Accounting, Organizations and Society xxx (2018) 1–15

Contents lists available at ScienceDirect

Accounting, Organizations and Society

journal homepage: www.elsevier.com/locate/aos

The influence of a good relationship between the internal audit and information security functions on information security outcomes

Paul John Steinbart [a], Robyn L. Raschke [b], Graham Gal [c], William N. Dilla [d, *]

[a] Department of Information Systems, W.P. Carey School of Business Arizona State University, Tempe, AZ 85287, USA
[b] Department of Accounting, Lee Business School, University of Nevada—Las Vegas, Las Vegas, NV 89154, USA
[c] Department of Accounting, Isenberg School of Management, University of Massachusetts—Amherst, Amherst, MA 01003, USA
[d] Department of Accounting, Debbie and Jerry Ivy College of Business, Iowa State University, Ames, IA 50011, USA

ARTICLE INFO

Article history:
Received 21 July 2016
Received in revised form
19 December 2017
Accepted 30 April 2018
Available online xxx

Keywords:
Information security
Internal audit
IT audit
Governance
Risk management
Security metrics

ABSTRACT

Given the increasing financial impact of cybercrime, it has become critical for companies to manage information security risk. The practitioner literature has long argued that the internal audit function (IAF) can play an important role both in providing assurance with respect to information security and in generating insights about how to improve the organization's information security. Nevertheless, there is scant empirical evidence to support this belief. Using a unique data set, this study examines how the quality of the relationship between the internal audit and the information security functions affects objective measures of the overall effectiveness of an organization's information security efforts. The quality of this relationship has a positive effect on the number of reported internal control weaknesses and incidents of noncompliance, as well as on the numbers of security incidents detected, both before and after they caused material harm to the organization. In addition, we find 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.

1. Introduction

Cybercrime can have a significant, direct economic impact on organizations through asset misappropriation, theft of sensitive private information, disruption of online operations, and legal costs to settle consumer claims about harm (Hong, 2016; ISACA, 2016; Minaya, 2015; PWC, 2016a, 2016b). It can also have an indirect economic effect, given that the disclosure of information security risk factors, governance policies, and information security breaches can significantly impact firm value (Gordon, Loeb, & Sohail, 2010; Higgs, Pinsker, Smith, & Young, 2016; Wang, Kannan, & Ulmer, 2013). In addition, cybercrime poses "a different focal point of concern [and] a different 'subject' of risk", (Power, 2013, p. 538), because perpetrators are often unknown agents outside the organization. This is in contrast to asset theft and financial disclosure risks, where the focus is typically on the actions of identifiable individuals within the organization. Hence, it is not surprising that information security ranks as one of the top concerns for both accounting professionals (Drew, 2015; Hill, 2015) and senior management (Luftman & Ben-Zvi, 2010).

Who should be responsible for managing information security risks? The obvious answer would seem to be a dedicated group within the IT function. An ISACA (2011) report, however, suggests that information security risk management is the responsibility of not just a dedicated group within the information technology (IT) function, but also should involve other functions within organizations, including the internal audit function (IAF).

The problem of information security risk management therefore provides an important context for research on internal audit as a governance and risk management mechanism. Sarens (2009) argues "… the IAF can have a positive impact on the quality of risk management and internal control processes" (p. 4). Indeed, top management *expects* the IAF to compensate for the loss of control that comes through increased organizational complexity by both "providing independent assurance" and by "actively contributing to improving of processes and internal controls" (Sarens & De Beedle,

* Corresponding author.
E-mail addresses: paul.steinbart@asu.edu (P.J. Steinbart), robyn.raschke@unlv.edu (R.L. Raschke), gfgal@isenberg.umass.edu (G. Gal), wdilla@iastate.edu (W.N. Dilla).

https://doi.org/10.1016/j.aos.2018.04.005
0361-3682/

2006, p. 238). Similarly, the practice literature indicates that two of the most important responsibilities of the IAF are to provide assurance about process effectiveness and insights about how to improve performance (Seago, 2017). Despite this consensus among academics, managers, and internal audit professionals that an effective IAF should improve governance and risk management, there is little research that addresses whether the IAF actually does improve governance and risk management *outcomes* (Carcello, Hermanson, & Ye, 2011; Eden & Moriah, 1996; Gramling, Maletta, Schneider, & Church, 2004). Instead, prior research has tended to focus on respondents' perceptions of the efficacy of the IAF in improving risk management *processes*, without reporting objective data on the outcomes from these processes (e.g., Arena, Arnaboldi, & Azzone, 2010; Carcello, Eulerich, Masli, & Wood, 2017; de Zwaan, Stewart, & Subramaniam, 2011; Ma'ayan & Carmeli, 2016; Paape & Speklè, 2013).

This study addresses the aforementioned gap in the literature. We use a unique data set obtained through the cooperation of the Information Management and Technology Assurance (IMTA) section of the AICPA that provides objective measures of leading and lagging information security outcomes. The leading measures are the number of internal control weaknesses related to information security and the number of IT-related noncompliance issues that were material enough to be brought to the attention to executive management or the Board of Directors. It is important to detect and subsequently correct internal control weaknesses because they represent vulnerabilities that criminals can exploit. Similarly, employee noncompliance with security policies (e.g., sharing passwords, clicking on links in fraudulent emails, and failing to update security-related software) often contributes to security breaches. The lagging measures are the number of incidents stopped before causing material harm, and the number of security incidents that were detected only after they caused material harm. The number of incidents detected and stopped before causing material harm is a primary objective of an effective information security program. The number of security incidents discovered after causing harm is important because organizations cannot "stop the bleeding" and take steps to recover from an incident until they discover that they have been attacked. Indeed, organizations often do not become aware of significant information security breaches until long after the attack occurred (Ernst & Young, 2015; Lewis, 2013; Verizon, 2015). Therefore, timely detection of security breaches after they cause harm can still potentially mitigate the organization's losses.

We examine how the quality of the working relationship between the internal audit and information security functions influences these four measures of information security outcomes. We focus on the quality of the working relationship between the internal audit and information security functions because relationships between the IAF and other business functions are important determinants of audit quality and the IAF's ability to add value to organizations (Havelka & Merhout, 2013; Merhout & Havelka, 2008; Stoel, Havelka, & Merhout, 2012).

Our results show that a higher-quality relationship between the internal audit and information security functions results in a greater number of reported internal control weaknesses and noncompliance incidents. We also find that the quality of the relationship between internal audit and information security has a positive effect on the number of security incidents detected, both before and after causing material harm to the organization. Furthermore, we find that the level of top management support for security improves the quality of the relationship between internal audit and information security. It also reduces the number of both security-related internal control weaknesses and compliance issues, but does not affect the number of incidents detected, either before or after causing harm to the organization. Finally, while independence of the information security function from the CIO improves the quality of the relationship between internal audit and information security, it does not affect any of the four security-related outcomes.

This study makes three primary contributions. First, it investigates the effectiveness of internal audit as a governance and risk management mechanism and informs practice regarding the influence of relationships between internal auditors and managers on internal audit's effectiveness. In particular, we provide empirical evidence to support Havelka and Merhout's (2013) propositions concerning the importance of a good working relationship between the IAF and other functions. Second, the study makes a contribution to the risk management literature by examining the influence of governance mechanisms on specific *actual outcomes*, rather than perceptions of such effects. Third, we show how the level of top management support for security and the independence of the information security function from the CIO affect the quality of the relationship between internal audit and information security and influences information security outcomes.

2. Background

The IAF should play an active role in information security governance and enterprise risk management efforts with respect to information security (Arena et al., 2010; Busco, Giovannoni, Riccaboni, Frigo, & Scapens, 2006; Havelka & Merhout, 2013; Héroux & Fortin, 2013; Merhout & Havelka, 2008; Stoel et al., 2012). According to COBIT5 (ISACA, 2012a), the regular monitoring of performance (Process MEA01) and independent auditing of security (Process MEA02) are an important part of these governance efforts. The IAF, however, is only one potential assurance provider in this area (Institute of Internal Auditors, 2013a). Regular monitoring and reviewing activities (e.g., analyzing computer logs) performed by the information systems function itself also improve the effectiveness of information security controls (Ransbotham & Mitra, 2009). Certainly, self-monitoring is useful, and indeed, "line management … provides assurance as a first line of defense over the risks and controls for which they are responsible" (Institute of Internal Auditors, 2013a, para 4). Yet, there is considerable evidence that people have great difficulty in identifying and in correcting errors in systems that they created themselves (Panko & Sprague, 1998; Panko, 1999; Powell, Baker, & Lawson, 2008; Ricketts, 1990; Teo & Tan, 1999). The presumed value of internal audit review is that the IAF maintains a greater degree of independence from information security activities than personnel within the IT function (Institute of Internal Auditors, 2013a). This independence enables the IAF to provide honest feedback about the effectiveness of existing controls (Merhout & Havelka, 2008; Stoel et al., 2012).

Both the information security and internal audit professions believe that the two functions play an important role in regards to managing information security risks (Center for Internet Security, 2015; Flora & Raj, 2015). Information security executives believe that both formal involvement of the internal audit function and informal coordination between the internal audit and information security functions are essential for the deployment of an effective information security strategy (Kayworth & Whitten, 2010). In addition, IT and security managers perceive that effective dialogue with auditors aids in the discovery of security vulnerabilities and in the design of recommendations for security improvements (Werlinger, Hawkey, Botta, & Beznosov, 2009). Furthermore, IT audit professionals believe that audits can potentially provide useful insights and recommendations for improving the effectiveness and efficiency of an organization's information security efforts

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

(Khan, 2016; Merhout & Havelka, 2008; Stoel et al., 2012). They also believe that the relationship between IT auditors and IT professionals is important to the success of the IAF in providing these insights (Havelka & Merhout, 2013; Merhout & Havelka, 2008; Stoel et al., 2012).

However, in many organizations, the relationships among the various functional groups involved in information security are less than ideal. Internal auditors often experience conflict and even adversarial relationships with other organizational functions (Ahmad & Taylor, 2009; Dittenhofer, Ramamoorti, Ziegenfuss, & Evans, 2010; Roussy, 2015; Van Peursem, 2005). Similarly, security professionals report experiencing conflict with the rest of the IT function and the CIO (ThreatTrack, 2016). Thus, it is not surprising that the relationship between the internal audit and information security functions is sometimes characterized by conflict and distrust (Steinbart, Raschke, Gal, & Dilla, 2012).

Indeed, all too often, instead of coordinating their information security efforts, the various functions operate independently of one another. It is up to senior management to mitigate these problems:

> The problem is politics; the solution is a culture of security … The most useful contribution senior management can make to a security culture, aside from intentionally championing its existence, is to ensure that all those with converging security responsibilities reinforce one another rather than needlessly, heedlessly fighting for their own "turf" at the expense of one another and the detriment of the security cultures in their enterprises (ISACA, 2011, p. 104).

Turf battles that impede multiple functions from sharing responsibility for information security perhaps represent only the most extreme of possible dysfunctional outcomes. Another possibility is that the various responsible parties will develop "silo" mentalities, and thus fail to cooperate and to coordinate their efforts (Arena et al., 2010). In either case, an effective IT governance structure is important to overcome those potential impediments to effective information security risk management (Love, Reinhard, Schwab, & Spafford, 2010). This governance structure consists of the Board of Directors, who provides oversight over information security, executive management, who provides leadership in the management of information security risks, managers, who have responsibility for implementing and monitoring information security controls, and internal auditors, who provide independent evaluations of information security risk management.

Consequently, the central focus of our research model, shown in Fig. 1, is the impact of the quality of the relationship between the IAF and the information security function on the effectiveness of an organization's information security efforts. The model includes two additional factors related to the efficacy of an organization's information security governance: (1) top management's support for and interest in information security issues, and (2) whether the CISO reports to someone independent of the information security function. These factors are predicted to not only affect information security outcomes, but also to affect the relationship between the internal audit and information security functions. The next section discusses each component of the research model in more detail.

3. Hypotheses

3.1. Influence of relationship between internal audit and information security functions on security outcomes

Havelka and Merhout (2013) develop a comprehensive model of the factors that influence audit quality, based on an extensive literature review and detailed interviews with internal IT auditors. One key component of their model is how the nature of the relationship between the IAF and other business units (part of what they refer to as the *enterprise environment*), and with the auditee in particular (which they refer to as the client's *audit posture*), affect audit quality, specifically the IAF's ability to provide advice that might improve operations. Havelka and Merhout (2013) argue that good working relationships between the IAF and other parts of the organization improve both audit efficiency and effectiveness because they improve the auditor's access to evidence and also increase the business unit's honesty and openness in communications with the IAF. Their arguments are consistent with earlier statements in the professional literature that a good working relationship with the auditee improves the auditor's access to evidence, especially "soft" evidence with respect to attitudes and behaviors (Dittenhofer, 1997).

Empirical research is consistent with those assertions. For example, one of Steinbart et al.'s (2012) respondents states that "… [in] a lot of places that I've seen and been, it's been a game of cat and mouse. The auditors are trying to catch IT doing something, IT is trying to prevent audit from finding out (p. 235)." The respondent also states that when internal audit and the information security function cooperate, they work together to identify risk, to reduce risk, and to fix problems that are identified. Consistent with this observation, Fanning and Piercey (2014) find that the internal auditor's interpersonal likability increases managers' receptivity to well-structured internal audit recommendations. In contrast, Roussy (2015) finds that internal auditors who experience role conflict with auditees engage in coping behaviors that compromise the auditors' independence. This in turn negatively impacts the ability of the auditor to successfully execute the audit engagement and to identify, develop, and communicate audit findings.

Thus, a good working relationship between the internal audit and the information security functions should facilitate the IAF's ability to identify security issues and suggest ways to address them. We refer to this as the *collaborative detection* effect. However, it is not the only positive outcome associated with a good working relationship between the two functions.

A second potential benefit from a good working relationship between the internal audit and information security functions is that it can lead to *knowledge transfer*, wherein the information security function uses advice from the IAF to improve the design and functioning of security controls. Havelka and Merhout (2013, p. 178) allude to this when they note, "it would be reasonable to assume that based on the results of an IT audit a system or process would be improved or changed." For example, Steinbart et al. (2012) report a situation where an internal auditor's ability to view security issues from a business process perspective influenced the information security manager's understanding of how to achieve effective segregation of duties. Dialogue between the security manager and the internal auditor helped improve the security manager's understanding of this issue and resulted in improved controls over access rights and permissions. Indeed, there is empirical evidence that cooperation between the IAF and the management of the audited process improves the quality of risk management processes (Arena et al., 2010), increases the likelihood that managers will accept and act upon audit recommendations (Arena & Azzone, 2009), and indirectly improves unit efficiency by facilitating auditees' learning from audits (Ma'ayan & Carmeli, 2016).

Knowledge transfer is more likely to occur when different units within the same organization perceive themselves as having a common set of values or sharing the same focus or purpose (Morris & Empson, 1998). In such cases, the recipient unit is willing to expend more time and effort in evaluating the merits of knowledge possessed by the other unit. For example, Bauer and Estep (2016) found that audit effectiveness improved when there was a good

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

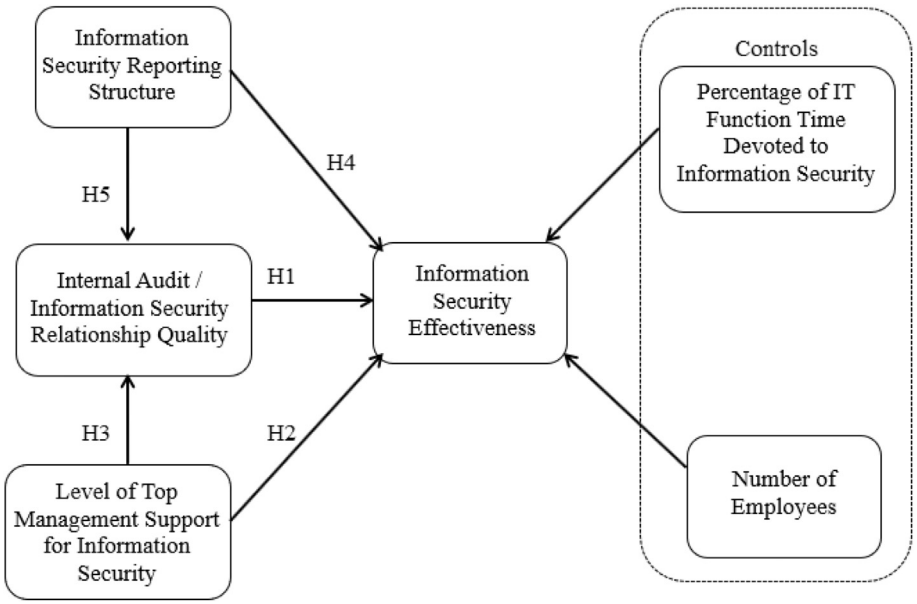

Fig. 1. Research model.

relationship between the financial and IT auditors in Big Four firms, because the sharing of knowledge resulted in more timely detection and resolution of audit issues.

However, groups do not automatically perceive a common purpose just because they have a formal relationship with one another. Arena et al. (2010) report variability across organizations in the degree to which internal audit and risk management functions cooperate with each other, and Steinbart et al. (2012) report variability across organizations in the degree to which internal audit and information security have a cooperative working relationship with one another. Similarly, Bauer and Estep (2016) also found variability across firms in the quality of the relationship between the financial and IT auditors. Therefore, it is reasonable to expect that the quality of relationships between the internal audit and the information security functions will vary from organization to organization and that those differences will be reflected in various measures of security outcomes.

The preceding discussion suggests that a good working relationship between the internal audit and information security functions can improve information security outcomes because greater cooperation and openness between the two functions enables the IAF to generate more and better recommendations (the collaborative detection effect). In addition, a good working relationship enables the information security function to have a better understanding of the reasoning behind the IAF's recommendations, therefore increasing the likelihood that the information security function will act on these recommendations (the knowledge transfer effect). However, the timing of the collaborative detection and knowledge transfer effects on leading and lagging measures of information security effectiveness is likely to differ.

The effects of collaborative detection can arise almost immediately, because the information security function will allow the IAF to have access to more and better information about existing processes and controls. Thus, the collaborative detection aspects of a better working relationship between the internal audit and information security functions may increase the number of security-related internal control weaknesses and noncompliance incidents that are detected and reported. This prediction is consistent with the finding by Lin, Pizzini, Vargus, and Bardhan (2011) that publicly traded firms are *more* likely to report material internal control weaknesses when the IAF coordinates audit activities with the external auditors.

On the other hand, the knowledge transfer effect suggests that the detection of leading indicators will decline over time, as organizations take steps to resolve previously identified issues. However, the benefits of any improvements in the design and the operation of security controls due to knowledge transfer may likely require additional time before being reflected in fewer security-related internal control weaknesses. Similarly, it will likely take time, and the enforcement of sanctions by management, before increased success in detecting employee noncompliance with security policies results in greater adherence to those policies.

Thus, at any given point in time it is not clear whether the collaborative detection or knowledge transfer effects will prevail. Therefore, we state the following non-directional hypothesis concerning the effects of relationship quality on leading measures of information security effectiveness:

H1a: The quality of the relationship between the internal audit and information security functions will influence leading indicators of an organization's information security effectiveness (i.e., number of security-related internal control weaknesses reported to the Board of Directors and number of incidents of employee noncompliance with IT policies).

In contrast to the preceding discussion, both the collaborative detection and knowledge transfer effects clearly predict that a better working relationship between the internal audit and information security functions will increase the number of attacks detected and stopped prior to causing material harm. The collaborative detection effect suggests that this will happen because a better working relationship increases the detection and reporting of security-related internal control weaknesses and noncompliance incidents, thereby enabling those vulnerabilities to be addressed. Fewer vulnerabilities means less opportunity for attacks to succeed. Similarly, the knowledge transfer effect suggests that a positive relationship between the internal audit and information security functions will result in improved design and operation of controls. Better controls means that more attacks are detected and stopped before they can cause material harm. Therefore, we posit the following directional hypothesis:

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

H1b: The quality of the relationship between the internal audit and information security functions will increase the number of attacks that are detected and stopped before causing material harm to the organization.

At first consideration, the collaborative detection and knowledge transfer effects appear to suggest that a quality relationship between the internal audit and information security functions should also reduce the number of attacks that are not detected until after causing material harm. As discussed above, improved detective capabilities should enable organizations to detect and stop attacks before they can succeed in causing material harm. In addition, over time, the improved design and operation of controls achieved through knowledge transfer should result in fewer vulnerabilities that can be exploited to conduct successful attacks.

However, the logic of the preceding arguments is contingent upon a stable base rate of attacks using known methods. That assumption is problematic; indeed, it is likely that the base rate of attacks is increasing, due in part to the increased number of opportunities associated with the continuous growth in connectivity, particularly that involving the Internet of Things (IoT), and also because continuous changes to IT infrastructure constantly create new potential avenues for attack (ISACA, 2016). Furthermore, new "zero-day" attacks (Tanaka & Goto, 2014) that take advantage of previously unknown software vulnerabilities to successfully bypass current defensive measures are constantly surfacing. Thus, a better working relationship between the internal audit and information security functions may not necessarily prevent attacks that use these new methods and vulnerabilities from succeeding. However, it should enable more timely detection, albeit only after the attack causes harm. Indeed, such belated discovery may still be beneficial if it helps organizations to "stop the bleeding" more quickly.

These competing possibilities suggest that a quality relationship between the internal audit and information security functions could either decrease or increase the number of information security incidents that are detected after causing harm. Therefore, we state the following non-directional hypothesis:

H1c: The quality of the relationship between the internal audit and information security functions will influence the number of attacks that are detected only after causing material harm.

3.2. Importance of top management support

Internal control frameworks (e.g., COSO, COSO-ERM, and COBIT5) stress the importance of the role senior management plays in effective governance. For example, IT internal control guidance recommends that senior management must "foster an information security-positive culture and environment" (ISACA, 2012b, Process EDM01.02, activity 6). To accomplish that objective, senior management should "promote the information security function within the enterprise" (ISACA, 2012b, Process APO02.06, activity 3), "proactively" support and communicate the importance of information security (ISACA, 2012b, Enabling Behavior 6), and create a culture of information security (Ross, 2011). Consistent with this normative guidance, the internal audit and the information security professions have long argued that top management support and involvement is important with respect to information security (Center for Internet Security, 2015; Flora & Raj, 2015; IT Governance Institute, 2008; Kayworth & Whitten, 2010; Khan, 2016).

Given the lack of directly observable measures of top management support, there is no direct evidence of an association between top management support and information security outcomes. One indirect indicator for top management support, however, is the level at which IT governance issues are addressed in the organization. Kwon, Ulmer, and Wang (2013) find that firms that include an IT executive as part of the top management team are less likely to report information security breaches. They also find a negative association between IT executives' compensation and the likelihood of an information security breach. Higgs et al. (2016) find that disclosures of security breaches are inversely related to the length of time that a company's Board of Directors has had a technology committee. Thus, both of these studies provide support for an association between top management involvement and improved information security outcomes.

A second indicator of top management support is the presence and nature of information security-related disclosures in a firm's annual report. Li (2015) finds a positive association between Chinese firms' disclosure of security-related content in their annual reports and the quality of their online security procedures. Wang et al. (2013) find that firms who report that they are proactively taking steps to manage cyber risks are less likely to have disclosed security breaches than firms who do not report they are actively mitigating cyber risks.

Thus, there is evidence that the active involvement of senior management in addressing security issues improves an organization's overall security. Such improvement should be reflected in both leading and lagging measures of security effectiveness. This leads to our second set of hypotheses:

H2a: A higher level of top management support for information security will improve leading indicators of an organization's information security effectiveness (i.e., reduce the number of security-related internal control weaknesses reported to the Board of Directors and number of incidents of employee noncompliance with IT policies).

H2b: A higher level of top management support for information security will improve lagging measures of the effectiveness of an organization's information security efforts (i.e., increase the number of attacks that are detected and stopped before causing material harm to the organization and decrease the number of attacks that are detected only after causing material harm).

The level of top management support for information security might also have a positive influence on the relationship between the internal audit and information security functions. The first way that this might occur is through top management directly encouraging a collaborative relationship between internal audit and information security. For example, Sarens and De Beedle (2006) find that in organizations where top management places a priority on managing risk and improving internal controls, management works to foster the acceptance and appreciation of the IAF. Similarly, Arena, et al. (2010) report that in an organization where top management strongly supported enterprise risk management (ERM) activities, the internal audit department and Chief Risk Officer worked together on ERM. On the other hand, in another organization where top management viewed ERM as a compliance exercise, the internal audit department struggled to cooperate with managers who were directly responsible for ERM. Consistent with these findings, an internal auditor from one of Steinbart et al.'s (2012) respondent organizations stated, "Our chief auditor and our senior vice president of IT are very much in that partnering mode, they really feel that [between] audit and IT, there should be a partnership, and it should not be adversarial (p. 237)." Similarly, the information systems security manager at the same organization explained:

> The senior executives identify that, they embrace it. They get along well. I don't see any conflict or territory battles or any of that here … That's the most important thing from the

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

> workforce point of view. When they see that demonstrated up high, that's how they follow suit. They watch this, and then they know that's the expectation and it's pretty effortless here. People partner and just get along well with the same goal in mind. It shows (Steinbart et al., 2012, p. 237).

Top management support for information security can also have an indirect influence on the relationship between the internal audit and information security functions by encouraging and enabling increased audit attention to information security issues. Even though the chief audit executive (CAE) is independent of management, internal auditing standards indicate that the CAE must consider senior management input on risks faced by the organization when planning internal audit activities (Institute of Internal Auditors, 2013b). Indeed, the information security managers interviewed by Steinbart et al. (2012) perceived that the level of internal audit resources devoted to information security depends on top management's interest in this area. Top management's provision of those resources is important, given that information security personnel perceive that the IAF's level of information security knowledge and the frequency with which the IAF reviews information security have a positive impact on the quality of the relationship between the two functions (Steinbart, Raschke, Gal, & Dilla, 2013).

Consistent with these findings, Ma'ayan and Carmeli (2016) also report a positive relationship between top management's support of the internal audit function and the quality of auditor/auditee relationships. Finally, greater top management support for information security and its importance as an overarching organizational objective is likely to increase the perceptions of the internal audit and information security functions that they share a common goal, which, in turn, should improve relationships between these organizational units (Kane, 2010). The preceding discussion leads to our third hypothesis:

H3: A higher level of top management support for information security improves the relationship between the internal audit and information security functions.

3.3. Importance of reporting structure for information security

The professional literature stresses that it is important to assign responsibility for information security to an individual at an appropriate level of management (ISACA, 2012b, Process EDM01.02, activity 2). A common title for such a position is Chief Information Security Officer (CISO). Organizations which have a CISO have more confidence in dealing with malware incidents in a timely manner, are more willing to extend assurances to customers about the safety of their data, and are twice as likely to have incident response teams, compared to organizations which do not have a CISO (ThreatTrack, 2016).

In addition to the *existence* of a CISO position in an organization, the reporting level and authority of the CISO is also important (PWC, 2016b). Ideally, the CISO should *not* report to the CIO because:

> … [there is an] inherent conflict of interest. Information security, due to its efforts to ensure security, is often perceived as a constraint on IT operations. CIOs and their IT departments are usually under pressure to increase performance and cut costs. Information security is often the victim of these pressures. Finally, it must be considered that for information security to be effective, it must be more closely aligned with business than with technology. (IT Governance Institute, 2008, p. 19).

The argument for having the CISO report to an independent party outside IT is similar to the arguments that the IAF should not report to management, because of the potential for conflict of interest (ISACA, 2012b). Information security is not just a technical issue to be delegated to the IT function, rather, cyber threats must be included as part of an organization's comprehensive risk management process. This objective is more likely to be accomplished if the CISO reports to the CEO, or to a chief risk officer, an individual who has overall responsibility for managing risk at the executive level (ISACA, 2012b; PWC, 2016b). An independent CISO should be able to deploy resources to more effectively manage both leading and lagging indicators of information security effectiveness. For example, Arena et al. (2010, p. 666) describe an organization where the:

> relevance of the SD (Security Department) is further legitimated by its direct relationships with the CEO and the Executive Committee … and the SD head negotiates directly with the Executive Committee on the budget for security costs and investments.

This leads to the following hypotheses:

H4a: Organizations in which the CISO reports to someone outside the IT function will have more effective leading measures of information security effectiveness (i.e., fewer security-related internal control weaknesses reported to the Board of Directors and fewer incidents of employee noncompliance with IT policies) than organizations in which the CISO reports to an individual inside the IT function.

H4b: Organizations in which the CISO reports to someone outside the IT function will have more effective lagging measures of information security effectiveness (i.e., a greater number of attacks that are detected and stopped before causing material harm to the organization and fewer attacks that are detected only after causing material harm) than organizations in which the CISO reports to an individual inside the IT function.

In addition, the reporting structure for the CISO may impact the way in which the IAF and information security groups interact. San Miguel and Govindarajan (1984) found that in organizations where controllers had independent reporting relationships (i.e., to someone other than the divisional general manager), internal auditors tended to focus more on efficiency and effectiveness auditing and less on compliance auditing, compared to organizations where the controllers were not independent. This suggests that in the context of information security, internal auditors might focus more on process improvements and less on compliance in organizations where the CISO has an independent relationship with senior management, rather than reporting to the CIO. Steinbart et al. (2012; 2015) find that when information security audits focus less on compliance and more on process improvements, a better working relationship between internal audit and information security exists. Therefore, having the CISO report independently of the IT function may also improve the quality of the relationship between the internal audit and information security functions. This leads to the following hypothesis:

H5: The relationship between the internal audit and information security functions will be better in organizations in which the head of information security reports to someone outside IT compared to organizations where information security reports to the CIO.

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

3.4. Control variables

Fig. 1 includes three other factors that are likely to influence the overall effectiveness of an organization's information security efforts. The first is the level of effort that the organization invests in information security. Increasing the effort devoted to information security should improve security outcomes (Ransbotham & Mitra, 2009). We use percentage of IT staff time devoted to information security as our measurement of effort. The second is the size of the organization. A recent ISACA (2016) survey of the state of cybersecurity reports that the three most common methods used in successful attacks are phishing, malware, and social engineering. The risk of such threats is directly related to the number of employees. Therefore, we use number of employees to measure size. The final control variable included in our model is whether or not the IAF is outsourced. Prawitt, Smith, and Wood (2009) argue that outsourcing the IAF may improve the quality of IT-related controls, especially in smaller firms, where it may be difficult to hire and retain specialized IT audit staff. On the other hand, Steinbart et al. (2012) report that outsourcing the IAF reduces informal communication between internal auditors and the information security function, which in turn may have a negative impact on information security outcomes. Therefore, we include whether IAF is outsourced as a control variable, but do not predict the direction of its effect on security outcomes.

4. Research method

4.1. Procedure

We conducted a web-based survey of IT auditors that were members of the IMTA section of the AICPA. The survey (see Appendix A) was part of a larger study that contained additional questions not related to the research questions explored in this study. The IMTA section's executive committee sent an email message to its members encouraging their participation in the study. Potential participants were informed that there would be a raffle to award an iPad mini to one randomly selected participant who completed the entire survey. A follow-up invitation was sent out two weeks after the initial email.

4.2. Independent and control variables

Relationship quality and top management support were both treated as reflective latent constructs. We used four questions that had been previously validated by Steinbart et al. (2013) to measure the quality of the relationship between the IAF and information security functions. We also used five questions that had been previously validated by Steinbart et al. (2013) to measure top management support. Responses to each question were on a five-point Likert scale that ranged from strongly disagree to strongly agree. Higher scores represent a better relationship and greater top management support.

To assess the organizational structure of the information security function, we asked respondents to indicate the title of the person to whom the individual with primary responsibility for information security reported. We created a dichotomous variable that was coded 0 if the security function reported to the CIO or another person in IT and 1 otherwise.

We assessed the level of effort invested in information security by asking respondents to indicate the percentage of the total IT time budget that was devoted to information security activities. The seven response choices represented ranges of effort in increments of 5%, beginning with 0%–5% and concluding with 30% or more. We coded the responses as an ordinal variable that ranged from 1 to 7. We measured size by asking respondents one question about the total number of employees at the organization. The seven response choices each represented a size range, beginning with less than 20 and concluding with more than 10,000. As with level of effort, we coded size as an ordinal measure that ranged from 1 to 7. We also asked respondents whether the organization's IAF activities were performed primarily in-house (i.e., 70 percent or more) or were outsourced.

4.3. Dependent variables

We collected four measures to capture different aspects of the effectiveness of an organization's information security program for the past three years. Two of the measures are leading indicators of the likelihood of future security incidents: (1) the number of internal control weaknesses related to information security and (2) the number of issues of employee non-compliance with IT policies. Both measures represent vulnerabilities that might lead to future exploits. We asked respondents to report the number of times both issues were serious enough to warrant being brought to the attention of executive management or the Board of Directors. Thus, both leading indicators reflect potentially serious problems, rather than trivial infractions.

Our other two measures are lagging indicators of information security effectiveness: (1) the number of security incidents that were detected and stopped before they caused a material financial loss, interruption of operations, or reputation problem, and (2) the number of incidents that were detected after causing material harm. The first of these measures is important, as the ultimate objective of information security is to prevent or at least detect and stop incidents before they cause material harm. Since it is not possible to prevent all incidents (Ross, 2015), we also include a measure of information security's ability to timely detect and stop incidents, so as to limit damage.

We used the same seven-point response scale for all four measures of information security program outcomes. The choices were zero, one, two, three, four, 5–10, and more than 10. Responses for all three years were combined to form a single reflective construct for each outcome.

5. Results

5.1. Demographics and descriptive statistics

Respondents who indicated that they were internal auditors or worked in some other functional role were asked to answer the survey questions for the organization that employed them. They were also asked to assign a letter grade (e.g., “A”, “B”, “C”, “D”, or “F”) to represent their assessment of the effectiveness of their employer's information security program. To ensure that we obtained information from a broad cross-section of organizations, respondents who identified themselves as being either external auditors or consultants were randomly assigned to two groups: one-half were asked to answer the survey questions for a client that would merit receiving a high grade (i.e., “A” or “B”) for information security effectiveness, and the other half were asked to answer the survey questions for a client for which they would assign a low grade (i.e., “C”, “D”, or “F”) for information security effectiveness.

Of the 190 IMTA section members who responded to the email invitation to participate in the study, 110 provided responses to all four outcome measures. To test for non-response bias, we compared responses from the 58 participants who responded the first day the survey was open to those of 19 who responded when a reminder was sent out two weeks after the survey launch date. None of the values for the study's variables differed significantly

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

($p > 0.10$) across these two groups.

Of the 110 individuals who completed the survey, 19 indicated that there was no IAF in their organization (either in-house or outsourced). Therefore, these respondents could not provide data about the relationship between the IAF and the information security function. Further inspection of the data revealed that another 14 respondents failed to answer all of the questions about the nature of the relationship between the internal audit and information security functions. Therefore, responses from 77 organizations are available to test our hypotheses.[1]

Table 1 provides demographic information about our sample. The majority of the respondents who provided usable responses were male, possessed the IMTA section's CITP certification (in addition to being a CPA or CA), and had more than 20 years of work experience. Our sample represents a wide cross-section of industries and includes considerable variation in organization size.

5.2. Model tests

Table 2 presents descriptive statistics for the variables used in our subsequent data analyses. Table 3 shows that our latent constructs are reliably measured.

We analyze the data using PLS, opposed to a covariance-based SEM technique for three reasons (Fayard, Lee, Leitch, & Kettinger, 2012; Hair, Ringle, & Sarstedt, 2011). First, we have a relatively small sample size. Second, PLS is less sensitive than covariance-based SEM techniques to deviations from normality. Finally, our main objective in this study is to assess whether internal audit/information security function relationships predict organizations' security outcomes, rather than confirm structural relationships. We used the WarpPLS v. 5.0 program to conduct our analyses (Kock, 2015).

We performed a test of lateral collinearity on the constructs to test for common method bias (Kock & Lynn, 2012). This test compares the full collinearity of all latent constructs. All variance inflation factors (VIFs) are below the recommended threshold of 3.3, indicating that the threat of lateral collinearity does not exist in the data.

5.3. Hypotheses test results

We first ran the model depicted in Fig. 1 separately for each of our four dependent measures. The path from internal audit outsourcing to security outcomes was not significant ($p > 0.10$) for any of the four outcome measures, therefore, we dropped internal audit outsourcing as a control variable and ran the models again.[2] Results from these analyses are reported below.

H1a predicts that a good relationship between the internal audit and information security functions (RELQLTY) will influence leading indicators of information security effectiveness. As shown in Fig. 2 and Table 4, the path coefficient from RELQLTY to both of the leading indicators is positive and significant. A positive relationship between the internal audit and information security functions increases the number of material internal control weaknesses related to information security ($b = 0.210$, $p = 0.027$) and the number of reported IT-related noncompliance issues ($b = 0.183$, $p = 0.047$). H1b predicts that a good relationship between the internal audit and information security functions will increase the number of attacks that are detected and stopped before they cause material harm. H1c predicts that the nature of the relationship between the internal audit and information security functions will be associated with the number of attacks that are detected after they cause material harm. Fig. 3 and Table 4 show that a positive relationship between the internal audit and information security functions increases the number of attacks detected and stopped before they could cause material harm ($b = 0.166$, $p = 0.064$) and the number of detected harmful incidents ($b = 0.161$, $p = 0.071$). Thus, the results are consistent with both H1b and H1c.

H2a (H2b) predicts that top management support will improve leading (lagging) measures of information security effectiveness. Fig. 2 and Table 4 show that top management support reduces the number of internal control weaknesses that are related to security ($b = -0.189$; $p < 0.042$) and the number of noncompliance issues ($b = -0.212$; $p < 0.025$). However, Fig. 3 and Table 4 show that top management support does not affect the number of incidents that were detected, either before ($b = 0.099$; $p = 0.186$) or after ($b = 0.027$; $p = 0.406$) causing harm. Thus, the results support H2a, but not H2b.

H3 predicts that top management support should improve the quality of the relationship between the internal audit and information security functions. As shown in Figs. 2 and 3 and Table 4, a higher level of top management support improves the quality of the relationship between the two functions ($b = 0.522$; $p < 0.001$). Thus, H3 is supported.

H4a (H4b) predicts that when the CISO reports to someone outside of the IT function, leading (lagging) measures of information security will improve. Figs. 2 and 3 and Table 4 show that the reporting relationship of the CISO does not affect any of the four outcome measures (all $p > 0.10$). Thus, H4a and H4b are not supported.

H5 predicts that the relationship between the internal audit and information security functions will be better when the CISO reports to someone outside the IT function. Figs. 2 and 3 and Table 4 show that CISO reporting outside the IT department improves the quality of the relationship between the two functions ($b = 0.300$; $p = 0.002$). Thus, H5 is supported.

Figs. 2 and 3 and Table 4 also show that the control variables influenced the effectiveness of an organization's information security efforts. Increasing the proportion of time that the IT function devotes to information security increases the number of incidents that were detected and stopped before causing harm ($b = 0.238$; $p = 0.014$) and reduces the number of incidents that caused material harm ($b = -0.217$; $p = 0.023$). The proportion of time that the IT function devotes to information security has no effect on either the number of issues of employee noncompliance with policies or the number of internal control weaknesses related to information security ($p > 0.10$ for both). As expected, the number of employees is positively related to all the outcome measures ($p < 0.01$ for all measures), indicating that larger organizations are more likely to have more security-related internal control weaknesses, more issues of employee noncompliance with policy, and more incidents and attacks.

6. Summary and discussion

The escalating rate of cybersecurity incidents and the magnitude of associated fiscal and reputational impact is driving organizations to pay increased attention to cybersecurity risk (ISACA, 2016). This study makes a significant contribution to the literature by providing evidence that the quality of the relationship between internal auditors and managers responsible for information security improves information security effectiveness. In doing so, it

[1] In addition, six participants provided incomplete responses to the measures of top management support. Two answered only three out of the five questions and four subjects answered four of the questions. We used each participant's mean responses to the questions that they did complete to infer values for the missing responses.

[2] Hypothesis test results are substantively equivalent for analysis models that include internal audit outsourcing as a control variable.

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

Table 1
Descriptive statistics.

Panel A: Respondent Demographics	
Employment Role	
Public Accounting	27
Consultant	12
Internal Auditing	11
Other	27
Internal Audit Outsourcing	
No	57
Yes	20
Gender	
Male	62
Female	15
Certifications Possessed	
CPA/CA	73
CISA	13
CISM	2
CIA	9
CISSP	5
CRISC	4
CITP	47
Other	19
None	3
Work Experience	
<5 years	4
6–10 years	10
11–15 years	9
16–20 years	6
>20 years	48
Panel B: Organization Demographics	
Industry	
Government	6
Mining and Construction	3
Manufacturing	14
Technology	5
Financial Services	12
Healthcare, Education, and Other Professional Services	15
Other	22
Size (number of employees)	
< 20	11
20–99	15
100–499	13
500–999	12
1000–4999	12
5000–9999	4
over 10,000	10
Internal Audit Employees	
1–5	23
6–10	9
11–20	10
21–50	4
>50	3
Don't know	8
Missing	20
Internal Audit Assigned to IT Audit	
0	5
1–5	37
6–10	1
11–20	3
21–50	1
Don't know	10
Missing	20
Number of Employees in IT	
1–10	33
11–25	11
26–50	5
51–100	8
>100	10
Don't Know	10
Number of Employees in IT dedicated to Information Security	
0	3
1–5	45
6–10	9
11–20	6
21–50	1
>50	1
Don't Know	12
Total Assets	
Zero to $10 Million	23
>$10 million to $50 million	5
>$50 million to $250 million	13
>$250 million to $500 million	7
>$500 million to $1 billion	9
>$1 billion to $50 billion	12
>$50 billion to $200 billion	3
>$200 billion to $500 billion	1
>$500 billion to $1trillion	1
more than $1 trillion	3

answers Gramling et al.'s (2004) call for research into how the IAF contributes to the overall effectiveness of governance. It also extends recent research on the association between internal audit working relationships and audit effectiveness (Ma'ayan & Carmeli, 2016) to the information security context.

This study's use of multiple outcome measures enables us to provide some insight into *how* the quality of the relationship between the IAF and the information security function affects outcomes. Prior research suggests that a good working relationship between the two functions can improve outcomes through a collaborative detection capability or through knowledge transfer (Havelka & Merhout, 2013). Our results for leading measures show that a better relationship between the internal audit and information security functions increases the number of information security-related internal control weaknesses and IT-related noncompliance incidents that are reported to the board of directors. This supports the notion that a key benefit of a good relationship between the internal audit and information security functions is improving the organization's collaborative detection capabilities to identify leading indicators of information security problems. This result is also consistent with Lin et al.'s (2011) finding that improved coordination between internal and external auditors results in a greater number of externally reported internal control weaknesses.

We also find that a better relationship between the information security and internal audit functions increases the detection of incidents both before and after they cause material harm. The first of these findings is consistent with the idea that a good relationship between the two functions improves security through both improved detection capabilities and via knowledge transfer that leads to remediation of discovered problems. At first, the second finding concerning the number of incidents detected only after causing harm may seem counter-intuitive. However, most organizations' IT infrastructure is constantly changing, thus making information security risk management a moving target. Further, organizations cannot take steps to contain a problem, "stop the bleeding," and take remedial action until they are aware that an incident has occurred. Surveys indicate that many organizations do not even know that they have suffered an incident until long after the attack (Ernst & Young, 2015; Lewis, 2013; Verizon, 2015). Consequently, low success in detecting attacks implies that there might be additional security incidents of which organizations are unaware (PWC, 2016b). Therefore, one could argue that a *higher* number of detected harmful incidents actually indicates *more effective* detective measures related to information security.

Our results also identify two antecedents to a good relationship between the internal audit and information security functions. The first is senior management's commitment to the importance of information security. This finding is consistent with prior research which suggests that visible management support for information

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

Table 2
Descriptive statistics.

Panel A: Independent and Control Variables

Construct	Frequency	Percentage	Mean	SD
Information Security Reporting Structure (Binary)			0.56	0.50
Reports to CIO (coded 0)	26	33.8%		
Reports to Other than CIO (coded 1)	33	42.9%		
Missing	18	23.4%		
Effort Devoted to Information Security			3.29	2.19
0–5% (coded = 1)	19	24.7%		
5–10%	16	20.8%		
10–15%	12	15.6%		
15–20%	14	18.2%		
20–25%	4	5.2%		
25–30%	1	1.3%		
>30% (coded = 7)	4	5.2%		
don't know	7	9.1%		
Number of Employees			3.66	1.92
less than 20 (coded = 1)	11	14.3%		
20–99	15	19.5%		
100–499	13	16.9%		
500–999	12	15.6%		
1000–4999	12	15.6%		
5000–9999	4	5.2%		
over 10000 (coded = 7)	10	13.0%		

Panel B: Latent Constructs

Construct	Min	Mean	Median	Max	SD
Relationship Quality[a]	1	3.67	3.75	5	0.91
Top Management Support[a]	1	3.49	3.60	5	0.99
Noncompliance Issues[b]	0	1.53	0.33	6	1.92
Internal Control Weaknesses[b]	0	1.68	1.00	6	1.99
Incidents Stopped Prior to Causing Harm[b]	0	2.20	1.30	6	2.21
Incidents Detected After Causing Harm[b]	0	0.42	0	5	1.10

[a] Scale: Strongly Disagree = 1 to Strongly Agree = 5.
[b] Scale: 0, 1, 2, 3, 4, 5 to 10 = 5, More than 10 = 6.

security may improve cross-functional relationships because it sends a message that management expects all functional areas to coordinate and focus their efforts on improving security (Steinbart et al., 2012). It is also consistent with normative arguments in the IT audit literature that top management must play a key role in establishing a culture of security and encouraging cross-functional collaboration (ISACA, 2011).

The second antecedent to a good relationship between the internal audit and information security functions is having the CISO report to someone independent of the information security function. It is likely that this occurs because the internal audit function focuses more on process improvements than on compliance when the CISO has an independent reporting relationship (San Miguel & Govindarajan, 1984). This is an important finding, since there is very little research on how the perceived status and independence of auditees influences the nature and scope of internal audit engagements.

Our findings with respect to the positive influence of both top management support and having the CISO report to someone outside the IT function on the relationship between the internal audit and information security functions have important implications for practice. These findings are consistent with COBIT 5's (ISACA, 2012a, 2012b) insistence on the importance of effective IT governance. Furthermore, because neither antecedent requires significant monetary investment, these results suggest a relatively low-cost strategy that organizations can follow to improve the effectiveness of their information security efforts.

This study contributes to the literature by using actual outcomes, rather than perceptions, as the dependent variable to represent the effectiveness of an organization's information security efforts. Because data on actual security outcomes is difficult to obtain, Steinbart, Raschke, Gal, and Dilla (2016) developed an instrument, which they named SECURQUAL, to measure perceptions about an organization's information security processes. They showed that it was a significant predictor of actual security outcomes, which in turn suggests that SECURQUAL might be useful as a surrogate measure for these outcomes. To further examine the potential of SECURQUAL as a surrogate measure, we conducted supplementary analyses (not tabulated) and found that the quality of the relationship between the internal audit and information security functions, top management support, and the CISO's reporting relationship all significantly ($p < 0.05$) affected SECURQUAL. However, when we added SECURQUAL to our research model, it did not significantly improve the amount of variance explained in any of our four outcome measures. Moreover, SECURQUAL also did not mediate the effect of relationship quality on actual security outcomes. Thus, our supplemental analyses suggest that SECURQUAL may be useful as a "silver standard" dependent variable when data about actual security outcomes are not available. However, there is no need for researchers to use SECURQUAL when actual outcome data are available.

This study also contributes to the literature by providing insight into *how* increased top management support improves information security. We find that increases in top management support for information security directly affect leading measures of organizations' information security efforts, reducing both the number of significant reported internal control weaknesses related to information security and the number of significant instances of employee non-compliance with IT policies. However, top management support does not affect either of the lagging measures of information security effectiveness. This pattern of results suggests that top management's support primarily improves the

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

Table 3
Latent construct reliability.

Panel A: Factor analysis: Cronbach alpha (in parentheses) and factor loadings	
Relationship Quality	(0.91)
Members of information security and internal audit work together to assure information systems are secure and reliable	0.88
There is little friction between internal audit and information security	0.88
The relationship between members of information security and internal audit staff is best described as close and personal	0.86
There is a good working relationship between information security and internal audit	0.92
Top Management Support	(0.93)
Top management provides adequate resources for information security	0.89
Top management regularly communicates the importance of information security	0.91
Top management believes that information security is an important issue	0.86
Top management is more proactive as opposed to reactive with respect to information security issues	0.89
Top management is sufficiently aware of business implications of information security issues to include consideration of these issues when assessing risk and choosing appropriate response	0.91
Noncompliance Issues	(0.96)
During 2013 how many IT-related non-compliance issues were reported to the board of directors or executive management?	0.95
During 2012 how many IT-related non-compliance issues were reported to the board of directors or executive management?	0.98
During 2011 how many IT-related non-compliance issues were reported to the board of directors or executive management?	0.95
Internal Control Weaknesses	(0.96)
During 2013 how many internal control weaknesses related to information security issues were communicated by the external auditors to management, board of directors, and/or executive management?	0.95
During 2012 how many internal control weaknesses related to information security issues were communicated by the external auditors to management, board of directors, and/or executive management?	0.98
During 2011 how many internal control weaknesses related to information security issues were communicated by the external auditors to management, board of directors, and/or executive management?	0.95
Incidents Stopped Prior to Causing Harm	(0.97)
During 2013 how many information security incidents were detected and stopped before they resulted in financial loss, business disruption, or public embarrassment?	0.97
During 2012 how many information security incidents were detected and stopped before they resulted in financial loss, business disruption, or public embarrassment?	0.98
During 2011 how many information security incidents were detected and stopped before they resulted in financial loss, business disruption, or public embarrassment?	0.97
Incidents Detected After Causing Harm	(0.96)
During 2013 how many information security incidents actually resulted in financial loss, business disruption, or public embarrassment?	0.96
During 2012 how many information security incidents actually resulted in financial loss, business disruption, or public embarrassment?	0.98
During 2011 how many information security incidents actually resulted in financial loss, business disruption, or public embarrassment?	0.97

Panel B: Multi-trait matrix[a]

Construct	CISORPT	TMS	PERC	RELQLTY	NEMP	NONCOMP	ICWEAK	STOPPED	DETECTED
CISORPT	**1.00**								
TMS	−0.32	**0.78**							
PERC	−0.15	0.05	**1.00**						
RELQLTY	0.36	0.09	0.01	**0.78**					
NEMP	−0.41	−0.01	0.32	0.11	**1.00**				
NONCOMP	−0.23	−0.20	−0.03	−0.03	0.30	**0.97**			
ICWEAK	−0.28	−0.02	0.03	0.01	0.41	0.65	**0.92**		
STOPPED	−0.19	−0.18	−0.03	0.20	0.40	0.42	0.29	**0.95**	
DETECTED	−0.18	−0.09	0.19	0.00	0.26	0.33	0.32	0.25	**0.94**

CISORPT: Information security reporting structure (coded 0 for within the IT function; 1 otherwise).
TMS: Top management support.
PERC: Level of effort devoted to information security.
RELQLTY: Relationship quality.
NEMP: Number of employees.
NONCOMP: Noncompliance issues.
ICWEAK: Internal control weaknesses.
STOPPED: Incidents stopped prior to causing harm.
DETECTED: Incidents detected after causing harm.
[a] The diagonal of the matrix is the Average Variance Extracted for each variable. The remainder of the table reports the bivariate correlation coefficients.

effectiveness of the organization's information security efforts by creating a positive security culture characterized by more effective design and operation of security-related controls.

In addition, we found that a control variable for percentage of IT staff effort devoted to information security has a positive influence on lagging indicators of information security effectiveness. Thus, our results support normative arguments that recommend multiple levels of assurance involving the support of top management, direct involvement by line management, and independent assurance by the IAF (ISACA, 2011, 2012b; Institute of Internal Auditors,

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

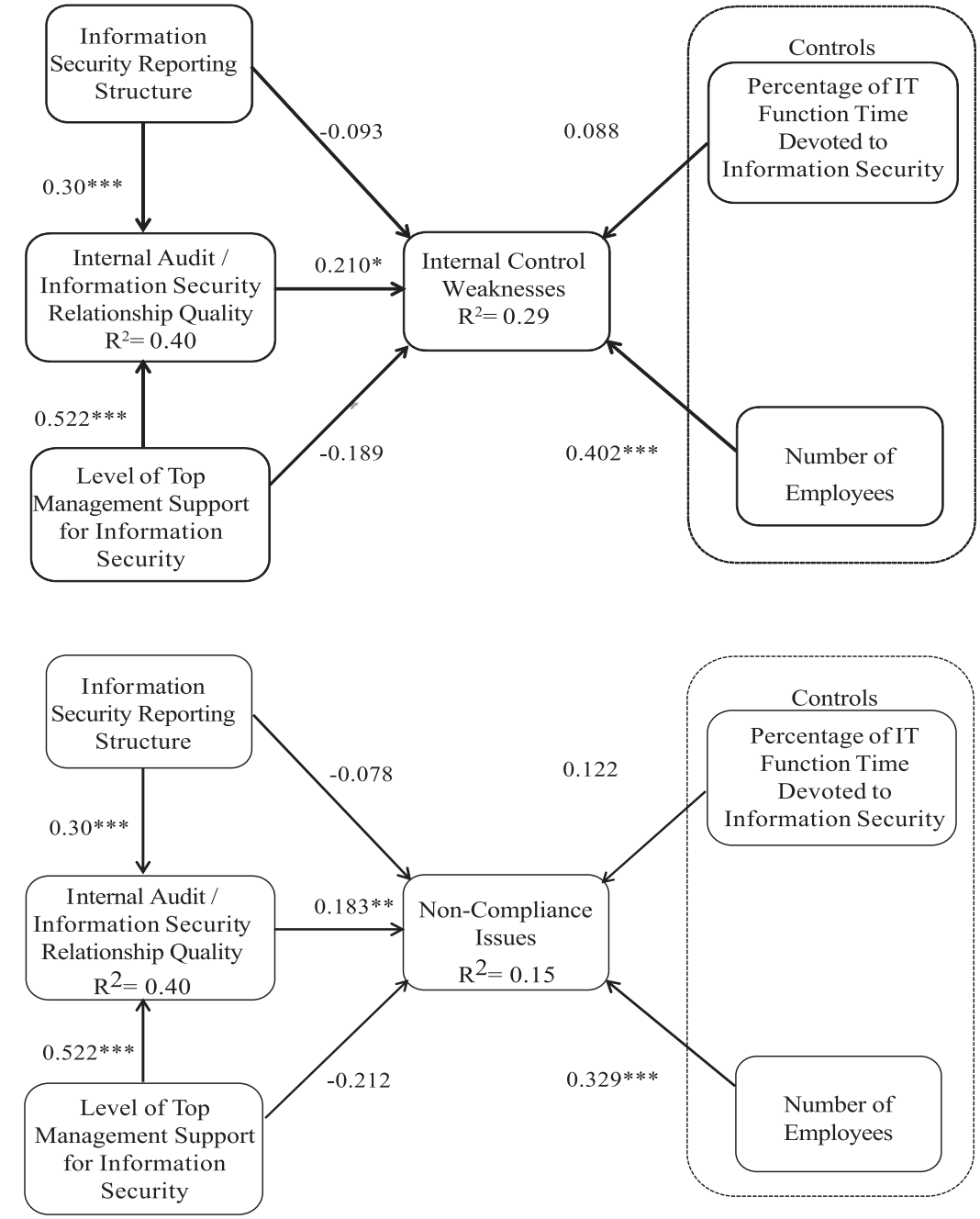

Fig. 2. Results for leading indicators of information security effectiveness.

Table 4
Path model test results.

	RELQLTY	ICWEAK	NONCOMP	STOPPED	DETECTED
PERC	N/A	0.088	0.122	0.238***	−0.217**
NEMP	N/A	0.402***	0.329***	0.316***	0.346***
RELQLTY	N/A	0.210**	0.183**	0.166*	0.161*
TMS	0.522***	−0.189**	−0.212**	0.099	0.027
CISORPT	0.300***	−0.093	−0.078	−0.029	−0.033
R^2	0.402	0.290	0.148	0.291	0.159
Adjusted R^2	0.386	0.240	0.088	0.241	0.100

See Table 3 for variable definitions. Significance levels: * = 0.10, ** = 0.05, *** = 0.01.

2013a).

Finally, it is important to note the limitations of our study. First, our analysis is based on cross-sectional data. Indeed, it may take several years for improvements in IT governance structures to have an influence on security outcomes (Higgs et al., 2016). Hence, our finding that a good relationship between the internal audit and information security functions increased the number of security-related internal control weaknesses and instances of employee non-compliance with security policies may indicate that organizations in our study are reaping the benefits of collaborative detection, but have not yet reached the point where knowledge

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

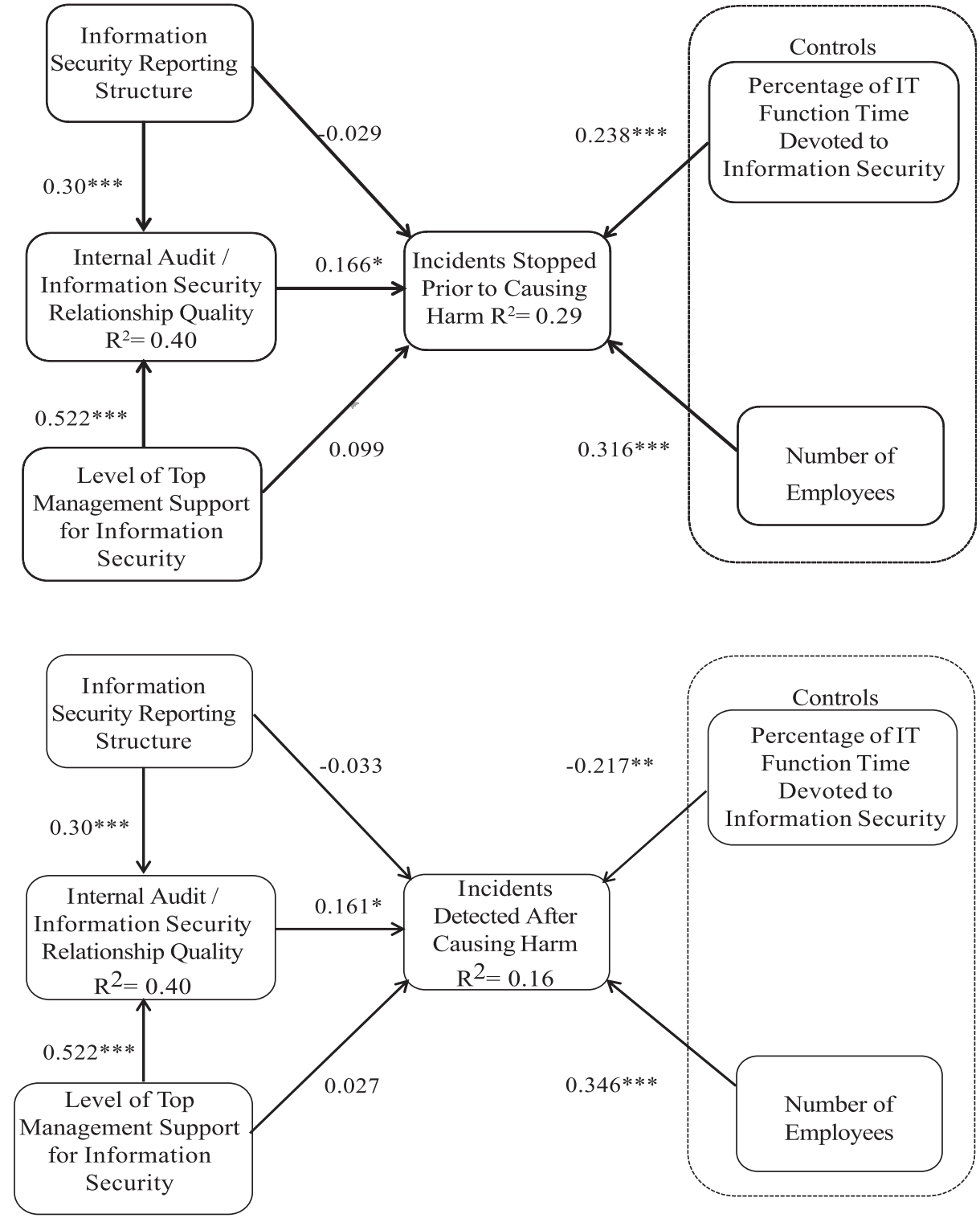

Fig. 3. Results for lagging indicators of information security effectiveness.

transfer reduces the number of such problems. Thus, investigation of the longitudinal effects of the relationship between the internal audit and information security functions on actual outcomes may help distinguish between the collaborative detection and knowledge transfer effects.

A second limitation is that our analysis is based on self-reported

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005

data about outcomes. Given that information security is a sensitive area, it is difficult to obtain direct empirical data on security outcomes and breaches (Ransbotham & Mitra, 2009). However, we mitigated this limitation by asking respondents to report specific objective measures, rather than merely asking for global, subjective assessments about the effectiveness of an organization's information security. Moreover, we collected such measures for three years, thereby increasing the reliability of our dependent measures.

Third, because of constraints to limit the length of our survey instrument in order to encourage participation, we were not able to collect information about various measures of internal audit quality, such as auditor independence, qualifications, knowledge, and skills. It is likely that those characteristics may significantly affect the quality of the relationship between the internal audit and information security functions (Merhout & Havelka, 2008; Stoel et al., 2012; Havelka & Merhout, 2013; Ma'ayan & Carmeli, 2016). Therefore, an important topic for future research is to investigate the influence of these internal audit quality measures, not only on the relationship between the internal audit and information security functions, but also on information security outcomes.

In conclusion, this study shows that the IAF can indeed contribute to the effectiveness of an organization's information security efforts by developing and maintaining a positive collaborative relationship with the information security function. Nevertheless, much additional research is needed to more fully understand how that relationship, and similar relationships with other organizational units that are involved in various aspects of risk management, improve the effectiveness of an organization's information security and its overall governance of IT.

Acknowledgements

We thank the selection committee of the first *Journal of Information Systems* Research Conference for supporting our proposal for providing access to professional participants. We also thank the IMTA section of the AICPA, especially Susan Pierce, for their assistance in obtaining the data analyzed in this manuscript. In addition, we appreciate the comments from the participants in the Rutgers University Accounting Research Workshop and the 2016 Dewald Roode Workshop on Information Security and Privacy on earlier versions of this manuscript. Finally, we want to acknowledge the anonymous reviewers and the editor for their feedback and assistance in improving this paper. Of course, we are accountable for any remaining errors.

References

Ahmad, Z., & Taylor, D. (2009). Commitment to independence by internal auditors: The effects of role ambiguity and role conflict. *Managerial Auditing Journal, 24*(9), 899–925.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations & Society, 35*(7), 659–675.

Arena, M., & Azzone, G. (2009). Identifying organizational drivers of internal audit effectiveness. *International Journal of Auditing, 13*(1), 43–60.

Bauer, T., & Estep, C. (2016). *One team or two teams? exploring relationship quality between auditors and it specialists and its implications for a collective audit team identity and the audit process*. Working Paper. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579198.

Busco, C., Giovannoni, E., Riccaboni, A., Frigo, M. L., & Scapens, R. W. (2006). Towards "integrated governance": The role of performance measurement systems. In M. J. Epstein, & J. Manzoni (Eds.), *Performance measurement and management Control: Improving organizations and Society: Studies in managerial and financial accounting* (Vol 16, pp. 159–186). Elsevier Ltd.

Carcello, J., Eulerich, M., Masli, A., & Wood, D. (2017). *Are internal audits associated with reductions in operating, financial reporting, and compliance risk?*. Working Paper. Available at: https://papers.ssrn.com/soL3/papers.cfm?abstract_id=2970045.

Carcello, J. V., Hermanson, D. R., & Ye, Z. (2011). Corporate governance research in accounting and auditing: Insights, practice implications, and future research directions. *Auditing: A Journal of Practice & Theory, 30*(3), 1–31.

Center for Internet Security. (2015). *Critical security controls for effective cyber defense v. 6.0*. San Mateo, CA: Center for Internet Security.

Dittenhofer, M. (1997). Behavioural aspects of internal auditing "revisited". *Managerial Auditing Journal, 12*(1), 23–27.

Dittenhofer, M. A., Ramamoorti, S., Ziegenfuss, D. E., & Evans, R. L. (2010). *Behavioral dimensions of internal auditing: A practical guide to professional relationships in internal auditing*. Altamonte Springs, IL: The Institute of Internal Auditors Research Foundation.

Drew, J. (2015). *CPAs select security as top technology priority*. Available at: http://www.journalofaccountancy.com/news/2015/apr/technology-security-cpa-firms-201512151.html.

Eden, D., & Moriah, L. (1996). Impact of internal auditing on branch bank performance: A field experiment. *Organizational Behavior and Human Decision Processes, 68*(3), 262–271.

Ernst, & Young. (2015). *How boards can help crack the cybereconomics equation*. Board Matters Quarterly, September, 14–15.

Fanning, K., & Piercey, D. (2014). Internal auditors' use of interpersonal likability, arguments, and accounting information in a corporate governance setting. *Accounting, Organizations & Society, 39*(8), 575–589.

Fayard, D., Lee, L., Leitch, R., & Kettinger, W. I. (2012). Effect of internal cost management, information systems integration, and absorptive capacity on inter-organizational cost management in supply chains. *Accounting, Organizations and Society, 37*(3), 168–187.

Flora, P. E., & Raj, S. (2015). *Navigating Technology's top 10 Risks: Internal Audit's role*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567–594.

Gramling, A. A., Maletta, M. J., Schneider, A., & Church, B. K. (2004). The role of the internal audit function in corporate governance: a synthesis of the extant internal auditing literature and directions for future research. *Journal of Accounting Literature, 23*, 194–244.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory & Practice, 19*(2), 139–152.

Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems, 14*(3), 165–192.

Héroux, S., & Fortin, A. (2013). The internal audit function in information technology governance: A holistic perspective. *Journal of Information Systems, 27*(1), 189–217.

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.

Hill, J. (2015, September 17). *Cyberwarriors with Calculators: The role of accounting and finance professionals in a Company's cybersecurity*. Available at: http://www.accaglobal.com/gb/en/technical-activities/technical-resources-search/2015/september/cyber-threat.html.

Hong, N. (2016). For consumers, injury is hard to prove in data-breach cases. April 26. *Wall Street Journal (Online)*. Available at: https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.

Institute of Internal Auditors. (2013a). *Practice advisory 2050-2. Assurance maps*. Altamonte Springs, FL: Institute of Internal Auditors.

Institute of Internal Auditors. (2013b). *International standards for the professional practice of internal auditing. Section 1110. Organizational independence*. Altamonte Springs, FL: Institute of Internal Auditors.

ISACA. (2011). *COBIT 5: The framework*. Rolling Meadows: ISACA.

ISACA. (2012a). *COBIT 5 enabling processes*. Rolling Meadows, IL: ISACA.

ISACA. (2012b). *COBIT 5 for information security*. Rolling Meadows, IL: ISACA.

ISACA. (2016). *State of cybersecurity: Implications for 2016*. Available at: https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.

IT Governance Institute. (2008). *Information security Governance: Guidance for information security managers*. Rolling Meadows, IL: IT Governance Institute.

Kane, A. A. (2010). Unlocking knowledge transfer potential: Knowledge demonstrability and superordinate social identity. *Organization Science, 21*(3), 643–660.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive, 9*(3), 163–175.

Khan, M. J. (2016). *ISACA Journal, 1*, 41–43.

Kock, N. (2015). *Warp PLS 5.0 user manual*. Laredo, TX: ScriptWarp Systems.

Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7), 549–580.

Kwon, J., Ulmer, J., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems, 27*(1), 219–236.

Lewis, J. A. (2013). *Raising the bar for cybersecurity*. Washington, DC: Center for Strategic & International Studies.

Li, D. C. (2015). Online security performances and information security disclosures. *Journal of Computer Information Systems, 55*(2), 20–28.

Lin, S., Pizzini, M., Vargus, M., & Bardhan, I. R. (2011). The role of the internal audit function in the disclosure of material weaknesses. *The Accounting Review, 86*(1), 287–323.

Love, P., Reinhard, J., Schwab, A., & Spafford, G. (2010). *Global technology audit guide (GTAG®) 15 information security governance*. Altamonte Springs, FL: The Institute of Internal Auditors. Available at: The Institute of Internal Auditors: ttps://na.theiia.org/standards-guidance/Member Documents/GTAG-15_edited_with_Ad_

05-20-20101.pdf - 1.
Luftman, J., & Ben-Zvi, T. (2010). Key issues for IT executives 2009: Difficult economy's impact on IT. *MIS Quarterly Executive, 9*(1), 49–59.
Ma'ayan, Y., & Carmeli, C. (2016). Internal audits as a source of ethical behavior, efficiency, and effectiveness in work units. *Journal of Business Ethics, 137*, 347–363.
Merhout, J. W., & Havelka, D. (2008). Information technology auditing: A value-added IT governance partnership between IT management and audit. *Communications Fo the Association for Information Systems, 23*, 26.
Minaya, E. (2015). Target reaches another data breach settlement. *Wall Street Journal (Online)*. December 2. Available at: https://www.wsj.com/articles/target-reaches-another-data-breach-settlement-1449085790.
Morris, T., & Empson, L. (1998). Organisation and expertise: An exploration of knowledge bases and the management of accounting and consulting firms. *Accounting, Organizations & Society, 23*(5/6), 609–624.
Paape, L., & Speklè, R. F. (2013). The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review, 21*(3), 533–564.
Panko, R. R. (1999). Applying code inspection to spreadsheet testing. *Journal of Management Information Systems, 16*(2), 159–176.
Panko, R. R., & Sprague, R. H., Jr. (1998). Hitting the wall: Errors in developing and code inspecting a 'simple' spreadsheet model. *Decision Support Systems, 22*(4), 337.
Powell, S. G., Baker, K. R., & Lawson, B. (2008). A critical review of the literature on spreadsheet errors. *Decision Support Systems, 46*(1), 128–138.
Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations & Society, 38*(6/7), 525–543.
Prawitt, D. F., Smith, J. L., & Wood, D. A. (2009). Internal audit quality and earnings management. *The Accounting Review, 84*(4), 1255–1280.
PWC. (2016a). *Global economic crime survey 2016*. PWC.
PWC. (2016b). *The global state of information Security® survey 2016*. PWC.
Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121–139.
Ricketts, J. A. (1990). Powers-of-ten information biases. *MIS Quarterly, 14*(1), 63–77.
Ross, S. J. (2011). *Creating a culture of security*. Rolling Meadows: ISACA.
Ross, S. J. (2015). Information security matters: Stanley Baldwin's bomber. *ISACA Journal, 5*, 4–6.
Roussy, M. (2015). Welcome to the day-to-day of internal auditors: How do they cope with conflicts? *Auditing: A Journal of Practice & Theory, 34*(2), 237–264.
San Miguel, J. G., & Govindarajan, V. (1984). The contingent relationship between the controller and internal audit functions in large organizations. *Accounting, Organizations & Society, 9*(2), 179–188.
Sarens, G. (2009). Internal auditing research: Where are we going? *International Journal of Auditing, 13*(1), 1–7.
Sarens, G., & De Beedle, I. (2006). The relationship between internal audit and senior management: A qualitative analysis of expectations and perceptions. *International Journal of Auditing, 10*(1), 219–241.
Seago, J. (2017). Climbing the scale. *Internal Auditor, LXXIV*(2), 38–43.
Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. (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., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems, 27*(2), 65–86.
Steinbart, P. J., Raschke, R., Gal, G., & Dilla, W. (2015). *The influence of internal audit on information security Effectiveness: Perceptions of internal auditors*. http://papers.ssrn.com/sol3/papers.cfm?abstractid=2685943.
Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems, 30*(1), 71–92.
Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems, 13*(1), 60–79.
Tanaka, Y., & Goto, A. (2014). N-RPOdetector: Proposal of a method to detect the ROP attack code on the network. In *Proceedings of the2014 workshop of cyber security analytics, intelligence and automation* (pp. 33–36). Available at: https://doi.org/10.1145/2665936.2665937.
Teo, T. S., & Tan, M. (1999). Spreadsheet development and 'what-if' analysis: Quantitative versus qualitative errors. *Accounting, Management and Information Technologies, 9*(3), 141–160.
ThreatTrack. (2016). *Security analysts say defending against advanced malware still a major struggle*. Available at: http://www.threattracksecurity.com/resources/white-papers/security-analysts-say-defending-against-advanced-malware-still-a-major-struggle.aspx.
Van Peursem, K. (2005). Conversations with internal auditors: The power of ambiguity. *Managerial Auditing Journal, 20*(5), 489–512.
Verizon. (2015). *2015 data breach investigations report*. Available at: http://www.verizonenterprise.com/DBIR/2015/.
Wang, T., Kannan, K. N., & Ulmer, J. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research, 24*(2), 201–218.
Werlinger, R., Hawkey, K., Botta, D., & Beznosov, K. (2009). Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies, 67*(7), 584–606.
de Zwaan, L., Stewart, J., & Subramaniam, N. (2011). Internal audit involvement in enterprise risk management. *Managerial Auditing Journal, 26*(7), 586–604.

Please cite this article in press as: Steinbart, P. J., et al., The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society (2018), https://doi.org/10.1016/j.aos.2018.04.005