing process will seek to obtain evidence of organisational cybersecurity policies and their efficacy for the protection of asset integrity, data confidentiality, and data access and availability. The study points out that managing cybersecurity is increasingly important for companies due to the growing dependence of firms on technology for conducting their business, creating a competitive advantage, and achieving success. [Islam et al. \(2018\)](#) examined the factors associated with the extent of cybersecurity auditing by the internal audit function (IAF) of the firm. Specifically, they focused on whether the internal audit function, the certified audit executive’s characteristics, the board involvement related to governance, the role of the audit committee, and the chief risk officer and the IAF tasked with ERM are associated with the extent to which the firm engages in cybersecurity auditing. Their results suggested that the extent of cybersecurity auditing by the 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 Islam et al. research did not find significant results related to the roles of the audit committee and the chief risk officer. To conclude, the research argued that comprehensive risk assessment conducted by the IAF and IAF quality have a significant and positive effect on a cybersecurity audit. Therefore, the study provides insights into the specific IAF/certified audit executive characteristics and corporate governance characteristics that can lead the IAF to contribute significantly to a cybersecurity audit.

In related work, [Kahyaoglu and Caliyurt \(2018\)](#) examined the cybersecurity assurance process from the internal audit perspective. They developed a model to introduce the way in which the internal audit and information-security functions could work together to support organisations in accomplishing a cost-effective level of information security. The key issues and approaches were explained regarding how to become a trusted cybersecurity advisor, and a sample cybersecurity awareness program checklist was provided. For instance, [Kahyaoglu and Caliyurt \(2018, p. 371\)](#) concluded that “internal auditors should expand their own IT audit capabilities to provide proactive insights and, in this way, they could make value-added recommendations to management”.

Finally, [Gyun No and Vasarhelyi \(2017\)](#) discussed whether external auditors should be involved in cybersecurity. First, they stated that cybersecurity can clearly influence the economic health of an organisation, because the estimated average costs of cyber-attacks are extremely high. Second, auditor competence in this highly technical area of cybersecurity raises further questions. For instance, are current auditors trained to be involved in cybersecurity issues? Hence, they stated that auditors might have training in other subject matters that may overlap with cybersecurity, such as valuation, in which the auditor relies on specialists to support key assertions. While some firms provide their employees with IT audit specialisation skills, the greater scope of accountant training precludes these skills ([Gyun No & Vasarhelyi, 2017](#)). Further, they argued that, if not auditors, then who should take the role of integrating financial and cyber-risk information into some form of assurance that can be provided to shareholders? Finally and most importantly, they discussed the risk assessment portion of future audits. They concluded that substantive research is needed on how to integrate the generally qualitative issues of the risk of cyber exposure into the traditional audit model.

Disclosure of Cybersecurity Activities

The fourth research theme contains articles examining the disclosure of cybersecurity activities. As mentioned earlier, [Gordon et al. \(2006\)](#) highlighted the impact of the SOX (2002) on the voluntary disclosure of information-security activities by corporations. They clearly emphasised that the SOX had a positive impact on such disclosure. To clarify, their findings indicated that the voluntary disclosure of information-security activities had increased by over 100% since the passage of SOX when compared with two years prior to the law's implementation. This was an interesting finding, because the SOX did not explicitly address the issue of information security. On a related note, [Gordon et al. \(2010\)](#) examined voluntary disclosures concerning cybersecurity and argued that voluntary disclosures in the annual report on cybersecurity allow a corporation to provide signals to the markets that "the firm is actively engaged in preventing, detecting and correcting security breaches". Accordingly, Gordon et al. suggested that it is a strategic choice whether or not a firm voluntarily decides to disclose items concerning information security; they further asserted that there is clear evidence that an increasing number of organisations are voluntarily disclosing information related to cybersecurity. Moreover, Gordon et al. provided empirical support for the argument that voluntary disclosures related to cybersecurity are positively and significantly related to the stock price. Their results indicated generic support for the signalling argument, which states that managers who disclose information voluntarily are consistent with increasing firm value. Most importantly, their results showed that "voluntary disclosures related to proactive security measures by a firm have the greatest impact on the firm's market" ([Gordon et al., 2010](#), p. 590).

In contrast, [Wang et al. \(2013\)](#) examined the association between the disclosure and the realisation of information-security risk and stated that firms often disclose information-security risk factors in public filings. [Wang et al. \(2013\)](#) argued that the internal cybersecurity information associated with disclosures may be positive or negative. They evaluated how the nature of the disclosed security risk factors, believed to represent the firm's internal information regarding information security, is associated with future breach announcements reported in the media. The paper presents a decision tree model, which categorised the occurrence of future

security breaches based on the textual contents of the disclosed security risk factors. The authors' model was able to associate disclosure characteristics accurately with breach announcements around 77% of the time. [Wang et al. \(2013\)](#) also used text-mining techniques to contribute a richer interpretation of the results. The results showed that the disclosed security risk factors with risk mitigation themes are less likely to be related to future breach announcements. Their results indicated that the market reaction following a security breach announcement differs depending on the nature of the preceding disclosure. To conclude, the study showed that the textual content of security risk factors is an adequate predictor of future reported breaches. More precisely, [Wang et al. \(2013\)](#) demonstrated that firms that disclose actionable (risk-mitigating) information are less likely to be associated with security incidents. The findings indicate that firms taking proactive action have an incentive to disclose their stance on information security truthfully.

In addition, [Li et al. \(2018\)](#) investigated whether cybersecurity risk disclosure is informative for future cybersecurity incidents. They focused on two measures: the presence of cybersecurity risk disclosure and the length of cybersecurity risk disclosure. They found that the presence of these risk factors in the pre-guidance period and the length of these risk factors are related to future reported cybersecurity incidents. However, the findings indicated that the association between the presence of cybersecurity risk disclosure and subsequently announced cybersecurity incidents become insignificant after the passage of the United States Securities and Exchange Commission's (SEC) cybersecurity disclosure guidance. Hence, the work of [Li et al. \(2018\)](#) supports the SEC's decision on underlining cybersecurity risk disclosure. However, Li et al. pointed out that the SEC's disclosure guidance may unintentionally encourage firms to disclose cybersecurity risks regardless of the level of the risks.

To conclude, the latest study within this research stream examined trade secrets and cybersecurity breaches. The study conducted by [Ettridge et al. \(2018\)](#) investigated the association between firms' disclosures in Forms 10-K of the existence of trade secrets and cyber theft of corporate data, which they defined as "breaches". The study contributes to the literature by focusing specifically on breaches that target trade secrets, finding that firms that mention the

existence of trade secrets have a significantly higher subsequent probability of being breached than firms that do not do so. The results were stronger among younger firms, firms with fewer employees, and firms operating in less concentrated industries.

Security Threats and Security Breaches

The fifth stream in this synthesis relates to security threats and breaches. [Ettredge and Richardson \(2003\)](#) had already examined information transfer among internet firms, defining internet firms as those that “operate in a variety of industries, but are similar in that they rely almost completely on IT when conducting such fundamental operations as buying and selling goods and services” (p. 71). More specifically, the article examined the stock market reaction to the denial of service attacks against certain widely known internet firms in February 2000. They found that negative mean abnormal returns occurred among internet firms that were not actually attacked. Interestingly, this happened both within internet industries in which some firms were attacked and within internet industries in which no firms were attacked. However, they also suggested that internet firms that were similar in size to those that were attacked (i.e., relatively large) were more likely to be attacked in the future. Similarly, [Boritz and No \(2005\)](#) discussed security threats and the limitations of security technologies. In addition, they studied the security requirements to ensure reliable, trustworthy financial reporting services. Finally, their paper explained several proposed security standards and suggested the Web Services Security Architecture as a suitable security mechanism for financial reporting services.

In contrast, [Abu-Musa \(2006\)](#) investigated the perceived security threats to computerised accounting information systems in the Egyptian banking industry and emphasised that “advanced technology has created significant risks related to ensuring the security and integrity of computerized accounting information systems” (p. 187). However, the findings of the study revealed that the accidental entry of bad data by employees, the accidental destruction of data by employees, the introduction of computer viruses to the system, natural and human-made

disasters, employees sharing passwords, and misdirecting prints and distributing information to unauthorised people are perceived to be the most significant security threats. Surprisingly, the results highlighted that the greatest security concerns are perceived to come from within rather than from outside the banks. [Abu-Musa \(2006\)](#) concluded that banks know the threats; their challenge is to overcome them.

[Carré et al. \(2018\)](#) examined consumer reactions to security breaches and sought the best approach for companies to minimise reputational damage, arguing that “participants viewed companies as being more responsible for data protection and more responsible after a data breach than were individuals” (p. 442). Hence, their findings emphasised that there was no significant difference between participants’ perceptions of companies’ responsibility to protect data and companies’ responsibility for a data breach occurring.

The fifth study categorised in this theme was conducted by [Curtis et al. \(2018\)](#). They focused on how security statement certainty (rated as overconfident, underconfident, or realistic) and the behavioural intentions of potential consumers influence the perceptions of companies in the presence or absence of a past security breach. [Curtis et al. \(2018\)](#) exposed participants to three types of security statements and randomly assigned them to the presence or absence of a previous breach. Their findings indicated that the presence or absence of such a previous breach had a large impact on company perceptions but a minimal impact on behavioural intentions to be more secure personally. The findings implied that companies need to be cautious about how much confidence they convey to consumers. In addition, the results have social implications; companies need to communicate personal security behaviours to consumers in a way that instils confidence in the company but also encourages personal responsibility. They summarised online security as being of great concern and stated that companies that have experienced a breach face reputational damage. Their findings further showed that this damage emerges regardless of how confidently the companies express themselves through security statements.

In contrast, [Higgs et al. \(2016\)](#) investigated the association between board-level technology committees and reported security breaches. The work highlighted that, following

several high-profile data security breaches, corporate boards are prioritising the oversight of IT risk. [Higgs et al. \(2016\)](#), p. 79) stated that “firms are also increasingly faced with disclosure decisions regarding IT security breaches”. Therefore, their paper suggested that firms can use the formation of a board-level technology committee as part of their IT governance to signal their ability to detect and respond to security breaches. Referencing reported security breaches during the period 2005–2014, the findings revealed that firms with a technology committee are more likely to have reported breaches in a given year than firms without a committee. Moreover, this positive relationship is driven by relatively young technology committees and external source breaches. To conclude, Higgs et al. highlighted that the perceived value of a technology committee mitigates the negative abnormal stock returns arising from external breaches. In summary, they emphasised that security breaches are costly to firms and the cost is continuing to increase; hence, firms are increasingly recognising this phenomenon and considering governance mechanisms in response. It can be interpreted that the establishment of a specialised board committee – specifically a technology committee – is an effective response to breach risk.

The second study related to IT governance mechanisms was conducted by [Kwon et al. \(2013\)](#). It studied how an IT executive’s position in a top management team and compensation are associated with the likelihood of information-security breaches. Using a sample drawn from multiple sources in the period from 2003 to 2008, they revealed that an IT executive’s involvement in the top management team is negatively related to the possibility of information-security breaches. Finally, further analysis indicated that the amount of behaviour-based (i.e., salary) compensation and the pay differences of outcome-based (i.e., bonuses, stock awards, and stock options) compensation between IT and non-IT executives are negatively associated with the likelihood of information-security breaches.

Furthermore, researchers have investigated the impact of cybersecurity breaches on the stock market returns of firms. ² For example, [Amir et al. \(2018\)](#) concluded that withheld cyber-attacks are associated with a decline of approximately 3.6% in equity value in the month when the attack is discovered. Using the market reactions to withheld and disclosed attacks, they

estimated that managers disclose information on cyber-attacks when investors already suspect a high likelihood (40%) of an attack. However, the final study within this stream investigated whether auditors price breach risk into their fees and whether a firm's internal governance can mitigate the potential increases in audit fees. [Smith et al. \(2018\)](#) suggested that breaches are associated with an increase in audit fees, but the result was driven by external breaches. They emphasised that the presence of board-level risk committees and more active audit committees may help to mitigate the breach risk audit fee premium. Finally, they argued that both past breach disclosures and future disclosures are associated with audit fees.

Citation Analysis

Citation analysis is important and useful because it allows influential authors to be identified, which, in turn, provides researchers with a solid basis for positioning their current contributions. Therefore, citation analysis was conducted in the context of cybersecurity-related studies. Google Scholar provides both citation counts and links to the sources of the citations ([Kenny & Larson, 2018](#)); hence, the number of citations for each article under review was collected. [Table 8.3](#) presents the distribution of citations of the articles under review. Of these articles, 12 have been cited between 1 and 4 times. However, it must be mentioned that many of the articles are very recent, which could explain the low number of citations. Furthermore, 8 of the articles have been cited between 5 and 30 times and 9 articles between 30 and 90 times. [Table 8.4](#) reveals the top ten ranking of the papers in terms of the highest number of citations. These articles have more than 90 citations. [Table 8.4](#) also presents the research streams into which the most-cited articles are categorised. Before discussing the findings, a few important points should be highlighted. The overall number of citations is 3,057 for all the articles under review. The most-cited article is that of [Gordon and Loeb \(2002\)](#), with over 1,000 citations. This paper introduced the Gordon–Loeb model, which forms the basis for making cybersecurity investment decisions. The huge amount of citations explains the importance of the model to the cybersecurity

8 Cybersecurity in Accounting Research

literature. The second most-cited study is [Gordon et al. \(2003\)](#), which suggested that information sharing concerning security breaches can lead to an increased level of information security. The third most-cited study was conducted by [Lainhart \(2000\)](#). The paper discussed COBIT™, which is a methodology for managing and controlling information and IT risks and vulnerabilities. To conclude, the topics of the ten most-cited articles stem from the five research streams identified. The citation numbers reflect the interest in and importance of the topics. Therefore, it can cautiously be suggested that cybersecurity investments have proven a fascinating topic according to the citation numbers.

Table 8.3 Distribution of Google Scholar citations (as of January 7, 2019)

Authors	Number of articles	Number of citations

8 Cybersecurity in Accounting Research

<p>Amir et al., 2018; Carré et al., 2018; Curtis et al., 2018; Ettredge et al., 2018; Gordon et al., 2018; Gyun & Vasarhelyi, 2017; Islam et al., 2018; Kahyaoglu & Caliyurt, 2018; Li et al., 2018; Rahimian et al., 2018; Smith et al., 2018; Stafford et al., 2018</p>			12	0–4
<p>Bose & Luo, 2014; Gansler & Lucyshyn, 2005; Gordon et al., 2016; Gordon et al., 2008; Higgs et al., 2016; Steinbart et al., 2018; Steinbart et al., 2016; Steinbart et al., 2013</p>			8	5–30

8 Cybersecurity in Accounting Research

<p>Abu-Musa, 2006; Gordon et al., 2015a; Gordon et al., 2015b; Hausken, 2007; Kwon et al., 2013; Pathak, 2005; Steinbart et al., 2012; Wallace et al., 2011; Wang et al., 2013</p>			<p>9</p> <p>30–90</p>
<p>Boritz & No, 2005; Ettredge & Richardson, 2003; Gordon et al., 2010; Gordon et al., 2006; Gordon et al., 2003; Gordon & Loeb, 2002; Hausken, 2006; Lainhart, 2000; Li et al., 2012; Tanaka et al., 2005</p>			<p>10</p> <p>90 →</p>

Source: Authors

Table 8.4 Ten most-cited articles in the field of cybersecurity (Google Scholar citations as of January 7, 2019)

8 Cybersecurity in Accounting Research

Authors	Citations and topics
Gordon and Loeb (2002) The economics of information-security investment	1258 (2)
Gordon et al. (2003) Sharing information on computer systems security: An economic analysis	304 (1)
Lainhart IV (2000) COBIT™: A methodology for managing and controlling information and Information Technology risks and vulnerabilities	141 (3)
Li et al. (2012) , The consequences of Information Technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports	135 (3)
Gordon et al. (2010) Market value of voluntary disclosures concerning information security	135 (4)

Gordon et al. (2006) The impact of the Sarbanes-Oxley Act on the corporate disclosures of information-security activities	133 (4)
Hausken (2006) Income, interdependence, and substitution effects affecting incentives for security investment	117 (2)
Tanaka et al. (2005) Vulnerability and information-security investment: An empirical analysis of E-local government in Japan	113 (2)
Boritz and No (2005) Security in XML-based financial reporting services on the Internet	112 (5)
Ettredge and Richardson (2003) Information transfer among internet firms: The case of hacker attacks	98 (5)

Source: Authors

Conclusions and Opportunities for Future Research

The growing dependence of both public and private firms on information technologies and networks for their financial management systems increases their vulnerability to cyber threats (e.g., [Gansler & Lucyshyn, 2005](#)). In addition, the economy has become more knowledge-based; therefore, protecting information assets has become a top agenda item for accountants and

managers ([Gordon et al., 2008](#)). Cybersecurity has thus increased, becoming one of the most significant risk management challenges facing every type of organisation within the space of just a few years. For instance, a decade ago, the IAF evolved and adapted to the increasingly important role that IT was playing in all aspects of business operations. Today, internal auditing faces the need to adapt once again to address the critical risks associated with cybersecurity (e.g., [IA, 2018](#)), and this study emphasises that cybersecurity has become more and more important for accounting and public policy. To avoid cyber threats, every organisation should implement a cybersecurity program or a cybersecurity strategy. This also applies to countries and jurisdictions, and hence it was argued that it is essential for countries to publish national cybersecurity strategies. Moreover, many countries frequently identify the state agencies in charge of setting minimum standards and responding to cyber incidents ([World Bank, 2018](#)). To conclude, this study aimed to provide an overview of the literature on what is currently known about cybersecurity in the accounting and auditing literature. While synthesising the literature, this chapter suggested a research framework that categorises the research themes related to cybersecurity. The following research themes were identified: cybersecurity and information sharing; cybersecurity investments; internal auditing and controls related to cybersecurity; disclosure of cybersecurity activities; and security threats and security breaches. Furthermore, this synthesis has practical and social implications. This synthesis underscores that information sharing is important and that companies and societies may benefit from it. However, the free-rider problem explains why firms are sometimes unwilling to engage in it ([Gordon et al., 2003](#); [Hausken, 2007](#)). Security breaches affect stock markets; therefore, the investment decisions related to cybersecurity should be made carefully and should utilise appropriate models to support the decisions. Finally, it should be noted that proactiveness matters while disclosing cybersecurity activities. For example, [Gordon et al. \(2010\)](#) indicated that voluntary disclosures related to proactive security measures have the greatest impact on the market value of a firm. In addition, [Wang et al. \(2013\)](#) suggested that firms taking proactive action have an incentive to disclose their stance on cybersecurity truthfully.

8 Cybersecurity in Accounting Research

While previous studies have examined cybersecurity under various research themes, research on the role of cybersecurity in private and public companies is still relatively scarce. However, this should not be interpreted as a sign of such research being less relevant. On the contrary, obtaining a sound understanding of the functioning and value of cybersecurity is of high importance, given the dominant and vital role that IT and digitalisation play in the world economy in terms of generating wealth, jobs, innovation, and growth. Hence, this synthesis highlights [Figure 8.2](#). as a mapping of the research discussed in the manuscript (left-hand-side themes) in relation to the research themes in other disciplines (right-hand-side themes). We encourage readers to use [Figure 8.2](#). as an instrument to identify possible interdisciplinary research avenues between accounting and other disciplines.

Furthermore, more research and research projects are needed to determine how to improve cybersecurity, for instance by establishing how the implementation of cybersecurity strategies and programs could be improved and, after implementation, how those programs should be maintained and developed. Future studies should also concentrate on how proactiveness could be enhanced in the context of security breaches. In addition, researchers should focus on how regulation affects the disclosure of cybersecurity-related issues and what kind of information firms and organisations disclose. The prior studies have been silent regarding how the awareness of cybersecurity investments could be improved, specifically among private firms. Most importantly, the role of cybersecurity in maintaining societal functionality should be examined carefully. In addition, the prior research has mainly concentrated on using data from the US, and future studies should focus on expanding the research, for instance to the European Union or Asia. For example, it would be interesting to know what kind of information investors are demanding about firms' cybersecurity practices. Given that investors hesitate to invest in firms with a history of cyber-attacks ([Islam et al., 2018](#)), future studies could address how investors' confidence could be maintained and/or restored. Research concerning the disclosure of cybersecurity information has been growing in recent years, and future studies should investigate how the validation of the disclosed information is performed and what role auditors perform in

cybersecurity risk management. Researchers could examine how the training and competence of auditors related to cybersecurity might be improved. Finally, future studies could utilise qualitative methods, as many of the research questions suggested above begin with a “how” term. Qualitative study techniques are the most appropriate for research on real-life practices where the purpose is to comprehend “how” and “why” (e.g., [Yapa, Ukwatte Jalathge, & Siriwardhane, 2017](#)). To conclude, this study encourages researchers to make use of these wide-ranging opportunities.

Notes

References

- Abu-Musa, A. A. (2006). Perceived security threats of computerized accounting information systems in the Egyptian banking industry. *Journal of Information Systems*, 20(1), 187–203.
- American Institute of Certified Public Accountants (AICPA). (2018a). *Cybersecurity risk management reporting fact sheet*. Retrieved November 13, 2018, from www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf
- American Institute of Certified Public Accountants (AICPA). (2018b). *SOC for cybersecurity: A background*. Retrieved November 13, 2018, from www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-background.pdf
- Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), 1177–1206.
- Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508–526.
- Boritz, J. E., & No, W. G. (2005). Security in XML-based financial reporting services on the Internet. *Journal of Accounting and Public Policy*, 24(1), 11–35.

- Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, 22(3), 194–208.
- Carré, J. R., Curtis, S. R., & Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*, 33(4), 436–446.
- Curtis, S., Carré, J., & Jones, D. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, 33(4), 425–435.
- Ettredge, M. L., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, 37(6), 564–585.
- Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: The case of Hacker attacks. *Journal of Information Systems*, Fall, 71–82.
- Gansler, J., & Lucyshyn, W. (2005). Improving the security of financial management systems: What are we to do? *Journal of Accounting and Public Policy*, 24, 1–9.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438–457.
- Gordon, L. A., & Loeb, M. P. (2006). *Managing cybersecurity resources: A cost – benefit analysis*. New York: McGraw Hill.
- Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6), 461–485.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5), 503–530.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34(5), 509–519.

- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). Externalities and the magnitude of cybersecurity underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, 6, 24–30.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, 9, 133–153.
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3), 567–594.
- Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C.-Y., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review*, 17(2), 215–241.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33–56.
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, 7, 49–59.
- Guffey, D., & Harp, N. (2017). The journal of management accounting research: A content and citation analysis of the first 25 years. *Journal of Management Accounting Research*, 29(3), 93–110.
- Gyun No, W., & Vasarhelyi, M. A. (2017). Cybersecurity and continuous assurance. *Journal of Emerging Technologies in Accounting*, 14(1), 1–12.
- Hausken, K. (2006). Income, interdependence, and substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy*, 25(6), 629–665.
- Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26, 639–688.
- Higgs, J. L., Pinsker, R., Smith, T., & Young, G. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, 30(3), 79–98.

- Institute of Internal Auditors (IIA). (2018). *The future of cybersecurity in internal audit*. A joint research report by the Internal Audit Foundation and Crowe Horwath. Retrieved June 15, 2018, from <https://bookstore.theiia.org/the-future-of-cybersecurity-in-internal-audit>
- Islam, M. S., Farah, N., & Stafford, T. S. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*, 33(4), 377–409.
- Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33(4), 360–376.
- Kenny, S. Y., & Larson, R. K. (2018). A review and analysis of advances in international accounting research. *Journal of International Accounting, Auditing and Taxation*, 30(1), 117–126.
- Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, 27(1), 219–236.
- Lainhart IV, J. W. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems*, 14(1), 21–25.
- Li, C., Peters, G. F., Richardson, V. J., & Watson, M. (2012). The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly*, 36(1), 179–203.
- Li, H., No, W., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information System*, 30, 40–55.
- Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: Undertaking a structured literature review in accounting. *Accounting, Auditing & Accountability Journal*, 29(5), 767–801.

- Pathak, J. (2005). Risk management, internal controls and organizational vulnerabilities. *Managerial Auditing Journal*, 20(6), 569–577.
- Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems*, 20, 38–64.
- Securities and Exchange Commission (SEC). (2018). *Commission statement and guidance on public company cybersecurity disclosures*. Retrieved November 13, 2018, from www.sec.gov/rules/interp/2018/33-10459.pdf
- Smith, T., Higgs, J. L., & Pinsker, R. (2018). Do auditors price breach risk in their audit fees? *Journal of Information Systems*, in press.
- Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216–229.
- Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training information security policy compliance. *Managerial Auditing Journal*, 33(4), 410–424.
- Steinbart, P. J., Raschke, R. L., Gal, G. F., & 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. L., Gal, G. F., & 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. L., Gal, G. F., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems*, 30(1), 71–92.
- Steinbart, P. J., Raschke, R. L., Gal, G. F., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, in press.

- Tanaka, H., Matsuura, K., & Sudoh, O. (2005). Vulnerability and information security investment: An empirical analysis of E-local government in Japan. *Journal of Accounting and Public Policy, 24*, 37–59.
- Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.
- Wallace, L., Lin, H., & Cefaratti, M. A. (2011). Information security and Sarbanes-Oxley compliance: An exploratory study. *Journal of Information Systems, 25*, 185–211.
- Wang, Y., Kannan, K., & Ulmer, J. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*(2), 201–218.
- Webster, J., & Watson, R. (2002). Analysing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii–xxiii.
- Weidenmier, M., & Ramamoorti, S. (2006). Research opportunities in information technology and internal auditing. *Journal of Information Systems, 20*(1), 205–219.
- The World Bank. (2018). *Financial sector's cybersecurity: Regulations and supervision*. Retrieved from <http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf>
- Yapa, P. W. S., Ukwatte Jalathge, S. L., & Siriwardhane, P. (2017). The professionalisation of auditing in less developed countries: The case of Sri Lanka. *Managerial Auditing Journal, 32*(4/5), 500–523.

1 This chapter was published in an earlier version as

© Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834.

Available here: www.emerald.com/insight/content/doi/10.1108/MAJ-09-2018-2004/full/html

Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) license.

2 The non IT-related security investment factors that were posited to influence a firm's performance are: policies and standards; risk assessment and management; security training/education/awareness; physical security; regulatory compliance; insurance for cyber security; and security personnel. The IT-related security investment factors are: network security; platform security; application security; mass storage security; file and data security; response to security attack/breach; and mobile security.