Technological Forecasting & Social Change xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Technological Forecasting & Social Change

Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital

Ye Hou [a], Ping Gao [b,*], Brian Nicholson [c]

[a] Lancaster University, Lancaster, United Kingdom
[b] School of Environment, Education and Development, University of Manchester, Manchester, United Kingdom
[c] Alliance Manchester Business School, University of Manchester, Manchester, United Kingdom

ARTICLE INFO

Article history:
Received 4 August 2015
Received in revised form 13 March 2017
Accepted 15 March 2017
Available online xxxx

Keywords:
China
Hospital
Information security management (ISM)
Institutional theory
Organisational response strategy
Regulative pressures

ABSTRACT

This paper advances existing theoretical understanding of the factors impacting upon organisational responses to regulative pressures in the process of information security management (ISM). Drawing on institutional theory, we conduct a case study of ISM in a Chinese hospital. A theoretical framework is presented, which proposes that organisational response strategies devised in response to regulative pressures are determined jointly by internal organisational incentives and external government supervision and enforcement. Practical implications for policymakers to promote organisational ISM are given and suggestions for future research based on the theoretical findings of the case study are provided.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

Recent decades have witnessed the broad application of information systems in society. The introduction of information systems presents security challenges, with myriad examples of information security failures causing significant financial losses and potential damage to the reputation of the organisations concerned (Norton, 2012). For example, in April 2011, the Sony PlayStation Network faced a series of hack attacks on three of its gaming systems, resulting in the theft of confidential information of over 77 million customers, including unencrypted bank accounts, purchase histories, passwords and billing addresses. This incident resulted in Sony suffering an estimated loss of $20 million in revenue, as a result of a two-week service breakdown; and a $32 billion loss was incurred as a result of losing control of customer data (Mawani, 2011). Sony was also castigated for putting the personal and financial data of numerous customers at risk, with Sony UK fined $395,000 by the UK Information Commissioner for the breach of Data Protection Act (BBC, 2013). In the healthcare sector, which is the focus of this article information security is the most critical issue in the operation of information systems, as the data that is stored and processed is particularly sensitive (Masrom and Rahimly, 2015). It is clear that if sensitive medical information, such as mental health history, is accessed by unauthorised users, the subsequent infringement of patient privacy could have serious consequences for the individual concerned (Win, 2005). Healthcare providers therefore have a duty to maintain the confidentiality of patients' data, and failing to do so may incur expensive fines and lawsuits. For example, in July 2013, the health company WellPoint was fined $1.7 million by the U.S. Department of Health and Human Services for allowing the medical and other personal information of hundreds and thousands of people to be publicly accessible via the Internet. Additional recovery actions, such as legal actions, new security control investments, extended credit protection services for victims and other related costs, pushed the cost to approximately $142 million (Filkins, 2014); while in March 2014, Stanford Hospital and Clinics, based in California, USA, was fined $4 million for allowing 20,000 patient records to be accessed via the Internet (Green, 2015).

Evidence to date has shown that the majority of failures in information security, especially in the healthcare sector (Masrom and Rahimly, 2015), arise as a result of human and organisational factors (Chang and Ho, 2006). A range of issues, including poor management (Wood, 1995), ignorance on behalf of top and middle management (Straub and Welke, 1998), employees' misuse of information systems (Siponen, 2000), a failure to comply with information security policy (Stanton et al., 2005), and the lack of an organisational information security strategy (Bakari et al., 2007) have each been shown to directly or indirectly precipitate information security failures. In response, information security

* Corresponding author.
E-mail addresses: y.hou2@lancaster.ac.uk (Y. Hou), ping.gao@manchester.ac.uk (P. Gao), brian.nicholson@manchester.ac.uk (B. Nicholson).

http://dx.doi.org/10.1016/j.techfore.2017.03.023
0040-1625/© 2017 Elsevier Inc. All rights reserved.

management (ISM) offers procedures and standards to protect information systems from unauthorised access and protect information from disclosure, disruption, modification, or destruction (Cazemier et al., 2000). As early as in 2008, Spagnoletti and Resca called for the urgent introduction of efficient ISM in organisations, asserting that information security failures cannot be solved solely by applying mechanisms such as firewalls and anti-virus software. Furthermore, it is clear that information security is not only an issue of individual and organisational behaviours, but also a matter for governments and regulative bodies. Existing studies highlight that the political power utilised by governments (Smith et al., 2010), coupled with regulative pressures (Hsu et al., 2012) impact upon organisational decision-making with regard to ISM activities. In terms of institutional theory (Oliver, 1991; Scott, 2001), government authorities often exert regulative pressures on organisations in relation to their ISM functions, and organisations are required to comply with such pressures. This case study focuses on the organisational responses arising from the regulative pressures on ISM.

In accordance with institutional theory, organisations may not always meet governmental demands and fully comply with the regulative pressures (Oliver, 1991). The failure to adhere to regulative demands is found to be a major factor in information security failure (Hsu et al., 2012; Stanton et al., 2005), although existing research to date emphasises compliance (Ransbotham and Mitra, 2009; Safar and Clark, 2009). Adding to the extant knowledge on the role of government in organisational ISM, this paper considers levels of organisational conformity, ranging from full compliance to the non-compliance behaviours of organisations. Our research question is: How do organisations respond to regulative pressures on ISM and why?

Bjorck (2004) highlights that institutional theory offers a means to explain organisational behaviours in response to the regulative pressures of ISM. Adopting an institutional perspective, we answer the research question through the use of a case study of a Chinese public hospital. To date, the majority of research into ISM has been conducted in the context of developed countries. However, developing countries are playing an increasingly important role in information security, and hence present an interesting research focus for ISM scholars. Furthermore, information security in developing countries is faced with severe challenges due to their poor legal infrastructure and weak legal systems (Gao, 2005; Luo, 2003; Yildirim et al., 2011), with calls for improved theoretical guidance on their ISM practices (Economic and Social Commission for Asia and Pacific, 2007). Due to the scale of its adoption of information systems, China is an excellent area for research, as it is prone to tremendous threats to its information security. In recent years, the Chinese government has made important efforts in providing a secure environment for the operation of its information systems, highlighting effective ISM as one of the most critical issues in its initiative of national informatisation (State Council, 2006); taking a number of steps to ensure that ISM is prioritised, especially in the public sector. Informatisation is the production and use of ICT hardware, software, and services (Kraemer and Dedrick, 1994). However, despite this, ISM in China still lags far behind that of developed countries. In 2012, a survey revealed that in most Chinese organisations, information security protection did not meet business requirements, and that government intervention in organisational ISM was ineffective (PWC, 2012).

The rest of the paper is organised as follows. In Section 2, we review the ISM literature, focusing on ISM research from an institutional perspective. In Section 3, we define ISM processes, introduce the concepts of institutional pressures and organisational response strategies, and develop our analytical framework for the case study. In Section 4, we present the research design and research method. Sections 5 details the case study. In the final sections, we outline the theoretical findings and draw practical implications from the case study, and discuss the research limitations and possible future research directions.

2. Literature review

Information security is the term used to describe the confidentiality, integrity and availability of information (Bishop, 2003). In recent years there has been recognition of the limited reliability of technologies such as firewalls and anti-virus software to protect information security, leading to a growing emphasis on ISM (Choobineh et al., 2007; Siponen, 2000). ISM provides an organisational management approach to the prevention of malicious information security breaches, designed to ensure the provision of an acceptable level of information confidentiality (von Solms, 1996).

ISM aims to offer “the development of a security management programme including the security policy, management committee, team structure, risk management, and employee education to preserve the confidentiality, integrity, and availability of information in organisations” (Hsu et al., 2012; p.3). Given its importance, we would argue that ISM is relevant to every part of an organisation, and is influenced by panoply of external actors, including governments (ISO/IEC, 2005). Despite this, the majority of the ISM literature currently considers the individual level, for example, considering employees' misuse of information systems (Hovav and D'Arcy, 2012), and failure to comply with information security rules (Guo et al., 2011; Johnston and Warkentin, 2010).

Kraemer et al. (2009) point to the need for a deeper understanding of organisational behaviours in ISM in a specific institutional context. In response, this paper focuses on the organisational level of ISM, which is largely ignored in the literature. In the limited extant research on organisational ISM, institutional theory offers a unique view of the rational and irrational behaviours of organisations in reaction to regulative rules (Bjorck, 2004). However, the current institutional research on organisational ISM has two key weaknesses. Firstly, ISM is a process consisting of a set of control activities concerning the management of people, policies, projects, programmes, technology facilities, and resources (Cazemier et al., 2000; Dhillon and Backhouse, 2001). Due to the complexity of the ISM process, previous research has focused on specific stages and particular aspects of ISM, failing to provide a comprehensive perspective. For example, Backhouse et al. (2006) find that a rising concern over information security breaches has triggered the initiative of developing information security standards, which shape the configuration of information systems and influence how information systems are used and managed. Hu et al. (2007) demonstrate how institutional forces shape the process of ISM system implementation in organisations; and Hsu et al. (2012) emphasise the influence of institutional pressures on the adoption and assimilation of new ISM methods.

Secondly, existing research largely focuses on the compliance phenomenon and the acquiescence strategy of organisations. For example, Smith et al. (2010) argue for an information security standard devised as an institution established by government and requiring obligatory compliance by organisations. Hu et al. (2007) analyse the mandatory compliance to a single regulative pressure: the Sarbanes-Oxley Act (2002), in the ISM system implementation stage; with both largely ignoring the fact that in reality organisations may challenge existing institutional requirements and use response strategies other than acquiescence (Silva and Backhouse, 2003); including compromise, avoidance, defiance and manipulation, as suggested by Oliver (1991). Overall, the literature lacks a holistic view of the interactions that occur between organisations and the regulative environment in the ISM process.

In this paper we draw upon institutional theory to conduct a case study of the whole ISM process, considering how an organisation responds using a mix of different strategies, each presenting varying levels of conformity to regulative pressures. Institutional theory allows us to analyse the interaction of organisations with external social structures (Scott, 2001; Zucker, 1983), providing a lens to explain how organisations respond to the regulative effects demanded by government on

متن کامل مقاله ← دریافت فوری

ISIArticles
مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات