2016

Legitimising Information Security Policy during Policy Crafting: Exploring Legitimising Strategies

Elina Niemimaa
Tampere University of Technology, elina.niemimaa@gmail.com

Legitimising Information Security Policy during Policy Crafting: Exploring Legitimising Strategies

Elina Niemimaa
Department of Information Management and Logistics
Tampere University of Technology
Tampere, Finland
Email: Elina.Niemimaa@gmail.com

Abstract

This study examines the crafting of an information security policy as a process of legitimising. Drawing on organisational research on legitimacy and legitimisation and on 15-month ethnographic study of a multinational corporation that sought to craft a new policy, the study identifies four legitimising strategies employed during policy crafting: (1) inviting participation, (2) embedding into existing practices, (3) advertising and (4) formalising and professionalising. The study conceptualises policy crafting as being constituted through iterative and recursive relationship of legitimising strategies and policy amendments. The study contributes to literature on information security management, on information security policies and on legitimacy.

Keywords Information security management, Information security policy, Policy development, Legitimacy

1 Introduction

Management and organisations research suggests that organisational policies that are perceived as illegitimate by organisational members are often decoupled from organisational practices (e.g., Bromley & Powell 2012; Dick 2015). In other words, organisations employ formal structures to meet the institutional demands of their environment but the structures remain disconnected from the actual practice (Meyer & Rowan, 1977; Oliver, 1991). Such decoupling may have devastating effects, as it may result in the institutionalisation of employee misconduct (MacLean & Behnam 2010). The policy's relationship with organisational goals and efficiency may further remain unclear or even questionable (Dick 2015).

In the context of information security (InfoSec) management, researchers have shown that organisations face institutional pressures to adopt information security policies (InfoSec policies) (Hsu et al. 2012). Such policies are central in managing risks to organisations' information assets, but only insofar as the policy and related procedures are complete, accurate, available and eventually implemented (Warkentin & Johnston 2008). Therefore, organisations invest time and resources in crafting policies. Yet, scholars have raised concerns that the policies seldom produce the intended outcomes (Karyda et al. 2005) and are never translated into organisational practice (Dhillon 2007). The policies remain decoupled from organisational practice and as symbolic gestures that likely do not improve organisation's InfoSec risk management (Spears et al. 2013). Little is still known about how organisations seek to overcome such decoupling. This lack of knowledge is also reflected within literature on InfoSec policy crafting, which calls for studies that illuminate the emergent process of policy crafting (e.g., Baskerville & Siponen 2002; Dhillon 2007) and for studies that investigate social aspects involved (e.g., Nasution & Dhillon 2012).

Against this backdrop, this ethnographic study examines the crafting of an InfoSec policy as a process of legitimising. In particular, it addresses the questions of *how policy becomes legitimised in the policy crafting process* and *what are the implications of legitimising for the policy*. The study draws on organisation's theory on legitimacy and legitimising and on ethnographic evidence from a multinational corporation that sought to craft a new InfoSec policy to replace the existing policy that had been decoupled from organisational practice.

2 Theoretical Background

2.1 Information Security Policies

Organisational InfoSec policy has a profound role in securing organisations' information assets, as it lays the foundation for organisations' InfoSec (e.g., Baskerville & Siponen 2002; Siponen & Iivari 2006; Warkentin & Johnston 2008). Indeed, there exists a strong consensus within the existing literature that the policy is the key mechanism for promoting effective InfoSec management practices (Doherty et al. 2009; Herath & Rao 2009). Compared to the importance of InfoSec policies for organisations, the existing literature on InfoSec policies is unfortunately scant. A literature review found that only 1, 64% of the surveyed articles were related to InfoSec policies (Siponen et al. 2008). Indeed, as Straub et al. (2008) argue, "Not only are the policies that protect this [organization's] information much less frequently discussed, but the processes that lead to effective policies are even less favo[u]red by scientists and practitioners" (p. 6).

In an organisational context, policies become established through complex processes that involve a multitude of challenges. Among others, a key challenge concerns the crafting of an InfoSec policy (Straub et al. 2008). Another important challenge concerns the need of accommodating the sometimes contradictory views of different stakeholders about the policy (Niemimaa et al. 2013; Njenga & Brown 2012). To address these challenges, one stream of research has proposed stepwise policy formulation methods (e.g., Rees et al. 2003; Whitman 2008; Knapp et al. 2009; Corpuz & Barnes 2010). Arguably, this body of research provides insight into policy, but it does not address the emergent process of policy crafting (Baskerville & Siponen 2002; Dhillon 2007) or its "ground realities" in practice. Therefore, another, although scarcer, stream of research has investigated social issues that shape the policy crafting using qualitative methods. For example, Lapke and Dhillon (2008) and Inglesant and Sasse (2011) analysed how power relations shape policy crafting and Karyda et al. (2005) identified contextual factors which influence policy crafting. These studies advocate a situated, practice-oriented focus for analysing InfoSec policy crafting and call for further studies into social aspects of the crafting. This study addresses these calls by highlighting the fundamental role of legitimacy and social processes of legitimising for the InfoSec policy process.

2.2 Legitimacy and Legitimising

In this paper, I have chosen the concepts of legitimacy and legitimising from the seminal work of Suchman (1995) to illuminate my field data for two reasons. First, they provide a strong theoretical basis from which to leverage understanding of legitimising processes of InfoSec policy crafting at the research site. Centrality of legitimacy, or its lack thereof arose from the field data. Second, this line of theoretical and empirical analysis contributes to and builds upon InfoSec research concerned with exploring the social and organisational aspects of InfoSec policy development.

Building and sustaining legitimacy is essential to organisations (Oliver 1991; King & Whetten 2008; Philippe and Durand 2011). Legitimacy empowers an organisation for growth, sustainability, resource acquisition, and strategic transformation (Zimmerman & Zeitz 2002). Legitimacy can be understood as "a generali[s]ed perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions" (Suchman 1995, p. 574). This means that legitimacy is always subjective, dynamic and something that people grant for an entity. Drawing on Suchman, (1995), three widely accepted types of legitimacy can be delineated (Constantinides & Barrett 2014): "pragmatic, based on audience self-interest; moral, based on normative approval; and cognitive, based on comprehensibility and taken-for-grantedness" (Suchman 1995, p. 571). The types co-exist and are interrelated. Although Suchman, (1995) analysed legitimacy in the context of organisation's legitimacy towards external audiences, researchers have since drawn on his tree types of legitimacy to understand, for example, legitimacy of an internal compliance program (MacLean & Behnam 2010) and information infrastructure development (Constantinides & Barrett 2014).

When a new practice (e.g., a new InfoSec practice) is introduced, actors in a social group grant or deny legitimacy to it (Kaganer et al. 2010). Importantly, practice is always necessarily provisional and its legitimacy endlessly tested and con-tested, thus, "[q]uestions of what is appropriate, what is legitimate, and what can be done are continuously tested in action, such that practice is necessarily provisional and tied to specific historical and material conditions" (Nicolini 2009, p. 1406). If the practice is not legitimised, it may become decoupled from organisational practice. To avoid the pitfalls of illegitimacy and decoupling, actors, while their autonomy and potency is constrained (Suchman, 1995), can employ micro-level legitimising strategies (Kaganer et al. 2010) to construe a new practice or policy as legitimate. Suchman (1995) posited overarching legitimising strategies aimed at fostering the aforementioned three types of legitimacy in the context of organisation's legitimacy towards external audiences (e.g., industry, customers and governments). Others have built upon them (e.g., Kaganer et al. (2010)). Such strategies enable actors to manoeuvre within their environment in order to construe some entity or action as legitimate. Table 1 describes the key strategies derived from Suchman (1995).

Type of legitimacy	Legitimising strategies from organisation's theory
Pragmatic legitimacy	• Co-opt constituents; exaggerate the participation of constituents • Give some measure of authority to affected audience • Engage in product advertising – persuade constituents to value the product • Respond to needs – meet the needs of the various audiences; response to constituents' self-interests
Moral legitimacy	• Produce proper, meritorious outcomes • Embed in existing institutions – embed the new practices in established institutions • Offer symbolic displays • Proselytise – build a winning coalition of believers
Cognitive legitimacy	• Conform to established models or standards • Formalise operations – codify informal procedures; bring activities under official control • Professionalise operations – link the new practices to external

definitions of authority and competence

Table 1. Legitimising Strategies from Organisation's Theory

As changes in organisational policies and practices require that such new arrangements are viewed as more legitimate than the prevailing ones (Suddaby & Greenwood, 2005), legitimisation strategies can be assumed to be important for InfoSec management and InfoSec policy crafting as well. As the strategies encompass the micro-level, situated efforts of actors, they must reflect the particular legitimation domain (Kaganer et al. 2010). That is, the general and overarching strategies described herein cannot be applied 'as is' to legitimation domain of InfoSec management, but can provide a starting point for understanding the legitimisation processes.

3 Methods

3.1 Research Setting

The analysis presented in this paper is based on data from 15-month InfoSec policy crafting project at a multinational corporation (Beta, a pseudonym), one of the global leaders in the field of mechanical engineering. The corporation operates in over 50 countries and servers hundreds of thousands of customers across the globe. The project provided a fruitful context for this study as it involved a complete renewal of the policy for a global organisation of which previous policy had been decoupled from organisational practice and which now wanted to avoid the pitfalls of such decoupling.

3.2 Data Collection and Analysis

The research approach of this study is ethnography. Ethnography is an accepted approach in information systems (IS) research (Baskerville & Myers 2015) and is particularly suited for studies that aim at understanding human, social, and organisational aspects of some organisational phenomenon (Myers 2009). It further offers a means for accounting what happens in practice (Rowe, 2012). Accordingly, it is well suited for this study, as the study is interested in the social and organisational aspects of InfoSec policy crafting in an organisation in real-time. As I entered Beta at the beginning of the policy project, I was able to follow the policy crafting in real time over the whole project and had unfettered access to observe meetings and interact with all employees that participated to the policy project. This is in line with the ethnographic approach, as it is characterised by researcher spending extended period of time at the research site seeing what people are doing there as well as what they say they are doing (Myers 1999).

Ethnographic research differs from case studies (Myers 1999) and other types of interview or document based research (Miettinen et al. 2009) by the extent to which researcher immerses herself in the situations, events and interactions at the research site. A chief distinguishing characteristic of ethnographic research is, thus, participant observation as a primary means for collecting empirical materials (Myers 1999). Accordingly, detailed field notes from 15-month participant observation form the primary empirical materials of this study. Additional data sources include notes from informal social contacts and documentary sources (e.g., Beta's old InfoSec policy, InfoSec instructions, information management policy, safety policy, privacy policy, PowerPoint presentations related to policy crafting, and tens of policy drafts and various other organisational documents).

As this study sought to understand InfoSec policy crafting in practice, data analysis was inductive and did not include predefined categories or theoretical constructs. The analysis proceed in four steps. First, I wrote a rich chronological description of policy crafting (Langley, 1999) with a focus on how the policy was crafted. Two consistent themes that began to emerge from the description were (1) the waning or lacking acceptance and support for InfoSec management and new InfoSec policy and (2) a corresponding increase in descriptions of events that in a way or another promoted or argued for the policy. As I delved into the literature to understand these emergent themes, it became apparent that these were underdeveloped in InfoSec management literature but organisational theory provided possible concepts for understanding them (i.e., legitimacy and legitimisation). Second, I analysed the description using "open coding" for incidents of legitimacy and legitimisation. This analysis resulted in first-order codes such as "Lack of authorisation", "Seeking authorisation/acceptance for policy" and "Seeking approval for policy's practices". Third, building from the first-order codes, I coded for similarities and differences to detect broader themes (uncovered themes included e.g., "Inviting participation", "Embedding into existing practices", "Advertising", "Formalising and professionalising") and to ensure consistency with the existing literature and to detect possible new themes. A key new theme was "Amending the policy" in response to various situations (such as a

request from participating actors and in an effort to make the policy more appealing). Finally, with the emergent themes in hand, I went back to the original description and other empirical materials to map the themes to the dynamics I had uncovered in the description of the policy project. This mapping afforded an opportunity to compare dynamics such as increasing or waning acceptance to amendments in the policy draft across different time periods as well as contextual factors (e.g., unexpected internal events, cultural norms) surrounding these dynamics. Eventually, this analysis resulted in an understanding of how legitimacy of the new InfoSec policy, legitimisation strategies, and policy amendments interrelated over time and ascertained the manner in which actors at Beta legitimised InfoSec policy and InfoSec management more broadly.

4 Findings: Legitimising Information Security Policy at Beta

Faced with institutional pressures for high InfoSec standards (cf. Hsu et al. 2012), changes in Beta's business and the fact that the existing InfoSec policy was decoupled from organisational practice, top level managers decided that Beta needed a new InfoSec policy. Policy crafting was characterised by efforts aimed at building support and acceptable for the policy crafting efforts, new InfoSec practices documented in the new policy, and InfoSec management more broadly. Different actors (e.g., Chief Information Security Officer (CISO), Chief Technological Officer (CTO), Head of enterprise risk management) engaged in various legitimising strategies in order to legitimatise the policy crafting and the policy itself. The strategies can be conceptualised as (see Table 2): (1) inviting participation; (2) embedding into existing practices; (3) advertising; and (4) formalising and professionalising. Gradually, through modifications to the policy, and through further legitimisation efforts, policy became to be seen as legitimate. Next, I explain the strategies in more detail.

Legitimising strategy	Strategy description	Central themes
Inviting participation	Involve actors from different organisational units and positions to policy crafting and give them real authority to influence the policy.	Workshops, presentations, emails, informal discussions and other means to socialite feedback, tentative tone when proposing new InfoSec practices, settling for policy crafting approach and for InfoSec practices written in the policy together with different actors. Modifications to policy drafts mindful to needs, requests and interests of participating actors.
Embedding into existing practices	Embed policy crafting practices and policy's new InfoSec practices into existing organisational practices.	Embracing organisationally accepted procedures, integrating into existing processes, methodologies, practices and technological infrastructure and illustrating the policy's practices as “the right thing to do”. Modifications to policy crafting and policy drafts mindful to organisational practices.
Advertising	Engage in advertising policy crafting and the policy.	Advertising benefits and expected outcomes of the policy, disseminating information, describing policy-making and persuading actors to value the policy.
Formalising and professionalising	Formalise and professionalise InfoSec practices and roles and responsibilities.	Defining mandatory InfoSec practices, formalising InfoSec operations and aligning InfoSec management with broader management practices. Modifications to policy drafts mindful to regulatory demands and Beta's formal management processes.

Table 2. Legitimising Strategies at Beta

Strategy 1: Inviting participation. The first strategy, involving actors from different organisational units and positions to InfoSec policy crafting and providing them with a real possibility to influence the crafting and its outcome, proved essential for the policy. Participation and support of those who participated was not only the means for legitimising the crafting and its outcome but also for increasing the legitimacy of InfoSec management. One senior InfoSec consultant explained the benefits of involving actors from various organisational positions to policy crafting from the very beginning as:

> *"It's great and important that people participate from the very beginning, because it means that implementation [of the policy] also begins immediately."* (Observation note)

Policy crafting showed that participation was much more than rather passive acceptance from the non-InfoSec actors (i.e., actors who were not InfoSec professionals or who did not pursue InfoSec responsibilities); it was about actors' real possibilities to influence the policy. Their possibilities to influence realised mostly through different workshops that formed the core of the policy crafting at Beta. In the workshops, InfoSec actors acted as facilitators and secretaries and presented the policy draft and its InfoSec practices. Non-InfoSec actors then considered and described the implications of implementing the suggested new InfoSec practices and often requested changes to them. For example, in one workshop, Chief Operating Officer (COO, who was responsible for IT operations) explained that the existing IT infrastructure did not support some of the suggested practices and the practices would imply large changes to the infrastructure. Often policy drafts were modified according to non-InfoSec actors' requests. Through the modifications, participation and solicitation for feedback, the policy became viewed as more proper and appropriate for Beta in the eyes of the participating actors. More broadly, their influence meant that policy was modified towards more proper and appropriate for Beta and its business context, allowing for a generalised perception among stakeholders that it was desirable and adequate and thus legitimate. Thus, inviting participation was as much about legitimising the policy as it was about obtaining input from various stakeholders. The strategy further convinced the non-InfoSec actors that the policy incorporated their interests and concerns, and thus pursued their goals (cf. pragmatic legitimacy in Suchman 1995).

Strategy 2: Embedding into existing practices. Embedding InfoSec into existing organisational practices meant both embracing organisationally accepted practices in the making of the policy and integrating new InfoSec practices, written in the new policy, with the existing organisational practices. First, InfoSec policy crafting garnered legitimacy through embracing organisationally accepted procedures (e.g., reviews, decision-making procedures) and techniques (e.g., estimating policy implementation costs). Second, integrating new InfoSec practices into the existing organisational practices meant that new practices included references to organisational processes and requirements. For example, in regard to human resources security the InfoSec policy draft stated: "Human resources security must be established…through integrating InfoSec requirements into the employment lifecycle phases" (Policy document). Inviting participation (strategy 1) offered valuable insights to organisational practices and made the integration easier. For example, the idea of referring to the corporation's formal project management methodology instead of using a generic statement "documented information systems development methodologies" arose through involving non-InfoSec actors. At the general level, the strategy of embedding into existing practices sought to represent policy crafting approach as socially accepted and its outputs – the policy drafts – as adequate and compatible with the existing organisational practices. Conforming to the prevailing organisational practices in the policy-making likely made it easier for different actors to consider policy-making as legitimate. Portraying new InfoSec practices in relation to organisational practices can be seen as an attempt to link the policy to the existing beliefs of what is appropriate – how things are done at the organisation in question. This can be interpreted as a manifestation of moral legitimacy that is about evaluations of whether some activity is "the right thing to do" (Suchman 1995). New practices linked to ones that were already considered to be the usual and the correct way of doing something seemed to harvest greater acceptance in the course of policy-making. It further demonstrated that InfoSec management pursued organisationally valued ends.

Strategy 3: Advertising. The third strategy actors employed at Beta was about engaging in advertising the making of the new InfoSec policy and the new policy itself. Early stages of policy-making were characterised by high ambiguity and unawareness surrounding the practices proposed in the policy, making communication efforts by InfoSec professionals necessary to help stakeholders better understand the key properties and the value of the practices and their implications. Through advertising the policy, knowledge of it was spread and its comprehensibility increased. Advertising comprised claims centred on the need for a new policy (e.g., claiming the existing policy was old fashioned and did not support Beta's InfoSec management and governance (PowerPoint presentation)), its benefits (e.g., with the new policy it would be possible to: "ensure that emerging cyber security threats and needs are identified and addressed in a timely manner" (PowerPoint presentation)), and the key features or mechanisms for achieving those benefits of the policy (e.g., defining scope and direction for InfoSec holistically and defining roles and responsibilities for policy implementation (PowerPoint presentation)). Later, when CTO had understood the *"beauty of the policy"* (Observation note) as he described it, he became an enthusiastic sponsor of the policy. For him, the policy project was the means to demonstrate that something "big" was happening to Beta's InfoSec. He was well-respected and his views carefully heard, thus his sponsorship likely influenced

stakeholders' legitimacy perceptions. CTO engaged in advertising the policy in encounters with management level actors during coffee and lunch breaks and sometimes even on a round of golf. The strategy of advertising conveyed the essence of the policy to stakeholders and attempted to persuade them to value the policy. Through advertising interventions, InfoSec actors and CTO were able to slightly manipulate the environment in which policy was made and develop bases of support for the InfoSec management. In essence, advertising evoked pragmatic legitimacy by delineating the needs that InfoSec policy was designed to address and showing how the policy met those needs.

Strategy 4: Formalising and professionalising. The fourth strategy was to formalise and professionalise InfoSec management practices. This entailed defining which practices were mandatory for securing Beta's information assets, determining their content on a general level, and linking them to external, widely acknowledged definitions (i.e., international InfoSec management standard ISO/IEC27001). The level was kept general as otherwise global implementation would be difficult to achieve (cf. Ansari et al. 2014). Formalising further meant that compliance and regulatory requirements were included in the policy and InfoSec activities were brought under centralised control. The strategy brought InfoSec practices in line with non-InfoSec actors' general understanding of management practices and, thus increased their comprehensibility.

In summary, the identified legitimisation strategies contributed to the legitimacy of the process of policy-making, policy itself and InfoSec management more broadly and were thus essential for the success of the policy crafting. The strategies brought to fore and entailed modifications to the policy draft throughout the policy process. Through modifications and legitimising strategies, InfoSec policy became to be perceived as appropriate and desirable, at least among those who participated to the policy project. It was the recursive process of legitimisation strategies and the amendments to policy that gave Beta's policy authoritativeness, as each version of the policy had absorbed those changes required by the legitimisation. Finally, legitimacy was of crucial importance for getting the policy approved by the top management and Beta's broad of executives.

5 Discussion

Despite the acknowledged importance of an InfoSec policy (e.g., Baskerville & Siponen 2002; Siponen & Iivari 2006; Warkentin & Johnston 2008), there are few studies of how InfoSec policy crafting actually occurs or how social aspects shape the process (e.g., Baskerville & Siponen 2002; Dhillon 2007; Nasution & Dhillon 2012). Against this backdrop, I analysed policy crafting at Beta and drew upon organisational and management literature on legitimacy and legitimisation to understand how policy becomes legitimised in the policy crafting process and what are the implications of legitimising for the policy. In illustrating the dynamics of legitimisation in policy crafting, this study contributes to literature that is interested in how InfoSec is managed in practice (e.g., Njenga; Tsohou et al. 2012; Hsu 2009) in general and how InfoSec policies are crafted in particular (e.g., Karyda et al. 2005; Lapke & Dhillon 2008; Inglesant & Sasse 2011; Nasution & Dhillon 2012; Niemimaa et al. 2013; Niemimaa & Laaksonen 2015).

Figure 1 summarises the findings of the study and depicts the legitimisation of the InfoSec policy in Beta. It is important to understand the recursive legitimisation-policy dynamics over policy process, through which the policy derived its authority and legitimacy. Over the course of policy crafting process, the policy draft was amended as deemed necessary to legitimise it. Through amendments, the policy absorbed those contextual nuances of Beta that could never be directly derived from, for example, international InfoSec management standards (Siponen 2006) and that were necessary for the legitimisation. The amendments responded to the needs and interests of the different organisational members and made the policy more appealing for them. The findings illustrate that organisational members held conflicting views over policy and many saw it would conflict with the existing organisational practices. The strategy of inviting participation was crucial for bringing the views to fore and making the necessarily changes to the policy draft and the strategy of embedding into existing practices alleviated the conflicts between policy and existing practices. The strategies of advertising and formalising and professionalising increased policy's comprehensiveness and persuaded organisational members about the potential of the policy in producing meritorious outcomes for Beta. As the policy draft increased in legitimacy over successive cycles of amendments and legitimisation strategies, its content became more fixed and less subject to changes (depicted as darkening colour of the policy draft in Figure 1). The policy text became increasingly authoritative and thus the text itself legitimised particular course of action (cf. Spee & Jarzabkowski 2011). As illustrated in Figure 1, the legitimisation strategies and the policy became closer together, with legitimisation

strategies supporting the policy and policy confirming the legitimacy claims, over successive cycles as the policy draft was considered more and more legitimate.

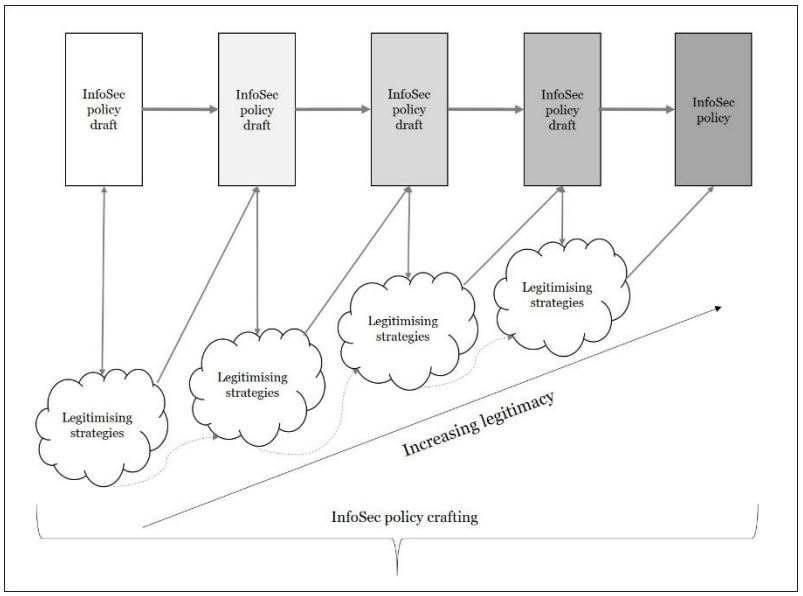

Figure 1: Legitimisation of Information Security Policy at Beta

The study contributes to literature as follows. First, the study illuminates legitimising processes that extent theorising on legitimacy, InfoSec policies and should inform how organisations develop InfoSec policies. A previously unidentified process of InfoSec policy crafting emerged from the focus on the under explored social aspects of policy crafting and on the notation that legitimacy is important for the policy level as well as organisational level. While organisations may gain external legitimacy by implementing InfoSec policies (Hsu et al. 2012), the policies may not turn into organisational practices unless legitimised internally. The lack of legitimacy likely facilitates organisational misconduct and employee non-compliance to the policy, and thus creates a latent threat to organisation's InfoSec. This richer understanding of the importance of legitimacy and the dynamics of building legitimacy during the InfoSec policy crafting answer to calls for increased understanding of social aspects of InfoSec policy crafting (Nasution & Dhillon 2012). It further provides a foundation for analysing legitimising efforts in other contexts.

Second, the study offers an alternative view on policy development by conceptualising it as a process of legitimisation, consisting of recursive legitimisation-policy cycles (Figure 1) that lead to a final policy. I illustrated that the illegitimacy of the policy draft and legitimisation strategies shaped the policy draft. This highlights the emergent process of policy crafting as Baskerville and Siponen (2002) and Dhillon (2007) called for and provides insight into processes that lead to effective InfoSec policies (Straub et al. 2008). It further suggests an alternative view on policy as a means of deterring misconduct, which currently assumes that the legitimisation of the policy is achieved only after policy has been formulated. Studies that focus on policy compliance after policy has been formulated overlook how policy is amended and legitimised already in the making and implications of this legitimisation for the policy. The findings show that legitimacy – justification of the policy – is not a process that occurs only after policy has been developed but rather is something that should be an integral part of policy development process itself. Without legitimisation, policy may be decoupled from organisational practice. Hence, I argue that it is the policy crafting process that is of more significance than often assumed for the policy compliance. Policy should not be seen as something separate from compliance (Niemimaa & Laaksonen 2015).

Finally, the study contributes to organisational literature on legitimisation as organisational literature often investigates how an organisation constructs legitimacy towards external audiences (e.g., governments, customers) but leaves internal legitimacy, or internal audiences aside (MacLean and Bahnam 2010). The findings provide novel insights and elaborate internal legitimisation processes by suggesting the cyclic interplay between legitimisation and policy. They further extend Suchman's (1995) legitimisation strategies that concern an organisation's legitimacy towards its environment by identifying strategies for achieving legitimisation internally, within an organisation. The identified strategies extent the generic strategies with the particularities of InfoSec policy crafting.

Implications for managing InfoSec in organisations. This study suggests that organisations can reduce misconduct and InfoSec policy non-compliance by engaging legitimisation strategies already during InfoSec policy development. These strategies will not only make the policy more suitable for the organisational context (e.g., aligned with organisational practices as was the case at Beta), but will also positively impact the way InfoSec management and InfoSec policies are perceived in the organisation and increase the positive perception of policy's legitimacy, which influences the conduct of organisational members. The strategies offer managers a means for avoiding the pitfalls of decoupling already in the crafting of an InfoSec policy. While other legitimisation strategies can be identified in other firms, the strategies identified herein serve as templates for reflection and as a source of ideas to managers.

6 Conclusion

Organisations and management scholars have long recognised the centrality of legitimacy for organisations and emphasised that legitimacy may quickly vanish. This study argued that legitimacy is as essential for InfoSec management as it is for organisations. When organisational practices are perceived as illegitimate, they are likely not visible in organisation's practices. InfoSec policy is not turned into actions and likely fails to produce the intended effects in securing organisation against InfoSec risks. Against this backdrop, this study analysed InfoSec policy crafting and identified strategies for legitimising the policy and InfoSec management more broadly. The findings highlight the profound role of legitimisation strategies in the policy crafting and in achieving successfully policy outcomes.

Limitations and future research. This study is not without limitations. Beta offered a fruitful context in which to analyse legitimisation processes of InfoSec policy crafting, but it only represents one example of the process. Future studies should analyse the processes more broadly across different contexts. Nevertheless, I believe the identified legitimisation strategies are likely to be present also in other settings beyond the single site of this study. The study was not intended to make statistical generalisations, but—by relating the uncovered local ideographic details to broader theoretical ideas—generalises to theory (Lee & Baskerville 2003). While Beta crafted its new InfoSec policy in hopes of actually deterring misconduct and translating policy into actions, other organisations may decouple their InfoSec policies from their core business activities and organisational practices, deploying a policy while avoiding integration of policy's practices into their day-to-day work. Such decoupling would produce symbolic gestures towards external audiences to, for example, satisfy regulatory requirements, but allow organisations to continue "business as usual". How common is such decoupling and how organisation legitimate the decoupling internally are fruitful avenues for future research.

7 References

Ansari, S., Reinecke, J. and Spaan, A. 2014. "How Are Practices Made to Vary? Managing Practice Adaptation in a Multinational Corporation," *Organization Studies* (35:9), pp 1313-1341.

Baskerville, R., and Siponen, M. 2002. "An Information Security Meta-Policy for Emergent Organizations," *Logistics Information Management* (15:5/6), pp 337-346.

Baskerville, R.L., and Myers, M.D. 2015. "Design Ethnography in Information Systems," *Information Systems Journal* (25:1), pp 23-46.

Bromley, P., and Powell, W.W. (2012). "From Smoke and Mirrors to Walking the Talk: Decoupling in the Contemporary World," *Academy of Management Annals (6/1)*, pp 483-530.

Constantinides, P., and Barrett, M. 2014. "Information Infrastructure Development and Governance as Collective Action," *Information Systems Research* (26:1), pp 40-56.

Corpuz, M., and Barnes, P.H. 2010. "Integrating Information Security Policy Management with Corporate Risk Management for Strategic Alignment," in *Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010)*, pp 1-7.

Dhillon, G. 2007. *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ: John Wiley & Sons, Inc..

Dick, P. 2015. "From Rational Myth to Self-Fulfilling Prophecy? Understanding the Persistence of Means–ends Decoupling as a Consequence of the Latent Functions of Policy Enactment," *Organization studies* (36:7), pp 897-924.

Doherty, N.F., Anastasakis, L., and Fulford, H. 2009. "The Information Security Policy Unpacked: A Critical Study of the Content of University Policies," *International Journal of Information Management* (29:6), pp 449-457.

Hsu, C., Lee, J.-N., and Straub, D.W. 2012. "Institutional Influences on Information Systems Security Innovations," *Information Systems Research* (23:3-Part-2), pp 918-939.

Hsu, C.W. 2009. "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization," *European Journal of Information Systems* (18:2), pp 140-150.

Inglesant, P., and Sasse, M.A. 2011. "Information Security as Organizational Power: A framework for Re-thinking Security Policies," in *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pp 9-16.

Kaganer, E., Pawlowski, S.D., and Wiley-Patton, S. 2010. "Building Legitimacy for IT Innovations: The Case of Computerized Physician Order Entry Systems," *Journal of the Association for Information Systems* (11:1), pp 1-33.

Karyda, M., Kiountouzis, E., and Kokolakis, S. 2005. "Information Systems Security Policies: A Contextual Perspective," *Computers & Security* (24:3), pp 246-260.

King, B.G., and Whetten, D.A. 2008. "Rethinking the Relationship Between Reputation and Legitimacy: A Social Actor Conceptualization," *Corporate Reputation Review* (11:3), pp 192-207.

Langley, A. 1999. "Strategies for Theorizing from Process Data," *The Academy of Management Review* (24:4), pp 691-710.

Lapke, M., and Dhillon, G. 2008. "Power Relationships in Information Systems Security Policy Formulation and Implementation," in *ECIS 2008 Proceedings*, paper 119.

Lee, A.S., and Baskerville, R.L. 2003. "Generalizing Generalizability in Information Systems Research," *Information Systems Research* (14:3), pp 221-243.

MacLean, T.L., and Behnam, M. 2010. "The Dangers of Decoupling: The Relationship between Compliance Programs, Legitimacy Perceptions, and Institutionalized Misconduct," *Academy of Management Journal* (53:6), pp 1499-1520.

Meyer, J.W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology,* (83), pp 340-363.

Miettinen, R., Samra-Fredericks, D., and Yanow, D. 2009. "Re-Turn to Practice: An Introductory Essay," *Organization Studies* (30:12), pp 1309-1327.

Myers, M. 1999. "Investigating Information Systems with Ethnographic Research," *Communications of the Association for Information Systems* (2:23), pp 1-20.

Myers, M. D.2009. *Qualitative Research in Business and Management*. London,UK: Sage.

Nasution, F.M., and Dhillon, G. 2012. "Shaping of Security Policy in an Indonesian Bank: Interpreting Institutionalization and Structuration," in *ECIS 2012 Proceedings*, paper 125.

Nicolini, D. 2009. "Zooming In and Out: Studying Practices by Switching Theoretical Lenses and Trailing Connections," *Organization Studies* (30:12), pp 1391-1418.

Niemimaa, M., and Laaksonen, A.E. 2015. "11: Enacting Information Security Policies in Practice: Three Modes of Policy Compliance," in *Materiality, Rules and Regulation: New Trends in Management and Organization Studies*, F.-X. de Vaujany, N. Mitev, G.F. Lanzara, and A. Mukherjee (eds.), Hampshire, UK: Palgrave Macmillan, pp 223-249.

Niemimaa, M., Laaksonen, E., and Harnesk, D. 2013. "Interpreting Information Security Policy Outcomes: A Frames of Reference Perspective," in *Proceedings of the 46th Hawaii International Conference on System Sciences*, pp 4541-4550.

Njenga, K., and Brown, I. 2012. "Conceptualising Improvisation in Information Systems Security," *European journal of information systems* (21:6), pp 592-607.

Oliver, C. 1991. "Strategic Responses to Institutional Processes," *Academy of Management Review* (16), pp 145-179.

Philippe, D., and Durand, R. 2011. "The Impact of Norm-Conforming Behaviors on Firm Reputation," *Strategic Management Journal* (32:9), pp 969–993.

Rees, J., Bandyopadhyay, S., and Spafford, E. H. 2003. "PFIRES: A Policy Framework for Information Security," *Communications of the ACM* (46:7), pp 101-106.

Rowe, F. 2012. "Toward a Richer Diversity of Genres in Information Systems Research: New Categorization and Guidelines," *European Journal of Information Systems* (21:5), pp 469-487.

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

Siponen, M., and Iivari, J. 2006. "Six Design Theories for IS Security Policies and Guidelines," *Journal of the Association for Information Systems* (7:7), pp 445-472.

Siponen, M., Willison, R., and Baskerville, R. 2008. "Power and Practice in Information Systems Security Research," in *ICIS 2008 Proceedings*, paper 26.

Spears, J. L., Barki, H. and Barton, R.R., 2013. "Theorizing the Concept and Role of Assurance in Information Systems Security," *Information & Management* (50:7), pp 598-605.

Spee, A. P., and Jarzabkowski, P. 2011. "Strategic Planning as Communicative Process," *Organization Studies* (32:9), pp 1217-1245.

Straub, D. W., Goodman, S., and Baskerville, R.L. 2008. "Framing the Information Security Process in Modern Society," in *Information Security: Policy, Processes and Practices*, D.W. Straub, S. Goodman, and R.L. Baskerville (eds.), Armonk, NY: M.E. Sharpe, pp 5-12.

Suchman, M. C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review* (20:3), pp 571-610.

Suddaby, R., and Greenwood, R. 2005. "Rhetorical Strategies of Legitimacy," *Administrative Science Quarterly* (50:1), pp 35-67.

Warkentin, M., and Johnston, A.C. 2008. "IT Governance and Organizational Design for Security Management," in *Information Security: Policy, Processes and Practices*, D.W. Straub, S.E. Goodman, and R. Baskerville (eds.), Armonk, NY: M.E. Sharpe, pp 46-68.

Whitman, M.E. 2008. "Security Policy: From Design to Maintenance," in *Information Security: Policy, Processes and Practices*, D.W. Straub, S. Goodman, and R.L. Baskerville (eds.), Armonk, NY: M.E. Sharpe, pp 123-151.

Zimmerman, M.A., and Zeitz, G.J. 2002. "Beyond Survival: Achieving New Venture Growth by Building Legitimacy," *Academy of Management Rev. (27:3)*, pp 414–431.