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