Towards a holistic understanding of security process: formal controls and informal relationships

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

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

Abstract
Despite a variety of existing approaches and techniques for securing corporate information assets, information security threats continue to present an ongoing challenge to business and governments. Existing research suggests that improving the effectiveness of information security depends on the customization of existing security models to specific businesses requirements. A greater socio-technical focus is also cited as necessary. We have used a relational processes lens to examine interactions between the key actors relevant to information security management in a large Australian financial institution from which we present the results of an in-depth case study. By examining organizational information security practices we identify how organizational actors engage in cognitive, social and political processes to achieve various security-related objectives. We suggest that a focus on social and political processes, such as networking and negotiation, complements formal policy and governance structures in achieving organizational security objectives and can assist information security stakeholders in working together more effectively.

1. Introduction

Information security threats are considerably costly for organizations. Businesses’ reliance on information technology, cloud computing, e-commerce and the proliferation of mobile devices and platforms has contributed to an increase in the number of potential threats. Many large organizations including those in the financial and energy sectors are under continuous attack from malicious actors [1]. While many firms recognize the problems posed by threats to information security and the necessity to invest in cyber protection, a greater challenge lies in how to effectively protect against attacks that are decreasing in number but increasing in severity [2].

2. Literature review

The last forty years have seen a steady evolution of approaches for addressing information security challenges [3]. From control checklists [4] and risk-management frameworks [5] to a wide-spread use of information security standards [6], 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 [7, 8].

In dealing with the difficulties of security standards being too generic, many industry or sector-based standards have evolved [9]. 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 the 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 [10].

In addition to the variety of views regarding the effectiveness of information security defenses, the literature has also evolved in focus from purely engineering solutions that were popular in the 60’s and 70’s [11] to attempts to understand human behaviors and attitudes towards security and information asset protection [12]. One of the key drivers behind this shift in focus has been an awareness of the continuous evolution of the nature of security challenges. This highlights the need to address information security from a more holistic organizational perspective, rather than through simple and generic approaches or with purely technical approaches [13].

A significant body of information security literature has sought to provide insights into individual behaviors related to information security controls and procedures. This has included evaluations of malicious insider behaviors [14] to evaluations of the effectiveness of policies and awareness programs [15, 16]. Such studies have examined how individuals working within organizations engage with a variety of information security controls. These studies have aimed to explain which ‘levers’ could be put in place to encourage a particular ‘modus operandi’ to produce a more secure organization.

While offering a broad range of useful and innovative insights, the majority of these studies tend to treat all individuals in organizations in the same generic way. The oft-examined interaction between a ‘rational economic actor’ and a particular security control rests on an implicit assumption that employees’ motivations are homogenous. Such explanations of individual behaviors may be useful but less applicable when considering complex modern organizations where individuals are different and many pursue their own agendas [17].

Hosking and Morley [17] have suggested an approach that examines human behavior based on the premise that various groups of actors exist with the organization, each with different, and at times conflicting agendas and priorities. The organizational actors aim to realize their agendas through initiating and completing discrete ‘projects’. Given the diversity in the aims of various actors, the successful completion of their ‘projects’ depends on their cooperation with other actor-groups and involving cognitive, social and political processes. These ‘relational processes’ usually involve networking, negotiation and the use of influence and power to achieve desired outcomes. Through these interactions actors also continuously shape the context in which they operate, while at the same time being inevitably influenced by their environment and context [18].

The concepts of power and politics are extensively discussed in the information systems literature, and in particular when considering the development and adoption of information systems. In one of the seminal papers on the topic, Markus [19] has examined theories of organizational resistance and politics in organizations in relation to information systems implementation. A number of other studies have discussed issues of acceptance, resistance and effective development and implementation and the use of information systems in business (see for example Hirscheim and Klein [20], Myers and Young [21], Silva and Backhouse [22]).

Several information security studies have also examined the relationship between power, organizational politics and how information security systems or governance frameworks are deployed. For example, Backhouse et al. [22] and Smith et al. [23] examine information security standard adoption through the lens of ‘circuits of power’ and how various agents within organizations relate to the implementation process. Others have examined the role of senior leadership support and punitive measures (which can be seen as an element of coercive power) in relation to the effectiveness of information security controls (e.g. Kotulic and Clark [24]). There does however appear to be a lack of research that examines political and power-related processes in relation to information security operations and the interaction between information security departments and the rest of the organization.

Research that considers social processes in relation to information systems has also focused
primarily on individual–to-individual relationships, such as models of social interaction between users and analysts [25-27]. Additionally the role of informal relationships and social processes has been considered as an element of informal organizational structure in studies of information system alignment [28]. While information security studies have looked at social relationships and organizational culture as an element of compliant and security-aware behaviors (e.g. Chan et al. [29]), an examination of a combination of social and political processes could offer a unique perspective on the matter.

Given the challenges faced by the information security field in developing approaches that are useful in integrating and contextualizing controls and the merits of viewing an organization as a collection of actors engaged in relational processes rather than a collection of similar individuals, we consider that it may be useful to examine existing information security practices through the lens of relational processes [17] and the use of networking, negotiation and influence in the strategizing and operation of information security controls.

Our research addresses the following questions:
1. Who are the main actors engaging in ‘projects’ with information security elements in organizations and what type of projects do they initiate?
2. How are relational processes used in achieving organizational information security objectives?

3. Theoretical model

In addressing our research questions we have used a theoretical model based on Hosking and Morley’s (1991) explanation of relational processes in organizations. The model assumes that various actors operate in organizations with differing priorities. In Hosking and Morley’s model [17] actors can be seen as groups of individuals with shared goals and ‘agendas’ – and with differences between the groups. These agendas are realized through ‘projects’ that are established by each of the actors. The projects can vary in length and purpose, but would usually involve the necessity to engage other actors to achieve desired outcomes. Given the likelihood of diverse aims and goals, such engagement is achieved using relational processes which combine the use of influence, power, negotiation and exchange to temporarily align the goals of other actors with the goals of the project.

Relational processes are considered to be cognitive, social and political. Cognitive processes, where actors seek to generate shared understandings and shape the context in which they operate; social processes, involving coordination and the establishment of team-dynamics for performance, often based on personal relationships and networking; and political processes requiring actors to use their influence and power to encourage cooperation of other parties.

We assume that a variety of actors exist in organizations, however we limit our examination only to the actors that have been found relevant to the realization of information-security projects. Our research seeks to establish who these actors are, what type of projects they engage in and how they use relational processes to achieve their desired outcomes.

4. Methodology

We use an in-depth single case study approach as it provided us with an opportunity to make in-depth contextual investigations of contemporary phenomena. This approach and is suitable to answering how and why questions. We have used methodological practices proposed by Walsham [30], Eisenhardt [31] and Klein and Myers [32] to guide our use of case study research. While some critics of a single case approach argue that it lacks depth and replicability [33], we agree with Dyer and Wilkins [34] and consider the single case research as allowing for a 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 theoretical model 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 [35]. 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 [36] this would be an interesting sector to explore. Our case (we refer to as BankCo.) is a large Australian bank. BankCo. provides a variety of banking services to corporate and retail clients, and operates both in Australia and overseas. The bank is structured around its various service lines, with its support services divided into separate departments. More than a hundred members
of BankCo’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 [30, 37]. For the research reported in this paper, we have conducted thirteen hour-long semi-structured interviews with security and non-security staff of BankCo. We have interviewed three senior managers, four middle managers/team leaders and six frontline analysts. We used field notes, public documents and internal documents to triangulate some of our findings. The theoretical framework we proposed (from Hosking and Morley [17]) was used as part of ‘an iterative process of data collection and analysis’ (Walsham [30], p. 76; [38]). We then coded our data using middle-range coding based on the categories suggested by our theoretical model and an inductive analysis of the data [39].

Following the process suggested by Klein and Myers [32] 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 [40], 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.

5. Findings

In addressing the research questions posed in earlier sections, our findings provide an examination of information security processes within a large financial institution. There are four key actor groups that are important to information security management (5.1). These actors pursue their own objectives and engage in a series of diverse projects. While some of these projects might have a security element, many do not. Those projects that are relevant to information security have either a low or high level of involvement from information security teams (5.2). To ensure effective delivery of these projects and security objectives, information security teams engage in social and political processes with other actors within the organization (5.3 and 5.4). Over time these processes play a broader role in strengthening the information security management process for the firm.

5.1 Actors shaping information security and their ‘projects’

Hosking and Morley [17] argue that organizational theorizing requires the examination of interdependent actors and their social relationships. Therefore in order to examine information security processes at our case organization, we identified four categories of actors engaging in projects relating to security. Actors in each category were observed as pursuing their own aims and objectives while having either a direct or tangential impact on the information security of the organization. Table 1 shows four key actors relevant to information security, their broad aims and how they interact with information security projects.

<table>
<thead>
<tr>
<th>Actor</th>
<th>Aims</th>
<th>Security projects involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security teams</td>
<td>Ensure protection of information assets</td>
<td>Initiate and drive information security projects</td>
</tr>
<tr>
<td>Business unit teams</td>
<td>Ensure performance against business goals</td>
<td>Consume some security projects Might need to involve security in own projects</td>
</tr>
<tr>
<td>Leadership teams</td>
<td>Ensure long-term organizational performance</td>
<td>Expect baseline security Set broad security goals</td>
</tr>
<tr>
<td>Support services teams</td>
<td>Ensure non-core business service provision</td>
<td>Consume some security projects Might need to involve security in own projects Support delivery of some security projects</td>
</tr>
</tbody>
</table>

Information security teams are actors tasked (by senior management of the organization) with ensuring availability, integrity and confidentiality of its information assets. We found this to be the only category for whom information security is seen as a major objective and is therefore a key element of the projects initiated by individuals and groups within this category.
Business unit teams are actors involved in day-to-day business operations, such as dealing with customers, sales, product marketing, investment and trading. These actors are driven by broader organizational objectives, such as improving market share in a particular segment or ensuring particular returns with an adequate level or risk. These teams initiate projects that might have a security element, but that are usually limited to compliance. These actors frequently view information security requirements as a nuisance or inhibitor of day-today activity that can prevent them from achieving their desired outcomes.

Leadership teams set the broad direction of the company and shape the bigger picture. Longer-term success is what broadly drives this group, with security being one of many issues that they deal with. While security has not historically been a major concern for actors within this group, the responsibility for information security is delegated to information security teams and the interest of leadership teams is usually limited to an expectation that information assets are secure without necessarily directly engaging with the issues.

Support services teams are actors that while not involved with customers are vital to ensuring that systems run smoothly and enable other actors to achieve their desired outcomes. These include non-security IT services, physical security services, risk, accounting and legal departments. While not responsible for information security, these actors are closely aligned with both the information security and business unit teams. Despite this alignment, these teams also pursue their own agendas that may or may not coincide with information security priorities.

5. 2 Information security projects - high and low involvement

As suggested by Fikes (1982 cited in Hosking and Morley [17]), negotiated agreement between groups is required for successful completion of projects. An examination of the interdependencies between actors requires an understanding of the collaboration they engage in with the purpose of achieving their own objectives [17]. We therefore needed to identify not only the actors dealing with information security processes, but also the types of projects they engage in. For the purposes of the research reported in this paper we have limited our analysis to information security projects, i.e. those initiatives within the organization involving requiring the protection of information assets either directly through the operation and implementation of security controls or via a broader use of information security policies and governance frameworks.

Actors tend to engage in a number of different projects on a continuous basis with some projects representing an ongoing operational commitment and others being discrete, time-limited engagements. We broadly classified information security projects into two categories – those with high or low information security involvement.

High involvement projects entail planning and the maintenance of baseline information security protection across the organization. This is seen as a key function of the information security teams - achieved through a combination of governance and compliance frameworks, clear security planning, architecture and security control operations. Most of these projects happen ‘behind the scenes’ with some aspects of the work communicated to the rest of the organization through formal training and information security policies. These projects are initiated and driven by information security teams and fall within their legitimate and delegated responsibility. Other actors would rarely be involved and if involved, mostly on a ‘need-to-know’ basis. At times the support services teams would be consulted and engaged in delivery of these projects, however the lead and responsibility remains with the information security teams.

Low involvement projects are non-security projects that nevertheless require an information security component. The information security teams are required to ensure all business initiatives comply with the broader security vision and do not pose excessive information security risks. Typically such projects would be initiated by business unit teams (e.g. a new marketing campaign or new product offering) or by leadership teams (e.g. a major infrastructure upgrade). Despite formal compliance and governance rules, information security teams tend to lack influence when it comes to such projects, with other actors frequently consulting information security teams at a superficial level or too late in the project implementation process. Often, ensuring the timely and effective involvement of security teams can be complicated by a negative reputation associated with the information security teams, who are seen as ‘blockers’ and unnecessary hindrances to business projects. We found that in order to address this reputation, information security teams relied on a number of social and political processes to complement the use of formal information security tools, policies and standards.
5.3 Cognitive and social processes: networking for shared understandings

Networking involves ‘patternings of influence and value’ (Hosking and Morley [17], p. 220) whereby actors engage in reciprocal relationships of influence to achieve their desired outcomes. Information security teams engage in networking with other actors on a regular basis in order to create long-lasting relationships. This is achieved through both formal organizational structures and through informal and interpersonal relationships.

In order to break down existing barriers when it comes to dealing with business unit teams, information security actors align themselves with the unique context of each business unit by assigning dedicated personnel to engage with each individual context. These people are regarded as ‘ambassadors’ and their role is to serve as both a single point of contact for the business unit, but also to build awareness, trust and understanding through personal relationships. The relationship, however, is not just used for exerting influence from information security teams to business units. Through these activities information security teams are able to contextualize their own offerings and produce more relevant and useful support programs to other parts of the bank.

This formal structural mechanism is further enhanced through the interpersonal relationships that the ambassadors build with their counterparts and colleagues within the business units. The personality and ability of information security team representatives who are placed in charge of a particular business area play a key role in building trust, improving the internal security brand and negotiating a shared understanding of security requirements that ensure early project involvement potentially improving the chances of successful project completion.

‘especially having dedicated personnel has helped to get into the business units, start having the security conversations and give the confidence to the business that they have always got single point of contact...that you can just use as a security sounding board’ – Security Project Manager

Networking with members of support services teams serves a similar purpose when a support service team consumes a security service. It can also present an additional benefit of improving collaboration when both information security and support services teams need to be involved in a business unit project. Again, relying on personal relationships, informal communication channels and building trust over time appeared to be a preferred avenue for ensuring long-lasting and mutually beneficial relationships - even where divergent aims and objectives existed.

Organizational leadership has a dual role of setting the overall goals of the organization and of assigning information security priorities. Consistent with prior research, the role of organizational leadership cannot be underestimated [29]. Networking between senior members of the information security teams and senior management of the organization offers greater awareness of aims and priorities in each actor group and creates a stronger sense of support for the information security team’s project(s), whilst reinforcing the legitimate mandate delegated from the board to the information security teams to protect information assets.

‘Our CEO had a note in terms of information security being so important, protecting the brand, the reputation, the customer’s trust – so that tone from the top flows down, and then becomes fundamental’ – Security Governance Manager

Despite a variety of formalized structures that create forums and round-tables for information security teams to network with other actors, our findings reinforce a strong reliance on informal mechanisms, often hinging on interpersonal relationships between people in key positions. Engaging in social processes across all teams reflects a common goal to build relationships and trust through informal connections and communication channels. Using informal social approaches, information security teams are able to align themselves more efficiently with the diverse and dynamic organizational context(s) that they encounter, while they contribute to shaping elements of their context to create a better footing for other relational processes – negotiation.

5.4 Political processes: negotiation, influence and cooperation

Negotiation and cooperation activities complement interpersonal networking when it comes to achieving information security teams’ aims both when working on high and low involvement projects. Information security teams cooperatively engage in shared cognitive activities to develop shared understandings of information security practices between their own teams and other actors.

Going beyond awareness, information security teams commonly use a ‘what’s in it for you’ approach to demonstrate the relevance and importance of information security work and to increase the effectiveness of their formal policies. By demonstrating the potential value that actors can
accrue as a result of frequent interactions with information security professionals offers a better bargaining and influence position when it comes to negotiating project delivery and participation, and in particular for low-involvement projects. Value, as a basis of cooperation between actors with divergent aims, is demonstrated through two avenues – contextualized offerings and positioning of the security teams as an enabler.

Firstly, information security teams shape their own offerings to provide targeted and contextualized engagement with different business units, organizational leadership and support services teams. This can range from providing targeted governance reports for senior leaders in different departments, to creating a dynamic role-driven information security policy. Clear and simple language of the policy that can adapt based on the role, responsibilities and obligations of the user improves the way a policy is accepted and consumed, especially when it comes to engaging with non-security personnel. Such practices demonstrate an awareness of the issues faced by other actors who are overloaded with information from a large number of policies and compliance requirements, and who might not be easily receptive of ‘yet another policy document’. Such contextualization allows addressing some of the challenges raised by current critics of the breadth of information security standards and policy best practice [7].

Secondly, through an in-depth understanding of their context, information security teams were able to clearly identify that the priorities of other actors might lie beyond the realm of security. To ensure timely involvement and to reinforce existing relationships, information security teams have positioned themselves as enablers for other actors’ objectives. Rather than serving as a ‘blocker’ or a ‘naysayer’, they proactively seek out opportunities that align with business unit teams objectives and assist them with achieving their goals.

‘I think people try sometimes to avoid us...we like getting our message across to the business – we are not here to stop you from doing anything, we are here to work with you to push initiatives through, but do that in a secure, risk-managed approach for the good of the firm’ – Senior Security Project Manager

For example – an opportunity to provide a more innovative marketing campaign that would not be previously possible due to security concerns is now enabled by a more creative security offering. Not only has this contributed to broader business unit objectives by helping them with the completion of their ‘projects’, but it has also assisted in establishing a stronger link and relationship with the information security teams.

The relationships between actors involved in the information security processes are dynamic and constantly evolving. Information security teams are thus required to adapt their engagement models depending on the type of project they are working on (high or low involvement) and the actor they are working with. Through the use of social and political processes, information security actors are able to enhance their interactions with other actors, build up trust and create a foundation for long-term collaboration. In the following section we discuss how such relational processes also reinforce formal security policies and frameworks and result in delivering a more holistic information security process.

6. Discussion

We proposed that information security practices in organizations can be usefully examined through a relational processes lens. Consistent with the literature, group rather than individual focus offered insights into organizational information security processes [18]. Our analysis revealed that when we consider information security, various groups within a large and complex bank perceive information security projects differently. This difference in perception and agendas leads to reduced effectiveness of traditional information security controls and formal tools when it comes to ensuring information security protection. In the case we examined, information security actors are required to complement formal approaches to information security with less formal social and political processes in order to amass goodwill and influence.

As noted in prior research, power remains one of the key elements in ensuring that information security objectives are accomplished [23]. Building on their increasing influence achieved through networking and negotiation has information security actors are able to reinforce their legitimate power and mandate through the use of relational processes. By engaging with leadership teams, they are able to shape the security context in which they operate, track for changes in priorities and guide future infrastructure development. Ensuring support at the top reinforces the formal role information security teams play in delivering overall information asset protection.

This accrued power is then used to ensure the effective delivery of high-involvement projects across the organization. As illustrated in Figure 1, combined with social influence amassed through
networking and negotiation activities, greater user awareness and acceptance of formal information security controls (such as information security policy and awareness programs) as well as monitoring and compliance mechanisms is achieved.

'We can build that engagement and that process in such a way that the security policy and the standards are your friends, because they help you, they give you the flexibility to achieve the business outcomes that you want, while staying within your risk appetite’ – Security Manager

With low-involvement projects, engaging in relational processes allows information security teams to fill the influence gap of its formal mechanisms. Through building relationships and interdependencies with business units and support services actors, information security teams are able to create a foundation for informal, yet very effective engagement mechanisms with projects initiated by other actors.

Despite the importance of relational processes, we do not deny the significant importance of formal structures and governance systems when it comes to managing information security. Without these, political and social processes might result in decreased protection. Informal relationships and social processes can however serve as a highly useful (an in our opinion essential) complement to existing approaches to security. Fostering networking and relationships between information security actors and other actors within the organization will make the job of managing information security easier and strengthen the ability of information security actors to influence others.

7. Limitations and future directions

Our research has largely focused on internal interactions in our case. While our findings can offer a useful insight into the behaviors and relationships between internal actors, additional research into the other relational processes that span organizational boundaries organization might bring other important factors to light. Future research projects could also examine specific interactions between relational processes and formal information security mechanisms, for example looking at how policy or awareness program effectiveness could be complemented by fostering informal communities and relationships.

8. Conclusion

Having examined how a large financial institution approaches their information security management, we find that information security actors strongly rely on relational processes to achieve their desired objectives of protecting information assets. We found that while reliance on formal information security structures and policies might be effective in relation to projects driven by information security teams, when it comes to dealing with other actors in the organization, information security teams engage in social and political processes in order to ensure early involvement and participation in the projects of others. By using networking and negotiation as well as developing clear understandings of context, information security teams are able to enhance their influence and power and reinforce the effectiveness of formal information security mechanisms. Our findings suggest that such actions might offer an additional way for organizations to enhance the effectiveness of their information security policies, controls and governance frameworks.

10. References


