ACIS 2013 Proceedings

Australasian (ACIS)

2013

Information security: a stakeholder network perspective

Max Soyref
The University of Sydney, max.soyref@sydney.edu.au

Philip Seltsikas
The University of Sydney, philip.seltsikas@sydney.edu.au

ACIS 2013
RMIT MELBOURNE

Information Systems: Transforming the Future

24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

Proudly sponsored by

nab
ACIS 2013 Principal Sponsor

RMIT UNIVERSITY

CITRIX®

GS1® Australia

acs AUSTRALIAN COMPUTER SOCIETY

ACS Foundation
Advancing ICT through Education and Research

ACPHIS

AAIS
Australasian Association for Information Systems

Information security: a stakeholder network perspective

Philip Seltsikas
Discipline of Business Information Systems
University of Sydney Business School
Sydney, Australia
Email: philip.seltsikas@sydney.edu.au

Max Soyref
Discipline of Business Information Systems
University of Sydney Business School
Sydney, Australia
Email: max.soyref@sydney.edu.au

Abstract

Despite existing approaches and techniques for securing corporate information assets, information security threats continue to challenge business and government. Research suggests that to improve the effectiveness of information security a clear understanding of the organisational context is required. We have used stakeholder salience and stakeholder networks lenses to identify key stakeholders who shaped the information security processes of a large Australian financial institution. We have also examined how the interrelationships between these stakeholders might impact on their role in a stakeholder network. Our research suggests that a number of key stakeholders exist who require attention and engagement from those responsible for information security. We also highlight several stakeholders that have traditionally been given lower priority, but should be seen as more important due to their positioning and influence on the stakeholder network. We suggest that a better understanding more concerted engagement with these stakeholders can assist information security teams in achieving organisational security objectives.

Keywords

Information security, stakeholders, stakeholder network

INTRODUCTION

Information security threats represent a major cost for organisations. Organisational boundaries have become more porous and the use of new technologies, such as cloud computing, mobile devices and e-commerce have increased the number of possible threats (Teller 2012). Despite recognition of the importance of the problem, many large organisations struggle to effectively protect their information assets against cyber-threats. Understanding the broad information security landscape is an imperative for successful information security management. Stemming from the results of our research we propose that a number of key stakeholders exist that need to be taken into account (in a concerted manner) by the information management teams within organisations. We use stakeholder salience and stakeholder network lenses to examine and determine the stakeholders and how their interrelationships impact on information security management practice.

In this paper we first present an overview of existing literature and examine current approaches to information security, stakeholder theories and their use in information systems research. We posit that stakeholder salience theory and stakeholder network perspective can offer a unique insight into examining information security practices. We propose that identification and classification of stakeholders relevant to information security is highly important, however these stakeholders need to be viewed through the lens of the totality of their complex interrelationships and not just their individual interactions with the security function within the firm. We present our findings from a single in-depth case analysis of a large Australian financial institution that shows how those responsible for information security perceive key stakeholders in the information security landscape and how these relationships have influenced their information security practice. We conclude by arguing that an understanding of the key stakeholder relationships and the network effect from their interactions can allow businesses to strengthen their ability to manage emerging threats and improve the way they interact with dynamic organisational contexts for their information security solutions.

LITERATURE REVIEW

Despite existing and extensive research efforts in the information security domain, information security remains a key challenge to modern organisations. On the software engineering side we see a continuous development of technical solutions to ever-evolving cyber threats. Malicious actors, however, often outpace these developments, forcing industry and the research community to defend, rather than proactively protect. This has led to a number of studies focusing on the socio-technical aspects of information security to create governance frameworks, policies and effective controls that can remain agile and dynamic regardless the threat landscape.

The last forty years have seen a steady evolution of approaches for addressing information security challenges (Salmela 2008). From control checklists (Baskerville 1993) and risk-management frameworks (Dhillon and Backhouse 1999) to a wide-spread use of information security standards (Siponen 2006). These approaches aim to put in place governance and control frameworks that ensure a baseline level of protection for organizations facing an ever-evolving landscape of threats. Despite many organizations seeing these approaches as a useful starting point, many of these have been critiqued by both researchers and practitioners where contextualizing the approach to individual organizational needs and dealing with unique circumstances and challenges is required (Siponen 2003; Stytz 2007).

In dealing with the difficulties of security standards being too generic, many industry or sector-based standards have evolved (Kankanhalli et al. 2003). For example ISO27011 and ISO27015 which offer guidance to the telecommunication and financial services industries respectively have developed out of the ISO27002 information security standard. Further to these sectoral approaches, a number of maturity and architecture frameworks have been developed to achieve alignment with business objectives and the business environment (see for example SABSA). Nevertheless, those responsible for information security face daily challenges to ensure that by applying good practice approaches they are adequately protected given their specific business situation (Siponen 2005).

Engaging with the context implies an understanding of the multitude of actors and stakeholders that are involved in shaping it (Hosking and Morley 1991). With increased numbers of outsourcing partners and contractors the boundary of a firm is much harder to define than before (Kotzab et al. 2009). Therefore, it has become necessary to better understand stakeholders involved in information security, and their relationships to information security teams within organisations and with each other. Examining the roles and relationships of all those affecting and affected by information security can offer opportunity for a clearer understanding of how modern firms deal with information security.

Stakeholders have been a focus of research studies in a variety of disciplines. Stemming from the discussion of corporate social responsibility (Freeman and Evan 1990), stakeholder research has examined a variety of ways for identifying, classifying and engaging with organisational stakeholders (Donaldson and Preston 1995). Stakeholders are classically defined by Freeman (Freeman 1984, p. 46) as ‘any group or individual who can affect or is affected by the achievement of the organization's objectives’. Despite this broad definition, an extensive debate exists on which actors can be seen as stakeholders and how engagement models can be differentiated between different types of stakeholders (Mitchell et al. 1997).

Information systems research has also embraced the importance of stakeholder identification and management. A variety of studies have looked at the necessity to examine stakeholders and their relationships in project management (Elias et al. 2002), information system development (see for example (Pouloudi 1999; Pouloudi and Whitley 1997)) and implementation (Boonstra 2006). These studies have ranged from examinations of the role of particular stakeholder groups, to in-depth investigations of stakeholder relationships. They offer an insight into how various groups might impact the use and placement of information systems within modern organisations.

Information security research has had some exposure to the examination of stakeholder roles. However, most of these studies have focused on the relationship between information security teams and one particular stakeholder relevant to their activity. For example, some studies have examined malicious actors (Cavusoglu et al. 2005; Galbreth and Shor 2010) or leaders (Chan et al. 2005). Others, have used broader theories, such as institutional theory to examine the relationships with internal and external actors (Hu et al. 2007). However there is a need for in-depth stakeholder evaluation in relation to information security practice. Such evaluation can offer insights into key influencers on the security practice within the firm and as other stakeholder theories provide mechanisms for more effective engagement and stakeholder management.

Building on over 20 years of prior research, Mitchell et al (1997) have proposed a theory of stakeholder salience. Their theory is based on the premise that all stakeholders can be examined through lenses of power, legitimacy and urgency. Where power is the ability to influence organisational behaviour, legitimacy is desirability and morality of actions and urgency is driven by time and criticality of the issue at hand. Each stakeholder could be compared against these three criteria to identify their salience and categorised as high, medium or low priority. Such categorisation can offer managers a way to prioritise their engagements with stakeholders as well as offer guidance on how these engagements could be conducted. Specifically in relation to security, examining power, legitimacy and urgency allows for a practical, yet effective classification mechanism that might simplify stakeholder interactions between information security teams and others within and beyond the organisation.

While Mitchell et al.'s (1997) theory provides a very useful lens to examine stakeholder relationships, some of the criticism of stakeholder theories has been the lack of consideration for relationships between organisational stakeholders that might affect how they interact with the organisation (Pouloudi and Whitley 1997). Therefore, when it comes to information systems and information security, stakeholders cannot be examined in hub-and-spoke relationships with the information security teams within a firm (Roloff 2008). Actors throughout the information security landscape do not only interact with information security teams within an organisation, but also influence each other, often changing or magnifying the role of particular stakeholders. In dealing with such concerns, Kivits (2011) has integrated the idea behind stakeholder salience with discourse and stakeholder network analysis to examine stakeholder engagements through a lens of complex multi-group interactions. We propose using a similar lens and examine the engagement of information security actors within organisation with relevant stakeholders. Given varied strengths and frequency of inter-stakeholder interactions, their positioning within the network can impact on their immediate power, legitimacy and urgency, thus shaping their salience and prioritisation requirements by information security managers.

We take a view similar to Pouloudi and Whitley (1997) that stakeholder relationships are dynamic and mutually shaping, where an information security department sits within a complex network of actors that shape the broader context of the information security field. Identifying who the stakeholders are, their relationship with information security teams within a firm and their relationships to each other will allow for a more in-depth understanding of actors and forces impacting on information security management within organisations. We therefore aim to address the following research questions:

- Who are the different stakeholders relevant to organisational information security practice and how could they be classified based on their salience?
- How do the relationships between stakeholders shape the way they are perceived by information security teams?

METHODOLOGY

We use an in-depth single case study approach as it offered us with an opportunity to make in-depth contextual investigations of contemporary phenomena. This approach is suitable to answering how questions. We have used methodological practices proposed by Walsham (1995), Eisenhardt (1989) and Klein and Myers (1999) to guide our use of case study research. While some critics of a single case approach argue that it lacks depth and replicability (Eisenhardt 1991), we agree with Dyer and Wilkins (1991) and consider single case research as allowing for unique in-depth investigation of phenomena. It has also allowed us to closely examine the relationship between the case organization, its context and the subjects of study. This has reinforced the richness of description and understanding communicated by us (the observer).

With our research questions in mind, we selected a case based on previous research in information security. Prior research has found that organizations in the financial services, telecommunication and utilities sectors present rich cases for information security research due to their greater focus on information security threats and protection (Chang and Yeh 2006). We chose an organization from the financial services sector. We also felt that as Australian financial organizations have performed extremely well despite global economic challenges (Gluyas 2012) this would be an interesting sector to explore. Our case (we refer to as FinCo.) is a large Australian financial institution. FinCo. provides a variety of financial and banking services to corporate and retail clients, and operates both in Australia and overseas. The firm is structured around its various service lines, with its support services teams belonging to separate departments. More than a hundred members of FinCo's staff have information security-related responsibilities, and are positioned mostly along reporting lines under the Chief Information Officer (CIO).

We used semi-structured interviews as our primary method of data collection as this has allowed us to engage with the field in an in-depth manner while being able to identify, clarify and discuss key findings during the process of inquiry (Bryman and Bell 2007; Walsham 1995). For the research reported in this paper, we have conducted thirteen hour-long semi-structured interviews with security and non-security staff of FinCo. We have interviewed three senior managers, four middle managers/team leaders and six frontline analysts in various security-related roles. The interviewees in security-related roles were part of various security teams positioned within the organisation and tasked with ensuring that organisational information assets are protected. We used field notes, public documents and internal documents to triangulate some of our findings. We have used purposeful sampling based on initial interviews to identify subsequent interviewees. We have followed the steps proposed by Poulodi and Whitley (1997) and started by first identifying the 'obvious' stakeholders, adding stakeholders from the literature and building our list through an iterative process of interview data collection, analysis and literature comparison (Walsham 1995). We then used further semi-structured interviews to discuss and examine the relationships of the identified stakeholders and the information security teams within FinCo. The second round of interviews included some repeat interviews with key information security team members as well as new interviewees to examine the strengths and the nature of stakeholder relationships. We then coded our data using middle-range coding based on the categories suggested by prior research and an inductive analysis of the data (Urquhart 2013).

Following the process suggested by Klein and Myers (1999) we treated emerging theoretical explanations with suspicion and examined them from multiple perspectives. Through interviewing subjects both with information security roles and non-security roles we were able to examine a multitude of views. While specific research findings can only apply in sufficiently similar contexts (Yin 2004), we feel that the propositions that we lay out in the discussion section will be of use to other complex organization's facing information security challenges.

FINDINGS

Through a combination of literature analysis and initial exploratory interviews we have identified eleven stakeholder groups relevant to information security processes within our case organisation. Three of these stakeholders could be seen as internal, with the remainder positioned outside of the organisation. Using Mitchell's et al (1997) methodology of examining stakeholder power, legitimacy and urgency we were able to classify the stakeholders as high, medium and low priority stakeholders. Using interviewee reflections we were able to assign power, legitimacy and urgency values from very low to very high. Based on combination of these factors, we were thus able to evaluate the priority and salience level based on the framework proposed by Mitchell et al (1997). We have then focused on examining the relationship between these stakeholders and the information security teams within the firm. Furthermore we were able to identify the extended relationships the stakeholders have between each other and how such relationships affect their role in information security management processes. Based on stakeholder interview triangulation, network effect was rated as either strong, medium or weak, depending on the influence of the stakeholder network positioning.

High priority stakeholders

High priority stakeholders tend to have the most say in the direction organisational information security teams take. Combining high power, legitimacy and urgency, stakeholders in this group need to be carefully managed and engaged in order to ensure information security objectives are met. The majority of such stakeholders are positioned within the organisation, or can often have a major impact on the businesses bottom line. Table 1 provides a summary of high priority stakeholders and their role in the broader stakeholder network.

Table 1. High priority stakeholders

Stakeholder	Power	Legitimacy	Urgency	Salience	Network effect
Senior management	Very high	High	High	High priority	Strong. Strongly affected by customers, media, and regulators. Have strong impact on internal stakeholders
Core business teams	Medium	High	High	High priority	Strong. Strongly affected by customers, often do not involve security, even when necessary. Important internal stakeholder.
Customers	High	High	High	High priority	Strong. Do not directly interact with security, but their behaviour is affected by malicious actors, media and business unit teams. One of the most important stakeholders in the network.

Senior management

Senior management is responsible for setting organisational objectives, including those relevant to security. Being one of the most powerful actors within the organisation, senior management plays an important role in how information security is managed and operated. By delegating the responsibility for protecting organisational information assets, senior management ensures the ability of information security actors to engage with the rest of the organisation. The ability of this actor to set priorities means that the rest of the organisation is driven by what senior management considers being important.

This ability demonstrates the extent to which senior managements' actions are able to influence other internal stakeholders. By signalling the importance of certain initiatives, such as information security awareness programs, senior management is able to improve the interactions between information security teams and other stakeholders within the business.

'[The CIO] has some strong views around certain aspects of security and those absolutely colour what we are doing from the strategy perspective and the same is true of some of the other senior business executives' Senior Security Strategy Manager

Senior management's perception of other stakeholders and trends within those (such as media, competitors, and customers) might impact on the priorities it sets for information security teams. However beyond the organisation, senior management has a relatively low impact on other stakeholders in the network and the way they relate to information security teams within the firm.

Business unit teams

Business unit teams are the major internal consumers of information security services. Information security actors need to ensure that the remainder of the organisation complies with the existing policy and governance frameworks. Business unit teams also frequently conduct initiatives and projects that necessitate information security teams' involvement, making the relationship with this stakeholder group vital to successful information security management. The quality of this relationship impacts upon the effectiveness of such controls as information security policy, success of awareness programs and the overall security culture within the organisation.

'to be more than just a 'back office, we just make sure the patches are on the workstations team' you then actually need the really tight integration and relationships with the business units, you need to know what the business is doing, you need to be sitting with marketing, you need to be chatting to the customer facing business, you need to be speaking with our offshore subsidiaries about what their challenges are' Security Manager

The priorities of this stakeholder are rather sensitive to the competitive landscape; however the stakeholder might have limited exposure to information security processes. However if other stakeholders in the greater network, such as customers or competitors focus or vocalise their focus on security, this might promote security as priority for the business unit teams.

Customers

Customers play a key role when it comes to managing information security effectively. While the relationship between customers and information security teams might not be as direct as for example a customer's relationship with business unit teams, customer trust is seen as one of the most important elements to support brand image and equity for a financial organisation. In case of a security breach, malicious actors usually compromise customer's data and funds, which makes protecting such assets not only a legal requirement, but also a business priority for information security teams.

'We as an organisation need to live and breathe in the same world our customers live and breathe in, we need to know how to connect to them, we need to know how they operate, and what they do.' Senior Security Analyst

Furthermore, customers are one of the most dynamic groups in the stakeholder landscape with constantly changing preferences and trends, which often require the business to move in new directions, potentially exposing it to new information security risks (e.g. new mobile apps, online access, etc.) that need to be effectively mitigated. They remain one of the most attractive targets for malicious actors within the stakeholder network, and thus play a key role in interacting with the majority of other stakeholders.

Medium priority stakeholders

Medium priority stakeholders (summarised in Table 2) tend to have less urgency, power or legitimacy when it comes to dealing with information security teams. This does not mean that they are not important. In fact a number of stakeholders within this group, such as malicious actors, vendors and regulators are dynamic in their roles and depending on the situation at hand and can become some of the highest priority actors within the stakeholder network.

Table 2. Medium priority stakeholders

Stakeholder	Power	Legitimacy	Urgency	Salience	Network effect
Malicious actors	Very high	Very low	Very high	Medium priority	Strong. Shape the behaviour of most actors in the network. Target both organisations and customers. Respond to changes in behaviour of actors to behave rationally.
Vendors	Medium	High	Low	Medium priority	Strong. Serve as a central point of information and best practice sharing in the network. Strongly affected by malicious actors.
Regulators	High	High	Medium	Medium priority	Weak. Mostly passive and dormant, have very high power if start to act
Auditors and consultants	Medium	High	Medium	Medium priority	Weak. Usually dependent on the organisation, limited impact across the network
Support services teams	Medium	High	Medium	Medium priority	Weak. Important internal stakeholder, with limited impact on the network as a whole
Competitors	Medium	Medium	Medium	Medium priority	Medium. Source of shared information, unusual cooperative behaviours within the network

Malicious actors

Malicious actors can be considered one of the stakeholders with least legitimacy. Their goal is to enact breaches and access organisational information assets. While not having legitimacy these stakeholders possess vast amounts of power over information security teams as they are the key instigators of attacks against the business and to some extent the '*raison de'etre'* for any information security team.

The reach of malicious actors however does not simply span the organisation itself. They are key to the overall stakeholder network, driving the behaviour of all the participants of the network. Consistent with prior research (Galbreth and Shor 2010), malicious actors can be seen as relatively rational actors, continuously evaluating cost-benefit trade-offs and thus often targeting the weakest link in the greater stakeholder network.

'We are an attractive target; we have a large customer base, who transact over the internet – that is appealing to cybercriminals. So there are definite challenges and we are a target of choice for people who want to take money out of someonelse's account without having earned it or worked for it.' CERT Analyst

Vendors

Vendors provide the organisation with software and hardware. Information security teams are highly dependent on security vendors in order to deliver a high quality level of protection. Given the dynamic and ever-evolving nature of the industry, the organisation is unable to continuously develop responses to new and untested threats and thus requires the products and innovations offered by vendors to stay up-to-date with their defences. Vendors collaborate very closely with information security teams in responding to new and emerging threats. Bi-directional learning and collaborative development of solutions is often characteristic of this relationship.

'You have to be actively engaging back in the industry and then trying to push the industry in the direction that you want them to get to.' Security Delivery Manager

In addition to their traditional role, vendors serve as a conduit for exchanging information and intelligence about the practices of malicious actors, as well as security practices of other businesses. This places vendors in a unique position and while being a medium priority stakeholder, vendors are one of the most important actors across the whole stakeholder network. This means that other actors have also have a close relationships with this stakeholder, often involving information and practice exchange, mutual support in intelligence initiatives and new product development.

Regulators

Regulators hold considerable power over the organisation and can impact what happens within its information security management processes. In Australia, regulators differ in each industry, with financial services being regulated by Australian Prudential Regulation Authority (APRA). While the regulator might intervene in case of major issues, it usually serves a more passive role, issuing guidance in relation to information security (see *Prudential Practice Guide PPG 234 Management of IT Security Risk*), rather than enforcing particular approaches. If however, the regulator might need to intervene, it will become one of the highest priority stakeholders in the network as it has the power to stop the organisation in conducting its operations (this can be done to other financial institutions as well).

'So guidance from a regulator really tends to be interpreted not as "this stuff you might want to think about", it's more - you need to make sure this is covered'. Security Policy Manager

Auditors and consultants

These stakeholders can be seen in a more advisory capacity, offering support to the business and providing guidance on ways to manage information security. When called upon, these stakeholders can exert considerable influence, but normally remain relatively passive – most of the time engagement would be initiated by the business. In case of auditors, information security management within the business could be influenced if controls lack protection required by accounting regulators. Security auditors would also be used by senior management stakeholders to provide external assurance of information security processes and become an important stakeholder for the internal information security team.

'They audit us here consistent with what they would expect the multinationals to have and they are massively investing in compliance activities. So it's sort of the macro and board level, people will come and tell them if there are issues in security and there are concerns...and that absolutely gets the attention the CIO and the Board.' Security Governance Manager

Support services teams

If business unit teams are the main internal consumer, support services teams are one of the key stakeholders within the business that can assist information security teams in achieving their objectives. While having only a moderate amount of power and urgency, these stakeholders are often key to ensuring that information security teams are able to protect the rest of the organisation. Support services teams are similarly positioned within the stakeholder network, and the relationship between information security teams and support services teams is very close and mutually beneficial.

'[When it comes to other support services] there is a good alignment there, we are plugged into their guys, we understand that we work on the security side of the fence and they are keeping the lights on, when it comes to their services. So there is a good understanding there.' Security Architect

Competitors

Generally for business, competition presents a long-term challenge in maximising organisational success. However, when it comes to information security issues, the relationship with competitors is not so clean cut. With malicious actors being the common 'enemy', it appears that information security teams from one financial institution frequently share information with information security teams in competing organisations. This is usually done informally, with sharing built around personal relationships. More extensive, often more formalised relationships exist with organisations in the same industry but operating in a different market, such as Europe and North America.

'A lot of other really good information comes from understanding other people's approach. I find that actually a set of interactions with people outside of Australia is very useful as well. So we typically do on a yearly basis meet with other people in similar roles in the US and Europe' Security Manager

Low priority stakeholders

Low priority stakeholders (summarised in Table 3) tend to be the ones that are important to monitor, but would rarely be actively engaged in dealing with information security processes within the firm. The 'network' effect means that while low priority stakeholders might have little direct influence on information security teams, their impact is magnified through their ability to influence perceptions and understandings of other stakeholders in the network.

Table 3. Low priority stakeholders

Stakeholder	**Power**	**Legitimacy**	**Urgency**	**Salience**	**Network effect**
Media	Low	Medium	Low	Low priority	Medium. Weak in relation to information security teams, but have strong influence on senior management and customers, which magnifies their significance
Standard setters	Low	High	Low	Low priority	Medium. Provide information and common language to stakeholders within the network

Media

Media serves as an information source for events relevant to information security. Often, their focus is on negative events, such as breach disclosure or privacy scandals. This means that while media can be seen as a much less relevant stakeholder when it comes to information security teams, its importance lies in the ability to shape the information landscape for the whole network and thus influence the behaviour of everyone involved. In particular when it comes to influencing the perceptions of customers and senior management, media remains a stakeholder that should be monitored, as it is able to highlight particular issues and thus motivate other actors to exert pressure on information security teams with the business.

'10 years ago the Boards were not even understanding security was something to ask about and if they were they would ask the risk guy, now they want to ask the security guy, they read about it in the news all the time' Senior Security Manager

Standard setters and researchers

Standard setters play a relatively passive, albeit important role in the whole network. They compile best and effective practice to develop internationally recognised standards and guidelines. A variety of frameworks exists but they serve as a starting point for establishing and improving information security systems in the organisation and therefore are of importance.

Specifically, we found that a number of standards play a pivotal role in creating a common language and shared understanding between several stakeholders. While having little impact on some of the high priority stakeholders, standards are considered to be highly useful in communicating information security issues with vendors, auditors and regulators. Through creating a common language and shared baseline controls, standards simplify interactions with these stakeholders and underpin long-term collaboration and relationships.

'So if [potential suppliers] have gone through a certification framework themselves or if they have already got an Information Security Management System that complies with the ISO view, it's very easy - so the barrier to entry for them is much easier to jump over.' Security Analyst

As we have discussed, there are a number of stakeholders shaping how information security is managed in the large financial institution we have studied. Stakeholder salience offers a way to classify these stakeholders as high, medium and low priority and offers guidance to information security managers on how to engage with these. Viewing stakeholders as a network of interdependent relationships also an explanation of the dynamic complexity of influences across the various stakeholders involved.

DISCUSSION

Our findings demonstrate that examining stakeholders in information security management offers a unique perspective on the influences and dynamic relationships that a firm's information security professionals and other actors experience as part of the security landscape. More broadly, however, it clarifies that any such examination requires an understanding of the complex mutually-shaping relationships between across the entire network of stakeholders. The positioning of some actors within the network places them in a unique role, and often changes how they impact upon information security teams within the organisation.

Understanding stakeholder salience, that includes power, legitimacy and urgency offers an insight into how to prioritise stakeholder groups and to develop more effective methods of engagement with them. Our findings of high priority stakeholders are consistent with existing literature that focuses on organisational leadership (Chan et al. 2005), business unit teams (such as research on the effectives and use of security controls within the organisation) and customers (Herath and Rao 2009; Salmela 2008). Paying close attention to trends within these stakeholder groups, can therefore underpin successful information security management.

Introducing a stakeholder network lens for the examination of stakeholder relationships offers insight into some actors, whose roles might have been underestimated in prior research. One of the key stakeholders with strong network impact are malicious actors. They are one of the most dominant stakeholders in the network and shape the behaviour of others. As mentioned earlier, they often cause the defensive nature of many modern information security teams. However, we have recently seen a shift towards more proactive protection mechanisms that involve intelligence, counter-surveillance and other proactive prevention techniques that affect where malicious actors might target their efforts.

The other stakeholder whose role is magnified by their relationship to others, are vendors, and in particular security product vendors. Traditionally vendors would be viewed as a medium or low priority stakeholder, because they play a regular supplier role and often dependent on the firm for their long-term business. However, when it comes to information security, due to their unique positioning, vendors take on a much larger role of information exchanges. They collect and share good practice in-between and within different industry sectors, they take charge of intelligence activities against malicious actors and they collaborate closely with information security teams on controls and response development projects.

Finally, some low priority stakeholders cannot be underestimated. In particular the role of the media, due to its ability to shape perceptions of senior management and customers. The media seems to play a much more important role in information security management than previously thought. This poses a potential challenge to take into account the behaviour of a low priority stakeholder as they influence other actors.

Understanding who the stakeholders are and how their interactions shape information security can allow for greater clarity in understanding and adapting to specific organisational contexts. Engaging with stakeholders from a perspective of a dynamic stakeholder network, rather than a more traditional view of ‘influencers’ can also allow for a better understanding of the role of each stakeholder in shaping organisational information security practices. Such views will inevitably shape approaches to the key areas in information security managements, such as policy provision, awareness programs and training and internal governance approaches.

LIMITATIONS AND FURTHER RESEARCH

Our research has largely focused on the perceptions and understandings of stakeholders from the perspective of the internal actors within our case. While our findings can offer a useful insight into the behaviours and relationships of a variety of stakeholders, additional research into the detailed perspectives of other stakeholders might bring important aspects of those interactions to light. Future research could also examine specific interactions between stakeholders in the network and how various aspects of information security (e.g. policy or awareness programs) are affected by these.

CONCLUSION

Having examined organisational information security from a perspective of stakeholder salience, we find that a number of stakeholders exist that shape how information security is managed. These stakeholders have a varying degree of influence on information security processes and therefore should be engaged in different ways. We also find that the prioritisation of stakeholders might change based on their positioning within the greater stakeholder network and specific circumstances impacting on the network. We find that while organisational leadership, customers, internal business unit teams and malicious actors have been traditionally seen as important players in the information security landscape, other lower priority stakeholders such as vendors and the media can take on a role of greater importance due to their interactions with other stakeholders in the network. Our findings suggest that understanding the dynamic nature of stakeholder relationships can allow information security managers to better implement their priorities.

REFERENCES

Baskerville, R. 1993. "Information Systems Security Design Methods: Implications for Information Systems Development," *ACM Comput. Surv.* (25:4), pp 375-414.

Boonstra, A. 2006. "Interpreting an Erp-Implementation Project from a Stakeholder Perspective," *International Journal of Project Management* (24:1), pp 38-52.

Bryman, A., and Bell, E. 2007. *Business Research Methods*, (2nd ed.). OUP Oxford.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), pp 28-46.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security* (1:3), pp 18-41.

Chang, A.J.-T., and Yeh, Q. 2006. "On Security Preparations against Possible Is Threats across Industries," *Information Management & Computer Security* (14:4), pp 343-360.

Dhillon, G., and Backhouse, J. 1999. "Managing for Secure Organisations: A Critique of Information Systems Security Research Approaches," The LSE Computer Research Centre.

Donaldson, T., and Preston, L.E. 1995. "The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications," *The Academy of Management Review* (20:1), pp pp. 65-91.

Dyer, W.G., and Wilkins, A.L. 1991. "Better Stories, Not Better Constructs, to Generate Better Theory: A Rejoinder to Eisenhardt," *The Academy of Management Review* (16:3), pp pp. 613-619.

Eisenhardt, K.M. 1989. "Building Theories from Case Study Research," *The Academy of Management Review* (14:4), pp 532-550.

Eisenhardt, K.M. 1991. "Better Stories and Better Constructs: The Case for Rigor and Comparative Logic," *The Academy of Management Review* (16:3), pp pp. 620-627.

Elias, A.A., Cavana, R.Y., and Jackson, L.S. 2002. "Stakeholder Analysis for R&D Project Management," *R&D Management* (32:4), pp 301-310.

Freeman, E.R., and Evan, W.M. 1990. "Corporate Governance: A Stakeholder Interpretation," *Journal of Behavioral Economics* (19:4), pp 337-359.

Freeman, R.E. 1984. *Strategic Management: A Stakeholder Approach*. Boston: Pitman.

Galbreth, M.R., and Shor, M. 2010. "The Impact of Malicious Agents on the Enterprise Software Industry," *MIS Quarterly* (34:3), pp 595-A510.

Gluyas, R. 2012. "Nation's Banks Get Moody's Approval," in: *The Australian*.

Herath, T., and Rao, H. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp 106-125.

Hosking, D.M., and Morley, I.E. 1991. *A Social Psychology of Organising: Persons, Processes and Contexts* London: Harvester Wheatsheaf.

Hu, Q., Hart, P., and Cooke, D. 2007. "The Role of External and Internal Influences on Information Systems Security a Neo-Institutional Perspective," *The Journal of Strategic Information Systems* (16:2), pp 153-172.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., and Wei, K.-K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp 139-154.

Kivits, R.A. 2011. "Three Component Stakeholder Analysis," *International Journal of Multiple Research Approaches* (5:3), 2013/06/18, pp 318-333.

Klein, H.K., and Myers, M.D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), pp 67-93.

Kotzab, H., Grant, D., Teller, C., and Halldorsson, A. 2009. "Supply Chain Management and Hypercompetition," *Logistics Research* (1:1), pp 5-13.

Mitchell, R.K., Agle, B.R., and Wood, D.J. 1997. "Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts," *The Academy of Management Review* (22:4), pp pp. 853-886.

Pouloudi, A. 1999. "Aspects of the Stakeholder Concept and Their Implications for Information Systems Development," *Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on*, p. 17 pp.

Pouloudi, A., and Whitley, E.A. 1997. "Stakeholder Identification in Inter-Organizational Systems: Gaining Insights for Drug Use Management Systems," *European Journal of Information Systems* (6:1), pp 1-14.

Roloff, J. 2008. "Learning from Multi-Stakeholder Networks: Issue-Focussed Stakeholder Management," *Journal of Business Ethics* (82:1), pp 233-250.

Salmela, H. 2008. "Analysing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach," *Journal of Information Technology* (23:3), pp 185-202.

Siponen, M. 2003. "Information Security Management Standards: Problems and Solutions," *PACIS 2003* p. Paper 105.

Siponen, M. 2005. "An Analysis of the Traditional Is Security Approaches: Implications for Research and Practice," *European Journal of Information Systems* (14:3), pp 303-315.

Siponen, M. 2006. "Information Security Standards Focus on the Existence of Process, Not Its Content," *Commun. ACM* (49:8), pp 97-100.

Stytz, M.R. 2007. "Who Are the Experts, and What Have They Done for Us Lately?," *Security & Privacy, IEEE* (5:6), pp 78-80.

Teller, T. 2012. "The Biggest Cybersecurity Threats of 2013," in: *Forbes.com*.

Urquhart, C. 2013. *Grounded Theory for Qualitative Research*. London: SAGE Publications Ltd.

Walsham, G. 1995. "Interpretive Case Studies in Is Research: Nature and Method," *European Journal of Information Systems* (4:2), pp 74-81.

Yin, R.K. 2004. *Case Study Research: Design and Methods*. Sage Publications.

COPYRIGHT