A CONCEPTUAL MODEL OF VIRTUAL BANK I.S. SECURITY META-POLICY FROM A NETWORK PERSPECTIVE

Smita Paul  
*University of Auckland Business School, smita.paul@auckland.ac.nz*

Ruilin Zhu  
*University of Auckland Business School, ruilin.zhu@auckland.ac.nz*

Follow this and additional works at: [http://aisel.aisnet.org/pacis2016](http://aisel.aisnet.org/pacis2016)

Recommended Citation
[http://aisel.aisnet.org/pacis2016/66](http://aisel.aisnet.org/pacis2016/66)
A CONCEPTUAL MODEL OF VIRTUAL BANK I.S. SECURITY META-POLICY FROM A NETWORK PERSPECTIVE

Smita Paul, Department of Management and International Business, University of Auckland Business School, Auckland, New Zealand, smita.paul@auckland.ac.nz
Ruilin Zhu, Department of Information Systems and Operations Management, University of Auckland Business School, Auckland, New Zealand, ruilin.zhu@auckland.ac.nz

Abstract

Despite a continued scholarly conversation on Information Systems Security (ISsec) policies and governance, a perspective that examines these issues at the organisational level has been generally neglected. This is of concern as managing ISsec is multi-level in nature for many organisations ranging from the individual level, such as BYOD (Bring Your Own Device) policies, to the strategic level, such as the use of Chief Security Officers (CSOs). This deficiency is also evident for virtual banks as a type of IS (Information System)-led organisation that develop flexible policies due to changing internal and external security environments.

In order to focus on the multi-level and flexible nature of ISsec policies of virtual banks, we borrow key concepts from the organisational network perspective to map organisation structure changes through ISsec development phases and shifting meta-policies.

The goal of this paper is to develop the theoretical framework and conceptual model needed to examine the multi-level and flexible nature of organisational ISsec policies of virtual banks. We start with building on relevant literature on ISsec meta-policy characteristics and then integrate network concepts from the ARA (actor, resource, activity) framework to map the changing ISsec policies at the individual, meso, and meta-organisational level.

Keywords: Information Systems Security, Virtual Banks, Organisational Network Theory, Meta-policy.
1 INTRODUCTION

As banks continue to move towards the integration of Information Systems as core-activities (Liao, Shao, Wang, & Chen, 1999) the role of virtual banking services has become increasingly integral for capturing and retaining customers for banks. Due to the increasingly ubiquitous nature of virtual banking services it is understandable that information systems security and privacy (ISsec) continues to be a significant concern for practitioners and academics alike. However the majority of studies still examine issues at the individual level of analysis, such as the adoption of mobile banking and internet banking services by customers (Lin, 2011; Wang, Wang, Lin, & Tang, 2003). The quality of virtual banking is not only determined by the information security behaviours at the individual level but also at the organisational or meta-policy level (Knapp, Morris Jr, Franklin, Marshall, & Byrd, 2009).

In addition, virtual banking organisations need to be more flexible compared to traditional banking organisations as they have constantly changing organisational structures and adaptive information security systems (Liao et al., 1999). This is because virtual banks can be defined as banks that provide traditional banking services through non-traditional means, such as mobile banking and internet banking, and do not currently have physical ‘bricks-and-mortar’ branches (Liao et al., 1999). We believe that the virtual banking phenomena offers a thought-provoking window into IS (Information Systems)-led organisational structures that are dynamic in nature and that there is a need to start conceptualizing the phenomena of virtual banking and their inherent organisational ISsec issues. In this vein, our overarching and exploratory research question is ‘what is the nature of organisational ISsec issues within virtual banks?’

Extant literature and theorizing on flexible organisational structures and ISsec meta-policies are fragmented in nature and practitioner-led (Williams, Hardy, & Holgate, 2013). The main scholarly conversations in ISsec focus on the individual level of analysis and integrate conclusions and theories from the behavioural sciences, such as psychology, and from a risk/investment perspective for IS governance, such as from economics (Bulgurcu, Cavusoglu & Benbasat, 2010; Lee, 2009). In order to conceptualize virtual banking structures as a flexible organisations and pinpoint where inherent multi-level ISsec issues may arise, we borrow and integrate concepts from the scholarly stream of organisational networks from the related discipline of organisational science. Organisational network research not only focuses and extends dynamic concepts of organizations but also looks at the activity structure within the firm (Brass, Galaskiewicz, Greve & Tsai, 2004). For example, network concepts can allow us to ‘map’ the influence of meta-policy changes through the organisation as it reconfigures sub-policies such as those for BYOD (Bring Your Own Device).

In addition, examining the adaptation of ISsec meta-policies through a network organisational structure lens may offer further insights into what makes virtual banks distinctive from traditional banks that are less reliant on IS technologies. Our core contribution to ISsec is an elucidation of inherent ISsec issues of virtual banking due to their multi-level organisational network structure and the nature of their adaptive ISsec meta-policies due to their flexible nature.

The goal of this paper is to develop the theoretical framework needed to understand the phenomena of virtual banking and organisational-level ISsec issues and flexible policies. In the next section we outline the relevant ISsec literature and our chosen theoretical lenses. This is followed by our conceptual model of organisational ISsec of emergent organisations which ends with some examples from virtual banking services and organisations and an outline of the next step of collecting empirical data.

2 THEORETICAL FRAMEWORK

2.1 Organisational ISsec meta-policy

ISsec policy addresses “the integrity, availability, and confidentiality of electronic data held electronic data held within and transmitted between information systems” (Knapp et al., 2009, p. 494) and is the
foundation of an organization’s information systems security (Straub, 1990). Previous work on ISsec governance and practices are practitioner-led with no unifying standards and are technology focussed. However there have been calls for a socio-technical perspective on organisational ISsec policy (Williams et al., 2013). Our first step in developing our theoretical framework was to perform a targeted literature search of top ranked (according to the Australian Business Deans’ Council) Information Systems journals, such as Management Information Systems Quarterly, on information security. We found that extant scholarly work generally falls within two categories, information security awareness at the individual level such as with employees, and at the strategic level such as the use of CSOs (Corporate Security Officers). For example, Siponen’s (2001) five dimensions of information security awareness includes an organisational component that is measured and understood at the individual level of analysis.

Concentrating at the organisational strategic level of analyses, conversations often fall on examining security risk management strategies. For example, Kotulic and Clark (2004) conceptualize organisational security issues through configurations of security risk management programs. These are designed according to the level of centralization of an organisational structure. However we depart from Kotulic and Clark’s (2004) work by concentrating on organizations whose structure does not rely on traditional organisational design elements, such as hierarchies and centralisation, and so have ensuing governance that are inherently dynamic, flexible and process based (Kankanahalli, Teo, Tan, & Wei, 2003). We do this because IS-led organisations, such as virtual banks, often work interdependently among business units as a centre of excellence in order to leverage their skills across the whole business network (Gerth & Rothman, 2007).

Knapp et al.’s (2009) work on process model of organisational-level ISsec governance puts the significance of an ISsec organisation-level policy to the forefront. They offer a comprehensive overview of the policy management and implementation phases taken to develop and implement ISsec policies with the influence of the categories from both internal and external factors. However, such categories stop short of exploring governance issues further, for example, what makes an essential ISsec policy? What is the chain of command and what type of senior management support influences ISsec organisational policy rather than a single policy going through its development stages?

Furthermore, Knapp et al. (2009) offer a process model but not a process perspective that captures the dynamic and flexible nature of organisations. The process model highlights linear stages with feedback loops but does not pinpoint reconfiguring events. How does the development of an organisational ISsec policy change over time? What are its emergent qualities and what events are they in response to? Answering such questions would lead to conclusions on what Baskerville and Siponen (2002) term ‘good security policies’ that take into consideration the socio-technical and management aspects.

Knapp et al.’s (2009) overarching category of ISsec governance was understandably nebulous given their level of analysis. As a step further, Baskerville and Siponen (2002) develop the concept of organisational ISsec policy as ISsec meta-policies for emergent organisations. They argue that ISsec policies should be multi-level in nature and link organisational policies (high-level policies) to individual level (lower-level security responses). In an organisation, a meta-policy would be a nested hierarchy of lower-level policies requiring input from all levels. Baskerville and Siponen (2002) also offer characteristics to evaluate meta-policies that go beyond “ready-made lists of particular actions” (p. 344).

As such, we take the first step for developing our organisational ISsec model for virtual banks with the policy development and implementation phases from Knapp et al.’s (2009) model. These phases are risk assessment, development, approval, awareness and training, implementation, monitoring (audits and automated tools), enforcement, review and retirement. We also focus on the internal influences of the model, more specifically senior management support, business objectives and internal threats. We do this in order to add to the extant ISsec literature that concentrates on either awareness or governance by examining how these two areas influence each other.

Therefore we narrow our research scope down to focussing on the internal elements of virtual banks, such as their employees and organisational ISsec systems. This is not to say that external influences
and ISsec threats from customers are not significant but we argue any relevant external threats should be present through internal ISsec policy development and implementation. Secondly, we also do not dismiss the internal influences of organisational culture and technology architecture but believe that the relevant outcomes from these two dimensions should be present in the policy development process. For example, the available technology architecture would be a key component of risk assessment and policy awareness and training and artefacts of organisational culture would be present in the policies being implemented and even retired. Our focus is on the processes and emergent properties of organisational ISsec policy rather than its predictors, such as fluctuating external legal requirements.

We then adapt Knapp et al.’s (2009) model by integrating Baskerville and Siponen’s (2002) meta-policy characteristics to examine organisational level ISsec. We do not separate out the governance issue hierarchically as Knapp et al. (2009) have done as we acknowledge that virtual banks are dynamic and are highly networked and multi-level with relation to information sharing within organisational structures.

We integrate Baskerville and Siponen’s (2002) four categories of meta-policy and (lower-level) policy features, which are firstly, the essential characteristics of identification and classification of security subjects and objects. The former refers to the different entities within banks that have various security concerns over their governance, operations and business and the later suggests the tangible or intangible assets being influenced by security that belong to the banks. Those subjects and objects should additionally be tailored to meet the requirements and needs for meta-policy. Secondly, the design processes through the creation of a policy and sub-policy hierarchy. Virtual banks should specify the processes from which policies are designed and implemented so that each level policy may have a different “level of abstractions and enforcement” (Baskerville & Siponen, 2002, p. 343). Lastly are implementation and testing. They advise that implementation should be closely matched to the level of security policy changes and testing fully validates any policy implemented. Being an IS-led organisation, virtual banks may have new divisions/departments that have not been introduced in traditional banks. They therefore need to understand how policies are implemented and whether new policies are consistently executed across different levels. We integrate and put these categories under the title organisational ISsec meta-policy. In our adapted model, this is situated above the policy development cycle to highlight its organisational and all-encompassing nature.

However, we also conceptualise virtual banking as an emergent and flexible organisation due to its rapidly changing information security internal and external landscape. The arguments for this conceptualisation and how we utilise the organisational network perspective to examine and integrate its dynamic and evolving nature is presented in the coming sections.

2.2 Virtual banks as flexible IS-led organisations

Organisations that responded to their internal and external environments with novel organisational structures were originally described as emergent organisations (Kay, 1984). Within the IS field, emergent organizations were originally defined by Truex, Baskerville and Klein (1999, p. 117) as social structures that are an outcome of “constant social negotiation and consensus building”. Truex et al., (1999) also used the term ‘emergent’ rather than ‘emerging’ to denote the constant evolving nature of such organizations and their policies in reaction to previous history and context. However since then little has been done to explore emergent organizations and their nascent ISsec issues. This may be because most IS-led organisations were understood to already be a form of emergent organisation due to their reliance on constantly changing IS technologies compared to more traditional organisations.

Some scholars have inexplicably subsumed ISsec governance and its ability to be flexible into the scholarly discussion on Agile IS (Salmela, Tapanainen, Baiyere, Hallanoro, & Galliers, 2015) while giving the same arguments as the emergent organisation concept. However most Agile IS scholars fall into determining flexibility and agility of physical IS assets, such as the flexibility of IT infrastructure (Salmela et al., 2015). Within the broader IS scholarly discipline, there are a few studies that attempt
to conceptualize ISsec thinking further, such as Knapp, Morris, Rainer and Bryd’s (2003) work on viewing network-based security as biological defensive mechanisms. Williams et al (2013) use institutional theory to understand the contextual factors of ISsec governance and reframe it as information protection governance. However both works position ISsec as a reactive stance, defensive or protective, rather than adaptive and proactive. Fortunately, Baskerville and Siponen’s (2002) work specifically on ISsec multi-level policies for emergent organizations comes closest to our view. However frustratingly little, theoretically and empirically, has since been done at the organisational level of IS-led organizations as a continuing scholarly conversation since then.

A form of IS-led organization, virtual banking, has gained prominence due to the evolving nature of banking services and wide-spread adoption of internet and mobile technologies by customers (Liao et al., 1999). Rather than a simple support service for traditional banking services, such as personal wealth and business banking, virtual banking has become a key service in its own right. It has and continues to be affected by its constantly changing environments, internally (such as BYOD security issues) and externally (such as hacking and phishing scams). Lee (2009) argues that ISsec continues to be a significant factor in the virtual banking domain.

One key issue for ISsec policies development of IS-led organizations, such as virtual banking divisions, is addressing a holistic perspective of which we integrate Baskerville and Siponen’s (2002) concepts of ISsec meta-policy. We also use their specific requirements for emergent organisations to analyse the flexible and adaptive nature of organisational ISsec policy, namely suppleness, political simplicity and criterion-orientation. Suppleness refers to a flexible security policies that change in tandem with organisational responses and goals. Political simplicity relates to soft security controls that do not force employees into non-compliance. Lastly, criterion-orientation requires meta-policies to be developed in relation to organisational compliance.

However, simply listing the requirements of a meta-policy does not explain the inherent ISsec concerns of IS-led organizations that are flexible in nature. A list also does not explain the structure of the organization, how the structure changes or how it has changed in reaction to internal and external ISsec events. Our arguments are also in line with Markus and Robey’s (1988) conclusions on the emergent perspective of IS. This perspective requires “detailed understanding of dynamic organisational processes in addition to knowledge about the intentions of actors and the features of information technology” (Markus & Robey, 1988, p. 589). Understanding such processes would allow scholars to delve deeper into the organisational ISsec of IS-led organisations to conceptualise and test specific native emergent constructs and also help practitioners to develop systems to map and implement organisational meta-policy effectively.

2.3 Flexible IS-led organisations from an organisational network perspective

In order to better understand how the structure of virtual banking as an IS-led organization and how its meta-policy is shaped by events, we borrow concepts on organisational networks from organisational science. We turn to the network perspective as it also has precedence in IS theorizing and there are similar underlying assumptions that enable the blending of concepts from these two research areas under the context of emergent ISsec issues. A significant precedent for our discussion is Ahuja and Carley’s (1998) work on the network structure in virtual organisations. They argue that most organisations can be considered complex networks of information sharing that run along and influence organisational structure and design. We take a similar view in our discussion of ISsec meta-policy, internal forces such as senior management support and internal threats shape the development and so the structure of ISsec organisational design, be in the form of an overseeing ISsec and Privacy CO and/or office. We also argue that the development and response of organisational ISsec meta-policy and its sub-policies develop along such complex network organisational structures. Tracing and mapping the ISsec organisational policy development through such network structure will enable us to examine meta-policy evolution and its multi-level nature.
Most organisational network research utilises concepts from social network theory (Brass et al., 2004). Scholars concentrate on trust and power and determine related dimensions, such as level of centralisation, structural holes, levels of hierarchy, and actor interactions (Ahuja & Carley, 1988; Ahuja, Soda, & Zaheer, 2011; Olsen, Prenkert, Hoholm, & Harrison, 2014). However, a sub-section of network scholars offer a more in-depth understanding of organisational structure in relation to actor bonds, resource ties, and activity links (Håkansson & Snehota, 1995). These three components form the scaffolding for the organisational network structure. Actor bonds are the relationships between two actors, such as at the individual level they can be between commercial banking relationship manager and an operations clerk. These can be strong or weak depending on the level of trust, ongoing projects etc. Actors may also exist at different levels, at the meso-level this may be a relationship between the wholesale banking subsidiary and the mobile banking division. At the organisational level, this could be a relationship between the Overseeing ISsec and Privacy CO subunit and a country sales unit. These relationships are influenced by their control of resources and what activities they pursue. For example, a private banking relationship manager at a virtual bank may have more human resources to attend to their customer online but not face to face due to pared down brick and mortar office space. The private banking relationship manager as an actor also influences the activities he/she may carry out, such as spending resources to develop a mobile banking service for a specific strata of clients. At the organisational level, the activity between the Overseeing ISsec and Privacy CO subunit and a country sales subunit could be the implementation of a localised ISsec policy, such as training for BYOD.

More significantly, the ARA model and network perspective allows us to analyse the multi-level network ISsec issues through understanding the internal organisational structures of the virtual banking unit. We utilize the concept of actor dyads to understand how such structures adapt to a flexible ISsec meta-policy. Dyads are the linkages between two key actors of an organisational structure (Halinen, Salmi, & Havila, 1999), such as relevant departments within virtual banking, which can reconfigure according to changes in ISsec policies. The linkages may be communication lines between departments that increase in frequency and intensity depending on current ISsec projects (Provan, Fish & Sydow, 2007). To understand the changes and source points of emergent ISsec issues, ‘snapshots’ of the network structure over time can be compared.

3 A CONCEPTUAL MODEL OF ORGANISATIONAL ISSEC META-POLICY FOR VIRTUAL BANKS

For our conceptual model of organisational ISsec meta-policy for virtual banks, we integrate the arguments made in the previous sections. We first developed an overall theoretical framework for understanding organisational ISsec meta-policy by integrating conclusions on Knapp et al.’s (2009) work on policy development and implementation with Baskerville and Siponen’s (2002) work on ISsec meta-policy. This was our first step towards conceptualizing organisational ISsec meta-policy and its sub-policies are multi-level in nature. Meta-policy definition and implementation is directly linked and holds nested groups of sub-policies that should directly related to organisational directives on ISsec. For example, within a virtual bank, as part of their meta-policy, the implementation of customer data security would meet the organisational directives to ensure the safeguard and trustworthiness of their services for their stakeholders. To ensure its implementation, there would be a number of sub-policies that would have to pass through the development and implementation phases, such as risk assessment and even which need to be retired.

Our next step was to focus on flexible IS-led organisations and therefore virtual banks. We argue that studying virtual banks will give us a window into a type of IS-led organisation that more reliant on IS technologies and ISsec governance than traditional banks with more brick and mortar infrastructure. Continuing on with our previous example, this type of organisation would also need to be more adaptive and flexible in its ISsec meta-policy and sub-policies as it would be more sensitive to changes in
IS technological opportunities for more effective customer service and threats to information security and privacy. We integrate Baskerville and Siponen’s (2002) dimensions for flexibility, that is, suppleness, political simplicity and criterion-orientation. Suppleness is understood as security policies that are flexible in nature. For example, a virtual bank may experience a breach in customer data security. In an attempt to mitigate fallout in customer trust, a meta-policy may be put in place to develop proactive policies and technologies to lower the risk of such a breach in the future. Political simplicity relates to ISsec controls that do not force employees into non-compliance. For example, if employees are expected to work during travel, they would be given work laptops with secure intranet connections that disallowed the ability to use personal cloud data software (for example, Dropbox) that would increase the risk of data security breaches. Criterion-orientation relates to organisational compliance, a key part of the banking sector. Meta-policies in virtual banks would be put in place to navigate local and international banking compliance needs. For example, a virtual bank can face changing government restrictions on the level of investment held by foreign customers from certain countries and a meta-policy should be in place to be proactive in handling such changes.

Lastly, we integrate the organisational network perspective in order to trace and map ISsec organisational policy development to examine meta-policy evolution and its multi-level nature. To do this we use the ARA model to form the scaffold of the organisational network and to understand how events influence and change ISsec meta-policy and its sub-policies over time. Taking ‘snapshots’ of the network in relation to actor bonds, resource ties and activity links allows us to directly map such changes. To continue with the example above, the actors in a virtual bank when implementing changing government restrictions may be the bank’s treasury and a sale country’s private banking section. Their resources would what access they had to foreign exchange amounts to deal with a large number of customers taking out capital due to changing investment regulations. This relationship between treasury and the sale country subunit may become less active over time as customers invest their dollars with another country or bank. However, this relationship may reactivate when similar situations arise in other sale country subunits and best practice may be transferred in order to reduce customer attrition.

Figure 1. A Conceptual model of organisational ISsec meta-policy for virtual banks
Coalescing these three concepts of a flexible, multi-level organisational ISsec meta-policy and the organisational network perspective give us our conceptual model for virtual banks (Figure 1). With this model, avenues for future research are varied and empirical testing remains to highlight the significant dimensions for virtual banks and their organisational structures.

4 CONCLUSION

In this paper we aim to present the theoretical framework and conceptual model for examining organisational ISsec meta-policies and their sub-policies of virtual banks. We focus on virtual banks as they present a germane context for understanding ISsec issues at the organisational level that is multi-level and dynamic – issues so far neglected in the extant literature.

We developed our framework and model from relevant literature, focussing on Knapp et al.’s (2009) phases of organisational ISsec policy development and implementation. We then integrate Baskerville and Siponen’s (2002) arguments on ISsec meta-policy of emergent organisations in order to examine its flexible nature. Lastly, we borrow network concepts from the related field of organisational networks in order to study and map the nested and multi-level nature of organisational ISsec.

We hope future empirical examinations and testing of the theoretical framework and conceptual model will provide fruitful enquiry into the flexible processes and requirements of organisational ISsec of virtual banks. We will first pursue an interpretive epistemological study utilising qualitative methods due to the nascent concepts of organisational level ISsec meta-policy (Edmondson & McManus, 2007). Given the complex and changing nature of virtual banks, we will concentrate on a single case study (Yin, 2009). We will use within-method triangulation (Jick, 1979) and analysis of data from semi-structured interviews, organisational documents, and participant observation to amend our conceptual model and offer propositions for further empirical testing (Myers & Newman, 2007). We also hope that any conclusions gathered may be applied to other organisations as they move towards less traditional structures and to ones that rely more on virtual services and dynamic and flexible organisational structures.

References


