SHAPING OF SECURITY POLICY IN AN INDONESIAN BANK: INTERPRETING INSTITUTIONALIZATION AND STRUCTURATION

M. Faisal Nasution
Virginia Commonwealth University

Gurpreet Dhillon
Virginia Commonwealth University

Roberto Akyuwen
Senior Executive Analist for MFI Development, Indonesia Financial Services Authority (OJK)
E-mail: roberto.akyuwen@ojk.go.id

Abstraksi

Studi ini meneliti pembentukan kebijakan keamanan pada sebuah bank di Indonesia dengan menggunakan teori institusional dan struktural sebagai kerangka teoritis. Penelitian mengenai keamanan sistem informasi pada umumnya kurang memperhatikan aspek-aspek sosial dalam perancangan dan pelaksanaan kebijakan keamanan. Penelitian ini menggunakan studi kasus dengan sebuah bank pemerintah di Indonesia sebagai unit analisis. Kasus ini dipilih karena terjadinya peristiwa penjebolan sistem keamanan pada saat penelitian ini dilakukan. Studi kasus ini membahas mengenai bagaimana kebijakan keamanan dibentuk dan pelajaran penting apa saja yang dapat ditarik dari sudut pandang teori institusional dan stukturasi. Hasil penelitian ini menunjukkan peranan penting dari sebuah desain sistem yang baik dan bagaimana faktor-faktor sosial dan politik dipertimbangkan ketika merencanakan kebijakan keamanan. Kontribusi yang diberikan oleh hasil penelitian ini, antara lain adalah, menunjukkan bagaimana teori institusional dapat digunakan untuk menjelaskan bagaimana kekuatan institusional mempengaruhi desain dan penggunaan kebijakan keamanan.

Kata Kunci: *keamanan dan privasi sistem informasi, kebijakan keamanan, teori institusional, teori strukturasi.*

1. INTRODUCTION

There is a problem with the management of information security in organizations. While significant research has been undertaken in defining good security policies (Dhillon, 1997; Dhillon and Torkzadeh, 2006), yet the compliance between rules prescribed by a security policy and what organizations actually do is limited at best. There is no clear indication as to how security policies are internalized and how such internalization prevents a security breach (Dhillon, 2007). While researchers of late have addressed the behavioral aspects of IS security, the related social aspects of the problem have largely been overlooked (Björck, 2004). Studies in information security have vaguely explored the link between security policies, security behaviors, and security breaches.

In this study we investigate how security policies are formed in organizations, insitutionalized, and therefore prevent security breaches. The context of our research is the Indonesian banking sector. For the purposes of this study we have identified a case study involving an Indonesian government-owned commercial bank. The Indonesian banking sector offers an interesting opportunity to undertake this research. This is because while information security is undoubtedly considered important, yet the rules pertaining to information security do not seem to have gotten entrenched. In this paper we make two assertions. First, a good security policy is a basis for a bank to ensure stability of its operations. Hence it is important to ensure that a security policy gets institutionalized. Second, the central bank needs to ensure that a proper climate for institutionalization exists. We explore these assertions in the context of our case research and in particular address the following research questions:

1. How information security policies and practices are shaped and assimilated in an organization.
2. How an external central governance body (e.g., the central bank) affects the institutionalization of information security policies and practices.
3. How security breaches reshape security policies and reassimilate these in an organization.

In addressing the research questions we use institutional theory (Powell and DiMaggio, 1991; Scott, 2008) and Gidden's structuration theory to understand the structural, processual, and dominance issues and how they shape institutionalization. The combination of institutionalization and structuration is undertaken based on Barley and Tolbert (1997) synthesis. Using institutionalization helps "explain why formal security structures and actual security behavior differs" (Björck, 2004, p. 5). An indepth case study approach in the tradition of Walsham (1993; 1995) and Eisenhardt (1989) is adopted.

2. PRIOR LITERATURE

However there is a gap in the literature as to which influences (e.g., security breach, external central governance body etc) shape and reshape security policies. The literature is also unclear about how new security policies that are gradually internalized direct the use of technical security artifacts and security behavior. There are three informing bodies of literature pertaining to the research presented in this paper – security policy formulation and implementation, institutionalization, and structuration, which are discussed below.

2.1. Security Policy Formulation and Implmentation

There is a general consensus as to what an information security policy might be. Smith and Jamieson (2006) for instance define information security policies as rules that ensure the confidentiality, integrity, and availability of information and assets to protect from theft, tampering, manipulation, or corruption. Chandra (2008) states that the initiation of information security policies denotes management's commitment to advance and safeguard information as an asset. Ross (2008) considers information security policies and standards to depict management objectives with respect to protection.

In the literature the relationship between formulation and implementation of security policies to security breaches is tenuous at best. Doherty and Fulford (2005) for example found no significant relationship between the formulation and implementation of information security policies and the incidence of severity of information security breaches. They suggest that factors such as difficulty in building awareness, problems in policy enforcement, complexity of policy standards, inadequacy of resources, and failure to cutomize policies, as the main reason for security breaches. Baskerville and Siponen (2002) also enunciate the importance to formulate security policy, particularly in an emergent organization, for the implementation and development of information systems security. They observe the importance of either a single security policy or several security policies derived from distinct policy levels or types. Doherty et al. (2009) state that the importance of formulating and applying formal security policy can prevent security breaches from occurring and hence safeguard organizational information.

Doherty and Fulford (2006) have also argued that by carefully and explicitly aligning information security policy and strategic information systems plan enhances the security of information systems. They find that there is a strong impact of a carefully designed information security policy on the planning of strategic information systems. Knapp et al. (2006) find that top management support has a significant impact on the enforcement of information security policy as well as the organization's security culture. Herath and Rao (2009) note that policy attitudes are determined by threat perceptions and organizational commitment.

Security policies therefore depict management objectives of and commitment to information security (Chandra, 2008; Ross, 2008). Intervention and support by management, or a higher authority, are crucial to formulate and implement security policies (Knapp et al., 2006). While security policies are an important determinant to achieve sound information security, concerns reside with an actors commitment and interaction with security policies (Doherty and Fulford 2005). Clearly a security policies may be cosidered seriously if a goven actor comprehends the seriousousness of potential threats (Herath and Rao, 2009). Unfortunately however many stakeholders exhibit a false sense of security and perceive their information asset to be safe (Rhee et al. 2005). Eventually when a security policy may be considered, there is usually a problem with current practices having been entrenched in the systems. This means that for a policy to be successful, sigificant unlearning and relearning is required. It is therefore important to ensure adequate interventions at suitable times such that the right kind of practices get institutionalized.

2.2. Institutionalization

An abstract view of an institution is that it is a result of ongoing *"typification of habitualized actions*" by social actors (Berger and Luckmann, 1966, p. 54). The concept entails a socially constructed representation of repetitive actions that become a habit among social actors. Institutionalization hence is a social process of creating an institutionalized social structure (Berger and Luckmann, 1966; Giddens, 1984; Powell and DiMaggio, 1991; Scott, 2008). Powell and DiMaggio (1991) state that formal organizations become institutions through institutionalization. Hence institutionalization is best represented as a particular state or property of a social pattern. Scott (1987) refers to institutionalization as a process to instil values beyond the technical requirements of a task over time, and as a process of creating social reality, which is independent of actor's view and actions, but is taken for granted. The "typification of habitualized actions" concept implies the impact of history and control on activities within an institution. History is needed for an institution to reflect on its past records, i.e., to reproduce itself in a modified form. Control is required as a method to ensure an institution to function according to its legitimacy. Powell and DiMaggio (1991) introduce four avenues of institutional reproduction: (1) the exercise of power, (2) complex interdependencies, (3) taken-for-granted assumptions, and (4) path-dependent development processes. Barley and Tolbert (1997) argue, however, that institutionalization has not depicted a comprehensive process of institutionalizing formal structure since institutionalists do not empirically denote the creation, alteration, and reproduction of institutions.

2.3. Structuration

Structuration is built upon the notion of rules and resources that shape social structures (i.e., signification, domination, and legitimation). According to Giddens (1984), the social structures are socially constructed through the interactions between agency and modalities (i.e., interpretation, artifacts, and regulations). The interactions create a continuous process of structures and enactment. Scholars have introduced the concept of duality of structure whereby agency's interactions with modalities affect the production and reproduction of social structures (Walsham, 1993; Walsham and Han, 1991). Orlikowski (1992) introduces the notion of duality of technology, providing a critique of the view of technology either as an objective force or as a social construction of reality. In her later work, Orlikowski (2000) focuses on how structures are dynamically enacted through various interactions between agency and technology. Similarly, Barley (1986) investigates how similar technologies can be used to produce dynamic and continuous technology-use structuration in two different entities, hence producing distinct social structures. He argues that the variety of social structures produced by the same technology can best be understood by viewing the social form and social action. Barley and Tolbert (1997) implement the concepts of social form and social action by integrating structuration and institutionalization as an attempt to complement each framework. In relation to information security, Huebner and Britt (2006) explore the three structures to investigate the impact of information security behavior on internal security controls.

The core of structuration is the duality of structure, which primarily focuses on the modalities. Two of the three modalities (i.e., artifacts and regulations) are particularly more important to our study. Orlikowski and Iacono (2001) state that an artifact is an object that is manufactured, used, or modified by humans. Regulations can be used to sanctioning the interaction between agency and artifacts. According to Selznick (1969, p. 8), law is required to enforce control and order, and is therefore necessary as a tool to promote *"peace, settle disputes, suppress deviance."* In relation to our study, such laws are embedded in an organization's security policy.

3. THEORETICAL DEVELOPMENT

As noted previously, central to our study is the combination of institutionalization and structuration. Structuration scholars have denoted that the duality of structure, which is a manifestation of synergistic relationship between agency and structures, to provide a basis for interactions between agency and modalities. In due course such interactions become routinized, are rationalized and subsequently taken for granted (Giddens, 1984; Orlikowski, 1992; Orlikowski, 2000; Orlikowski et al., 1995; Walsham, 1993; Walsham and Han, 1991). As interactions become rationale and regimented amongst members of a social system, social order and stability begin to take effect. By nature, institutional theory resents the notion of change. Such resentment therefore inquires the epistemic and the ontology of maintaining and reproducing social order and stability (Burrell and Morgan, 1979). Members of a social system strive to achieve similar goals and are tempted to internalize and repeat their actions to maintain social order, thus creating an institution (Scott, 2008). In order to depict the maintenance of social order, Giddens introduces two realms (as noted by Barley and Tolbert, 1997) - agency representing action and structures representing institution. Our view of an institution is informed by Powell and DiMaggio (1991, p. 145)'s definition – *"a social order or pattern that has attained a certain state or property."* According to Scott (2008), however, an institution always changes forms as it is being challenged and is never created from inexistence. When an institution is challenged and social change unavoidably takes effect, an institution changes its appearance, replacing the older format. Hence it is said that an institution is reinstitutionalized (Powell and DiMaggio, 1991). The new format forces members of a social system to reinternalize new routines of action until such actions become established. Integrating institutionalization and structuration therefore demands that the two realms – action and institution – be analyzed in conjunction to modelling how social structures are created, maintained, and altered.

3.1. The Institutional Realm

The notion of "institutional realm," introduced by Barley (1986) and Barley and Tolbert (1997), lends the concept of resistance to change to the duality of structure. Institutional realm is an abstract framework of typifications and rules derived from a cumulative history of action and interaction (Barley, 1986; Barley and Tolbert, 1997) by which an agency utilizes to make sense of its actions. The institutional realm inscribes three social structures– signification, domination, and legitimation – as being abstract institutional properties that are produced, maintained, and altered.

Despite being institutional properties, the three social structures are simply assumed and are not central to the maintenance of the institutional realm. Scholars of institutionalization and structuration have the tendency to focus on different impacts of actions on institutional realm as a whole. While they provide individual views of such impacts on signification, domination, and legitimation, the social structures are merely an abstraction of reality with limited empirical evidence (Barley and Tolbert, 1997). Focusing on institutionalization alone does not guarantee useful insights to the process of organizing as both institutional and structuration theory complement one another. Using the institutional realm to represent the three social structures allows for modeling processes of institutionalization.

3.2. The Realm of Action

Another important concept is the realm of action, which depicts the *"actual arrangements of people, objects, and events in the minute-by-minute flow of the setting's history"* (Barley, 1986) or the "*social life's unfolding"* (Barley and Tolbert, 1997). This realm represents the continuous interaction between agency and resources, taking into account the impact of other modalities such as interpretive schemes and regulations. It does not, therefore, represent agency alone. While the institutional realm is labelled "realized structure," the realm of action is termed "interaction order" (Barley, 1986).

The interaction between agency and technology has long been a focus to scholars of technology and organizations. Orlikowski (1992) states that technology is both a human creation (i.e. an objective force) and a meaningful artifact to humans when used in an ordered manner (i.e. social construction of reality). She maintains, however, that viewing the two perspectives independently causes failure to investigate how the use of technology becomes structured. Her later work shows that ongoing use of technology recursively produces structures of technology use in different patterns as agency may experience interaction with different technologies (Orlikowski, 2000).

3.3. Institutionalization

The institutional realm and the realm of action represent the link between action and institution, which according to Barley and Tolbert (1997), help in delineation of recursive structurations. Action and institution recursively shape each other over time: a structuralized institution shapes agency's actions while agency's actions structuralize institution. Institution is enacted using a script, which serves as a link between action and institution

(Barley, 1986; Barley and Tolbert, 1997). Script represents the interaction order, indicating *"observable, recurrent activities and patterns of interaction characteristics of a particular setting"* (Barley and Tolbert, 1997, p. 98).

While the term structure is used rather differently by scholars (i.e., Barley, Orlikowski, and Walsham), Barley uses the term structure and institution interchangeably. Rather than looking at how the use of resources shapes structures (as per Orlikowski's conception), Barley focuses on structuration as a process and hence uses the word institutionalization to refer to structuration. Our theoretical stance is closely aligned with Barley's conceptualization.

In the information security context, the institutional realm manifests the interplay between security-control dimensions: technical, formal, and informal controls (Dhillon, 2007; Dhillon and Moores, 2001). Whereas technical controls focus on the use of security technology as well as overlooking the technical aspect of information security, formal controls and informal controls dictate actors' behavior to promote information security in an organization. The stable structuration (or institutionalization) of information security is a product of managing the integrity of the three security-control dimensions in an organization (Dhillon, 2007). The institutionalization framework by Barley and Tolbert (1997) is important to describe the case study and to structure the discussion and findings. The case study is therefore divided into two subsections: the *normal condition* and the *security breach incident* that specifically explains the reinstitutionalization instance. The case study research presented in the next section looks at how security policy in a commercial bank becomes institutionalized and structuralized in a series of formulation, implementation, and modification (or reformulation).

4. THE CASE STUDY

This section presents the empirical analysis for our study. We use an interpretive case study of security policy institutionalization in a large Indonesian government-owned commercial bank.

4.1. Research Methodology

The combination of institutional theory and structuration theory appropriates the use of an interpretive scheme, since structuration theory involves the communicative interaction among subjects; a property captured only by using an interpretive scheme (Berger and Luckmann, 1966; Giddens, 1984). An interpretive research design thus requires that the methodology begin with "the position that our knowledge of reality, including the domain of human action, is a social construction by human actors" (Walsham, 2006, p. 320). The interpretive scheme provides various methodologies to analyze data: ethnography, hermeneutics, case study research, grounded theory and action research. Our study uses the case study method, which allows social scientists "to retain the holistic and meaningful characteristics of real-life events – such as individual life cycles, organizational and managerial processes, neighborhood change, international relations and the maturation of industries" (Yin, 2003, p. 2). Furthermore, "a case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups or organizations)" (Benbasat et al., 1987, p. 370). Several important procedures in a case-study research are selection of cases, crafting instruments and protocols which allow researchers to select appropriate data collection methods, analyzing within-case data when exhaustive amount of data is present, and searching for cross-case patterns by creating categories and looking for similarities in the categories (Eisenhardt, 1989).

We select Centro Metropolitan Bank as our unit of analysis since the bank is a mature, large government-owned commercial bank with excellent customer service and a large financial asset. Our findings indicate that such success is attributed to the bank's good information systems and significant experiences in dealing with information security. The case study was conducted between summers of 2010 and 2011 when the banking regulatory and supervisory function was still assumed by the central bank. Interviews were undertaken with key stakeholders, including top ranking executives, middle managers and front-end staff. IT personnel were also included into the respondent pool. In all over 30 hours of interview data was collected. While interviews were the primary source of data, extensive secondary materials were also reviewed and analyzed. We used semi-structured interviews to allow for flexibility in probing respondents. We transcribed the interviews and analyzed patterns and categories that match the focus of our study (e.g., security policy, rules, EDC machines, IT, security, control, etc.).

4.2. The Case of Centro Metropolitan Bank

The Centro Metropolitan Bank, formed in October 1998 as part of the Government of Indonesia's bank restructuring program, establishes IT infrastructure that provides straight-through processing and a unified interface for customers. The bank is directed by an executive management team of Board of Directors, headed by a President. The management and governance is supervised by the Board of Commissioners appointed directly by the nation's Ministry of State-Owned Enterprise. As a large institution, each division is managed by a director and each oversees groups that play a significant role supplying the bank's operational needs. The governance and practices of information security are managed solely by the IT security department, which is part of the IT Planning, Architecture, and Business Continuity Planning (BCP) group. This group is structured under the Technology and Operations Division, which is responsible for overseeing all issues regarding the implementation of IT system in the bank and by the bank's customers.

Centro Metropolitan Bank regards reputational risk, which is closely linked to operational risk, as a leading cause to crowding out of customers, potentially creating financial loss. With regard to information security and to security of using technology, Centro Metropolitan Bank identifies access to information and the use of technology to exhibit potentially damaging risk when they are not properly handled. The bank characterizes such risk as an operational risk and abides to the handling of such risk using Basel II framework as a guideline.

4.3. Security Policy Formulation and Implementation

The internal information-security practices in Centro Metropolitan Bank are initiated solely by the IT security department. In the words of the Vice President of IT Security:

"The vision and mission of the IT security department is based on the idea to safeguard our information assets. The formal statement is prescribed in the functionality statement of our department, stating to conduct the analysis, the formulation, the synthesis, the development, the implementation, and the evaluation of an IT security instrument to ensure the security of information technology as an asset, whether physical or logical (i.e., data and information) of the bank in a short term and in a long term."

The IT security department is responsible for the creation and adoption of security rules. The department consists of three subunits: (1) the IT security solutions unit that conducts the IT security systems development, (2) the IT security access and control unit that oversees the user access and privilege, and (3) the IT security strategy and planning unit that formulates the IT security strategic plan and blueprint as well as the IT security policy and procedures. The IT security policy and procedures are therefore an exclusive privilege of the IT security department. Not only are the policies aligned with the bank's organizational culture and strategy (Doherty and Fulford, 2006), but the policies are also initiated according to the central bank's information security guidelines. As a practice to adhere to the central bank's policies and regulations, Centro Metropolitan Bank, as a commercial bank, delivers regular (e.g., weekly, monthly, or annual) reports to the central bank and welcomes audit visits by a team dispatched by the central bank. Despite its diligent reporting practices, Centro Metropolitan Bank attempts not to involve the central bank in issues that the bank is confronting; rather the bank strives to conform and abide to the central bank's policies and regulations and to consult security issues with the central bank when necessary. The interference by the central bank often results in bad publicity for a commercial bank since this bank may be perceived as being unreliable and unable to resolve problems on its own. Despite allowing for minimum interference from the central bank, Centro Metropolitan Bank strives to maintain good institutional relationship with the central bank.

Centro Metropolitan Bank rigorously maintains its information systems and their security, particularly through the bank's IT security department. As a result, it possesses some of the most well designed corporate information systems in the nation. The bank prides itself in assuring that its most precious information (i.e., its customers' data) has never been breached. The information technology security is maintained and preserved by the IT security department. One of the department's goals is to assure the security of information technology assets, either the physical or logical components (i.e., data and information), both in the short and long run. This department also formulates policies and regulations of how information technology and electronic applications are to be used to preserve information security. Electronic applications include the bank's intranet system, electronic banking, ATMs, electronic data capture (EDC) machines, etc. In addition to maintaining the proper use of information technology, the department also educates stakeholders and raises their awareness of the importance of information security. The Head of IT Audit Unit maintains that:

"All tasks that include regulating, enforcing, controlling, and revising standard operating procedures or policies regarding risk of using IT are performed by the information technology department. They assume full responsibility for these tasks."

In addition to managing technology risk, the bank also believes that threat to information security may be due to human factors. The practice of securing its information adheres to the definition of operational risk by Basel II. When auditing the bank's information systems, the central bank's audit team investigates factors that contribute to operational risk: people (e.g., faults due to human error or lack of responsibility), process (e.g., false procedures), external factors (e.g., hackers or outsiders), and system (i.e., technology) (Flores et al., 2006, p. 384; Scandizzo, 2005). Many procedures and standards are formulated in a way that belong to and comprehended by bank's personnel and customers. These procedures and standards are developed using ISO 27001 framework, particularly for a certain specific scope such as the one that regulates data centers. To audit the bank's information systems and its security, the auditory team uses a combination of ISO 27001 and COBIT (i.e., for high level maintenance use such as governing risks related to the use of information technology). In addition to these frameworks, procedures and standards are formulated to conform and reflect regulations issued by the central bank.

An Instance of Electronic Data Capture (EDC) Fraud

The institutionalization of security policy in Centro Metropolitan Bank can best be depicted by the case of electronic data capture (EDC) fraud. In general, the EDC fraud case is an information security fraud case of which a fictitious merchant, a fictitious customer, and hence a fictitious transaction provided financial loss to a commercial bank. Parties other than the fictitious merchant and customer directly involved in this case, which occurred while the study was being conducted, include Centro Metropolitan Bank and another commercial bank, Blue Silver Bank, which directly suffered from the financial loss. This case also drew interference from the central bank, which acted as an intermediary between the two banks and as a consultant. This case indirectly involved a credit card issuer, which in this case was Visa. The case had never been made public as it had the potential to significantly damage the reputation of both the commercial banks involved. Both banks realized that if the case became public, they would lose reputation and credibility in the eyes of the public. In addition, Blue Silver Bank suffered a financial loss of more than US $1 million. The accounting and payment system supervisors of Blue Silver Bank examined Centro Metropolitan Bank and demanded progress reports on resolution, action plan, and mitigation progress from Centro Metropolitan Bank through the audit department. Progress was monitored and reports were requested and delivered for a period spanning six months prior and after the breach. In addition, the central bank also conducted random inspections to all EDC machines as an attempt to ensure that EDC machines are for online transaction only and enacted a policy that commercial banks should provide merchants with EDC machines that only allow online transaction. The central bank provided a six-month grace period for commercial banks with offline-transaction EDC machines to switch to machines for online transaction only. The central bank also heightened the policy to request EDC machines from a merchant to a commercial bank.

Centro Metropolitan Bank undertook several important measures, particularly its security policies, to prevent a similar case from occurring. The bank modified its EDC transaction policies and ensured that all such transactions were online, including those involving another bank as either the issuing bank or the acquiring bank. The bank upgraded the security of its EDC machines, reformatted the merchant acquisition policies to ensure no fictitious merchants are involved in EDC transactions, formed a new unit whose task was to monitor transactions involving debit card and maintain the card's fraud control, and modified the back office that handled electronic transactions so that it is able to immediately detect a transaction that were suspected to be fraudulent.

The EDC fraud incident also triggered the heightening of other security policies for Centro Metropolitan Bank's electronic banking. For example, the bank reinforces the importance to use PIN on its text-messaging banking system through extensive customer education. The text-messaging banking system is a unique electronic-banking system that allows customers to use simple-text messaging service to conduct electronic-banking transactions. The E-Banking Product Manager describes the heightened policies for text-messaging banking system as follow:

"We provide policies for customers who wish to use our SMS (i.e., text-messaging) banking system and educate our customers on how to use this system. For example, they are required to create a PIN during activation and we show them how to do this through pamphlets. This breakthrough program is not a required electronic banking product decreed by the central bank."

5. DISCUSSION

The case study provides insights as to how security policy in an organization is formulated, implemented, and reformulated when an incident of security breach occurs. These three processes reflect an institutionalization of a resource modality. We treat the security policy depicted in the case study as a resource modality that institutionalizes security structure at Centro Metropolitan Bank. Our case study, however, depicted an external interference by the central bank in the institutionalization of security in Centro Metropolitan Bank. Such interference forces participation of the bank's executives and managers in championing security policy (Knapp et al., 2006). We develop our case analysis discussion using mainly Barley and Tolbert's sequential model of institutionalization (see Barley and Tolbert, 1997, p. 101). We focus our attention on the structuration of institutional realm and its reciprocal effect on the realm of action. We also focus on the impact of script enactment in the institutionalization.

The institutional realm is an abstraction of regulated use of resources/materials drawn from experience. As an organization, Centro Metropolitan Bank has had such established abstraction creating an institutionalized information security or a stable structure of information security. In addition, as a commercial bank, the institutionalization of information security has a strong influence by the central bank. The institutionalization of information security through formulation and implementation of security policy is accomplished due to the cultural aspects of Centro Metropolitan Bank as a unique and independent entity (Huebner and Britt, 2006), implementing security policy that reflects the characteristics and cultures of the bank. Security culture implemented in an organization, including Centro Metropolitan Bank, reflects shared patterns of regulated use of security resources in a formal system (organizational structure), supported by the informal system (social members sharing their experience in informal communications) (Dhillon, 2007). In our case study, the institutional realm is reestablished when the central bank decrees new information security guidelines or when a security breach incident occurs (e.g., the case of EDC fraud).

The realm of action signifies the compliance with security policy and the impact of such compliance. Agency requires formal controls (e.g., regulations) and informal controls (e.g., informal shared norms and beliefs) to interact with resources and materials (e.g., EDC machines). Only in this way does the interaction become institutionalized and satisfy the organization's cultures and strategy (Doherty and Fulford, 2006). The established and internalized realm of action strengthens the institutional realm and helps maintain the social order. Our case study demonstrates the continuous interaction between Centro Metropolitan Bank's management staffs and employees (i.e., the agency at the Centro Metropolitan Bank) with EDC machines directed by the use of security policy. When the central bank passes new security guidelines, the agency is required to formulate new security policies that adopt the new guidelines and to implement the new policies. When the new policies are adopted and implemented over time, agency's use of the new security policies become habitualized and structuralized and agency's interaction with IT artifacts is well directed. The EDC fraud case, however, is the force to the reinstitutionalization of security policy in Centro Metropolitan Bank, prompting the central bank to decree new security guidelines to be adopted by commercial banks and financial institutions without exception.

Figure 1 depicts the institutionalization of security policy in Centro Metropolitan Bank using Barley and Tolbert's model of sequential model of institutionalization. The model depicted in the figure demonstrates three moments of scripts enactment: (1) the first box (i.e., setting T1) depicts a moment when the central bank passes new security guidelines, (2) the second box (i.e., setting T2) depicts a moment when Centro Metropolitan Bank's personnel and customers are familiar with the new policies and have habitualized the use of EDC machines, and (3) the third box (setting T3) depicts how the EDC fraud case causes the reinstitutionalization of security policies. Each box depicts four distinct processes shown by four arrows.

When the central bank issues new security guidelines, the institutional principles that contain the new security guidelines as the raw ingredient are encoded in the scripts for setting T1 (see arrow a). As the scripts become available, the bank's personnel enact the scripts that encode the institutional principles (see arrow b). The scripts become a guideline for the personnel to use IT artifacts (e.g., an EDC machine) according to the policies. As the scripts are new due to the central bank's recent enforcement, Centro Metropolitan Bank's personnel have yet had the opportunity to internalize the scripts and habitualize their actions. The Centro Metropolitan Bank's personnel are aware and conscious of their behavior to follow the scripts to use the security policies, signifying the modification of an institution (Barley and Tolbert, 1997, p. 102) of security policies. Arrow c depicts a situation when the personnel's actions replicate the scripts that were initially guiding the personnel's actions. We do not offer a revision to the scripts due to the nature of commercial banks' conformity to the central bank's prudential supervision to maintain *status quo* (i.e., stability). Hence we assume that revision to the scripts derives only from the central bank's new guidelines or any security breach incident. Finally, arrow d signifies the moment when the scripts that contain replication of personnel's actions become objectified and externalized in the institutional realm.

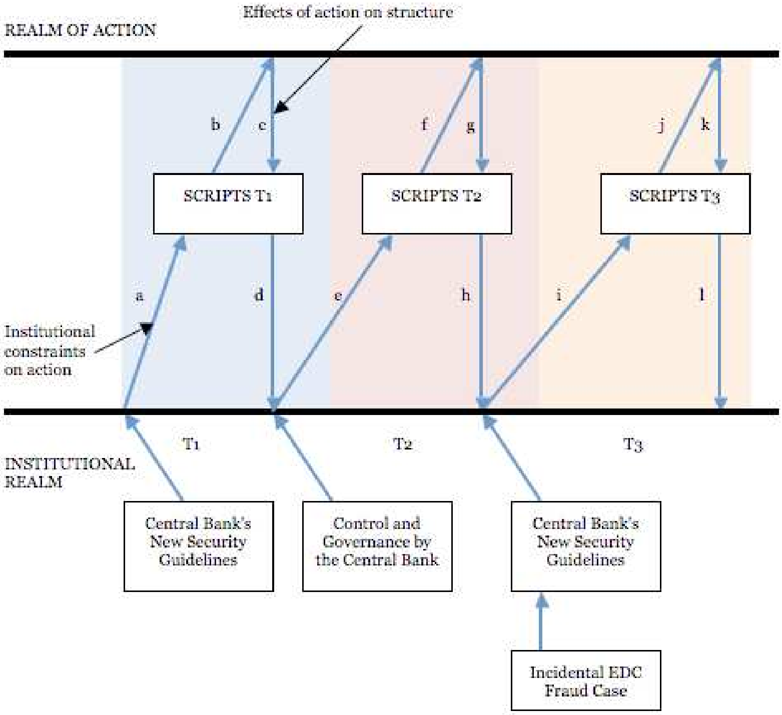
Effects of action on structure
REALM OF ACTION
b
c
f
g
j
k
SCRIPTS T1
SCRIPTS T2
SCRIPTS T3
a
d
e
h
i
l
Institutional constraints on action
T1
T2
T3
INSTITUTIONAL REALM
Central Bank's New Security Guidelines
Control and Governance by the Central Bank
Central Bank's New Security Guidelines
Incidental EDC Fraud Case

Figure 1.
A Sequential Model of Security Policy Institutionalization at Centro Metropolitan Bank Based on Barley and Tolbert (1997)

Setting T2 depicts the controlled maintenance of the scripts and actions. This setting begins with the central bank regularly monitoring the use of EDC machines of commercial banks, including such machines belonging to Centro Metropolitan Bank. Such monitoring (i.e., control and governance) is conducted by the central bank by regularly dispatching auditory team to visit Centro Metropolitan Bank while Centro Metropolitan Bank regularly submits policy implementation reports to the central bank. This monitoring, however, does not aim to modify the implementation of security policies. Instead, the monitoring activities aim to maintain stability of such implementations. Arrow e depicts the encoding of familiar institution of security policies in the scripts, which are enacted by Centro Metropolitan Bank's personnel (see arrow f). The difference is that the personnel may have internalized the scripts. The bank's personnel may automatically act according to the scripts and may be unconscious of what they are doing. This is the moment when their actions become internalized and are viewed as rational amongst their colleagues and supervisors in the bank. They further unconsciously replicate the scripts (see arrow g) and the scripts remain an objectification in the institutional realm (see arrow h). Setting T2 demonstrates, however, that strong involvement and interference by the central bank exercising a centralized, concentrated, power proves *"to compel a change in the culture of regulation"* (Schooner and Taylor, 2009, p. 272), particularly in developing countries such as Indonesia. Literature and observations do not, however, support such statement in developed countries such as the United States. Too much concentrated power by the central bank may actually cause negative effects (e.g., a commercial bank might be reluctant to exercise its freedom to formulate and implement security policies due to fear of the central bank retaliating by limiting the commercial bank's security activities) in banking sector of developed countries (Schooner and Taylor, 2009). The transfer from setting T1 to setting T2 depicts the formulation and implementation of security policies in an organization. Setting T1 particularly deals with the development of security policy (arrow a), consultation and approval (arrow b), and security awareness and policy education (arrows b and c) (see the security policies building summary provided by Hong et al., 2006). Setting T2 resembles the dissemination of security policies and delineates the moment when security policies become aligned with the bank's strategic information systems plan in preserving security of information in the bank (Doherty and Fulford, 2006), signifying the internalization and habitualization of security policy use.

Setting T3 demonstrates how incidental case drives the central bank to exercise its deontic power and constitutive power once more by formulating and enforcing new security guidelines. Deontic power is a power ascribed to the central bank due to its authoritative status in banking sector while constitutive power is a power possessed by the central bank to decree and enforce rules (Hall, 2008). The difference between setting T1 and setting T3 is that setting T1 may or may not be driven by a security-breach incidental case. The institutionalization of security policies in setting T3 (arrows i, j, k, and l), however, is similar to the process depicted in setting T1 (arrows a, b, c, and d). Assuming there is no other incidental case occurring, setting T2 recurs as setting T4 as Centro Metropolitan Bank's adopts the new security guidelines to formulate its own security policies and internalize the implementation of its new security policies to direct personnel's interaction with EDC machines.

6. CONCLUSION

This study demonstrates how security policies in a commercial bank are formulated and become institutionalized over time to direct security behavior and prevent security breaches. We are concerned with the fact that security policies are being rigorously formulated yet security breaches are still an issue. We are therefore looking at what actually occurs should compliance take effect and also when an incident of security breach takes place. We choose to combine institutionalization and structuration to investigate such effects taking place. Hence the use of a combination of institutional theory and structuration theory is appropriate for modelling the institutionalization of security policies. We conduct an empirical observation involving a large government-owned commercial bank in Indonesia as an example of how institutionalization of security policies proceeds (recall that scholars have denoted that institutions *never* emerge from nothing). Our empirical observation indicates a major finding that entails stable institutionalization of security policies as an impact of strong involvement and interference by the central bank. This is because the central bank exercises not only its power to regulate the formulation and implementation of security policies, but also its power to control and monitor such formulation and implementation among commercial banks. The paper provides useful insights for scholars to establish their research agenda by making use of our findings and for practitioners to consider our findings as a best practice to implement security policies.

The use of either institutional theory or structuration theory is not common in studies of information security since scholars tend to focus so much on the technical aspects of information security (Dhillon and Backhouse, 2001). Findings of research presented in this paper provide a major contribution to the socio-organizational studies of information security by demonstrating the effectiveness and efficiency of formulating and implementing security policies from a sociological stance. The highlight of such contribution is the delineation of how internalized security policies control security behavior and direct the use of IT artifact's security features that prevent security breach from occurring in subsequent episodes. In terms of theory, our study illustrates how institutional theory can be used to demonstrate how institutional forces (e.g., formal structure and the central bank's involvement) affect the design and the use of security policies (Björck, 2004). Our study also shows that security breach incident and central bank's interference are a contributing factor to improve and internalize security policies.

The field-work was however not without limitations. Firstly, our empirical observation is conducted in a developing country. Literature has indicated a different approach of control and governance by the central bank in developed countries. We suggest conducting empirical observations in banking sector of developed countries as a comparison to our study. Secondly, literature in banking studies has introduced the concept of prudential supervision by the central bank. Our study has yet to demonstrate an intense institutional relationship between a commercial bank and the central bank. We are certain that the information security governance elucidates the interaction between knowledgeable human agents and the wider social system within which they are elucidated. By taking into account the concepts of information security governance and prudential supervision, we believe that scholars should be able to delineate and demonstrate holistic information security governance in banking sector.

Our findings may be a source of theoretical model to formulate and implement security policies in a commercial bank. Practitioners can benefit from the theoretical model by looking at the impact of control and governance of an external higher authority on their operational activities. Practitioners can also benefit from considering the extent to which using security artifacts needs the effort to raise employee's awareness of security issues and taking into account reasonable amount of time and resources to allow for effective and efficient use of security artifacts.

REFERENCES

Barley, S. R. 1986. Technology as an occasion for structuring: Evidence from observations of CT scanners and the social order of radiology departments. *Administrative Science Quarterly*, 31, pp. 78-108.

Barley, S. R. and Tolbert, P. S. 1997. Institutionalization and structuration: Studying the links between action and institution. *Organization Studies*, 18(1), pp. 93-117.

Baskerville, R. and Siponen, M. 2002. An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5/6), pp. 337-346.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. The case research strategy in studies of information systems. *MIS Quarterly*, 11(3), pp. 369-386.

Berger, P. L. and Luckmann, T. 1966. The Social Construction of Reality: A Treatise in the Sociology of Knowledge. Anchor Books, New York.

Björck, F. 2004. Institutional theory: A new perspective for research into IS/IT security in organisations. In Proceedings of the *37th Hawaii International Conference on System Sciences*, Waikoloa, Hawaii.

Burrell, G. and Morgan, G. 1979. *Sociological Paradigms and Organizational Analysis*. Ashgate Publishing Co., Vermont.

Chandra, I. 2008. The five C's of IT policy. *The Internal Auditor*, 65(6), pp.23-24.

Dhillon, G. 1997. *Managing Information System Security*. Macmillan, London.

Dhillon, G. 2007. Principles of Information Systems Security: Texts and Cases. John Wiley & Sons, Inc., New Jersey.

Dhillon, G. and Backhouse, J. 2001. Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11, pp.127-153.

Dhillon, G. and Moores, S. 2001. Computer crimes: Theorizing about the enemy within. *Computer & Security*, 20(8), pp. 715-723.

Dhillon, G. and Torkzadeh, R. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal*, 16, pp. 293-314.

Doherty, N. F. and Fulford, H. 2005. Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal*, 18(4), pp. 21-39.

Doherty, N. F. and Fulford, H. 2006. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), pp. 55-63.

Doherty, N. F., Anastasakis, L., and Fulford, H. 2009. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29, pp. 449-457.

Eisenhardt, K. M. 1989. Building theories from case study research. *Academy of Management Review*, 14(4), pp. 532-550.

Flores, F., Bonson-Ponte, E., and Escobar-Rodriguez, T. 2006. Organizational risk information system: A challenge for the banking sector. *Journal of Financial Regulation and Compliance*, 14(4), pp. 383-401.

Giddens, A. 1984. *The Constitution of Society*. University of California Press, California.

Hall, R. B. 2008. Central Banking as Global Governance: Constructing Financial Credibility. Cambridge University Press, Cambridge.

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

Hong, K. S., Chi, Y. P., Chao, L. R., and Tang, J. H. 2006. An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, 14(2), pp.104-115.

Huebner, R. A. and Britt, M. M. 2006. Analyzing enterprise security using social networks and structuration theory. *Journal of Applied Management and Entrepreneurship*, 11(3), pp. 68-77.

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, F. N. 2006. Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1), pp. 24-36.

Orlikowski, W. J. 1992. The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, 3(3), pp. 398-427.

Orlikowski, W. J. 2000. Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science*, 11(4), pp. 404-428.

Orlikowski, W. J. and Iacono, C. S. 2001. Research commentary: Desperately seeking the 'IT' in IT research – A call to theorizing the IT artifact. *Information Systems Research*, 12(2), pp. 121-134.

Orlikowski, W. J., Yates, J., Okamura, K., and Fujimoto, M. 1995. Shaping electronic communication: The metastructuring of technology in the context of use. *Organization Science*, 6(4), pp. 423-444.

Powell, W. W. and DiMaggio, P.J. 1991. *The New Institutionalism in Organizational Analysis*. The University of Chicago Press, Illinois.

Rhee, H. S., Ryu, Y. U., and Kim, C. T. 2005. I am fine but you are not: Optimistic bias and illusion of control on information security. In Proceedings of *the International Conference on Information Systems* (Avison, D. E. and Galletta, D. F. Eds.), Las Vegas, Nevada.

Ross, S. J. 2008. Enforcing information security: Architecture and responsibilities. *Network Security*, 2(7), 7-10.

Scandizzo, S. 2005. Risk mapping and key risk indicators in operational risk management. *Economic Notes*, 34(2), pp. 231-256.

Schooner, H. M. and Taylor, M. W. 2009. *Global Bank Regulation: Principles and Policies.* Elsevier Inc., Massachusetts.

Scott, W. R. 1987. The adolescence of institutional theory. *Administrative Science Quarterly*, 32(4), pp. 493-511.

Scott, W. R. 2008. *Institutions and Organizations: Ideas and Interests*. 3rd Edition. Sage Publications, California.

Selznick, P. 1969. *Law, Society, and Industrial Justice*. Russell Sage Publications, California.

Smith, S. and Jamieson, R. 2006. Determining key factors in e-government information system security. *Information Systems Management*, 23(2), pp. 23-32.

Walsham, G. 1993. *Interpreting Information Systems in Organizations*. John Wiley & Sons, Inc., Chichester.

Walsham, G. 1995. Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems*, 4, pp. 74-81.

Walsham, G. 2006. Doing interpretive research. *European Journal of Information Systems*, 15, pp. 320-330.

Walsham, G. and Han, C. K. 1991. Structuration theory and information systems research. *Journal of Applied Systems Analysis*, 17, pp. 77-85.

Yin, R. K. 2003. *Case Study Research: Design and Methods*. 3rd Edition. Sage Publications, Inc., California.