Understanding Organisational Responses to Regulative Pressures in Information Security Management: The Case of a Chinese Hospital

Ye Hou
Lancaster University
Email: y.hou2@lancaster.ac.uk

Ping Gao (corresponding author)
School of Environment, Education and Development
University of Manchester
Email: ping.gao@manchester.ac.uk

Brian Nicholson
Alliance Manchester Business School
University of Manchester
Email: brian.nicholson@manchester.ac.uk

Understanding Organisational Responses to Regulative Pressures in Information Security Management: The Case of a Chinese Hospital

Highlights

- We present a case study of information security management in a Chinese hospital.
- We focus on the organisational strategies of response to regulative pressures.
- The determinants are governmental enforcement and organisational self-awareness**.**
- A framework of organisational responses to regulative pressures is developed.
- Practical implications and directions for future research are discussed.

Understanding Organisational Responses to Regulative Pressures in Information Security Management: The Case of a Chinese Hospital

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.

Keywords: China, hospital, information security management (ISM), institutional theory, organisational response strategy, regulative pressures

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 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 is also a matter for governments and regulative bodies. Existing studies highlight that the political power utilised by governments (Smith, Winchester and Bunker, 2010), coupled with regulative pressures (Hsu, Lee and Straub, 2012) impact upon organisational decision-making in 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, Lee and Straub, 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, Lee and Straub, 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, Carayon and Clem (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, Overbeek and Peters, 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, Hsu and Silva (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, Hart and Cooke (2007) demonstrate how institutional forces shape the process of ISM system implementation in organisations; and Hsu, Lee and Straub (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, Winchester and Bunker (2010) argue for an information security standard devised as an institution established by government and requiring obligatory compliance by organisations. Hu, Hart and Cooke (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 their ISM strategies. Organisations in developing and emerging economies, where the legal systems often do not function efficiently, are more likely to challenge or ignore government demands on ISM than those in developed countries (Yildirim et al., 2011). With this in mind, and with a paucity of similar research, China provides a suitable research setting for us to consider the determinants of different levels of organisational conformity to regulative pressures, while also addressing the urgent need for ISM research in developing and emerging economies. In 2011, the Norton

Global Information Security Survey claimed that the worldwide financial losses that year directly attributable to information security breaches amounted to some $114 billion, with almost half ($46 billion) occurring in China. That same year, India and Brazil lost around $16 billion in total, and Europe lost approximately $16 billion (Norton, 2012). In our review of 24 leading journals relevant to ISM, we found only two articles that investigated ISM in emerging economies, and therefore it is clear that research on ISM in China is of timely and significant academic and practical interest.

3. Theoretical Framework

3.1. The ISM Process

The ISM process consists of five stages: strategy formation and goal setting for information security, information security policy (ISP) making, information security awareness (ISA) training, implementation of security mechanisms and policies, and the evaluation, monitoring and improvement of the process (ISO/IEC, 2005). An ISM initiative starts when an information security strategy is devised supported by a set of information security protection goals, which should align with the wider business strategy of the organisation (Hsu, 2009). ISP provides direction and support to organisational ISM (Knapp et al., 2009), while ISA training aims to educate organisational employees to comply with ISP in their everyday use of information systems (Puhakainen and Siponen, 2010; Straub and Welke, 1998). When an ISP is enforced effectively, influenced by organisational, environmental, and behavioural factors (Herath and Rao, 2009), an information security system will be implemented to protect digital assets from the threat posed by various technological or human forces. Information security monitoring is responsible for tracking the security status and detecting potential breaches in information security, while the term information security evaluation refers to the internal and external audits carried out to determine security performance. The results of such evaluations provide the basis for information security managers to monitor an organisation's security status and take any necessary action to improve information security.

3.2. Institutional Pressures and Organisational Responses

Institutional theory asserts that organisations inhabit an institutional environment comprised of three pillars: cultural-cognitive, normative, and regulative institutions (Scott, 2001). The cultural-cognitive institutional pillar emphasises the influence of culture as the context that shapes cognition. The normative pillar is based on agents' social obligations, which are observable through values and norms, while normative rules define the actors' behaviour through "prescriptive, evaluative and obligatory" values and norms (Scott, 2001, p. 54). The regulative pillar addresses how actors' behaviours are constrained and regulated under coercion by rules and laws and the fear of sanctions. In summary, Scott proposes that institutional pressures are comprised of control mechanisms exerted by cultural-cognitive, normative, and regulative structures (institutions) each designed to constrain actors' behaviour (Gosain, 2004; Mignerat and Rivard, 2009).

In this paper we focus on one of Scott's (2001) three pillars, the impact of regulative institutions situated in a specific legal environment. A review of the literature reveals that there are two kinds of regulative pressures that are particularly relevant to ISM in Chinese organisations. One area of regulative pressure is laws and regulations, which describe the set of rules instituted by government or other legislative authorities that seek to constrain the behaviour of organisations and individuals. Chinese organisations are subject to different levels of laws and regulations (Gao, 2005; Luo, 2003). In the healthcare sector, at a national level, the National People's Congress issued the Criminal Law on February 28th, 2009; while at an industry level, the Ministry of Health issued the Decree No. 66 - Administrative Measures for Internet Medical and Health Information Services, on July 1st, 2009. In addition, each province devises its own information security regulations for local healthcare organisations. Information security standards are technical regulations that organisations are required to comply with. In September 1999, the Ministry of Public Security issued GB 17859-1999, the Computer Information Systems Security Protection Classification regarded as the most important national information security standard (GB is the acronym of *Guojia Biaozhun*, which in Chinese means national standard). It offers a set of terminologies for ISM system design, implementation and

evaluation for every Chinese organisation. Another important standard, GB/T 19716-2005, the Code of Practice for Information Security Management (later replaced by GB/T 22081-2008) issued by State Bureau of Quality Technical Supervision and the Standardisation Administration in October 2005. It provides national guidelines for ISM practice. In addition, hospitals are required to comply with all relevant local standards issued by their local government.

Another area of regulative pressure is national policy, which provides advisory legislation, guidelines and codes of practice for organisations (Ku, Chang and Yen, 2009; Sundt, 2006). On March 16th, 2006 the Chinese State Council promulgated the National Eleventh Five-Year Plan (2006-2010), which called on all organisations to address their ISM and strengthen their information security infrastructure. On May 8th, 2006 the State Council issued the National Informatics Development Strategy (2006-2020), calling on organisations to devise ISPs and improve their ISM.

Oliver (1991) identifies five organisational strategies in response to institutional pressures, as illustrated in Table 1. In order of level of conformity to institutional pressures, these strategies are acquiescence, compromise, avoidance, defiance and manipulation. The acquiescence strategy implies full conformity, and the actions of an organisation employing an acquiescence strategy may include habitation, taking institutional requirements for granted; or imitation, where other organisations are consciously or unconsciously mimicked, or suggestions from industry experts are universally accepted.

Table 1 Organisational Response Strategy to Institutional Pressures

Strategies	Tactics	Examples
Acquiesce	Habit	Following invisible, taken-for-granted norms
	Imitate	Mimicking institutional models
	Comply	Obeying rules and accepting norms
Compromise	Balance	Balancing the expectations of multiple constituents
	Pacify	Placating and accommodating institutional elements
	Bargain	Negotiating with institutional stakeholders
Avoidance	Conceal	Disguising nonconformity
	Buffer	Loosening institutional attachments
	Escape	Changing goals, activities, or domains
Defiance	Dismiss	Ignoring explicit norms and values
	Challenge	Contesting rules and requirements
	Attack	Assaulting the sources of institutional pressures
Manipulation	Co-opt	Importing influential constituents
	Influence	Shaping values and criteria
	Control	Dominating institutional constituents and processes

Source: adopted from Oliver (1991); cited in Modell (2001)

To adopt compromise and avoidance strategies illustrates a moderate level of conformity to institutional pressures. Specifically, to adopt a compromise strategy is to try to "balance, pacify or bargain with" external pressures (Oliver, 1991; p. 153). To balance external pressures requires organisations to partially meet institutional expectations, to pacify means organisations intend to achieve the minimum institutional expectations; while to bargain requires organisations to negotiate with an institutional entity regarding its expectations. When adopting an avoidance strategy, an organisation appears to comply with institutional rules but in fact tries to "reduce and escape" them (Oliver, 1991; p. 154). In this instance, organisations do not actually comply with institutional rules, but rather attempt to show 'symbolised' acceptance of institutional pressures (Meyer and Rowan, 1977). Organisations may design an action plan in response to institutional pressures but not implement it; may decouple institutional attachments to minimise external inspection; or change

organisational goals and activities in order to escape the rules imposed by external entities (Modell, 2001).

The defiance and manipulation strategies outlined in Table 1 are nonconformity responses, where organisations deliberately resist institutional rules. When defiance occurs, an organisation ignores or even challenges institutional rules, while manipulation involves co-opting, influencing or controlling institutional expectations to align with organisational interests. By co-opting the source of the pressure, for example by persuading an institutional constituent to join the organisation, the organisation seeks to neutralise institutional opposition and enhance its legitimacy. By influencing institutional rules, an organisation shapes the design of institutional norms, values and expectations; and by controlling such rules; organisations establish power and dominance over the external constituents applying pressure upon them (Oliver, 1991).

3.3. Analytical Framework

Our research considers the organisational responses to the regulative pressures present in the ISM process. Based on the review of the literature, our analytical framework is illustrated at Figure 1. The ISM process consists of a number of stages and activities, including the formation of an information security strategy and security goal setting, ISP making, ISA training, the implementation of security techniques, and the evaluation and improvement of the adopted strategy (ISO/IEC, 2005). During the ISM process, an organisation encounters regulative pressures in the shape of laws, regulations and national policies. At this point, organisations respond with the strategies of acquiescence, compromise, avoidance, defiance, or manipulation (Oliver, 1991).

Strauss and Corbin (1990) propose to understand social interactions between organisations and their environment by considering both the internal rationale for and the external constraints on the interactions, and therefore we link internal incentives and the external enforcement of the pressures to organisational response strategies.

Ma, Schmidt and Pearson (2009) posit that an organisation has incentives to comply with the regulative pressures deemed to fit within its business objectives; an organisation may choose to adopt a modest level of conformity or nonconformity to a regulative pressure when it conflicts with the business objectives of the organisation (Oliver, 1991). Furthermore, Hechter, Opp and Wippler (1990) argue that an organisation decides how to respond to a particular regulative pressure by balancing the associated rewards and penalties for abiding by or breaking it. Thus it is argued that organisations may selectively comply with regulatory pressures as balanced against the strength of enforcement of the rules by regulators, and therefore an organisation may choose to not fully comply with regulatory pressures that are weakly enforced by government, meaning that nonconformity is likely (Oliver, 1991).

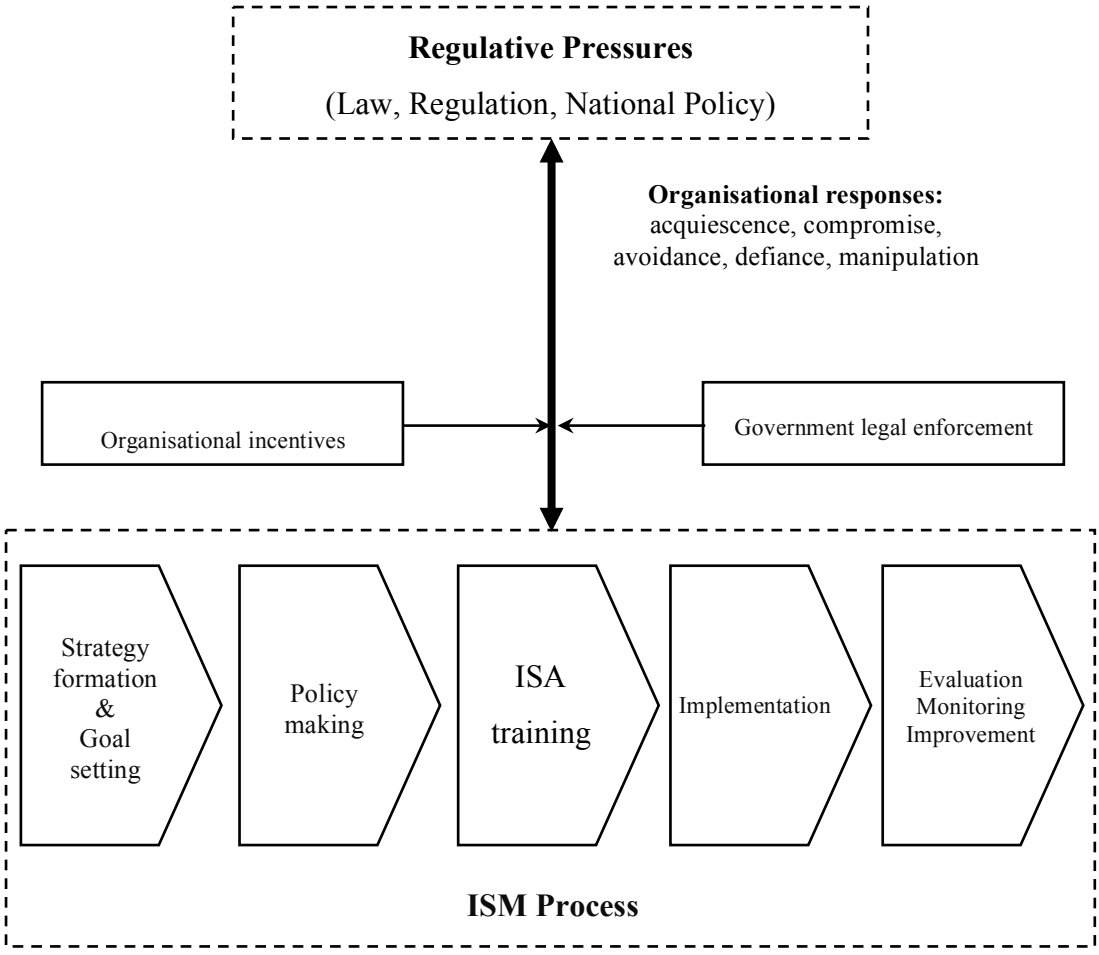

Figure 1 Analytical Framework:
Organisational Responses to Regulative Pressures in the ISM Process

4. Research Methods

As the research framework outlined in Figure 1 shows, our aim is to explore the impact of internal incentives for compliance and the external enforcement of regulative pressures on organisational response strategy. In doing so, we adopt an in-depth case study method, which is widely viewed as appropriate for addressing "how" and "why" questions (Yin, 2008); and is particularly suited to our objective to understand how and why organisations respond to regulative pressures in the ISM process. The focus of our case is Dynasty Hospital (a pseudonym), a public hospital in China. In China, government actors are afforded direct control over public organisations (Gao, 2005; Luo, 2003), meaning that government intervention in ISM may be greater than in the private sector, and thus the sector would be expected to be more compliant to government pressures in relation to ISM, and therefore should be better equipped than private sector organisations to comply with regulative requirements regarding ISM. Our case study of a public hospital can improve understanding about the challenges that the governments face when promoting ISM in a developing country context, allowing us to draw important theoretical insights and provide likely implications on ISM.

The analytical framework at Figure 1 provides the 'sensitising theory' to guide the collection and analysis of data (Klein and Myers, 1999). Furthermore, the, framework adheres to the basic elements of case study research design as outlined by Yin (2008), providing as it does the research question, the unit of analysis, the requirements for the data, and the rules of analysis. Specifically, our research unit of analysis is the organisational response strategies to regulative pressures moderated by organisational incentives and regulative enforcement. Following this framework, in the data collection stage we have delineated the process line of ISM in Dynasty Hospital into five stages, and identified the key milestones and critical activities at each stage. We have also collected data on regulative pressures, be they laws, government regulations or national policies; the response strategies of the case organisation; and other relevant internal and external factors impacting upon organisational ISM behaviours.

To ensure we achieved a holistic view, we collected data from different sources (Markus et al., 2006). The websites and archives of Dynasty Hospital and relevant authorities were useful to obtain background information and the ISM history of the hospital, and to identify the regulative pressures on ISM in China, particularly those impacting upon Dynasty Hospital. During March 2011 and February 2012, we visited the case organisation on four separate occasions, each time for between two and four weeks (see Table 2). During these fieldtrips, we made direct observations. For example, in April 2011, we were in the research setting for one month, spending some 4-6 hours each day observing the common information security problems that emerged in different departments, and the solutions offered by the Information Centre to overcome them. In each visit to the hospital we also conducted semi-structured interviews, each being held in a private environment and lasting for approximately one hour. After each round of interviews, we maintained contact with our informants by email and telephone in order to clarify our understanding of regulative pressures and organisational responses during the data analysis phase. All interview data was recorded, translated into English and transcribed. When selecting interviewees, we identified actors that were knowledgeable about ISM practices and their context, and who were representative of the key ISM stakeholders in the case hospital. The interviewees include administrative staff, doctors and nurses in their role as end-users: as well as ISP makers, security implementation and maintenance engineers, and information systems managers. These interviewees were also demographically representative of the employee population of the hospital. Specifically, our interviewees from the case hospital included 12 males and 7 females, aged from their mid 20s (one nurse) to their early 60s (one doctor), with the majority aged between mid- 30s to late 40s. The interviewees' length of employment varied from five to 32 years. In terms of education level, one nurse had a college diploma, the Chief Information Systems Officer and two doctors held PhD degrees, and the other participants held bachelor or masters degrees. Outside the hospital, we interviewed two technicians from an information security product contractor, who were able to provide information on the ISM system in the case hospital as well as more general information security techniques. To aid our understanding of the policy context surrounding ISM, we also interviewed one officer from the local Shannxi Provincial

Health Bureau in charge of information security regulation, and two Chief Information Systems Officers in other two hospitals located in the same province.

Table 2: Interview Arrangements

Time period	Topics covered	Informants (Unless specified, all from Dynasty Hospital)
February and March 2011 (2 weeks)	• History of ISM development • Perceptions of ISM • ISM status in healthcare sector	• Chief Information Systems Officer • 2 Technicians from an information security product contractor • Head, Software Centre • Head, Hardware Centre • Head, Database Centre
April 2011 (4 weeks)	• Regulative forces in China's healthcare sector • Examples of ISM failure • Healthcare informatisation and the ISM development process • Organisational response to regulative forces • Perceptions of ISM from middle and senior management	• Chief Information Systems Officer • Director, Information Centre • 1 Administrator, Development Division • Vice Head, Information Steering Committee • Head, Software Centre • Head, Hardware Centre • Head, Database Centre • 2 Technicians from an information security product contractor • Officer, Public Health Department, local Provincial Health Bureau • 2 Chief Information Systems Officers in 2 hospitals in the same province
October and December 2011 (2 weeks)	• ISP and information security / ISM regulations • External and internal influences	• Chief Information Systems Officer • Director, Information Centre • 1 Administrator, Development Division • Vice Head, Information Steering Committee
January and February 2012 (3 weeks)	• Employees' perception of information security • Employees' security behaviour • ISA training and education	• Chief Information Systems Officer • 2 Doctors, Clinical Registration Office • 1 Doctor and 3 Nurses, Inpatient Registration Office • 3 Doctors, Clinic Department • 3 Doctors, Inpatient Department

The objective of data analysis is to understand organisational response strategies to regulative pressures in different stages of the ISM process. Using the analytical framework outlined in Figure 1, we have developed our understanding regarding the choices made by Dynasty Hospital of response strategies by exploring the relevant internal reasons (incentives) and external contextual factors (enforcement) (Strauss

and Corbin, 1990). Data regarding ISM processes, organisational response strategies and organisational incentive and regulative enforcement factors were coded chronologically and by ISM stage in the transcripts, and analysed in two steps. In the first step, we investigated key information security incidents, regulative pressures and the organisational responses in each ISM stage that occurred between 2001 and 2012. In the second step, we categorised the internal incentives to comply with ISM, along with the external enforcement of regulative pressures that impacted upon the organisational response at different stages of the ISM process. In an attempt to avoid bias; data triangulation and investigator triangulation were conducted (Yin, 2008). The results of data triangulation are shown in Table 3. Data were interpreted, refined and tested along with the research, and discussion meetings were held among the authors from China and Europe, each of who are experts in information systems in China's public sector and/or information security.

Table 3: Data Collection and Triangulation

Data	**Data collection methods**	**Date Source 1 (interviews)**	**Data Source 2 (documents)**	**Data Source 3 (observations)**
Regulative pressures	Interviews; Documents; Observations	• Chief Information Systems Officer • Director of Information Centre • Administrator in Development Division • Vice Head, Information Steering Committee • Heads of Software Centre, Hardware Centre, Database Centre • An Officer, local Provincial Health Bureau • 2 Chief Information Systems Officers at 2 local hospitals	Information security laws, regulations, policies, standards (see Appendix)	4 informatisation development meetings; 2 information systems evaluation meetings
Organisational responses to regulative pressures	Interviews; Documentations; Observations	• Chief Information Systems Officer • Director of Information Centre • Administrator in Development Division • Vice Head, Information Steering Committee • Heads of Software Centre, Hardware Centre, Database Centre	Hospital documents (organisational policies, roles, and responsibilities of the hospital)	4 informatisation development meetings; 2 information systems evaluation meetings; 4 weeks of daily observations (9am- 5pm) (April 2011)
ISM process (7 stages)	Interviews; Documents; Observations	• Chief Information Systems Officer • Director of Information Centre • Administrator in Development Division • Heads of Software Centre, Hardware Centre, Database Centre • 2 Technicians from an information security contractor • 9 Doctors in different departments • 3 Nurses, Inpatient Registration Office	Hospital documents (ISM development history)	4 informatisation development meetings; 4 weeks of daily observations (9am- 5pm) (April 2011); 3 weeks of daily observations (9am- 5pm) (January and February 2012)
Information security incidents	Interviews; Documents	• Chief Information Systems Officer • Director of Information Centre • 3 Doctors from Inpatient Department	Hospital internal documents (failure reports); Information systems logs	
External and internal influences	Interviews; Observations	• Chief Information Systems Officer • Director of Information Centre • Administrator in Development Division • Vice Head, Information Steering Committee • Officer, local Provincial Health Bureau • 2 Chief Information Systems Officers at 2 local hospitals		4 informatisation development meetings; 2 information systems evaluation meetings; 2 weeks of daily observations (October and December 2011)

5. The Case Study: Regulative Pressures on ISM and the Responses of Dynasty Hospital

State-owned Dynasty Hospital is a leading medical research centre and healthcare facility in Xi'an, the capital city of Shannxi Province located in the west of China. It has 16 functional departments consisting of 67 divisions, and employs some 1200 staff. The Information Centre is responsible for information systems operation and ISM. This centre is comprised of five divisions: the Network Centre, the Software Centre, the Hardware Centre, the Database Centre and the Patients Case Centre. Dynasty Hospital began a programme in mid 2001 to deploy information systems throughout the hospital and to use information systems in its business operations. The first stage of this work was finished in mid 2003, when the hospital established its clinical information systems but did not implement information security mechanisms. By the end of 2005, the IS infrastructure was established and the hospital had constructed its own Intranet. As information systems were rolled out and used in everyday tasks, information security incidents began to emerge and the hospital started to focus on information security protection and pay attention to ISM. In this section, we apply the analytical framework introduced at Figure 1 to investigate each stage of the ISM process at Dynasty Hospital. Specifically, we present Dynasty Hospital's selection of response strategies by examining their internal rationale and external regulative pressures. The results are summarised in Table 4.

Table 4: Organisational Responses to Regulative Pressures on ISM in Dynasty Hospital

ISM Process	Regulative Pressures	Organisational Responses
Strategy formation and goal setting	• Regulations: Decree No. 27, 136, 147; National Standard GB 17859-1999 • National Policy: National Healthcare Informatisation Policy 2003-2010; National Informatisation Strategy 2006-2020	Defiance at the outset when there is no government inspection; followed by acquiescence when government inspection is scheduled. Originally deemed as being of low interests to the organisation.
Policy making	• Laws and Regulations: Criminal Law National Standards GB 17859-1999, GB 4943-1995, GB 9361-88 • National Policies: National Healthcare; Informatisation Policy 2003-2010; National Informatisation Strategy 2006-2020	Compromise Defiance, acquiescence Defiance. Deemed as not offering clear information regarding what should be considered when designing the ISP
Awareness training	• Regulations: Decree No. 27, 136 National Standards GB 17859-1999, GB/T 20269-2006 • National Policy: National Healthcare Informatisation Policy 2003-2010; National Informatisation Strategy 2006-2020	Avoidance at the outset. Deemed as not useful to the organisation. Acquiescence after security incidents occurred. Then viewed as of high interest to the organisation Strict enforcement by government
Implementation	• Laws and Regulations: Decree No. 51, 136, 147 National Standards GB 17859-1999, GB/T 20270-2006, GB/T 20273-2006, GB/T 20272-2006, GB/T 20281-2006; • National Policies: National Healthcare; Informatisation Policy 2003-2010; National Informatisation Strategy 2006-2020	Acquiescence with or without the government enforcement Of high interest to the organisation
Monitoring, evaluation, improvement	• Laws and Regulations: Decree No. 27, 66, 136, 147 National Standard GB 17859-1999 • National Policy: National Healthcare Informatisation Policy 2003-2010; National Informatisation Strategy 2006-2020	Defiance at the outset, when no government inspection, and acquiescence once inspection was scheduled Initially viewed as being of low interests, before later the attitude changed

5.1. Strategy formation and goal setting

The information security strategy of an organisation represents its plan for information security goals, policies and actions (Beebe and Rao, 2010). Information security goals establish what an organisation should expect to achieve when protecting information security in any given time period (ISO/IEC, 2005). As discussed in Section 1, the government and regulatory authorities in China have introduced a number of laws and regulations regarding information security over the past two decades. All have urged public organisations including hospitals to devise an information security strategy and to set clear information security protection goals and objectives. However, according to the Chief Information Systems Officer at Dynasty Hospital, at the time this legislation was being introduced, the hospital's top priority was building their information systems infrastructure and ensuring that it would function efficiently. As a consequence, the hospital chose to adopt a defiance strategy in response to these national policies and regulations.

This changed when the local Provincial Health Bureau released Decree No. 136 on September 8th, 2008. This decree set the criteria for healthcare informatisation for hospitals in this province, which contained a requirement for hospitals to devise an information security strategy. Crucially, the Provincial Health Bureau established a timetable for field inspections in every hospital to check their compliance with this regulative pressure. As suggested by Hechter, Opp and Wippler (1990), such a measure of government supervision would prove effective, as it included direct consequences for reward or punishment. At this point, Dynasty Hospital moved to an acquiescence strategy. The Chief Information Systems Officer said:

> We chose to comply closely with the government supervision and have our information security strategy and goals in writing, as we do not want to be set as the bad example in ISM for peer hospitals, which would damage our reputation.

From late 2008, Dynasty Hospital introduced ISM as an important part of its information systems operation, with senior management emphasising the importance of information security strategy design. At this point, the hospital devised a five-year programme to meet its ongoing information security goals, which according to the Director of the Information Centre were mainly based on State Council Decree No. 147 issued in February 1994, Regulation on Safety Protection of Computer Information Systems. Following Article 3 of this decree, Dynasty Hospital defined its information security goals as being

> to enforce the safety of information systems and the operation, the safety of computer and its complementary sets of equipment, facilities and network, the safety of operating environment, and the safety of patient and hospital information; to safeguard the normal performance of information systems functions.

5.2 Policy Making

As discussed above, ISP provides the ISM direction for an organisation and defines the positive and negative behaviours of information systems usage. ISP is regarded as an important part of ISM in the healthcare sector (Stahl, Doherty and Shaw, 2012). An effective ISP is characterised by its breadth, clarity and brevity in contents (Goel and Chengalur-Smith, 2010), although ISP making is often restricted by an organisation's information security strategy and goals; and therefore when this security strategy and goals change, the ISP must be modified accordingly (ISO/IEC, 2005). However, in the case of Dynasty Hospital, the decision to prioritise the production of the ISP meant that the ISP design was completed in

late 2007, whilst the strategy and goals were incomplete. According to the Director of the Information Centre, this was done with the aim of normalising employee behaviour when using information systems in order to prevent breaches in information security. At the same time, and following the work of Karyda, Kiountouzis and Kokolakis (2005), the Chinese government exerted control over the organisation's ISP by enacting laws and regulations but without imposing any associated enforcement measures. In designing their ISP, Dynasty Hospital deliberately adopted only those parts of the regulations that it believed useful for guiding their ISM practice. For example, Dynasty Hospital adopted a compromise strategy to the Criminal Law. Article No. 286, which stipulates that "any person who deletes, amends, adds or disturbs functions and causes the malfunctions of a computer information system shall be sentenced fixed-term imprisonment". Correspondingly, the Dynasty Hospital's ISP states "anyone violating the Criminal Law, Article No. 286, should be recorded a demerit conduct, or dismissed from job, or be prosecuted if the consequence is serious", while other parts of the law were ignored.

It is therefore clear that Dynasty Hospital intended to adopt only selected security standards for its ISP. For example, the hospital took a defiance strategy to national security standard (GB 17859-1999) on information security classification. According to the Head of the Software Centre, this standard was not of benefit to the hospital when formulating its ISP, as it was perceived as too complex to follow and did not offer specific guidance for ISP making. In contrast, Dynasty Hospital included standards GB 4943-1995 - Safety Requirements for Information Techniques Facilities, and GB 9361-88 - Safety Requirements for Computer Centre Field into its ISP, as these standards were concerned with physical security issues, which were useful to the hospital when constructing its information infrastructure, and therefore in this instance an acquiescence strategy was adopted.

National information security policies provide guidance for organisations when developing policies (Knapp et al., 2009). Specifically, the National Healthcare Informatisation Policy 2003-2010 and National Informatisation Strategy 2006-2020 defined the targeted macro environment of information security in the required period, which were not considered when Dynasty Hospital designed its ISP. The Director of the Information Centre explained its defiance strategy to us as follows: "we need something solid to help us design the specific and useful ISP for our hospital, but these national policies only give us a direction for the future".

5.3. ISA Training

ISA aims to widen the understanding of the importance of information security and the recognition of potential information security risks by both organisations and individuals (Bulgurcu, Cavusoglu and Benbasat, 2010). ISA also includes ISP awareness, as an organisation's ISP will only be effective if the individuals working within an organisation are aware of and comply with it (Puhakainen and Siponen, 2010). ISA training can improve users' awareness of and further compliance to ISP, and ensure ISM effectiveness (Straub and Welke, 1998; Tsohou et al., 2010). However, Chinese information security laws and regulations rarely mention ISA, although the National Healthcare Informatisation Policy 2003-2010 highlighted that hospitals should pay attention to ISA training in order to improve individuals' basic information security knowledge and skills. Furthermore, in Decree No. 136, the local Provincial Health Bureau specified the time and scope of ISA training for relevant hospitals, and noted that the ISA training programme for hospitals would be inspected. With

this in mind, Dynasty Hospital initiated its ISA training programme in March 2009, six months before the scheduled inspection, although the hospital showed only a symbolic acceptance of institutional pressures (Meyer and Rowan, 1977), and 'disguising nonconformity' (Oliver, 1991, p. 154). In terms of institutional theory as outlined in Table 1, Dynasty Hospital took an avoidance strategy. The Chief Information Systems Officer explained to us:

> We realised ISA training was useful to prevent security breaches by our employees who lacked knowledge of information security and information systems usage. This issue was that these regulations and rules did not specify how to do the training. We were not ready to organise such kind of trainings at that time. But we had to show the government we have done something. We have only organised several simple lectures to the end-users. Our curriculums were tailored to this group of trainees, almost entirely on technologies like virus software usage, firewall protections and physical layer security. Most of the people coming to the training were from our centre. Our doctors, nurses and administrators told us they were too busy with routine medical care to spare time for attending the trainings. Top-level managers were not involved in the training programme, though they should be core training subjects for their medical background lacking basic knowledge on information systems and information security.

Consequently, the training introduced was of very limited use, and ISP compliance by employees could not be successfully achieved. This was demonstrated by the occurrence of a system failure soon after the ISA training programme was complete, which was caused by the introduction of a virus imported via a memory stick brought into the organisation by a member of staff. When interviewed, it was discovered that she knew nothing about computer viruses and the potential consequences of virus attack. As part of our research, we also interviewed a number of medical staff that had attended the ISA training, and they told us that they felt that the training had been a waste of time.

Following the 2009 government inspection, at the end of 2011 Dynasty Hospital reorganised their ISA training programme. The emergence of system failures caused by user misuse and the increasing number of incidents exposing patients' medical information alerted the hospital to the importance of ISA and led them to re-examine the relevant regulative pressures. The hospital took an acquiescence strategy to relevant regulations, national standards and national policy, choosing to work with security professionals from external organisations to greater understand the usefulness of the regulative requirements. Consequently, a new training programme was designed and implemented based on the ISA training and education requirements and the guidelines of State Council Decree No. 27 issued in September 2003 - Regulations on Strengthen Information Security Protection, the National Informatisation Strategy 2006-2020, and national standards GB 17859-1999 and GB/T 20269-2006.

5.4. The Implementation of Information Security Techniques

By 2007, Dynasty Hospital had installed anti-virus software and a firewall on its computer hardware, and had installed air-conditioning and digital locks to enhance the safety of its computer facilities. At the end of 2008, with breaches in information security becoming increasingly prevalent in China, the organisation decided to institute further measures to meet emerging security challenges and more rigorous government inspections. According to the Chief Information System Officer of Dynasty Hospital, along with an interviewee from a company involved in the hospital's ISM system implementation; the selection of the information security mechanisms represented an acquiescence strategy employed in response to the legal requirements for information security protection. Hospital management believed that these mandatory requirements provided useful information regarding the level of

information security protection required and how this could best be achieved. Dynasty Hospital drew upon Decree No. 147, which stipulates the information security standard that organisations should achieve, and Decree No. 51 (Computer Virus Protection Measures for the Administration), which was issued by the Ministry of Public Security on April 26th, 2000, and which stipulates that every organisation should implement anti-virus protection measures, and use authorised security products and services. As seen previously, Dynasty Hospital once again adopted an acquiescence strategy to the mandatory information security standards in relation to information security implementation, including GB/T 20270-2006 on network systems, GB/T 20281-2006 on firewalls, GB/T 20273-2006 on database management systems, and GB/T 20272-2006 on operating systems.

5.5. Monitoring, Evaluation and Improvement

The monitoring, evaluation and improvement of ISM aims to track ISM operations in an organisation, evaluate its effectiveness in meeting the planned organisational goals and objectives in relation to information security, and to improve where appropriate previous activities in order to achieve better results in the future (ISO/IEC, 2005). The Chinese National Informatisation Strategy 2003-2010 placed a requirement upon organisations to conduct such ISM monitoring, evaluation and improvement, but Dynasty Hospital adopted a defiance strategy to it. According to the Director of the Information Centre, for a long time the hospital did not have any mechanisms for monitoring information security, in part due to a lack of awareness of its importance, while at the same time, the government requirements were deemed unhelpful in instituting monitoring practices.

This situation changed when the hospital was given notice of a government inspection, due to take place in 2009. Decree No. 136 set clear criteria for the inspection of healthcare information, requiring all hospitals to have in place security monitoring systems, well-established evaluation processes, and relevant procedures to institute any necessary improvements. Set against the backdrop of a growing number of breaches in information security in China, Dynasty Hospital acknowledged that the regular monitoring and evaluation of its information security was a necessity, and at this point the hospital switched to an acquiescence strategy in response to the regulative pressures on information security, monitoring and evaluation. As a consequence, the hospital President agreed to invest in security monitoring systems, and in September 2008, the Hospital Information Steering Committee initiated three-month checks, half-year checks and annual check on the performance of the hospital's network security, information integrity and availability, user behaviour and server security; culminating in a thorough examination of the security weaknesses and vulnerabilities of the hospital's information systems at the end of that year. The evaluation was largely guided by the Ministry of Healthcare Decree No. 66, and the Chinese Computer Information Systems Security Protection Classification Standards (GB 17859-1999). As evidence of its improvement, by mid 2010, Dynasty Hospital had formalised its ISA training methods, using the National Informatisation Strategy 2006-2020 as its guidance; and by the end of 2011, a new version of the ISP was released, which provided greater detail about the security procedures and security requirements of the organisation, in accordance with Decree No. 27 and Decree No. 147. According to some doctors and nurses, Dynasty Hospital has increased its efforts in tackling information security threats, although as the Chief Information Systems Officer remarked: "ISM improvement needs time. Now Dynasty Hospital can only meet some of the requirements by the regulations

and national policies. We have a long way to go and we need to continuously improve our ISM".

6. Discussion: Organisational Responses to Regulative Pressures

6.1. Organisational Incentives, Regulative Enforcement and Organisational Conformity

Our case study adds to the limited existing literature that seeks to explain organisational conformity with regulative pressures from the perspective of internal incentives (Ma, Schmidt and Pearson, 2009), or external enforcement (Hechter, Opp and Wippler, 1990). An organisation's awareness of the importance of particular regulative pressures on its ISM is an important factor in selecting an appropriate response strategy. The more useful a regulative pressure is deemed to be to the protection of information security of an organisation, the higher conformity strategy the organisation will adopt. As observed in this research, Dynasty Hospital had relatively high awareness of the role of technical solutions in its protection of its information security, and therefore adopted high conformity with the regulations and policies that required the introduction of technical solutions. For example, in the implementation stage, Dynasty Hospital adopted an acquiescence strategy to Decree No. 51, which required the establishment of anti-virus measures, GB/T 20270-2006 on the standard of network systems, GB/T 20281-2006 on firewall standards, GB/T 20273-2006 on database management techniques, and GB/T 20272-2006 on operating systems techniques. In contrast, at the beginning of the ISM process, the hospital chose a defiance strategy in response to some national policies, for example the National Healthcare Informatisation Policy 2003-2010,

which required public organisations to devise an information security strategy and set goals for information security protection. At this point, these requirements did not align with the existing plans of Dynasty Hospital, which gave information security strategy and goals a low priority. Similarly, at the policy making stage, Dynasty Hospital took a defiance strategy to national security standard GB 17859-1999, which it believed did not offer specific enough guidance on ISP making. However, the hospital adopted an acquiescence strategy to standards GB 4943-1995 and GB 9361-88, which were useful for the hospital when designing its policy on physical security. In relation to ISA training, Dynasty Hospital first selected an avoidance strategy, believing that the regulations requiring ISA were of no interest to the organisation, as they failed to offer specifications in relation to how to organise the necessary training. Similarly, at the beginning of the security monitoring and evaluation stage, the government's regulative requirements were regarded as unhelpful and thus a defiance strategy was implemented. Interestingly, in both these phases of the ISM process, the hospital later adopted an acquiescence strategy, in response to a breach in information security caused by user misuse; at a time when such incidents were becoming increasingly common in China. Widespread concern about lapses in information security alerted Dynasty Hospital to the importance of regulative requirements on ISA training and information security monitoring and evaluation, and precipitated this change in strategic response.

It is clear that there is a positive relationship between the strength of government enforcement of regulations and the level of conformity from organisations. In China, the government not only enacts the policies, laws and regulations that guide social actors' behaviours, but also acts as a legitimate coercion institution. Government actors may intervene directly in organisational responses to regulations and exert supervision enforced by penalties in the event of infringement (Gao, 2005; Luo, 2003). All state-controlled Chinese organisations are

subject to regular inspections and subsequent assessments by the government on the progress of their informatisation initiatives. In the case of Dynasty Hospital, government supervision moderates organisational decisions on the strategies adopted in response to regulative pressures. For example, in the stages of information security strategy formation and the setting of goals; and security monitoring and evaluation, Dynasty Hospital switched from a defiance strategy to an acquiescence strategy in response to relevant regulative requirements when the organisation's management knew that a poor government inspection result would be followed by the imposition of sanctions. This study has found that whilst government supervision is likely to compel organisations to comply with laws, regulations and policies, weak legal enforcement without involving an associated penalty or potential for a loss of reputation is the key determinant for the adoption of non-compliance strategies (such as defiance).

6.2. A Framework to Determine the Organisational Strategies Employed in Response to Regulative Pressures

As discussed above, awareness by organisations regarding the importance of relevant legislation to its information security protection impacts upon organisational conformity. The selection of a response strategy is likely impacted upon by the strength of legal enforcement employed by the government. By considering both the existing literature and the empirical insights offered by this research on the impact of organisational incentives and regulative enforcement on organisational conformity with regulative requirements, it is possible to develop a theoretical framework that categorises the organisational response strategies to regulative pressures (as shown in Figure 2).

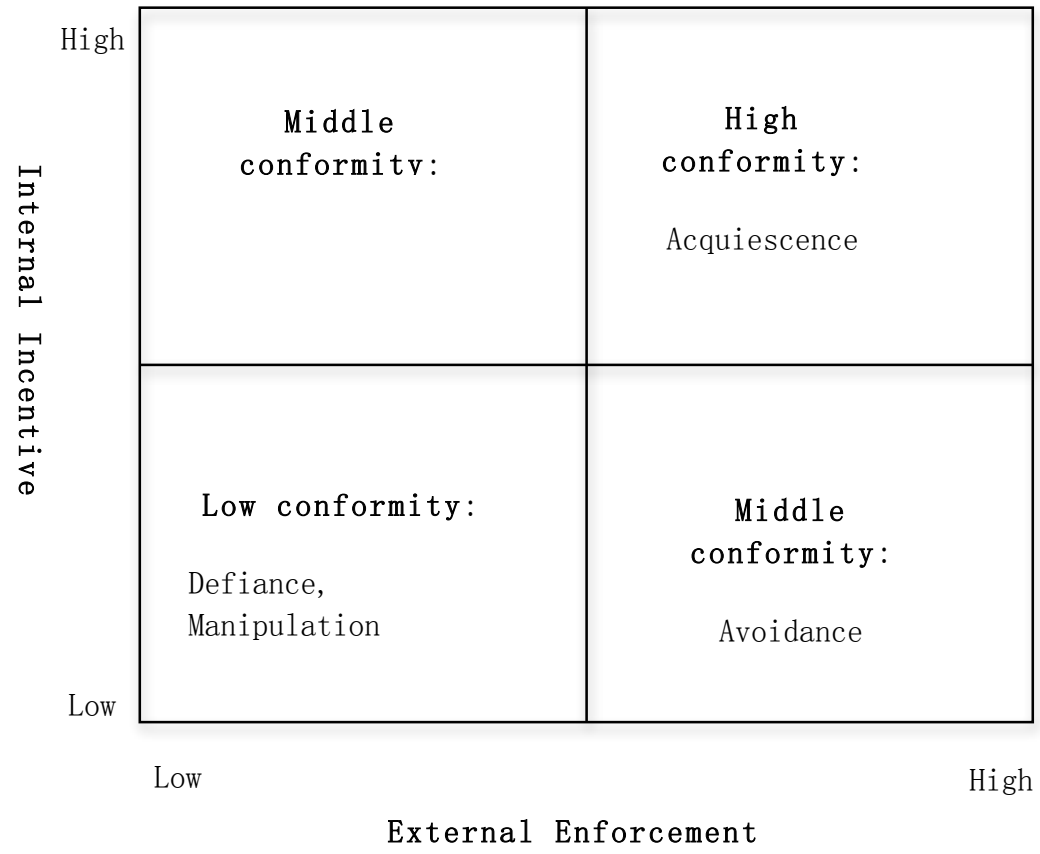

Figure 2: A Framework to Determine the Organisational Strategies Employed in Response to Regulative Pressures

The weakest conformity emanates from regulative pressures (government orders and legal documents) that are perceived as unhelpful by an organisation, and when the associated legal enforcement is interpreted as weak; and leads to the adoption of defiance and manipulation strategies. In the Dynasty Hospital case study example, national security standard GB 17859-1999 was considered too vague and complex for organisational ISP making, and there was no arrangement of government inspection on its adoption, and consequently Dynasty Hospital chose a defiance strategy and ignored the regulative pressures when devising its ISP.

When there are low internal incentives and high external enforcement, the avoidance strategy at the moderate level of conformity tends to be adopted. For example, Decree No. 136 issued by the local healthcare authority required Dynasty Hospital to follow relevant national policies and standards to organise ISA training, and also established a timetable for field inspections. Despite this regulatory demand, the hospital believed this statutory guidance to be unhelpful and instead adopted an avoidance strategy. Viewed through the lens of Oliver (1991) and considering the findings of Modell (2001), the hospital tried to disguise nonconformity; offering some training courses but failing to meet the content required by the authority.

When there are high internal incentives and low external enforcement, an organisation tends to adopt a compromise strategy that offers a moderate level of conformity. For example, in China the government enacted laws and regulations on organisational ISP but did not include any enforcement measures, and in designing its ISP in accordance with its ISM priority, the hospital selectively adopted the government requirements that they believed useful for guiding their ISM.

The highest conformity strategy of acquiescence will occur when an organisation clearly recognises the role of institutional pressure in helping it improve its ISM, and when there is strong legal enforcement in place. For example, in relation to its ISA training, Dynasty Hospital eventually abandoned the avoidance strategy and adopted an acquiescence strategy instead, as the result of a serious system failure caused by a staff member using a memory stick. This episode caused hospital management to realise that efficient training was vital in educating its employees about the importance of complying with ISP in their daily work (Puhakainen and Siponen, 2010; Straub and Welke, 1998), in order to avoid such incidents in

the future. In another example, the hospital adopted an acquiescence strategy when responding to the requirements outlined in Decree No. 136 regarding devising an information security strategy, as the hospital were aware that such a strategy played an important role in guiding its ISM practices, and were also aware that a government inspection would soon take place.

6.3. Generalising Beyond the Case of Dynasty Hospital

Generalizability or external validity has long been a cause for concern amongst case study researchers. Whilst single case research design is generally accepted, and has many precedents (e.g. Eisenhardt and Graebner, 2007), it is sometimes criticised for its lack of generalisation potential. This paper has focused on theoretical development in the form of a combined framework and provides an illustration of the concept from an empirical case offering rich insight. We follow the guidance of Klein and Myers (1999) and Yin (2008) on the generalisation of case studies, where longitudinal case study design coupled with appropriate theory offers theoretical generalisation, allowing researchers to track cause and effect effectively (Tsang, 2014).

Referring to what Yin (2008) calls analytic generalisation in case study, Seddon and Scheepers (2012) have developed a generalisation-justification logic for justifying the support for generalisations from a single study, and have used this logic to analyse the MIS Quarterly best paper of Markus et al. (2006) in terms of the generalizability of their findings. Analytic generalisation is essentially theoretical generalisation (Tsang, 2014), and means arguing a point based on similarities between relevant attributes of items in a sample and in other

(broader) settings; asserting that broad claims based on the sample are also likely to hold true in those other settings. Following this logic, and its application in evaluating the case study of Markus et al. (2006), we can justify the generalizability of our case study findings in two steps. Firstly, based on careful analysis of the case of Dynasty Hospital, we have developed a theoretical framework (provided at Figure 2). Secondly, because the internal and external forces that impact upon the behaviour of the case organisation are also likely to exist in other settings, we argue that our findings are also likely to be applicable in those other settings. Specifically, we believe that in one country, organisational ISM is relevant to every functional part of an organisation (ISO/IEC, 2005). In ISM, a failure to comply with government regulations is a global phenomenon across industries, whether in the USA in healthcare sector (Green, 2015), or in e-business in the UK (Mawani, 2011). We would argue that the elements provided in our framework are common to many different kinds of organisations in different country contexts, and as a consequence assert that the findings we have gathered from the Chinese case as represented by the framework in Figure 2 are generalizable to other organisational, industrial and country contexts.

However, as Tsang (2014) has pointed out, the generalizability of case study results can only be assessed by observing future cases and by applying the developed theory in order to understand patterns of behaviour. “In any case, it is ultimately an empirical question” (Markus et al., 2006, p. 462) whether findings of a case study may be generalizable in broader contexts. We therefore encourage future research on this question in order to robustly test our proposed framework beyond our case study hospital within the healthcare sector, particularly in different country contexts.

7. Conclusions

Drawing upon the institutional theory concepts of institutional pressures and organisational responses, and based upon the five stages of the ISM process, this paper offers a case study of ISM in one public hospital in China. A theoretical framework is developed, which argues that the organisational strategic response to regulative requirements on ISM are determined jointly by an internal self-awareness of the organisation regarding the importance of particular regulative forces, along with the internal incentive of the organisation to comply with such forces; and the external law enforcement employed by government through supervision and inspection. Specifically, the more useful an organisation feels a regulative pressure to be to its information security protection, and the stronger the government enforcement on this regulative pressure is likely to be, the more compliant are the strategies the organisation will adopt; which range from a high to a low level of conformity and which include acquiescence, compromise, avoidance, defiance and manipulation.

Important practical implications can be drawn from this research. In order to effectively promote organisational ISM, the government must ensure that the relevant statutory documents and associated policy guidance are useful for organisations seeking to protect their information security, and thus provide an incentive to comply. At the same time, the government should also consider the importance of enacting strict enforcement measures (such as supervision and inspections) to ensure that the laws relating to organisational ISM are respected in practice. Legal enforcement on behalf of governments is particularly important in developing countries such as China, where the legal infrastructure is relatively weak and legal systems often do not function efficiently (Gao, 2005; Luo, 2003; Yildirim et

al., 2011). We would suggest that these countries attach penalties and sanctions to the most important regulative requirements in order to ensure increased compliance.

Our work offers a number of opportunities for future research into ISM. This case study deals with a public healthcare organisation, the Dynasty Hospital, in China, where conformity strategies dominate the ISM process, and no evidence of selecting a manipulation strategy was observed. Like the case study hospital, organisations under close governmental control are unlikely to challenge and manipulate regulative pressures (Gao, 2005), whilst in professional organisations like the Dynasty Hospital, information systems and ISM often receive little attention from senior management. Future research could employ our framework to analyse organisations within other industries and in different countries. By considering cases subject to different levels of government intervention, and with various levels of information security awareness, future research may generate broader findings regarding organisational responses to regulative pressures, with internal incentives and external law enforcement as the moderating factors. For example, the patterns of organisational response in different stages of the ISM process; and the correlation of particular regulative forces, such as law, regulation and national policy, along with different strategies of organisational response, could all be considered.

There are a number of limitations to our research. We have only considered self-awareness as the internal determinant of organisational strategy in response to government requirements. Further research may cover other internal factors, such as organisational structure, governance or business characteristics. Moreover, whilst our case study is based on institutional theory, it only considers the regulative dimension of institutional pressures.

Further research could consider normative and culture-cognitive pressures, which may also impact upon the organisational ISM process in different ways.

References

J. Backhouse, C.W Hsu, C. W, L. Silva, Circuits of power in creating de-jure standards: shaping an international information systems security standard, MIS Quarterly, 30 (2006) 413 438

J.K. Bakari, C.N. Tarimo, L. Yngstrom, C. Magnusson, S. Kowalski, Bridging the gap between general management and technicians: a case study on ICT security in a developing country, Computer & Security, 26 (2007) 44 55

BBC (2013) Sony fined over 'preventable' PlayStation data hack, BBC News, January 24, retrieved February 9, 2015, available at: http://www.bbc.co.uk/news/technology-21160818

N.L. Beebe, V.S. Rao, Improving organisational information security strategy via meso-level application of situational crime prevention to the risk management process, Communications of the Association for Information Systems, 26 (2010) 329 358

M. Bishop, Computer Security: Art and Science, Addison-Wesley, Boston, MA, USA 2003

F. Bjorck, Institutional theory: a new perspective for research into IS/IT security, in Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS-37), January 5-8, Big Island, HI, USA (2004)

B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Quarterly, 34(3) (2010) 523 548

J.A Cazemier, P.L. Overbeek, L.M. Peters, L. M. Security Management, IT Infrastructure Library Series, Stationery Office, UK 2000

S.E. Chang, C.B. Ho, Organisational factors to the effectiveness of implementing information security management, Industrial Management & Data Systems, 106(3) (2006) 345 361

J. Choobineh, G. Dhillon, M.R. Grimaila, J. Rees, Management of information security: challenges and research directions, Communications of the Association for Information Systems, 20(4) (2007) 958 971

G. Dhillon, J. Backhouse, Current direction in IS security research: towards socio-organisational perspectives, Information Systems Journal, 11 (2001) 127 153

Economic and Social Commission for Asia and Pacific (2007) Information Security for Economic and Social Development, retrieved January 31, 2013, available at: http://www.unescap.org/publications/detail.asp?id=1290

K.M. Eisenhardt, M.E. Graebner, Theory building from cases: opportunities and challenges, Academy of Management Journal, 50(1) (2007) 25 32

B. Filkins, Health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon, SANS Institute, (2014) retrieved October 9, 2016, available at:

http://www.sans.org/reading-room/whitepapers/firewalls/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

P. Gao, Using actor-network theory to analyse strategy formulation, Information Systems Journal, 15(3) (2005) 255 275

S. Goel, I.N. Chengalur-Smith, Metrics for characterising the form of security policies, Journal of Strategic Information Systems, 19 (2010) 281 295

S. Gosain, Enterprise information systems as objects and carriers of institutional forces: the new iron cage? Journal of the Association for Information Systems, 5(4) (2004) 151 182

M. Green, 15 of the biggest data breach settlements and HIPAA fines, Becker's Health IT & CIO Review, (2015) October 14, retrieved October 9, 2016, available at: http://www.beckershospitalreview.com/healthcare-information-technology/15-of-the-biggest-data-breach-settlements-hipaa-fines.html

K.H. Guo, Y.F. Yuan, N. Archer, C.E. Connelly, Understanding non-malicious security violations in the workplace: a composite behaviour model, Journal of Management Information Systems, 28(2) (2011) 203 236

M. Hechter, K.D Opp, R. Wippler, Social institutions: their emergence, maintenance and effects, Aldine de Gruyter, New York, USA 1990

T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, European Journal of Information Systems, 18(2) (2009) 106 125

A. Hovav, J. D'Arcy, Applying an extended model of deterrence across cultures: an investigation of information systems misuse in U.S. and South Korea, Information & Management, 49 (2012) 99 110

C. Hsu, Frame misalignment: interpreting the implementation of information systems security certification in an organisation, European Journal of Information Systems, 18(2) (2009) 140 150

C. Hsu, J.N. Lee, D.W Straub, Institutional influences on information systems security innovations, Information Systems Research, 23(1) (2012) 1 22

Q. Hu, P. Hart, D. Cooke, The role of external and internal influences on information system security - a neo-institutional perspective, Journal of Strategic Information Systems, 16(2) (2007) 153 172

ISO/IEC, Information technology - security techniques - information security management systems - requirements, International Organisation for Standardisation/International Electro technical Commission, Geneva 2005

A. C. Johnston, M. Warkentin, Fear appeals and information security behaviour: an empirical study, MIS Quarterly, 34(3) (2010) 549 566

M. Karyda, E. Kiountouzis, S. Kokolakis, Information systems security policies: a contextual perspective, Computer & Security, 24 (2005) 246 260

H. K. Klein, M. D. Myers, A set of principles for conducting and evaluating interpretive field studies in information systems, MIS Quarterly, 23(1) (1999) 67 94

K. J. Knapp, R. F. Morris Jr., T. E. Marshall, T. A. Byrd, Information security policy: an organisational-level process model, Computer & Security, 28 (2009) 493 508

S. Kraemer, P. Carayon, J. Clem, Human and organisational factors in computer and information security: pathways to vulnerabilities, Computer & Security, 28(7) (2009) 509 520

K. Kraemer, K., J. Dedrick, Payoffs from investment in information technology: lessons from the Asia-Pacific region, World Development, 22 (12) (1994) 1921-1931

C. Y. Ku, Y. W. Chang, D. C. Yen, National security policy and its implementation: a case study in Taiwan, Telecommunications Policy, 33(7) (2009) 371 384

Y. D. Luo, Industrial dynamics and managerial networking in an emerging market: the case of China, Strategic Management Journal, 24(13) (2003) 1315 1327

Q. X. Ma, M. B. Schmidt, J .M. Pearson, An integrated framework for information security management, Review of Business, 30(1) (2009) 58 70

M. L. Markus, C. W. Steinfield, R. T. Wigand, G. Minton, Industry-wide information systems standardisation as collective action: the case of the U.S. residential mortgage industry, MIS Quarterly, 30 (2006) 439 465

M. Masrom, A. Rahimly, Overview of data security issues in hospital information systems, Pacific Asia Journal of the Association for Information Systems, 7(4), Article 5 (2015)

V. Mawani, The economics of Sony PlayStation Network and Qriocity Identity hacks, Industry Leaders, May 6 2011, retrieved September 11, 2013, available at: https://www.industryleadersmagazine.com/the-economics-of-sony-playstation-network-qriocity-identity-hacks

J. W. Meyer, B. Rowan, Institutionalise organisations: formal structure as myth and ceremony, American Journal of Sociology, 83(2) (1977) 340 363

M. Mignerat, S. Rivard, Positioning the institutional perspective in information systems research, Journal of Information Technology, 24 (2009) 369 391

S. Modell, Performance measurement and institutional processes: a study of managerial responses to public sector reform, Management Accounting Research, 12 (2001) 437 464

Norton (2012) Norton Cybercrime Report, Symantec, retrieved March 21, 2013, available at: http://investor.symantec.com/files/doc_news/2012/2012_Norton_Cybercrime_Report_Master_FINAL_050912%281%29.pdf

C. Oliver, Strategic responses to institutional processes, Academy of Management Review, 16(1) (1991) 145 179

P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: an action research study, MIS Quarterly, 34(4) (2010) 757 778

PWC (2012) The Global State of Information Security, Price Waterhouse Coopers, retrieved March 7, 2013, available at: http://www.pwc.pl/en/publikacje/global-state-of-information-security-survey-2012.html

S. Ransbotham, S. Mitra, Choice and chance: a conceptual model of paths to information security compromise, Information Systems Research, 20(1) (2009) 121 139

H. Safar, J. G. Clark, Current state of information security research in IS, Communications of the Association for Information Systems, 24 (2009) 557 596

W. R. Scott, Institutions and Organisations (2nd ed.), Sage Publications, Thousand Oaks, CA, USA 2001

P. B. Seddon, R. Scheepers, Towards the improved treatment of generalisation of knowledge claims in IS research: drawing general conclusions from samples, European Journal of Information Systems, 21 (2012) 6 21

C. Shen, Opinions on information security industrialisation, Computer Security, 24(2) (2003) 17 21

L., Silva, J. Backhouse, The circuits of power framework for studying power in institutionalization of information systems, Journal of the Association for Information Systems, 4(1) (2003) 294 336

M. T. Siponen, A conceptual foundation for organisational information security awareness, Information Management & Computer Security, 8(1) (2000) 31 41

S. Smith, D. Winchester, D. Bunker, Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organisation, MIS Quarterly, 34(3) (2010) 463 486

P. Spagnoletti, A. Resca, The duality of Information Security Management: fighting against predictable and unpredictable threats, Journal of Information System Security, 4(3) (2008) 46 62

B. C. Stahl, N. F. Doherty, M. Shaw, Information security policies in the UK healthcare sector: a critical evaluation, Information Systems Journal, 22 (2012) 77 94

J. Stanton, K. Stam, P. Mastrangelo, J. Jolton, Analysis of end user security behaviours, Computers & Security, 24(2) (2005) 124 133

State Council (2006) National Informatisation Strategy 2006–2020, May 8, retrieved January 30, 2012, available at: http://www.gov.cn/gongbao/content/2006/content_315999.htm

D. W. Straub, R. J. Welke, Coping with systems risk: security planning models for management decision making, MIS Quarterly, 22(4) (1998) 441 469

A. Strauss, J. Corbin, Basics of Qualitative Research, Sage Publications, Newbury Park, CA, USA 1990

C. Sundt, Information security and the law, Information Security Technical Report, 11(1) (2006) 2 9

E. W. K. Tsang, Case studies and generalisation in information systems research: a critical realist perspective, Journal of Strategic Information Systems 23 (2014) 174 186

A. Tsohou, M. Karyda, S. Kokolakis, E. Kiountouzis, Aligning security awareness with information systems security management, Journal of Information System Security, 6(1) (2010) 36 54

R. von Solms, Information security management: the second generation, Computer & Security, 15(4) (1996) 281 288

K. T. Win, A review of security of electronic health records, Health Information Management, 34(1) (2005) 13 18

C. C. Wood, Information security problems as evidence of management failures, Computer Fraud & Security, 11 (1995) 14 16

E. Y. Yildirim, G. Akalp, S. Aytac, N. Bayram, Factors influencing information security management in small-and medium-sized enterprises: a case study from Turkey, International Journal of Information Management, 31(4) (2011) 360-365

R. K. Yin, Case Study Research: Design and Method (4th ed.), Sage Publications, Thousand Oaks, London 2008

L. G. Zucker, Organisations as institutions, in: S. B. Bacharach, (ed.) Perspectives in organisational sociology: theory and research, ASA series 2, JAI Press, Greenwich, CT, USA 1983

Appendix

Chinese Information Security Laws and Regulations (including national standards)

Administrative Measures for Internet Medical and Health Information Service, Decree No. 66, Ministry of Health, July 1, 2009, retrieved January 30, 2013, available at: http://www.gov.cn/flfg/2009-06/23/content_1347818.htm

Computer Information Systems Security Protection Classification Standards, national standard GB 17859-1999, Ministry of Public Security, September 1999

Computer Virus Protection Measures for the Administration, Decree No. 51, Ministry of Public Security, April 26, 2000, retrieved January 29, 2013, available at: http://www.mps.gov.cn/n16/n1282/n3493/n3823/n442104/452209.html

Criminal Law, Amendment VII, Article No. 286, NPG, February 28, 2009, retrieved January 29, 2013, available at: http://www.NPG.gov.cn/englishNPG/Law/Frameset-page6.html

Criteria for Shaanxi Province Healthcare Informatisation, Decree No. 136, Shannxi Province Health Bureau, September 8, 2008

Information Security Management Code of Practice, national standard GB/T 19716-2005, State Bureau of Quality Technical Supervision and the Standardisation Administration, October 1, 2005

Information Systems Security Standards, GB/T 20269-2006, State Bureau of Quality Technical Supervision, December 1, 2006

Network Security Standards, GB/T 20270-2006, State Bureau of Quality Technical Supervision, December 1, 2006

Operating Systems Security Technique Requirements, national standard GB/T 20272-2006, State Bureau of Quality Technical Supervision, December 1, 2006

Regulation on Safety Protection of Computer Information Systems, Decree No. 147, State Council, February 18, 1994, retrieved January 20, 2013, available at: http://www.asianlii.org/cn/legis/cen/laws/rfspocis719/

Safety Requirements for Information Techniques Equipment, national standard GB4943-1995, State Bureau of Quality Technical Supervision, August 1, 1996

Safety Requirements for Computer Centre Field, national standard GB 9361-88, State Bureau of Quality Technical Supervision, October 1, 1988

Regulations on Strengthening Information Security Protection, Decree No. 27. State Council, September 7, 2003. Retrieved September 2, 2013, available at: http://www.scopsr.gov.cn/pub/newzybb/dzzw/zcfg/201203/t2

Chinese Information Security Policies

National Healthcare Informatisation Policy 2003-2010, Ministry of Health, March 24, 2003, retrieved January 30, 2013, available at: http://www.moh.gov.cn/mohbgt/s6693/200804/23876.shtml

National Informatisation Strategy 2006–2020, State Council, May 8, 2006, retrieved January 30, 2013, available at: http://www.gov.cn/gongbao/content/2006/content_315999.htm

The 11th Five-Year-Plan, The National People's Congress, October 18, 2005, retrieved April 26, 2013, available at: http://news.xinhuanet.com/politics/2005-10/18/ content_3641362.htm