Information & Management 52 (2015) 385–400

Contents lists available at ScienceDirect

Information & Management

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

Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources

Huseyin Cavusoglu [a,1,2], Hasan Cavusoglu [b,3], Jai-Yeol Son [c,*], Izak Benbasat [b,4]

[a] Naveen Jindal School of Management, University of Texas at Dallas, 800 West Campbell Road, Richardson, TX 75083, USA
[b] Sauder School of Business, University of British Columbia, 2053 Main Mall, Vancouver, BC, Canada V6T1Z2
[c] School of Business, Yonsei University, 50 Yonsei-ro, Seoul 120-749, South Korea

ARTICLE INFO

Article history:
Received 28 May 2013
Received in revised form 10 September 2014
Accepted 2 December 2014
Available online 14 April 2015

Keywords:
Organizational security management
Security controls
Resource-based theory
Institutional theory
PLS

ABSTRACT

To offer theoretical explanations of why differences exist in the level of information security control resources (ISCR) among organizations, we develop a research model by applying insights obtained from resource-based theory of the firm and institutional theory. The results, based on data collected through a survey of 241 organizations, generally support our research model. Institutional pressures and internal security needs assessment (ISNA) significantly explain the variation in organizational investment in ISCR. Specifically, coercive and normative pressures are found to have not only a direct impact but also an indirect impact through ISNA on organizational investment in ISCR.

1. Introduction

The dependency on the connectivity enabled by the Internet has created unprecedented challenges for organizations to establish more secure information technology (IT) infrastructures. Even a single security breach may result in irreparable damage to firms in terms of corporate liability, loss of credibility, and reduced revenues [9]. High-profile security incidents in recent years have raised awareness of information security and brought it to the forefront of corporate priorities [20]. Many firms today rate information security as one of the highest priorities for their IT expenditures [13].

The early research stream on management of information security focused on developing comprehensive checklists for security procedures and controls, encompassing various areas of threats [14]. This approach later led to the development of risk management methodologies to assess the magnitude of risk using the probability of occurrence of a security lapse and the cost associated with it [3]. Later studies focused on information security policies and investigated drivers for compliance and violations (e.g., [8,53,54]). Despite a widespread belief that organizations can successfully address security issues by investing in technical and socio-organizational resources [17], there is still a lack of theory on and empirical support for what constitutes a coherent set of organizational resources for information security controls and why variations exist in the amount of such resources among organizations. In the wake of recent high profile security breaches at Target and Neiman Marcus, our research will provide insights as to why the other retailers, such as Wal-Mart and Sears, have different resources that protected them from malware stealing payment card numbers from the memory in cash registers in retail stores during the payment process or payment authorization [28].

This study intends to fill this gap in the literature with two objectives. First, drawing upon the resource-based view (RBV) of the firm [64], we first examined the nature of organizational resources deployed for better security—hereafter referred to as *information security control resources* (ISCR) in organizations. We used the typology of Grant [24] as a theoretical lens to identify three distinct but interrelated dimensions – *information security*

* Corresponding author. Tel.: +82 2 2123 5456; fax: +82 2 2123 8639.
E-mail addresses: hcavusoglu@gmail.com (H. Cavusoglu), cavusoglu@sauder.ubc.ca (H. Cavusoglu), json@yonsei.ac.kr (J.-Y. Son), izak.benbasat@ubc.ca (I. Benbasat).
[1] The co-authors have contributed equally to this paper.
[2] Tel.: +1 972 883 5939; fax: +1 972 883 2089.
[3] Tel.: +1 604 822 8894; fax: +1 604 822 0045.
[4] Tel.: +1 604 822 8396; fax: +1 604 822 0045.

http://dx.doi.org/10.1016/j.im.2014.12.004
0378-7206/

technologies, qualified information security personnel, and *security awareness of organizational users* – of ISCR in organizations. Second, based on institutional theory and its recent development, we explicate antecedents of an organization's investment in ISCR. We posit that organizations heterogeneously respond to institutional pressures related to information security by making different levels of investment in ISCR. In particular, we argue that institutional pressures, such as *mimetic, coercive, and normative pressures*, exerted from the external environment have both direct and indirect impacts through ISNA on organizational investment in ISCR.

2. A resource-based view of information security controls

The RBV literature suggests that the set of resources a firm possesses can explain its performance [64]. Viewed either as a strength or a weakness of a firm, resources are considered assets that enable the firm to conceive and execute strategies that improve efficiency and effectiveness [64]. Although the RBV tends to define resources broadly to include capabilities, resources and capabilities have been considered as distinct concepts [5,24]. Resources refer to the principal assets needed for the activities performed by the firm, whereas capabilities refer to the firm's ability to leverage those resources, such as organizational processes and routines [5,24]. Resources have direct and indirect impacts on performance through the firm's capabilities and are viewed as central to explaining organizational performance [63]. We apply this line of reasoning within the context of organizational security management in explaining organizational security performance, which is defined as the extent to which information and technology assets of an organization are protected from both internal and external threats. To do so, we first identify the key components of ISCR that firms should possess to improve their information security performance.

A number of categorization schemes have been proposed to classify resources (e.g., [5,24,35,37,47,49]). We applied the typology suggested by Grant [24] in the information security context. Grant classifies resources into three groups: tangible, human, and intangible. Tangible resources include financial resources that determine a firm's resilience and capacity for investment and physical resources that reflect the firm's production potential. Human resources are the productive services that organizational members offer to the firm in terms of their skills, knowledge and decision-making ability. Intangible resources include technology-related intangibles (e.g., intellectual property, patent portfolio, copyrights, and trade secrets) and reputation [24].

We define **ISCR** *as the extent to which an organization possesses three different security-related resources of information security technologies, qualified information security personnel, and security awareness of organizational users for safeguarding the organization's information assets*. Rooted in the RBV and consistent with the "defense-in-depth" approach used in practice to create multiple layers of protection around information assets [66], we posit that the three major resources characterize an information security control environment of an organization. We consider information security technologies as tangible resources, qualified information security personnel as human resources, and security awareness of organizational users as intangible resources.

2.1. Information security technologies

Numerous surveys revealed that organizations often rely mainly on technology-based solutions as part of their effort to secure their systems [15,20]. The prior literature has also identified technology-based solutions as an important predictor of security performance [56]. When security technologies such as firewalls, anti-virus software, and intrusion detection systems are configured properly, they provide security without user intervention. They either prevent security violations before they arise or detect security violations as they occur [10]. Drawing on the RBV, information security technologies are tangible resources in the information security context. IS studies utilized various terms to refer to tangible resources: technology resources [47], IT infrastructure [5], technology assets [49], technological IT resources [37], and proprietary technology [35]. Hence, tangible resources were often viewed as physical IT assets, including hardware and software.

Consistent with the RBV, we define **information security technologies** *as the extent to which an organization possesses preventive and detective technical solutions to address vulnerabilities within information technology infrastructure in which critical information assets reside*. The massive security breach in Target's systems in late 2013, in which 70 million customers' personal information along with 40 million payment card records were stolen, showed that proper information security technologies are needed to defend against emerging information security threats [27]. We posit that an organization's information security technologies are an important component of the organization's ISCR.

2.2. Qualified information security personnel

Organizations need human resources with expertise and skills to design security programs and to implement and maintain technology-based solutions. Security personnel with knowledge and expertise in information security can identify the security needs of an organization and design an appropriate security program [40]. Moreover, security personnel who are responsible for installation, configuration and maintenance of security technologies and the acquisition and evaluation of security-related information can manage information security functions on a day-to-day basis [41]. The lack of security personnel and/or their lack of knowledge may result in security lapses.

Following the RBV, we view qualified information security personnel as human resources in the information security context. In the IS literature, human resources are often referred to as human assets [49] or human IT resources [5,37]. Human resources include technical skills, such as the know-how and expertise needed to build IT applications and operate them, and managerial skills, such as the ability to manage the IS function, and the capacity to coordinate and interact with other business functions [5,35,37]. Technical and managerial IT skills are considered strong drivers of performance in implementing information technologies [5,49]. Prior research has also found that an increase in security personnel reduces the number of internal IS abuses [56].

We define **qualified information security personnel** *as the extent to which an organization possesses professional staff members who can define, execute, and maintain the information security program of the organization*. Suby [58] argues that rapidly changing technology and threat landscapes necessitate highly qualified information security professionals to safeguard their information's assets. We consider qualified information security personnel one of the key components of the ISCR.

2.3. Security awareness of organizational users

Although technology-based solutions and qualified information security personnel help organizations address the risks associated with design and implementation vulnerabilities, their information assets remain at risk unless users at all levels of the organization are aware of their roles and responsibilities with regard to security. Instead of using technical means to breach information assets, attackers can exploit human vulnerabilities to cause a similar type of damage. This approach can be especially effective because of the

users' proximity to information assets. For instance, social engineering attacks use social skills to convince users to reveal access information to attackers or to run the attacker's code. In addition, users can inadvertently cause a breach in security, such as posting passwords in places accessible by others. If users are not aware of security issues, they may nullify even the best technical security controls. Security-aware users are an essential protection against threats that exploit weaknesses in human nature.

Prior research has argued that organizations can manage their information security function more effectively if the emphasis goes beyond the technical means of protecting information assets [57]. Many studies have made calls to consider the socio-organizational and human aspects in managing IS security [16]. As Mitnick and Simon [39] note, people who interact with the information assets of the organization are "truly security's weakest link" (p. 4). According to Segev et al. [52], the key to security "lies not with technology, but with the organization itself" (p. 85). Furthermore, Trompeter and Eloff [62] argue that although dealing with information security at a technical level is important, "its implementation must also take cognizance of ethical and human considerations" (p. 384). The more formidable the technical safeguards are, the more attractive target users become for those who intend to gain access to an organization's information.

Every person in an organization whose actions can intentionally or otherwise affect the security of the organization should have the responsibility to ensure information security [40]. The most effective vehicle to achieve this is to cultivate *awareness* and provide *security training* [42]. Security awareness programs enable users to recognize security concerns and acquaint them with the organizational sanctions that might be imposed as a consequence of security lapses. These programs are directed at encouraging users to change inappropriate behavior and adopt good security practices. Training, however, aims at imparting the relevant security skills and competencies needed to protect the information assets entrusted to them [42]. Awareness and training together enable organizational users to be in a better position to prevent security violations due to negligence or error, as well as those that stem from malicious activities. Effective information security programs should consider security-aware users as a safeguard to information security.

Drawing upon the RBV [24,64] and the literature on information security, we consider the security awareness of organizational users as an intangible resource in the security context. Organizational users, unlike security personnel, do not have direct responsibilities with respect to security. Therefore, their mere existence does not contribute to security. Organizational users can add to security if their state of knowledge, i.e., awareness of security threats and knowledge about avoiding them, is adequate. Information security awareness is often referred to as an intangible control for information security among practitioners because it complements technical controls. Hence, we classify the security awareness of organizational users as an intangible resource for information security. There is growing evidence in the IS literature that intangible resources are as valuable as tangible ones. Bharadwaj [5] argues that IT-enabled intangibles, such as customer orientation and knowledge assets, are key drivers of superior performance. Similarly, Melville et al. [37] note that non-IT human capital resources, which we regard as including organizational users who are outside the IT function (i.e., outside IT human capital), are complementary to IT resources in explaining organizational performance.

We define **security awareness of organizational users** *as the extent to which employees interacting with the information assets of an organization are fully informed, well-trained, and aware of security-related issues and assume security as their everyday responsibility*. Privacy Rights Clearinghouse (www.privacyrights.org) reveals that more than two-thirds of the data breaches disclosed since 2005 were classified in breach categories, which are caused by individuals within the organization. We believe that the success of an information security program depends in part upon the effective behavior of the individuals using the IT resources of the organization, and therefore, security-aware organizational users constitute an important dimension of ISCR.

3. Theory and hypotheses development

Our research model is developed by employing institutional theory and its recent development. Institutional theory suggests that the main objective in organizational decisions is to gain greater legitimacy from the stakeholders in its environment, and this legitimacy can be gained by adopting processes, structures, and strategies that others in the environment have already adopted. As Scott and Meyer [51] posit, the institutional environments "are characterized by the elaboration of rules and requirements to which individual organizations must conform if they are to receive support and legitimacy" (p. 149). The proponents of this theory focus on the social and cultural aspects of organizational environments [43]. Hence, values, norms and beliefs external to the organization play a significant role in determining organizational decisions. Organizations seek this legitimacy by conforming to three distinct types of institutional pressures: *mimetic*, *coercive*, and *normative* [18].

Institutional theory has been successfully used as a theoretical lens to explain whether specific organizational behaviors are consistent with institutional forces. It has received growing acceptance in IS research. For example, the theory has been applied to explain organizational adoption of EDI [59] and enterprise systems [33]. More recently, researchers have argued that organizational responses to institutional pressures can vary within certain boundaries [7]. Organizations can have the freedom to make strategic responses to external pressures rather than simply copying what others have adopted. Further, organizations can internalize institutional pressures differently for various reasons such as time, space, or local competition, and the internalization process can well explain differences in organizational response to institutional pressures [7]. For instance, although some organizations could adopt ISO 9000 standards without much consideration if many other organizations have already adopted them, many organizations often responded to such institutional pressure by examining whether the adoption would increase technical efficiency of operations [4]. We employ this line of reasoning to explain why organizations often engage in ISNA in responding to institutional pressures within the context of security management. In particular, we argue that organizations internalize institutional pressures on security investment by responding to the pressures through ISNA. Hence, organizations would make varying levels of investment in ISCR in the event of institutional pressures on security investment.

Our research model, which focuses on both direct and indirect impacts of institutional pressures through the internalization process on ISCR investment, is shown in Fig. 1.

3.1. Direct influence of institutional pressures

3.1.1. Mimetic pressure

Mimetic pressure causes organizations to imitate actions taken by others, such as competitors, without significant consideration [18]. Organizations often closely monitor actions and successful practices applied by others within their industry. In turn, these successes by others serve as the basis of imitation [29]. Faced with high levels of uncertainty about the outcomes of a particular course of action, organizations may achieve legitimacy by

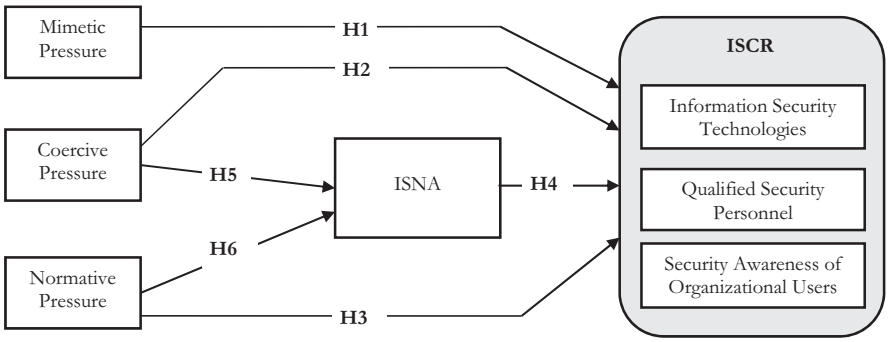

Fig. 1. Research model.

following the collective actions of early movers [61] and the practices adopted by other similar organizations [18]. Such imitative behavior is deemed desirable, especially when organizations face similar problems and are not clear about expected outcomes of the organizational means to address the problems.

Within the IS discipline, the role of mimetic pressure has been examined to understand organizational motivations to take a variety of IS-related actions. Furthermore, although not addressed under the rubric of the mimetic pressure effect, prior studies have recognized that a firm's IT-related decisions often emulate the collective actions taken by others in its industry [34]. Similarly, it is expected that organizations are often concerned with whether their spending on IS security is in line with that of their competitors. Thus, we develop the following hypothesis:

H1. Mimetic pressure, manifested by perceived level of investment in security among competitors, will positively influence investment in ISCR.

3.1.2. Coercive pressure

An additional major impetus toward homogeneity among organizations is conformity to *coercive pressure*, which implies that organizations are subject to pressures exerted by other organizations and cultural expectations [18]. For example, regulatory agencies may exert direct pressure on organizations in certain industries by mandating particular organizational practices [38]. Even without direct attempts to influence a firm, certain strategic actions taken by dominant organizations in an industry may give rise to indirect pressures on other organizations in the industry. According to the resource-dependency theory [46], the source of those pressures generally arises from the ability of stakeholders to control scarce resources critical to the survival of the organizations being influenced.

Recent regulations imposed on corporations, such as the Gramm–Leach–Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the Sarbanes–Oxley (SOX) Act, California SB 1386, and the European Union's Data Protection Directives, are notable examples of coercive pressure that organizations face in the context of information security. These regulations demand compliance with their requirements. For example, the Payment Card Industry Data Security Standards (PCI DSS) defines what aspects of credit card data are sensitive, describing access control requirements for credit card information and encryption requirements for transmission and storage. These regulatory forces allow organizations to determine the security controls needed to comply with their requirements. Indeed, a recent survey found that compliance with regulations is the most influential driver of organizations' information security practices [20].

Firms today must comply not only with federal and industry-specific regulations but also with various security standards imposed by their business partners. An organization is only as secure as its least secure partner. A firm cannot establish proper security if its partners do not perform due diligence in ensuring transactional security. For example, Visa has developed a formal information security standard. Merchants' compliance with the security standard is often deemed mandatory [60]. Although no direct pressure is exercised by a dominant player to require certain security precautions, business partners may nevertheless perceive coercion, insofar as their information security practices have a potential influence on their relationships with the dominant player. Failure in that regard might hurt future business prospects with the dominant player. In fact, a recent study reported that managers of supplier firms see information security as a qualifier to do business with the buyer firm [19]. Based on the above arguments, we argue that coercive pressure is exerted mainly through two sources: business partners and security regulations. Thus, we develop the following hypothesis:

H2. Coercive pressure, manifested by perceived pressure from business partners and pressure from regulations, will positively influence investment in ISCR.

3.1.3. Normative pressure

Homogeneity among organizations over time is attributed in part to organizations' conformity with *normative pressure* [50]. Organizations are likely to adjust their behavior based on their beliefs about what is viewed as appropriate among members of their social networks and consequently adopt techniques and methods that reflect the current standards of those networks. Normative pressure can be exerted from a variety of sources, including business partners and trade and professional associations. Because firms within a value chain generally share common goals, a firm is subject to normative pressure originating from other members of its value chain. A firm's decision to adopt new technologies [33,59] and organizational practices [25] is often influenced by how its business partners take action with respect to those technologies and practices.

An additional type of normative pressure originates from participation in trade and professional associations [59]. Normative rules about organizational behavior are defined and promulgated through active participation in an array of events, such as conferences, workshops, and educational programs organized by trade and professional associations [18]. These events act like forums to share experience about security practices and to learn about common security frameworks and standards. Participation in leading security associations, such as the SANS Institute, the Information Systems Audit and Control Association (ISACA), and the Software Engineering Institute (SEI), as well as attendance at

their training and certification programs, provides organizations with knowledge about the best security technologies, standards, and practices. Recent surveys have shown that organizations are keen to adopt security standards, such as ISO 17790 and BS 7799 [15,20]. Many practitioners believe that information security standards are beneficial because these standards allow them to demonstrate their commitment to better security practices and to establish their company's brand and customer loyalty [20]. Hu et al. [30] reported that professional associations and security publications are important sources behind security initiatives. Based on the above arguments, we argue that normative pressure is exerted mainly through two sources: business partners' investment in security and exposure to security practices. Thus, we develop the following hypothesis:

H3. Normative pressure, manifested by perceived level of investment among business partners and exposure to security practices through professional associations and publications, will positively influence investment in ISCR.

3.2. Internal security needs assessment

We define internal security needs assessment (ISNA) as an organization's internal response to institutional pressures on security investment through an effort to assess security risks and justify the investment. In particular, we propose that security investment rationale and risk analysis are two key components of ISNA. These two components for ISNA are *inherent* in the contemporary risk management processes and consistent with the prior studies in security management [55].

The two components of ISNA correspond to two essential steps in making a business case about organizational investment in ISCR: formulating *why* the organization needs to invest in security controls at the strategic level and determining *how* to deploy security controls at the implementation level. It can be argued that the security investment rationale represents the ultimate reason for organizational investment in information security. Risk analysis, on the other hand, refers to the process of identifying and assessing the organization's vulnerabilities to facilitate control of the inherent security risks in the operating environment. Hence, risk analysis is the vehicle through which organizations determine the most efficient and effective ways of achieving strategic objectives in security management[1]. As Adler [1] asserts, defining the rationale for security investments and conducting risk analysis should be performed to determine the controls necessary to support the information security goals of the organization. Thus, we develop the following hypothesis:

H4. The extent of ISNA, manifested by security investment rationale and risk analysis, will positively influence investment in ISCR.

3.2.1. Security investment rationale

Well-formulated strategies of a firm can influence the firm to choose certain organizational arrangements. For instance, firms often develop a strategic investment rationale, which refers to value propositions that can enable the identification of promising organizational opportunities and justify commitments of resources toward implementation of attendant projects [11]. That is, a well-developed strategic investment rationale highlights the importance of explicit decision-making tools for organizational justification. Decisions are made to achieve the desired organizational state, which is itself reflected in the strategic investment rationale.

Within the context of information security, a well-developed security investment rationale provides senior managers with a set of criteria to justify organizational investment in information security. Firms could take into account the economic as well as the non-economic consequences of investment decisions. Economic criteria, such as return on investment (ROI), permit evaluations of the economic feasibility of a control in terms of the value of assets to be protected by the control and the cost of the investment [66]. Non-economic criteria, such as retention of customer goodwill, emphasize organizational and operational feasibility. The organizational and management literature also suggests that a well-defined strategic investment rationale is an integral part of the formation of processes leading to organizational adoption and change [48]. Therefore, we conceptualize that security investment rationale is a key component of ISNA.

3.2.2. Risk analysis

In the information security domain, risk is the possibility of something adverse happening [40]. Risk analysis in information security focuses on systems security risks. As a formal tool to identify, assess, and prioritize information security risks, risk analysis in information security has evolved from ad hoc security checklists [14] to a more organization-centric, requirements-oriented, and bottom-up process [21]. Risk analysis today is a process of discovering and assessing risks to an organization's information assets and defining alternative courses of action to control those risks. The purpose of risk analysis in information security is to organize and prioritize limited resources to determine security investments.

A well-defined risk analysis, if conducted effectively, can help organizations identify appropriate security controls [41]. Whitman [65] observed that organizations invest in information security controls based on threats to organizational assets and their significance for security. Most managers view information security as a risk management exercise [15]. Therefore, we view risk analysis as a key component of ISNA.

3.3. Indirect effects of institutional pressures through ISNA

Recent studies on institutional theory argue that organizations are able to make decisions beyond simply conforming to institutional pressures [32] by incorporating more explicitly the role of actors' self-awareness and self-interest into the theory [18]. Decision makers either take institutions as a possible set of alternative organizational arrangements that can be made within their organization [48] or recognize that institutional practices might not be appropriate for the organization and a change is needed [22]. This is different from a classic view of institutional theory in which the organization, to gain legitimacy in the environment, is viewed as an actor with no volitional control over adopting new processes, structures, and strategies. Consistent with this line of argument in the literature, we argue that institutional pressures related to information security can trigger organizations to engage in ISNA.

In fact, the recent development in the literature on institutional theory coincides with the viewpoint of several scholars within the community of information security research about how institutional theory can be employed to study organizational decisions regarding security investments. For instance, Bjorck [6] argued that formal information security belief structures and processes in organizations are mainly created as a response to institutional forces in the external environment. A case study by Hu et al. [30] found that institutional pressures prompted a multi-national

[1] Risk analysis is effective because it enables firms to identify those vulnerabilities that are threats to strategic objectives; it is efficient because not all vulnerabilities that are threats to strategic objectives require the same level of attention.

company to develop formal security management practices. In particular, we argue that two types of institutional pressures, coercive and normative, have strong impacts on an organization's decision to engage in organizational practice of ISNA. Unlike mimetic pressure, which is generally exerted by competitors, coercive and normative pressures are considered more informative in that these two types of pressures are often associated with the communication of the inherent desirability of investing in ISCR and effective security management processes. Through direct and indirect interactions with business partners, government regulatory agencies, and professional security associations that exert coercive and/or normative pressure, organizations can learn about the possible security controls available to them and the various reasons for investment in those security controls. As a response to these two types of institutional pressures, they shape their internal rationale for making similar investments and decide how security risks should be dealt with to protect their information assets.

Coercive pressure arising from recent regulations, including the GLBA, the HIPAA, the FISMA and California SB 1386, demand that organizations be in compliance with their requirements without clearly indicating the types of controls needed for such compliance. Even for SOX, which does not specifically address information security requirements, security has emerged as a critical foundation for compliance. Organizational management is responsible for ensuring that their organization complies with all applicable laws and regulations because failure to do so can result in stringent legal action against them. These regulatory requirements trigger managers to review their current security situation (i.e., risk analysis) and to make a business case for the investment in security resources, if necessary. For example, GLBA, HIPAA, and California SB 1386 all have provisions pertaining to the proper handling of sensitive customer information to avoid unauthorized disclosure, misuse and alteration, which otherwise results in liability. In addition, coercive pressure originating from other organizations on which an organization is dependent is another force influencing the organization's security investment rationale and risk analysis. In particular, contractual agreements specify the security objectives that have to be met by the awarded firm to maintain a contract, thereby affecting not only the organization's rationale for its investments in security controls but also its evaluation of security risks. Thus, we develop the following hypothesis:

H5. Coercive pressure, manifested by perceived pressure from business partners and pressure from regulation, will positively influence ISNA.

We consider the involvement of organizational management in professional security associations and attendance at practitioner security events, such as workshops, symposiums, and conferences, as an important source of normative pressure. Via these interactions, organizations learn about the reasoning behind security initiatives taken by other organizations and professional security standards that are promoted by governments, technology suppliers, and industry associations. These influences, reflecting the current standards of professional networks to which organizations belong, in turn build the foundation for ISNA activities and lay the ground for ISCR deployment. In fact, Hu et al. [30] concluded that professional associations had a pivotal normative influence on the organization's security investments. In particular, through participation in industry and professional security associations, many organizations learn about how to use international standards, such as the ISO 27002 framework, to build their security program and the underlying principles for security initiatives. With their knowledge of institutional norms, as a logical response to uncertainty, management forms beliefs about why their organization should invest in ISCR in the first place. For example, the BS 7799 standard offers information security advice based on ten broad security categories and serves as a starting point for organizations to begin forming a clear information security rationale and an approach to addressing security risks. Apart from pressure arising from involvement in security associations, firms can feel implicitly pressured if their business partners regard security as a priority and make large investments in ISCR. Given that security in an extended enterprise is as good as the weakest link [19], firms can modify their security management practices to make sure that their security investments are in line with those of their partners. Based on all these arguments, we propose that ISNA is influenced by institutional norms that are prevalent in their external environment.

H6. Normative pressure, manifested by perceived level of investment among business partners and exposure to security practices through professional associations and publications, will positively influence ISNA.

We incorporated three control variables, IT capabilities, industry type, and organization size, into our research model. Firms with high levels of IT capabilities are more likely to invest in information security because they are more ready to invest in ISCR. Organizations in the financial sector have more to lose than those in other industries, which results in a higher level of ISCR.

4. Research method

4.1. Measure development

We borrowed existing measurement scales whenever available in the literature. When existing scales are not available, new measures were developed by tightly operationalizing definitions of constructs in this study. Appendix A presents all measurement items. We operationalized ISCR as a second-order construct with three subconstructs: information security technologies, qualified security personnel, and security awareness of organizational users. The second-order construct was modeled as formative so that the three first-order constructs of ISCR were viewed as formative indicators of ISCR. Each of the three subconstructs was measured with its own indicators developed for this study and was modeled as formative as well. The decision to model both the second-order construct and first-order constructs as formative was made in consideration of several decision criteria (e.g., item interchangeability, direction of causality between a construct and its items) [45]. For instance, the three subconstructs used to measure ISCR are not interchangeable because they tap into different aspects of the construct, and dropping one of the subconstructs would influence the meaning of ISCR. Similarly, indicators intended to measure each subconstruct are not interchangeable. For instance, information security technologies were measured with three items intended to capture the extent to which an organization has implemented technical controls to (i) authenticate and authorize an entity to access systems at various layers, (ii) prevent dangerous information from moving between the trusted network inside and the untrusted network outside, and (iii) detect security breaches, such as IDS and audit trails. Because these three items are not interchangeable, it seemed appropriate to model information security technologies as formative.

Mimetic pressure was modeled as reflective and measured with four items developed for the study. Coercive pressure and normative pressure were modeled as second-order constructs with their own subconstructs. We modeled these second-order constructs as formative so that their subconstructs were viewed as formative indicators. Following our conceptualization of coercive

Table 1
Measurement approach.

Construct	Type	Subconstructs	Type	Items
Information security control resources	F	Information security technologies	F	3
		Qualified security personnel	F	3
		Security awareness of organizational users	F	4
Mimetic pressure	R			4
Coercive pressure	F	Business Partner Pressure	R	2
		Government Regulation	R	2
Normative pressure	F	Security investment among partners	R	3
		Exposure	F	3
Internal security needs assessment	F	Security investment rationale	F	6
		Risk analysis	F	4
IT capabilities	F			4

F: formative; R: reflective.

pressure manifested by two subconstructs of business partner pressures and government regulations, we measured each of the subconstructs with multiple items developed for this study. Similarly, following our conceptualization of normative pressure manifested by security investment among business partners and exposure to security practices, we measured each of the subconstructs with multiple items developed for this study. Except for the subconstruct of exposure to security practices, each of the subconstructs was modeled as reflective.

Following our conceptualization of ISNA with two components, we operationalized the construct as a second-order construct with two subconstructs: security investment rationale and risk analysis. Security investment rationale was measured with items asking subjects to indicate the extent of the importance placed on six different decision criteria in justifying security-related expenses in their firm. The six decision criteria were developed for the specific context of this study, but the measurement approach of asking the extent of importance for different decision criteria was borrowed from Chatterjee et al. [11], which measured firms' investment rationale in the context of web technologies. Risk analysis was measured with four items developed for this study. The multiple items were designed to measure the extent to which organizations are involved with risk analysis activities that enable them to understand the security risks facing them. Because items intended to measure security investment rationale and risk analysis tap into slightly different aspects of the constructs, we modeled both security investment rationale and risk analysis as formative.

Finally, we modeled IT capabilities as formative and measured the construct with four items. Three of the items were adapted from Grewal et al. [26], and one additional item was developed for this study. Industry type was measured with a binary variable (1 = financial, 0 = non-financial). Table 1 summarizes our measurement approach for all multi-item constructs[2].

Several faculty members with experience in survey research methods provided their feedback after reviewing the initial version of the measurement items. In their review, particular emphasis was placed on content validity so that they assessed whether the concept of research constructs was operationalized appropriately with our measurement items. Prior to the main survey, we randomly selected a small number of respondents (n = 100) drawn from the sample frame that we used in the main survey. They were invited to participate in the survey, but unlike in the main survey, we asked them to provide feedback about the clarity of the instructions and questions in the questionnaire. Twenty-five respondents completed the questionnaire in the pilot test, leaving some feedback on the questionnaire. Based on their feedback, the questionnaire was slightly modified[3].

4.2. Data collection

The unit of analysis for our study is the individual organization. IT professionals at the managerial level were chosen as survey respondents for their organizations. A professional data collection firm in the United States that has a large number of IT professionals as its panel members provided us with a nationwide sample frame of 1577 IT professionals at the managerial level. Because we had randomly chosen 100 respondents for the pilot test described above, the data collection organization sent an e-mail invitation to the remaining 1477 respondents to participate in a Web-based questionnaire survey. Data were collected by administering a Web-based questionnaire survey because all target respondents in the sample frame have ready access to computers connected to the Internet.

Target respondents of the survey were senior- and mid-level IT managers who were sufficiently knowledgeable about IS security practices and operations in their organization. To reduce desirability bias, which is known as a potential source of common method variance (CMV), we assured the respondents that their responses were completely anonymous. Several steps were undertaken to ensure that our final sample could include only target respondents. First, we asked the data collection company to choose IT professionals only at the managerial level. Second, the email invitation message sent to potential respondents indicated that they could participate in the survey only if they were familiar with the IS security practices and operations of their organizations. Third, at the beginning of the survey, we explicitly communicated the eligibility (i.e., mid- and senior-level IT managers, familiarity with security practices and operations) to potential respondents for participating in the survey[4]. Finally, we took the conservative approach of including in our sample only respondents with job titles that can be clearly classified as those at the mid- or senior-level.

We obtained a total of 409 responses from the main survey, yielding a response rate of 27.7%. As described above, we deleted 117 completed responses in our sample based on job titles reported. We further discarded 51 responses because they had many

[2] Because it is often difficult to make the distinction between formative and reflective constructs, we analyzed our data by re-specifying all the formative constructs into reflective constructs for verification purposes. All path coefficients in the model remained the same in terms of their significance after re-specification ($p < 0.05$).

[3] Their responses were not included in the final sample because of the modifications made after the pilot test.

[4] We found that 114 potential respondents left the survey website without proceeding to the questionnaire. We think that most of them did so because they did not meet the eligibility criteria.

Table 2
Loadings and weights of measurement items.

Factor	Mean	Standard Deviation	Item	Weight	Loading	*t*-Value
Mimetic pressure	4.97	1.24	MMT1		0.935	55.92
			MMT2		0.954	78.47
			MMT3		0.907	30.64
			MMT4		0.954	61.90
Business partner pressure	5.57	1.26	BPP1		0.917	47.47
			BPP2		0.933	83.42
Government regulation	5.86	1.34	GR1		0.939	48.96
			GR2		0.939	43.10
Security investment among partners	4.96	1.28	SIP1		0.904	37.63
			SIP2		0.949	91.11
			SIP3		0.947	61.48
Exposure	5.29	1.40	EXP1	0.451		5.47
			EXP2	0.380		3.80
			EXP3	0.252		3.43
Security investment rationale	5.72	0.94	SIR1	0.241		2.22
			SIR2	0.261		1.71
			SIR3	0.210		1.06[a]
			SIR4	0.327		2.52
			SIR5	0.026		0.18[a]
			SIR6	0.200		1.15[a]
Risk analysis	5.56	1.38	RA1	0.431		2.34
			RA2	0.284		1.51[a]
			RA3	0.211		0.94[a]
			RA4	0.126		0.62[a]
Information security technologies	5.80	1.16	IST1	0.303		3.22
			IST2	0.302		3.12
			IST3	0.483		4.64
Qualified security personnel	5.87	1.20	QSP1	0.450		4.29
			QSP2	0.146		1.48[a]
			QSP3	0.459		4.00
Security awareness of organizational users	5.21	1.37	SKW1	0.251		1.73[a]
			SKW2	0.380		3.98
			SKW3	0.042		0.34[a]
			SKW4	0.429		3.69
IT capabilities	5.86	1.06	ITC1	0.386		1.85
			ITC2	0.316		1.25[a]
			ITC3	0.343		0.90[a]
			ITC4	0.732		3.07

[a] Not significant at the $p < 0.05$ level.

unanswered questions or multiple responses could be obtained from a single organization[5]. Consequently, we obtained our final sample with a total of 241 responses, yielding an effective response rate of 16.3%. As reported in Appendix B, our sample represented a wide array of industries and a fair distribution in terms of size. Organizations in the sample ranged from relatively small firms with total revenue of less than $10 million (18.2%) to large firms with total revenue of more than $1 billion (32.3%). They also varied widely in the number of employees; 27.8% of the organizations in the sample had fewer than 500 employees, while 39.9% of the organizations in the sample reported more than 5000 employees.

It appears that nonresponse bias did not pose a serious concern because no significant differences between the first one-third and last one-third of all respondents were found in the key research variables under study, nor were they found in other variables such as organization size or IT capabilities.

5. Data analysis

The components-based PLS approach was used to evaluate the psychometric properties of the measurement scales and to test research hypotheses. We used Smart PLS version 2.0 for both validating measurement scales and testing the research model. The partial least squares (PLS) approach rather than the covariance-based modeling approach was used because the PLS approach is often considered to optimize the predictive power on the dependent variable (e.g., ISCR in our study). In addition, the PLS approach does not suffer from the model identification issue that often occurs when a research model with formative constructs is analyzed [31].

5.1. Measurement validation

The measurement quality of reflective constructs was assessed by examining several psychometric properties. First, convergent validity was assessed based on individual item loadings and the average variance extracted (AVE). All item loadings were greater than the recommended minimum value of 0.70 [12] (see Table 2), and the AVE for all reflective constructs were greater than the recommended minimum value of 0.50, adequately demonstrating convergent validity (see Table 3). Second, discriminant validity was assessed based on the following two criteria. The square root of the AVE for each reflective construct was larger than the correlations between the construct and other constructs (see Table 3). In addition, the examination of the correlations between items and factor scores for reflective constructs did not reveal cross-loading issues at the individual item (see Table 4). Taken together, the discriminant validity of the scales was adequately demonstrated. Finally, all composite reliability values were greater

[5] We did not ask the name of the organization for which respondents answered the questionnaire so that the respondents would be comfortable in providing sensitive information about their organization. To increase the possibility of including only one response from a single organization in the final sample, we carefully examined the 5-digit zip codes of organizations in the initial sample, their industries, and their sizes. The examination led us to delete four responses in the initial sample.

Table 3
Descriptive statistics, reliability, and correlations of the constructs.

	CR	AVE	MMT	BPP	GR	SIP	EXP	QSP	IST	AOU	SIR	RA	ITC	IDT
MMT	0.97	0.88	0.94											
BPP	0.92	0.86	0.53	0.93										
GR	0.94	0.88	0.52	0.68	0.94									
SIP	0.95	0.87	0.70	0.67	0.61	0.93								
EXP	n/a	n/a	0.58	0.70	0.63	0.68	n/a							
QSP	n/a	n/a	0.49	0.67	0.56	0.55	0.73	n/a						
IST	n/a	n/a	0.51	0.70	0.61	0.56	0.71	0.75	n/a					
AOU	n/a	n/a	0.57	0.65	0.49	0.66	0.71	0.72	0.67	n/a				
SIR	n/a	n/a	0.53	0.67	0.59	0.57	0.71	0.69	0.67	0.65	n/a			
RA	n/a	n/a	0.50	0.65	0.52	0.58	0.77	0.68	0.67	0.70	0.75	n/a		
ITC	n/a	n/a	0.39	0.53	0.49	0.46	0.64	0.72	0.64	0.56	0.59	0.58	n/a	
IDT	n/a	n/a	0.04	0.06	0.14	−0.02	0.06	0.03	0.07	0.01	0.02	0.01	0.00	n/a

MMT = mimetic pressure; BPP = business partner pressure; GR = government regulation; SIP = security investment among partners; EXP = exposure; SIR = security investment rationale; RA = risk analysis; IST = information security technologies, QSP = qualified security personnel; AOU = security awareness of organizational users; ITC = IT capabilities; IDT = industry type; CR = composite reliability; AVE = average variance extracted. Diagonal elements display the square root of AVE for factors measured with reflective items.

than the commonly accepted cutoff value of 0.70 [23], adequately demonstrating scale reliability (see Table 3).

Items used to measure formative constructs do not necessarily correlate to each other because they are posited to create an emergent factor [31]. Hence, measurement validation procedures used above to test psychometric qualities of reflective measures are not applicable to formative measures [12]. Instead, the weight of an item used to measure a formative construct can be used to evaluate the extent to which the item contributes to the formation of its posited underlying factor [12]. Table 2 displays item weights and associated t-values to assess the level of each item's contribution to the overall factor, in addition to descriptive statistics of all constructs including means and standard deviations.

Harman's one factor test was used to examine CMV. We performed an exploratory factor analysis with all the measurement items. A general factor did not emerge that accounts for the majority of the covariance among the measurement items, suggesting that CMV is not a serious threat to this study. We also statistically examined the issue of CMV by adding a latent method factor to the structural model and linked all indicators to the method factor [33]. Because the method factor loadings are not significant and the indicators' substantive variances are substantially greater than their method variances, we concluded that CMV is unlikely to be a serious concern.

5.2. Structural model testing

A structural model was set up by specifying relationships between constructs, as proposed in our research model, and analyzed using the PLS approach to structural equation modeling. A second-order formative factor model was constructed in the structural model for the ISCR construct and its associations with three subconstructs: information security technologies, qualified security personnel, and security awareness of organizational users. Similarly, a second-order formative factor model was constructed for each of the two institutional pressures – coercive and normative pressures – and its associations with subconstructs. A second-order formative factor model was also constructed for ISNA and its associations with its subconstructs. Fig. 2 presents the results of the structural model estimation including standardized path coefficients, their *t*-statistics and significance based on one-tailed *t* tests, and the amount of variance explained (R^2). We employed one-tailed *t* tests because all hypotheses were one directional. The standard errors were computed using the bootstrap resampling method (500 resamples).

Table 4
Loadings and cross-loading for reflective constructs.

	MMT	BPP	GR	SIP
MMT1	**0.938**	0.495	0.509	0.637
MMT2	**0.955**	0.520	0.542	0.661
MMT3	**0.903**	0.492	0.438	0.667
MMT4	**0.954**	0.479	0.476	0.657
BPP1	0.522	**0.925**	0.542	0.673
BPP2	0.457	**0.925**	0.700	0.578
GR1	0.504	0.628	**0.939**	0.545
GR2	0.482	0.633	**0.939**	0.598
SIP1	0.607	0.619	0.572	**0.908**
SIP2	0.685	0.646	0.564	**0.947**
SIP3	0.663	0.628	0.569	**0.946**

We tested hypotheses by assessing the significance of path coefficients and confidence intervals. Based on the significance of path coefficients and confidence intervals (see Fig. 2 and Table 5), all coefficients on hypothesized paths except for the path coefficient from mimetic pressure to ISCR were found to significantly differ from zero ($p < 0.05$ or $p < 0.01$). Hence, we concluded that all hypotheses except H1 were supported[6]. Approximately 78.7% of the variance is explained for ISCR. Weights of subconstructs used as indicators for second-order formative constructs were all significant ($p < 0.01$), suggesting that each of them significantly contributed to the creation of the underlying overall factor. Approximately 67.6% of the variance is explained for ISNA.

To test mediation effects, we removed the mediator of ISNA from the structural model and assessed the significance of the coefficients on direct paths from coercive and normative pressures to ISCR. As reported in Table 6, both of the path coefficients were significant. Next, we added the mediator to the model and examined the significance of several path coefficients to test mediation effects. While the magnitudes were decreased, both of the coefficients on the direct paths (coercive pressure → ISCR and normative pressure → ISCR) remained significant. The path coefficient from ISNA to ISCR was significant, and all the path coefficients from coercive pressure and normative pressure to ISNA were significant. Taken together, we concluded that the effects of both coercive and normative pressures on ISCR are *partially* mediated through ISNA [36].

Additionally, we assessed the indirect effects of coercive and normative pressures through ISNA on ISCR. As reported in Table 7,

[6] As indicated earlier, we deleted 117 responses from the original sample ($N = 358$) to guarantee that our respondents were IT managers only at the mid- or senior-level. We also tested our hypotheses with the data from the original sample. The results of hypothesis testing were the same between the two samples because no changes were found on the significance of path coefficients.

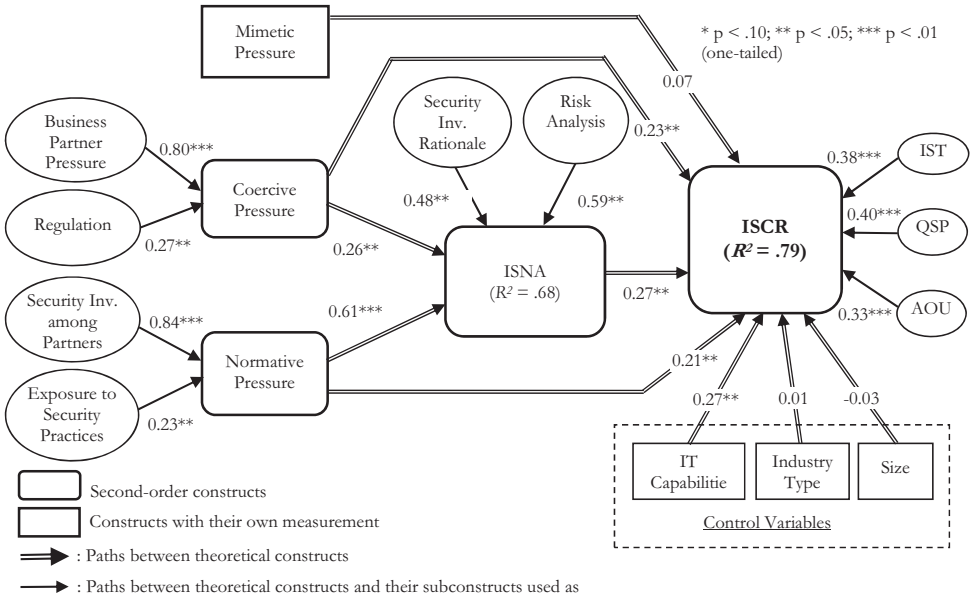

Fig. 2. Results of the structural model testing.

Table 5
Path coefficients, confidence intervals, and hypotheses testing.

Hypothesis	Path	Path coefficient (*t*-value)	Confidence interval	Hypothesis testing
H1	Mimetic pressure → ISCR	0.07 (1.03)	[−0.04, ∞]	Not supported
H2	Coercive pressure → ISCR	0.23** (2.12)	[0.05, ∞]	Supported
H3	Normative pressure → ISCR	0.21** (1.86)	[0.02, ∞]	Supported
H4	ISNA → ISCR	0.27** (2.27)	[0.07, ∞]	Supported
H5	Coercive pressure → ISNA	0.26** (2.10)	[0.05, ∞]	Supported
H6	Normative pressure → ISNA	0.61*** (5.79)	[0.44, ∞]	Supported

** $p < 0.05$.
*** $p < 0.01$ (one-tailed).

Table 6
Summary of mediation effect testing.

Ind. variable	Dep. variable	Mediator	Path without mediator	Coefficient	Path with mediator & coefficient	Coefficient	Testing result
Coercive pressure	ISCR	ISNA	Coercive pressure → ISCR	0.29***	Coercive Pressure → ISCR Coercive Pressure → ISNA ISNA → ISCR	0.23** 0.26** 0.27**	Partial
Normative pressure	ISCR	ISNA	Normative pressure → ISCR	0.34***	Normative pressure → ISCR Normative pressure → ISNA ISNA → ISCR	0.21** 0.61*** 0.27**	Partial

** $p < 0.05$.
*** $p < 0.01$ (one-tailed).

Table 7
Significance of indirect effects.

Indirect effect	Mediated path	Indirect path coefficient	*z* Stat
Coercive pressure → ISCR	Coercive pressure → ISNA → ISCR	0.07	1.63*
Normative pressure → ISCR	Normative pressure → ISNA → ISCR	0.17	2.28**

* $p < 0.10$.
** $p < 0.05$.

the indirect effect of normative pressure was significant ($p < 0.05$); on the other hand, the indirect effect of coercive pressure was marginally significant. Coercive and normative pressures were found to have significant direct effects on ISCR. Hence, we concluded that they have both direct effects and indirect effects through ISNA on ISCR.

We examined the presence of multicollinearity by computing variance inflation factors (VIFs) with the following two regression equations.

$$\text{ISCR} = b_0 + b_1 \times \text{mimetic pressure} + b_2 \times \text{coercive pressure} + b_3 \times \text{normative pressure} + b_4 \times \text{ISNA} + b_5 \times \text{IT capabilities} + b_6 \times \text{financial industry} + b_7 \times \text{organization size} + \text{e1}$$

$$\text{ISNA} = b_0 + b_1 \times \text{coercive pressure} + b_2 \times \text{normative pressure} + \text{e1}$$

VIFs from the estimation of the first regression equation range from 1.03 to 4.21. The estimation of the second regression equation resulted in VIF of 2.50 for both of the two independent variables. Because these values are well below the cut-off value of 5, we have concluded that multicollinearity is not a serious concern.

We performed additional analyses to obtain richer insight on the determinants of ISCR. Specifically, we examined how each of the three dimensions of ISCR is affected by different types of institutional pressures and ISNA. As reported in Table 8, the results of the analyses generally remain the same as those of the original analysis with the second-order factor of ISCR. The extent of ISNA was a strong determinant of each of the three dimensions as well as the second-order factor of ISCR. Mimetic pressure had a marginally significant impact on security awareness of organizational users but did not have a significant impact on information security technologies and qualified security personnel. On the other hand, normative pressure was found to have a significant impact only on security awareness of organizational users.

We examined the possibility of interactions between different types of institutional pressures because it seems plausible to expect that the different types of institutional pressures may interact with each other to affect ISCR. To do so, we added three interaction terms (mimetic pressure × coercive pressure, mimetic pressure × normative pressure, and normative pressure × coercive pressure) to the original structural model and estimated the modified structural model. None of the interaction terms were significant. Similarly, we examined if IT capabilities moderate the effects of ISNA and the three types of institutional pressures on ISCR. We thus added four interaction terms to the original structural model and estimated the modified structural model. None of the interaction terms were significant, suggesting that IT capabilities do not have significant moderating roles.

6. Discussion and implications

6.1. Discussion of the findings

Our study identifies three distinct types of ISCR – information security technologies, qualified information security personnel, and security awareness of organizational users – to provide theoretical explanations of what constitutes a coherent set of organizational resources for information security controls. Specifically, we developed a second-order construct of ISCR with the three types of control resources as subconstructs and a research model to explain why differences exist in the level of ISCR among organizations. We identified three types of institutional pressure and examined their direct and indirect effects through ISNA on ISCR. In particular, consistent with recent developments in institutional theory, we argued that organizations internalize institutional pressures by engaging in ISNA that constitutes risk analysis and security investment rationales.

Normative pressure is found to influence both organizational engagement in ISNA and investment in ISCR. That is, normative pressure not only has an impact on an organization's decision to invest in ISCR but is also effective in formulating a good business case for the investment by establishing a security investment rationale as well as determining how to address the security risks. When an organization makes investments in information security consistent with those of its business partners, it is likely to be recognized as a secure partner, improving its position in the eyes of its partners. Adopting best information security practices promoted by industry or professional security bodies can signal that an organization follows the standards of due care and due diligence [66]. If an organization is faced with legal liability resulting from a security breach, the organization can use its investment as a legal defense and argue that it was not negligent because it followed the best practices, as any prudent organization would do in similar circumstances.

With respect to the direct effect of normative pressure on ISCR, additional data analyses found that normative pressure made a strong impact only on security awareness of organizational users. However, the impact of normative pressure on the other two dimensions, information security technologies and qualified security personnel, were positive, although not statistically significant. Given the significant relationship from normative pressure to information security technologies and qualified security personnel through ISNA, normative pressure seems to exert indirect, rather than direct, influences on these two types of ISCR.

As expected, the results also suggest that coercive pressure influences an organization's decision to invest in ISCR. This result is consistent with the emerging view that government regulations significantly affect organizations' information security practices [20]. For example, firms that use the Control Objectives for Information and Related Technology (COBIT) framework to comply with the U.S. Sarbanes–Oxley Act (SOX) of 2002 should acquire the appropriate technological solutions and human resources and train their users. Further, the results suggest that coercive pressure has a strong effect on ISNA. Coercive pressure from government regulatory agencies and business partners seems to be successful

Table 8
Results of additional data analyses.

	Dependent variable			
	Original model: ISCR (second-order factor)	Model 1: Info. security tech only	Model 2: qualified security personnel only	Model 3: security awareness of organizational users only
Mimetic pressure	0.07	0.03	0.03	0.13*
Coercive pressure	0.23**	0.31**	0.18*	0.11
Normative pressure	0.21**	0.15	0.14	0.31**
ISNA	0.27**	0.20*	0.24**	0.28**
IT capabilities	0.28**	0.23**	0.37***	0.10
Industry type	0.01	0.04	0.01	−0.03
Size	−0.03	0.02	−0.01	−0.10
R^2	0.79	0.65	0.69	0.64

* $p < 0.10$.
** $p < 0.05$.
*** $p < 0.01$ (one-tailed).

in making a business case for organizational investment in ISCR and in determining how to address information security risks.

With respect to the direct effect of coercive pressure on ISCR, our additional analyses revealed that coercive pressure has a significant impact on information security technologies and qualified security personnel but not on security awareness of organizational users. This is presumably because government regulations and requests from business partners generally focus on security technologies and standards. To comply with such government regulations and business partner requests, we would expect that organizations also need to invest in qualified information security personnel with expertise and skills. However, such regulations and requests did not have a direct impact on the extent of security awareness of knowledge workers in our sample organizations.

We did not find strong evidence regarding the effects of mimetic pressure on ISCR. Although mimetic pressure was expected to influence the level of ISCR, the effects are not significant when the effects of other factors, such as coercive and normative pressures, are controlled for. Our findings indicate that coercive and normative pressures predominate in motivating organizational investments in ISCR. Organizations seem to believe that implementing the same solutions as their competitors will not necessarily improve their security problems. Unlike normative and coercive pressures, we proposed that mimetic pressure does not have a strong impact on ISNA. To find empirical evidence for this assertion, we added one path, from mimetic pressure to ISNA, in our structural model. The path coefficient was not significant ($p > 0.10$), confirming our assertion.

Consistent with our expectation, the activity of ISNA has a strong impact on an organization's level of ISCR deployment. The results suggest that organizational decision makers are more likely to invest in ISCR when they conduct a good assessment of their organization's internal security needs by establishing a security investment rationale and focusing on risk analysis. A similar conclusion was reached by Spears [55], who investigated the impact of regulatory pressures, a form of a coercive pressure, on organizations' risk management practices. Her analysis revealed that regulations help formalize *risk management practices*, which correspond to *internal security risk assessment* in our model. Furthermore, she found that *well-defined processes* to address risks and *business participation* in these processes to ensure that strategic and economic considerations inform information security-related decision making contribute to institutionalized risk management practices.

With respect to the effects of the control variables, we find that IT capabilities exert a strong positive influence on the level of ISCR. Interestingly, industry type and organization size have no significant effect in explaining the level of ISCR among organizations. That is, our results indicate that the level of ISCR in organizations can be better explained by the theoretical variables identified in this study rather than by industry type and organization size.

6.2. Theoretical implications

This study makes important contributions to the emerging body of knowledge in organizational security management. First, to the best of our knowledge, this study is the first to offer theoretical explanations, along with empirical support for them, of what constitutes a parsimonious set of ISCR that organizations should possess to improve their security performance. Specifically, it successfully applies the RBV of the firm to conceptualize an organization's ISCR with three types of resources: information security technologies, qualified information security personnel, and security awareness of organizational users.

Second, this study provides theoretical explanations for organizational decisions to invest in ISCR. As one of the first studies in the IS discipline to have built on recent developments in theoretical reasoning from the institutional perspective, we formally propose and test direct and indirect impacts of institutional pressures through ISNA on organizational investment in ISCR. Specifically, our study demonstrated that ISNA, as an organizational response to institutional pressures on security, is a central driver for organizational investment in ISCR. Consistent with our findings, Liang et al. [33] showed that institutional forces influence the assimilation of ERP in organizations directly as well as through top management. A more recent study [44], which investigated the drivers and outcomes of organizational privacy responses in a healthcare context, argued that the impact of institutional pressure on organizational privacy responses is mediated through privacy impact assessment, which is an organizational-level activity. These results underscore the importance of organizational responses to institutional pressure as well as the need for detailed investigations on organizational factors as responses to institutional pressures.

Finally, we found that two types of institutional pressure, normative pressure and coercive pressure, affect the organization's decision to invest in ISCR directly and indirectly through ISNA. By clarifying the role of institutional pressure in organizational security management, our study offered a deeper understanding on the dynamics of organizational motives with regard to investments in ISCR. As one of the first studies in the IS field to develop and empirically test a model by taking a recent development in institutional theory that focuses on heterogeneous responses to institutional pressure through internal management practices among organizations, we believe that this study sheds light on the nature of organizational motives in taking certain IT-related actions.

6.3. Managerial implications

The findings of this study also have several important practical implications for public policymakers, security vendors, and individual organizations. First, public policymakers are advised to keep supporting government-sponsored security groups (e.g., CERT and NIST) and to work closely with professional security associations and councils (e.g., ISSA) to design regulatory rules on security and to promote best security practices for organizations because these groups are likely to be sources of normative pressure. We also recommend that regulatory rules on security focus on all the distinct dimensions of security control mechanisms because the three dimensions constitute a coherent set of ISCR, which can lead to improvements in the security performance of organizations. Despite the recognition that today's information security problems cannot be effectively resolved by *solely* focusing on technology and that the human factor must be part of the framework addressing security issues, organizations seem to remain focused mainly on technology-based solutions to address their security-related issues. Our results fortify the emerging view that information security is not solely about technology and that to ward off security threats, organizations should invest in both technology-based solutions and knowledge-based assets [66]. In this regard, governments should support initiatives such as the Human Firewall Project to promote the importance of an effective mix of the various dimensions of security controls.

Second, because organizational decisions on security investments are strongly influenced by the extent of their exposure to security practices, vendors are advised to actively participate in security associations and to sponsor trade shows, seminars and conferences about information security to promote their solutions.

Another implication for vendors is that they should focus on value chains across organizations to market their security solutions. Because organizations that are interconnected in a value chain, typically through Extranets and VPNs, observe the security investments of their business partners, vendors may need to target the dominant players of the value chain as much as possible. Once a dominant player invests in security controls, other organizations in the value chain will follow the dominant player's lead in security practices because of the normative pressure exerted. The other implication is that, along with the implementation of technology-based products, they should promote the importance of qualified information security personnel and awareness of organizational users and emphasize the potential synergy that products and personnel are likely to create.

Finally, organizations are advised to consider information security as an issue that can be managed with a combined portfolio of control mechanisms consisting of information security technologies, qualified information security personnel, and security awareness of organizational users. For instance, businesses should pay close attention to security education because security education is a major way to inform users about their roles and responsibilities regarding security and to promote appropriate behavior among them.

7. Study limitations

The study is not without limitations. First, while the organizations that our participants work for represent a broad range of industries, they are for-profit organizations. Our data does not include not-for-profit firms. Therefore, the findings of the study should be interpreted accordingly. Motivations for security investment might differ for not-for-profit organizations. For instance, Anthony et al. [2] found that for-profit hospitals are more (less) likely to comply with a mandatory (non-mandatory) rule stipulated in the HIPAA regulation compared to not-for-profit hospitals. Future research should investigate differences in institutional pressures between for-profit and not-for-profit organizations.

Second, the data in our study were collected based on perceptual measures, rather than actual measures, from a single respondent in each organization. Thus, self-selection bias might have been introduced, and thus, the extent of the relationships between research constructs might have been inflated. For instance, we cannot exclude the possibility that respondents who were greatly concerned about security issues in their organizations were likely to participate in the survey and as a consequence inflate relationships between research constructs (e.g., ISNA and ISCR).

Third, our study could have been better, with more elaborate measurement scales. For instance, we measured first-order constructs such as business partner pressure and government regulation with only two items. In general, at least three items are recommended to measure a construct.

Fourth, our data collection effort could have been better if multiple respondents answered the survey questionnaire for an organization. A single respondent of an organization would not be knowledgeable about every aspect of security issues in the organization. For instance, non-IT employees rather than IT employees could have more aptly answered questions that measured research constructs such as security awareness of organizational users.

Finally, we might have omitted some important control variables that are potentially important in explaining the variations of ISCR among organizations. For instance, organizations for which front office business operations are heavily dependent on IT may need to invest in ISCR to a great extent. For such organizations, IT plays a critical role in supporting interactions with customers (e.g., sales, marketing, and customer support). Thus, security issues in their IT systems could have huge negative impacts on their revenue and reputation. On the other hand, when IT is simply viewed as a supporting technology in the back office, organizations may invest less in ISCR. Our study could have been strengthened if the effects of such variables were controlled for.

8. Future research directions

This study offers several avenues for future research. One avenue for future research is to empirically investigate the link between ISCR and security performance. It seems that such an investigation, while of great importance, poses formidable challenges for researchers. One reason is the lack of reliable metrics in measuring the security performance of organizations. It is difficult or impossible to use traditional performance metrics in an information security context. Thus, we first need to develop security-specific performance metrics to assess the effect of ISCR on security performance. Additional challenges to investigating the link between ISCR and security performance include the fact that firms are reluctant, in general, to reveal their security performance to others, and even if they are willing to do so, they may not be aware of all the successful security breaches that have taken place.

Another interesting research direction is to identify factors that may strengthen (or weaken) the relationships between institutional pressure or ISNA and ISCR of organizations. For instance, the impact of institutional pressure and ISNA on ISCR examined in this study may vary depending on whether an organization is an upstream member or downstream member in a supply chain. Similarly, it would be interesting to examine whether the impact of ISCR on the security performance within organizations varies depending on the types of security threats (e.g., internal vs. external security threats), the interconnectivity of an organization's information systems, etc.

9. Concluding remarks

Despite the growing importance of information security, our understanding of organizational approaches to managing IS security remains rudimentary. In particular, this study answered a fundamental question regarding what constitutes ISCR and why variations exist in the level of ISCR among organizations. We offered theoretical explanations for both of the questions and gave strong empirical support for our arguments. Nonetheless, we cannot exclude the possibility that other theoretical perspectives could better answer the question. As with other organizational management practices explained by a variety of theoretical perspectives, IS researchers are expected to identify other theoretical perspectives and apply them to the subject. We hope that this paper will stimulate academic interest in the subject and pave the way for a research stream that extends our knowledge on IS security management.

Appendix A. Measurement items

Note: Except for the security investment rationale and risk analysis, all constructs were measured on seven-point scales with items anchored with strongly disagree to strongly agree.

A.1. Mimetic pressure

1. Our competitors have made large investments in security during the past three years.

2. Our competitors are currently making large investments in security.
3. Security is currently among the highest IT spending priorities of our competitors.
4. Our competitors have deployed large resources for security controls during the past three years.

A.2. Business partner pressure

1. Our ability to do business with our business partners is related to our level of security.
2. It is important for us to comply with the security standards required by our business partners.

A.3. Government regulation

1. It is important for our firm to comply with government regulations on security.
2. There are severe penalties for noncompliance with government regulations on security.

A.4. Security investment among partners

1. Our business partners have made large investments in security in the past.
2. Security is among the highest IT spending priorities of our business partners.
3. Our business partners have deployed large resources for security controls.

A.5. Exposure to security practices

1. We actively participate in industry or professional security bodies in which we are or have been exposed to best security practices.
2. We diligently follow security publications, newsletters, e-mail lists, and Internet websites and are therefore constantly exposed to the best security practices.
3. We regularly attend trade shows, seminars, and conferences about security to be exposed to the best security practices.

A.6. Information security technologies

1. Our firm has the technical mechanisms to authenticate and authorize the entity accessing system at the network, host and application layers, such as access control software, smart cards, and biometrics.
2. Our firm has the technical controls to prevent dangerous information from moving between the trusted network inside and the untrusted network outside, such as firewalls and email filtering.
3. Our firm has the technical controls to detect security breaches, such as IDS and audit trials.

A.7. Qualified security personnel

1. We have personnel with higher credentials to define our information security program.
2. We have personnel with higher credentials to install and maintain technical security controls, such as firewalls and IDS.
3. We have personnel with higher credentials to obtain and evaluate information security notices, such as bug reports and security alerts, issued by vendors, government agencies, and/or professional associations.

A.8. Security awareness of organizational users

1. Most employees consider security to be part of their everyday responsibilities.
2. Most employees receive adequate training in relevant security topics, such as appropriate use of the Web, physical access, and incident response.
3. Most employees consider that keeping computer systems up-to-date with patches, virus definitions, etc. improves information security.
4. Most employees are aware of the consequences and sanctions that will result from a breach of security, intentional or otherwise.

A.9. IT capabilities

1. Our firm has strong IT planning capabilities.
2. Our firm has skilled IT staff.
3. Our firm has the knowledge necessary for deploying IT applications.
4. Our firm is experienced in deploying IT applications.

A.10. **Security investment rationale** *(seven-point scales, anchored with none to very great)*

1. Meeting return on investment (ROI) criteria.
2. Meeting changing business requirements.
3. Preventing potential liability.
4. Retaining customers' goodwill.
5. Preventing productivity loss.
6. Preventing damage to information assets.

A.11. **Risk analysis** *(seven-point scales, anchored with none to extensively)*

1. We assess the security risks of information assets in our firm.
2. We develop a list of information assets we need to protect.
3. We identify a list of threats our information assets are exposed to.
4. We prioritize our information assets based on their risk levels.

Appendix B. Profiles of respondents and responding organizations

	Frequency	Percentage
Profiles of respondents		
Senior level IT managers: CEO, VP of IS, CIO, CTO	44	18.3
Middle level IT managers: director of IT/MIS, senior IT/IS manager, director of IT services, IT manager, IT infrastructure manager, compliance manager, information systems assurance manager	197	81.7
Total	241	100.0
Industry groups		
Consumer products	9	3.7
Electronics	8	3.3
Financial services	50	20.7
Hospitality	6	2.5
Information technology	85	35.3
Industrial products	12	5.0

Appendix B (*Continued*)

	Frequency	Percentage
Pharmaceutical/medical/Bio-Tech	21	8.7
Retail/wholesale	23	9.5
Transportation	9	3.7
Others (automotive, printing/publishing, chemicals, etc.)	18	7.5
Total	241	100.0
Annual sales revenue (in US$)		
$1 million–$5 million	21	8.7
$5 million–$10 million	23	9.5
$10 million–$50 million	31	12.9
$50 million–$200 million	30	12.4
$200 million–$500 million	26	10.8
$500 million–$1 billion	32	13.3
$1 billion–$5 billion	36	14.9
More than $5 billion	42	17.4
Total	241	100.0
Number of employees		
Fewer than 100	30	12.4
100–499	37	15.4
500–999	24	10.0
1,000–4,999	54	22.4
5000–10,000	32	13.3
More than 10,000	64	26.6
Total	241	100.0

References

[1] M.P. Adler, A unified approach to information security compliance, EDUCASE Rev. 41 (5), 2006, pp. 46–59.
[2] D.L. Anthony, A. Appari, M.E. Johnson, Institutionalizing hipaa compliance: organizations and competing logics in U.S. Healthcare, J. Health Soc. Behav. 55 (1), 2014, pp. 108–124.
[3] R. Baskerville, Risk analysis: an interpretive feasibility tool in justifying information systems security, Eur. J. Inf. Syst. 1 (2), 1991, pp. 121–130.
[4] N. Beck, P. Walgenbach, Technical efficiency or adaptation to institutionalized expectations? The adoption of ISO 9000 standards in the german mechanical engineering industry Organ. Stud. 26 (6), 2005, pp. 841–866.
[5] A.S. Bharadwaj, A resource-based perspective on information technology capability and firm performance: an empirical investigation, MIS Q. 24 (1), 2000, pp. 169–196.
[6] F. Bjorck, Institutional theory: a new perspective for research into IS/IT security, in: Proceedings of the 37th Hawaii International Conference on System Sciences, Big Island, Hawaii, USA, 2004.
[7] E. Boxenbaum, S. Jonsson, Isomorphism, diffusion and decoupling, in: R. Greenwood, C. Oliver, K. Sahlin, R. Suddaby (Eds.), The Sage Handbook of Organizational Institutionalism, (vol. 1), Sage, Thousand Oaks, CA, USA, 2008.
[8] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. 34 (3), 2010, pp. 523–548.
[9] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of Internet security breach announcements on market value: capital market reaction for breached firms and Internet security developers, Int. J. Electron. Com. 9 (1), 2004, pp. 69–105.
[10] H. Cavusoglu, B. Mishra, S. Raghunathan, The value of intrusion detection systems (IDSS) in information technology (IT) security, Inf. Syst. Res. 16 (1), 2005, pp. 28–46.
[11] D. Chatterjee, R. Grewal, V. Sambamurthy, Shaping up for e-commerce: institutional enablers of the organizational assimilation of web technologies, MIS Q. 26 (2), 2002, pp. 65–89.
[12] W.W. Chin, The partial least squares approach to structural equation modeling, in: G.A. Marcoulides (Ed.), Modern Methods for Business Research, Lawrence Erlbaum Associates, London, 1998, pp. 295–336.
[13] S. Collett, Forecast 2014: How to Wring Value from Your IT Budget, Computerworld, September, 2013.
[14] R. Courtney, Security risk assessment in electronic data processing, in: Proceedings of the AFIPS Conference NCC, Arlington, VA, USA, 1977.
[15] Deloitte Touche, 2005 Global Security Survey, Deloitte Touche, London, UK, 2005.
[16] G. Dhillon, J. Backhouse, Information system security management in the new millennium, Commun. ACM 43 (7), 2000, pp. 125–128.
[17] G. Dhillon, J. Backhouse, Current directions in IS security research: towards socio-organizational perspectives, Inf. Syst. J. 11 (2), 2001, pp. 127–153.
[18] P.J. DiMaggio, W.W. Powell, The iron cage revisited—institutional isomorphism and collective rationality in organizational fields, Am. Sociol. Rev. 48 (2), 1983, pp. 147–160.
[19] S. Dynes, H. Brechbuhl, M.E. Johnson, Information security in the extended enterprise: some initial results from a field study of an industrial firm, in: Proceedings of the Workshop on Economics of Information Security, Boston, MA, 2005.
[20] E&Y, Global Information Security Survey 2005: Report on the Widening Gap, E&Y, 2005.
[21] R. Fisher, Information Systems Security, Prentice Hall, Englewood Cliffs, NJ, 1984.
[22] R. Garud, C. Hardy, S. Maguire, Institutional entrepreneurship as embedded agency: an introduction to the special issue, Organ. Stud. 28 (7), 2007, pp. 957–969.
[23] D. Gefen, D. Straub, M. Boudreau, Structural equation modeling and regression: guidelines for research practice, Commun. Assoc. Inf. Syst. 4 (7), 2000, pp. 1–77.
[24] R.M. Grant, Contemporary Strategy Analysis, Blackwell Publishers, Boston, MA, 2005.
[25] K.E. Greenaway, Y.E. Chan, Theoretical explanations for firms' information privacy behaviors, Commun. AIS 6 (6), 2005, pp. 171–198.
[26] R. Grewal, J. Corner, R. Mehta, An investigation into the antecedents of organizational participation in business-to-business electronic markets, J. Marketing 65 (3), 2001, pp. 17–33.
[27] A.E. Harris, N. Perlroth, N. Popper, H. Stout, A sneaky path into Target customers' wallets, N.Y. Times (January), 2014, http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html?_r=0.
[28] E.A. Harris, N. Perlroth, N. Popper, Neiman Marcus data breach worse than first said, N.Y. Times (January), 2014, http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html.
[29] H.A. Haveman, Follow the leader—mimetic isomorphism and entry into new markets, Admin. Sci. Q. 38 (4), 1993, pp. 593–627.
[30] Q. Hu, P. Hart, D. Cooke, The role of external and internal influences on information systems security—a neo-institutional perspective, J. Strategic Inf. Syst. 16 (2), 2007, pp. 153–172.
[31] C.B. Jarvis, S.B. MacKenzie, P.M. Podsakoff, A critical review of construct indicators and measurement model misspecification in marketing and consumer research, J. Consum. Res. 30 (2), 2003, pp. 199–218.
[32] B.G. King, T. Felin, D.A. Whetten, Finding the organization in organizational theory: a meta-theory of the organization as a social actor, Organ. Sci. 21 (1), 2010, pp. 290–305.
[33] H.G. Liang, N. Saraf, Q. Hu, Y.J. Xue, Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management, MIS Q. 31 (1), 2007, pp. 59–87.
[34] L. Loh, N. Venkatraman, Diffusion of information technology outsourcing: influence sources and the Kodak effect, Inf. Syst. Res. 3 (4), 1992, pp. 334–358.
[35] F.J. Mata, W.L. Fuerst, J.B. Barney, Information technology and sustainable competitive advantage: a resource-based view, MIS Q. 19 (4), 1995, pp. 487–504.
[36] J.E. Mathieu, S.R. Taylor, Clarifying conditions and decision points for mediational type inferences in organizational behavior, J. Organ. Behav. 27 (8), 2006, pp. 1031–1056.
[37] N. Melville, K. Kraemer, V. Gurbaxani, Information technology and organizational performance: an integrative model of IT business, MIS Q. 28 (2), 2004, pp. 283–322.
[38] S.J. Mezias, An institutional model of organizational practice: financial reporting at the fortune 200, Admin. Sci. Q. 35 (3), 1990, pp. 431–457.
[39] K.D. Mitnick, W.L. Simon, The art of Deception: Controlling the Human Element of Security, Wiley, Indianapolis, IN, 2002.
[40] NIST, An introduction to computer security, NIST-800-12 Handbook, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, 1995.
[41] NIST, Risk management guide for information technology systems, NIST-800-30 Handbook, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, 2001.
[42] NIST, Building information technology security awareness and training program, NIST-800-50 Handbook, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, 2003.
[43] C. Oliver, Strategic responses to institutional processes, Acad. Manage. Rev. 16 (1), 1991, pp. 145–179.
[44] R. Parks, C. Chu, H. Xu, L. Adams, Understanding the drivers and outcomes of healthcare organizational privacy responses, in: Proceedings of the Thirty Second International Conference on Information Systems, Shanghai, 2011.
[45] S. Petter, D. Straub, A. Rai, Specifying formative constructs in information systems research, MIS Q. 31 (4), 2007, pp. 623–656.
[46] J. Pfeffer, G. Salancik, The External Control of Organizations: A Resource Dependence Perspective, Harper and Row, New York, NY, 1978.
[47] T.C. Powell, A. Dent-Micallef, Information technology as competitive advantage: the role of human, business and technology resources, Strategic Manage. J. 18 (5), 1997, pp. 375–405.
[48] P.W. Roberts, R. Greenwood, Integrating transaction cost and institutional theories: toward a constrained-efficiency framework for understanding organizational design adoption, Acad. Manage. Rev. 22 (2), 1997, pp. 346–373.
[49] J.W. Ross, C.M. Beath, D.L. Goodhue, Developing long-term competitiveness through IT assets, Sloan Manage. Rev. 38 (1), 1996, pp. 31–42.
[50] W.R. Scott, Institutions and Organizations, Sage, Thousand Oaks, CA, 2001.
[51] W.R. Scott, J.W. Meyer, The Organization of Societal Sectors, Sage, Beverly Hills, CA, 1983.
[52] A. Segev, J. Porra, M. Roldan, Internet security and the case of bank of America, Commun. ACM 41 (10), 1998, pp. 81–87.
[53] M. Siponen, A. Vance, Neutralization: new insights into the problem of employee information systems security policy violations, MIS Q. 34 (3), 2010, pp. 487–502.
[54] J. Son, Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies Inf. Manage. 48 (7), 2011, pp. 296–302.
[55] J.L. Spears, Institutionalizing Information Security Risk Management: A Multi-method Empirical Study on the Effects of Regulation, The Pennsylvania State University, Pennsylvania, 2007 (Ph.D. Dissertation).
[56] D. Straub, Effective IS security: an empirical investigation, Inf. Syst. Res. 1 (3), 1990, pp. 255–276.
[57] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, MIS Q. 22 (4), 1998, pp. 441–469.
[58] M.P. Suby, The 2013 (ISC)2 Global Information Security Workforce Study, 2013 Last accessed at: ⟨https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf⟩.

[59] H.H. Teo, K.K. Wei, I. Benbasat, Predicting intention to adopt interorganizational linkages: an institutional perspective, MIS Q. 27 (1), 2003, pp. 19–49.
[60] N. Tisdale, Visa Security Standards, SANS Institute, Bethesda, MD, 2002.
[61] P. Tolbert, Institutional environments and resource dependence: sources of administrative structure in institutions of higher education, Admin. Sci. Q. 30 (1), 1985, pp. 1–13.
[62] C.M. Trompeter, J.H.P. Eloff, A framework for implication of socio-ethical controls in information security, Comput. Secur. 20 (5), 2001, pp. 384–391.
[63] M. Wade, J. Hulland, The resource-based view and information systems research: review, extension, and suggestions for future research, MIS Q. 28 (1), 2004, pp. 107–142.
[64] B. Wernerfelt, A resource-based view of the firm, Strategic Manage. J. 5 (2), 1984, pp. 171–180.
[65] M.E. Whitman, Enemy at the gate: threats to information security, Commun. ACM 46 (8), 2003, pp. 91–95.
[66] M.E. Whitman, H.J. Mattord, Management of Information Security, Course Technology, Boston, MA, 2004.