Author(s): Niemimaa, Marko; Niemimaa, Elina

Title: Abductive innovations in information security policy development : an ethnographic study

Year: 2019

Version: Accepted version (Final draft)

Please cite the original version:

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development : an ethnographic study. European Journal of Information Systems, 28(5), 566-589. https://doi.org/10.1080/0960085X.2019.1624141

Abductive innovations in information security policy development: an ethnographic study

The Version Record of this manuscript has been published and is available in European Journal of Information Systems 9/20/2019 http://www.tandfonline.com/ DOI: 10.1080/0960085X.2019.1624141

Marko Niemimaa

University of Jyvaskyla, Faculty of Information Technology

marko.i.niemimaa@jyu.fi

Elina Niemimaa

Secrays Co.

elina.niemimaa@gmail.com

Developing organisational information security (InfoSec) policies that account for international best practices but are contextual is as much an opportunity for improving InfoSec as it is a challenge. Previous research indicates that organisations should create InfoSec policies based on best practices (top-down) and simultaneously encourages participatory development (bottom-up). These contradictory suggestions place managers in a dilemma: Should they follow a top-down or bottom-up approach? In this research, we build on an ethnographic approach to study how an innovative engineering company (MachineryCorp) managed the contradiction when the firm developed an InfoSec policy. Drawing on the dialectical theory of organisations as a lens, the findings suggest the InfoSec policy development is a recurrent process consisting of three phases: (1) drawing interpretations of InfoSec requirements from best practices (deductive adoption) and (2) constructing possibilities for local implementation (inductive adjustment) (3) that engender tensions between best practices and local contingencies facilitating innovative local resolutions (synthetic innovation). We call this process abductive innovation. At MachineryCorp, a triangle of tensions surfaced due to economic realities, infrastructure affordances, and social arrangements, and were necessary in explaining how the InfoSec policy gradually and iteratively materialised and resulted in an organisationally contingent policy.

Keywords: Information security policy development; ISS policy; ethnography; abductive innovation

Introduction

Digitalisation of products and services has elevated information security (InfoSec) to the top organisational concern (Kappelman, Mclean, Johnson, & Torres, 2016). Digitalisation through instantiations of such techniques as the Internet of Things (IoT; Atzori, Iera, & Morabito, 2010) not only renders the boundary between the physical and the virtual increasingly porous but also increases the sensitivity and value of the information possessed and processed by organisations as nearly everything about us and around us becomes transformed into bits and bytes (Tene & Polonetsky, 2012). Simultaneously, industry surveys indicate an increase in the sophistication of malicious programs used to steal information and an overall increase in the expected occurrence of InfoSec breaches (Av-Test Institute, 2017; EY, 2018; Ponemon Institute, 2017; PwC, 2015). On the cusp of these changes, organisations face the need to reconsider and evaluate the competency of their technical and administrative InfoSec measures to protect the flow and use of their information.

In an effort to manage InfoSec, organisations need to formulate effective InfoSec policies (Boss et al., 2009). As organisation-wide policy documents that define an organisation's expectations and measures for protecting information, InfoSec policies are developed through complex processes that involve several challenges (Karyda, Kiountouzis, & Kokolakis, 2005; Knapp, Morris, Marshall, & Byrd, 2009). Amongst others, a key challenge concerns the development of policies that are meticulous and comprehensive in a way that ensures information assets are protected against various threats. Another challenge is to develop policies that align with organisational efficiency goals and practices such that InfoSec does not become an impediment, as often the most secure practices are not the most efficient and vice versa.

To address these challenges, different approaches for developing InfoSec policies are needed. Previous literature suggests that organisations should primarily create policies based on international

best practices (von Solms & von Solms, 2004a), but it also suggests that in particular, organisations that treat security as fungible need approaches in which policies emerge from employees' work practices (Hedström, Kolkowska, Karlsson, & Allen, 2011) and contextual factors (Karyda et al., 2005). Although best practices increase policy comprehensiveness due to the collective expert knowledge they contain (Backhouse, Hsu, & Silva, 2006; Baskerville & Pries-Heje, 2014), the literature suggests issues are likely to emerge if the policies do not reflect organisational contingencies, such as employees' values (Hedström et al., 2011; Kolkowska, Karlsson, & Hedström, 2017), frames (Albrechtsen, 2007; Laaksonen et al., 2013; Niemimaa et al., 2015), domain-specific expertise (Siponen, 2005a), or organisational culture and structure (Karyda et al., 2005), as the policies may not be enactable in practice and as they may conflict with organisational performance goals. When policies emerge from work practices, the policies can include employees' domain-specific expertise and support alignment with organisational performance goals, but also improve workplace democracy. Employees may influence the policies that so profoundly define the conditions under which the employees perform their work (Alvesson & Willmott, 1996). However, literature also notes that policies should be seen as non-negotiable (von Solms, 2004a) as deviations from best practices are seen to impede comprehensiveness and lead to suboptimal security (Smith, Winchester, Bunker, & Jamieson, 2010). Thus, challenges are only partially met which may contribute to the explanations of why policies often fail to meet the goals set (Karyda et al., 2005).

Organisational policy-makers face a dilemma emerging from seemingly contradictory suggestions to create policies from best practices (top-down) or to allow policies to emerge from work practices (bottom-up). To alleviate the issues identified in the top-down approach, scholars suggest that the observed shortcomings should be overcome with strict governance and control structures that enforce policies with sanctions and rewards (von Solms, 2005a, 2005b). Researchers also suggest that the issues cannot be overcome unless the organisational contingencies are addressed. For instance, Karyda et al. (2005) argued that "[a] rigid hierarchical structure may be a problem for information

security management since the application of a security policy often requires organisational flexibility" (p. 257). Further, what appears to be employees' resistance and reluctance to appropriate the policies and comply with them may actually originate in the policy development and promotion practices (Niemimaa & Laaksonen, 2015), and cannot be overcome with mere added control and governance. Instead, scholars urge that participatory development methods are needed that include employees as a *constitutive* part of policy development to negotiate the policies (James, 1995). Although a balanced approach seems like a potential way forward, studies are lacking, as indicated in a recent call for research (Cram, Proudfoot, & D'arcy, 2017).

These concerns warrant closer inspection and provide the justification for us to examine a key question: How do organisations develop InfoSec policies that are sensitive to employees' work practices and organisational contingencies but also align with the technical expert knowledge contained in InfoSec best practices? We investigate this question by drawing on empirical material from a 15-month ethnographic study (Klein & Myers, 1999; Myers, 1999) of an InfoSec development project at an innovative and highly profitable corporation, MachineryCorp (a pseudonym). The project, which led to the complete restructuring of the firm's InfoSec policy, was a response to changes in the corporation's legislative environment and IoT-based product innovations that transformed the organisation from a product manufacturer to a service-oriented producer. This project initially started as a top-down, best practice–driven process, but confronted tensions emerging from contradictions between what was required and what was (organisationally) possible that required MachineryCorp to find innovative local resolutions.

We use the dialectical theory of organisations (Benson, 1977, 2013) as a lens for understanding how policy-makers entertain and reconcile the contradictions inherent in the complex process of developing an InfoSec policy. We contribute with a conceptualisation of the process as *abductive innovation* that improves understanding of the development of InfoSec policies and

contributes to practice with a fair, participatory, and emancipatory description of the development process that recognises the contingent and contextual nature of InfoSec policies.

We organised the paper as follows. In the next section, we juxtapose existing approaches for developing InfoSec policies and then introduce the theoretical lens of the study. In the third section, we provide a description of the research approach and give a brief introduction to the historical and social contexts of the study. In the fourth section, we present the findings by illustrating how the InfoSec policy emerged as a local resolution of socially constructed organisational constraints that necessitated innovative and socially acceptable solutions. In the fifth section, we provide a discussion of the findings and their broader implications for research and practice in InfoSec management and policy development. In the last section, we draw conclusions.

Dialectics of the development of an information security policy

Organisational top-down and bottom-up approaches have been broadly discussed in literature. For example, in relation to Information Systems (IS) development, these concepts denote whether a "design process starts with specifying the global system state and assuming that each component has global knowledge of the system" (top-down) or whether "the design starts with specifying requirements and capabilities of individual components, and the global behaviour is said to emerge out of interactions amongst constituent components and between components and the environment" (bottom-up; Crespi et al., 2008, p. 303). In relation to IS infrastructures, the top-down approach denotes management-driven initiatives to control infrastructure development whereas the bottom-up approach denotes the tendency of infrastructures to evolve by "drifting" away from management control (Ciborra & Hanseth, 2000; Constantinides & Barrett, 2014). In relation to management literature, these concepts refer to organisational change enforced by senior management (top-down) or emerging from the grassroots (bottom-up). We use the concept top-down to denote the development of InfoSec policies in which policies are derived from international best practices whereas bottom-up denotes development that creates policies from considerations of local

contingencies (Hedström et al., 2011). Next, we discuss how these approaches appear in the literature. Whilst doing so, we remain aware of the variation within and the overlap of these approaches. We emphasise the particular streams within each approach which enables us to highlight the contrasts and contradictions between the approaches.

Juxtaposing approaches to the development of information security policies

InfoSec management focuses on "managerial actions that promote a secure environment" (Ransbotham & Mitra, 2009, p. 122). InfoSec policies are said to form the foundation for those actions and an organisation's InfoSec management efforts (Doherty, Anastasakis, & Fulford, 2009; Siponen & Iivari, 2006; Warkentin & Johnston, 2008). The policies are direction-setting documents for an organisation's InfoSec (Höne & Eloff, 2002) that define roles and responsibilities (Whitman, 2004), administrative and behavioural processes and procedures (Knapp et al., 2009), as well as technologies, which constitute the key measures for promoting effective InfoSec management practices (Herath & Rao, 2009). In short, as advocated by the international ISO/IEC 27001 standard for InfoSec management, the objective of an InfoSec policy is to "provide management direction and support for information security in accordance with business requirements and relevant laws and regulations" (ISO/IEC, 2013, p. 10).

InfoSec managers in all organisations, whether commercial, governmental, not-for-profit, or other, confront the need to develop organisational InfoSec policies (Straub, Goodman, & Baskerville, 2008). Often, policy development and implementation efforts fail to produce the desired results (Karyda et al., 2005). To address this challenge, researchers have proposed models for developing InfoSec policies for managers to follow (Knapp et al., 2009; Rees, Bandyopadhyay, & Spafford, 2003; Whitman, 2008). Typically, the models suggest phases through which a policy should be developed without detailing what ought to be done in each phase. For example, Knapp et al. (2009) suggest policy development involves risk assessment, policy development, policy approval, policy

awareness and training, policy implementation, monitoring, policy enforcement, and policy review phases.

Others suggest InfoSec policies should be based on "best practices" in international InfoSec management standards such as ISO/IEC 27001 and ISO/IEC 27002 (Ma, Johnston, & Pearson, 2008; Saint-Germain, 2005; von Solms, 1999, 2005a). InfoSec management "is often built on a top-down-approach, where information security managers develop security measures (i.e., administrative routines or technical controls) based on international standards such as ISO 27000-series" (Hedström et al., 2011, p. 381). In the past, this approach has been suggested as the "best method" for developing policies (Ma et al., 2008) and as an effective approach for managing InfoSec risks (Straub & Welke, 1998).

Another similar stream of research emphasises management control and governance in the development of InfoSec policies. Von Solms, Thomson, and Maninjwa (2011) suggest organisations should control and direct InfoSec by developing policies and note that this requires a set of policies that facilitates "complete control" over the organisation. They argue that an organisation's executive management should issue directives that are written as InfoSec policies to dictate how InfoSec should be understood and implemented. Von Solms and von Solms (2004b) reiterate this point by stressing that policies must clearly define the senior management's intent. In the same vein, Whitman (2008) sees InfoSec policies as dictating how organisational actors should act and behave. From this starting point, he suggests that an InfoSec policy should be formulated by an authorised entity and ratified. The ratification should be signed by an organisation's chief executive officer (CEO) to show executive commitment to and buy-in of InfoSec (von Solms & von Solms, 2004a).

Developing InfoSec policies based on best practices, control, and governance aims at what Hedström et al. (2011) call the "control-based compliance model," and Kirlappos, Beautement, and Sasse (2013) the "comply or die" approach. It is primarily concerned with employee control and behavioural regulation with the aim of forcing employees to comply with the policy through means

of deterrence. Von Solms (2005b) summarised this view well by arguing the following: “The fact that an unenforced policy is not worth the paper it is written on, is a generally accepted fact” (p. 445). Consequently, these InfoSec control and governance practices form pseudo-natural constraints and are often seen as oppressive. In top-down approaches, employees have no direct impact on the development of such policies.

Such *top-down* approaches seem to presume that InfoSec managers are the primary actors who develop the policies, that these managers are in a position to enforce the policies, and that policy development relies on perceptive managerial action. These approaches have been criticised for failing to pay adequate attention to organisational differences (Baskerville & Siponen, 2002) and for being unable to account for the social nature of InfoSec problems (Dhillon & Backhouse, 2001). These approaches may overlook organisations’ business requirements and other situated characteristics with the result that the situated characteristics and the InfoSec policy may conflict. As top-down approaches do not allow employees an active role, these approaches can be characterised as promoting the technical role of InfoSec and technical control of employees that, in turn, may be detrimental for the organisations’ InfoSec (Siponen, 2005a). Developing policies through a top-down approach may simply fail, because in modern organisations, employees are used to collaborating and showing initiative; and they should be the principal agents who decide how InfoSec is implemented in specific contexts (Kirlappos et al., 2013).

In contrast to top-down approaches, the proponents of *bottom-up* policy development are concerned with an organisation’s idiosyncratic qualities and the organisational context where policy development takes place, and often allow different organisational actors and their voices more discretion. An analysis based on the theory of contextualism suggests that the development and implementation of InfoSec policies are affected by the organisational context and by the power relations and cultural elements within which the policies happen (Karyda et al., 2005). Organisational groups without formal power, such as subject matter experts, may exercise power over policy

development and implementation (Lapke & Dhillon, 2008). Social structures may also shape policy (Nasution & Dhillon, 2012). Echoing these empirical studies, an analysis of modern InfoSec development approaches suggests that they should be emancipatory and enable employee participation, not only because employee input in and knowledge of InfoSec are themselves valuable but also because participation promotes social acceptance of security techniques and procedures (Siponen, 2005b; see also James, 1996).

Recent studies offered additional arguments for employee participation. For example, in the context of healthcare, healthcare professionals should be a resource in policy-making (Hedström et al., 2011). Participation may further converge InfoSec professionals' and other employees' frames of reference, thus making policies more acceptable to the employees (Niemimaa et al., 2013). In general, employees' participation in InfoSec management activities may improve the employees' perception of the significance of the InfoSec measures (Spears & Barki, 2010). Additional aspects of involvement, such as collaboration, may have a positive effect on employees' attitude towards policy compliance (Safa, Von Solms, & Furnella, 2016). Communicating respectfully and maximising employee rights, as well as promoting trust and fairness, may improve organisational efforts to implement InfoSec policies (Lowry, Posey, Bennett, & Roberts, 2015).

As the discussion above indicates, the literature seems to give contradictory suggestions. Although approaches that combine top-down and bottom-up approaches have been called for (Siponen, 2005b), the research addressing the calls seems to fall short (Kirlappos et al., 2013). Part of the problem likely reflects that most studies on the development of InfoSec policies are conceptual (Cram et al., 2017), or they document controlled interventions in policy development (James, 1996). By doing so, the studies tend to emphasise the instrumentality and normativity of how policy development *ought* to happen rather than how the development *actually* happens within an organisation. Such studies tend to represent sanitised accounts of the events and activities in development that hide contradictions and the struggles that characterise organising (Benson, 1977),

and omit the details of how organisations develop local policies and practices from abstractions (Niemimaa & Niemimaa, 2017). We seek to address the shortcomings by turning to empirical material to develop an alternative and empirically veracious understanding of the process for developing InfoSec policies.

Dialectical view on innovation for the development of information security policies

The dialectical view is fundamentally concerned with the processes through which different organisational arrangements are socially produced and maintained (Benson, 1977). In the rudimentary form, the dialectical view posits that organising and change is a synthesis that results from the conflicting demands of the thesis and the antithesis (Benton & Craib, 2001). An organisational arrangement exists "in a pluralistic world of colliding events, forces, or contradictory values that compete with each" (Van de Ven & Poole, 1995, p. 517). Such oppositions confront and engage one another in conflict. Consequently, the social world is in a continuous state of becoming driven by the contradictions that provide a source of tension (Benson, 1977). Organisational arrangements that may seem permanent and fixed are temporary, emergent, and often arbitrary (Benson, 1977). The dialectical view differs from the related view of paradoxes (Farjoun, 2016; Hargrave & Van de Ven, 2017), as this view sees that contradictions can be reconciled (Benson, 1977) whereas in paradoxes, contradictory elements have a "persistent coexistence" (Hargrave & Van de Ven, 2017, p. 320) and thus, can only be managed or sustained (Smith, 2014).

Following Benson (1977), the dialectical view entails four principles—social construction, contradiction, totality, and praxis. The three first principles characterise the social life and provide a framework for understanding organisational arrangements and developing empirical work around them (Benson, 2013).

(1) Social construction. People continually construct organisational arrangements through their practices and interactions under circumstances and conditions not of the individuals' own choosing.

In so doing, they confront contradictions between opposing interests and established arrangements. This implies that practices may not result in the most efficient or effective arrangements.

(2) Contradiction. Oppositions and conflicts are deeply rooted in organisations. Social construction involves contradictions that enable change.

(3) Totality. Arrangements must be studied and understood in their contexts. Any arrangement is always part of a larger whole rather than an isolated abstract phenomenon. Social construction happens within a social context.

The fourth principle of *praxis*[1] is a commitment "to the production of forms of social organization" (Benson, 2013, p. 3-4) which calls "for a praxis of enlightenment and liberation to guide [research]…rather than a narrow pursuit of effectiveness and efficiency." (Benson, 2013, p. 2) It recognises the performativity of theories to the construction of social organisation as a dialectical relation and takes critical reflection and emancipation as the overarching goals of all social sciences (Benson, 1977).

In the context of an InfoSec policy, the development process becomes established within a particular social and organisational culture where "agency and action (be it word or deed) rest on social meanings" (van Maanen, 2011a, p. 221) that are socially constructed and emergent. In this context, "[c]ulture simply refers to the meanings and practices produced, sustained, and altered through interaction" (van Maanen, 2011a, p. 221). The development process unfolds between the contradictions of the interpretation of best practices and the socially constructed local demands, constraints, and expectations. Previous researchers suggested that such dialectical tensions may give rise to innovation as a problem-solving activity to reconcile the oppositions and conflicts and enable change such that "one set of arrangements gives way to another" (Benson, 1977, p. 3).

In the context of the adoption of best practices for InfoSec, Hsu, Lee, and Straub (2012) define innovation as "any idea, practice, or material artifact perceived to be new by the unit of adoption"

[1] Benson's (1977; 2013) notion of praxis should not be confused with its use in practice theories (e.g., Whittington, 2006).

(Zaltman et al., 1973, p. 158, in Hsu et al., 2012). Thus, what some might consider as "reinventing the wheel" may represent newness and novelty to another community or group: "[I]t is the perception of newness that is distinguishing, not whether or not that something is new 'everywhere'" (Hellström, 2004, p. 634). Therefore, an innovation differs from a *radical innovation* that is often considered to be new to the world (Wittell, Snyder, Gustafsson, Fombelle, & Kristensson, 2016). Further, what differentiates an innovation from a mere change is the dialectical relationship "involved in acting to resolve a problem of some kind, i.e. finding the interface between the abstract (what a problem is, what one wants to do, what a need is) and the concrete (how to make thing happen, how to mould the environment, physical acts)" (Hellström, 2004, p. 634). Thus, an innovation often signifies the process and the outcome (Wittell et al., 2016) as only analytically separate acts of resolving the problem and applying a solution to the problem. That is, the (contextual) use transforms a mere idea or invention into an innovation (Wittell et al., 2016).

The dialectics of innovation has also emerged in IS studies (Cho, Mathiassen, & Robey, 2006; Lyytinen, Yoo, & Boland, 2016; Svahn, Henfridsson, & Yoo, 2009). These studies proposed that within a web of social relationships, people's perspectives often conflict, but people need to align their interests to achieve a temporary dialectic synthesis (Lyytinen et al., 2016). A digital innovation can be seen as a continuing dialectic process of resisting established social structures and accommodating, for example, new practices and the establishment of new social structures (Svahn et al., 2009). A crucial point for the digital innovation adoption process arises because of the inherent contradictions within and across the adopting organisations (Cho et al., 2006).

The concept of latent but ever-present conflict is fundamental for the dialectical dynamics of innovation (Hargrave & van de Ven, 2006). Conflict is a source of creativity, and by implication, an innovation. When InfoSec policies are developed, conflicting demands may surface, for instance, from a best practice requirement that enforces the use of strong and complex passwords whilst the technological solutions may be considered too expensive (for that context). This scenario drives the

organisation to seek innovations that meet the requirement and the local constraints which may result in unexpected and unforeseen solutions that do not directly reflect the best practices or the local organisational arrangements. For instance, in lieu of implementing an expensive technological solution, an organisation may enact a new policy that encourages the use of strong passwords and the periodic use of freely available password cracking tools to discover the strength of employees' passwords. Thus, the dialectics of innovations may significantly contribute to understanding how the development of InfoSec policies proceeds in practice. In the following, after providing details of the research approach and empirical material, we empirically illustrate how the tensions that drive the dialectical process for developing InfoSec policies emerge.

Research approach

We build on the ethnographic research approach to study the development of InfoSec policies. Ethnography is a research method and a writing genre (Schultze, 2000; van Maanen, 2011a;b). As a research method, ethnography enables researchers to study *in situ* "how people make sense of things, events and phenomena in their everyday lives" (Schultze, 2017, p. 1) to develop deep insight (Myers, 1999; Walsham, 2006) into informants' practices (Feldman & Orlikowski, 2011). That is, "[a] defining feature of the ethnographic approach is thus the researcher's immersion in a social setting referred to as the field, as well as his[/her] engagement with its participants" (Schultze, 2017, p. 1). Ethnography is a writing genre, as this method relies on a specific type of writing and reporting that seeks to convey a sense of "being there" with the aid of narratives (Jarzabkowski, Bednarek, & Lê, 2014) and "thick" descriptions (Geertz, 1973). Previous IS researchers utilised ethnography to study a broad range of social processes and practices, such as digital disruptions (Utesheva, Simpson, & Cecez-Kecmanovic, 2016), distributed systems development (Sarker & Sahay, 2004), information infrastructure development (Star & Ruhleder, 1996), organisational learning (Orr, 1996), intraorganisational strategy (Corbitt, 2000), and eHealth networks (Duclos, 2016).

Ethnographies and interpretive case studies share similarities (Klein & Myers, 1999). However, ethnographies differ in that researchers are expected to interact closely with informants and live the organisational life over prolonged periods of time (van Maanen, 2011b): "organizational ethnographers do not study organizations, they study in organizations" (van Maanen, 2011a, p. 221). For these reasons, we see ethnography as well suited and even the privileged mode of inquiry (Rowe, 2012) for this study. Ethnography allows us to closely observe in a naturalistic setting *in situ* and over time (Guba, 1981) as the actors jointly make sense of the InfoSec best practices and local contingencies to construct an InfoSec policy in a specific context (Benson, 1977). Immersion in the research site allows us to create an interpretive and critical understanding of the InfoSec policy process (Siponen, 2005a) that is "rigorously developed *along* with practice" [emphasis ours] (Siponen, 2005b, p. 369). By relating empirical particularities to the dialectical view on innovation, we provide a theory-informed account (i.e., a "realist tale"; van Maanen, 2011b) of the development of an InfoSec policy. In the appendix, we review the criteria for assessing the quality of ethnographic studies and provide a detailed assessment of the present study compared to the criteria. Next, we briefly outline the context of the study after which we provide the methodological details of constructing and analysing the empirical material.

Research site

MachineryCorp is a multinational corporation and a global leader in the field of mechanical engineering. Although headquartered in Finland, the firm operates in more than 50 countries with multiple subunits that are linked through shared policies and a business strategy. During the last few years, the company's business model and products changed rapidly from traditional machinery to intelligent services connected to and maintained through the Internet, making the corporation one of the early adopters of the IoT (Atzori et al., 2010). Traditionally, the company's InfoSec professionals have not perceived the company as a relevant target for hackers, and InfoSec at MachineryCorp focused on information technology (IT) security and on protecting the company's IS and trade secrets.

The changes in MachineryCorp's business model and products (i.e., the company now processes more data of and about its clients, but the data are not highly sensitive) together with the recent increase in the regulation of privacy (e.g., the European Union [EU] General Data Protection Regulation), growing pressure to comply with InfoSec best practices, and skyrocketing media coverage of InfoSec threats pushed MachineryCorp to widen the scope of the company's view of InfoSec. Consequently, the company needed a new InfoSec policy.

The InfoSec policy construction project seemed interesting to us because it involved a total update of the policy for an organisation whose InfoSec threat environment is undergoing a large reorganisation. We chose the policy project as the unit of observation, which allowed us to observe the activities and the actors producing the policy as the project unfolded, rather than prejudging which activities, events, or actors might be central (Kaplan & Orlikowski, 2013). As the second author joined MachineryCorp as an InfoSec professional to act in the role of "consulting-researcher" (Rowe, 2012, p. 473) at the beginning of the company's discussions about the development of an InfoSec policy, we were able to follow the policy-making in real time. The research project was carried out with the consent of the company's management, and the project participants were informed. We were not in a position nor in a role to determine the course and content of the policy development process but acted along with the practitioners to know about the policy process (Feldman & Orlikowski, 2011) which we constantly kept in mind as our primary goal. While the closeness and rapport with informants is a precondition for quality ethnographic work (Van Maanen, 2011b), as we were external to MachineryCorp, we were not associated with any of the social groupings that could have promoted favouring one group over others. Further, one of the authors was not closely involved with the practitioners or the actual events unfolding at the site and thus maintained a neutral position towards the empirical material. We agreed to reveal details of the company only to the extent necessary for reporting the research and to use a pseudonym.

Construction of empirical material and analysis

We constructed the empirical material (Klein & Myers, 1999) primarily through participant observation (Ingold, 2014; Myers, 1999) that allowed the second author to be immersed in the site (Schultze, 2000, 2017) "to attend to persons and things, to learn from them, and to follow in precept and practice" (Ingold, 2014, p. 387). Field notes collected over a period of 15 months covered the whole process during which MachineryCorp developed their InfoSec policy. Additional data sources included notes from informal social contacts and documentary sources. The empirical material is summarised in Table 1.

Table 1. Empirical material and its use.

Data source	**Type of data**	**Use in the study**
15-month participant observation	The second author followed InfoSec policy development observing, discussing, and participating (e.g., attending several meetings and 23 workshops). Observed actors included InfoSec professionals, the chief technology officer (CTO), the head of risk management, compliance officer, legal representatives, the R&D representative, and the chief information officer (CIO) board members. The field note template was adapted from Schultze (2000, p. 17); 181 pages of field notes (font size 12, line spacing 1.5), excluding the documentary sources.	Produce a description of the project and reveal micro-level, situated dynamics by which the policy was made, and analyse the collective construction of local InfoSec practices. Become familiar with the organisational context, gain trust of the actors, discuss and clarify project-related issues, and support emerging interpretations. Describing and understanding the context of the studied phenomenon are crucial for ethnographic studies (Klein & Myers, 1999).
Documentary sources	Documentary sources included old InfoSec policy, InfoSec instructions, the information management policy, the safety policy, the privacy policy, 31 PowerPoint presentations related to policy crafting, 29 policy drafts, 12 policy requirements drafts, and various organisational documents, as well as best practice documents (e.g., ISO/IEC 27001/27002).	Become familiar with the organisational context. Support the evidence and clarify interpretations from observations and social contact (Smets, Morris, & Greenwood, 2012). Support the identification of the differences between best practices and local documented practices to reconstruct the changes between the best practices and local practices. Keep a record of the outcome of project episodes.
Informal social contact	The second author engaged in social contact with different actors throughout the participant observations and wrote	Integrate observations with actors' accounts.

	down the observations as field notes. Owing to the quality of access, she was able to stay at the research site for lunches and coffee breaks and talk freely with the actors.	Provide opportunities to clarify open matters and challenge emerging understanding.

As we followed the inductive research approach, we did not analyse the empirical material using predefined categories or theoretical constructs, but allowed them to emerge from the data. That is, we viewed theory as an end rather than as a means (Walsham, 1995, 2006), and focused on the "central role of data in developing and extending conceptual insight and strong knowledge claims" (Lyytinen, 2009). The phenomenon of interest and the research approach supported the inductive approach. We wished to construct an empirically trustworthy account (Golden-Biddle & Locke, 1993; Guba, 1981; Lincoln & Guba, 1985) of the process for developing an InfoSec policy that was best supported by the rich empirical material and deep insight that characterise ethnographic research (Myers, 1999).

We analysed the empirical material in four steps: (1) writing a chronological description, (2) identifying periods of policy development, (3) making sense of what was happening and uncovering policy development phases, and (4) analysing the tensions in the development of the policy. Firstly, the second author wrote a rich chronological description of the project (Langley, 1999) concentrating on how the policy was created. Secondly, we coded and analysed the chronological description to identify distinct periods during which the policy was constructed (Table 2). Period 1 involved discussions about the increasing importance of MachineryCorp's information assets to its business, the increasing InfoSec risks and changing InfoSec threat landscape, the growing need to comply with industry best practices in InfoSec, initial discussions about the need and goals for the new InfoSec policy, and finally, the decision to craft the policy. The executives who made the decision were committed to the project, and the chief technology officer (CTO) was selected as its sponsor. During period 2, InfoSec professionals, led by the chief information security officer (CISO), crafted the first policy draft, drawing on international InfoSec best practices. The draft included roles and

responsibilities, InfoSec principles for governing, managing, and operating InfoSec at MachineryCorp, and a set of requirements that augmented the principles. In period 3, versions of the draft were presented to and reviewed by a group of managers and executives. The policy was amended according to the group's requests and comments. After the final review, the group approved the draft for wider consultation. This consultation and the requested changes were mandatory, as without them MachineryCorp's CIO Board was unwilling to approve the policy. In period 4, the draft went through major changes as it was discussed in 14 workshops. The workshop topics ranged from network security to identity and access management (i.e., IT security issues), from secure IS development to architecture, and from InfoSec risk management to InfoSec governance. Various organisational members, ranging from the chief financial officer (CFO) to the chief operating officer (COO), participated. The policy was finalised during the fifth period and approved first by the CIO Board and then by MachineryCorp's executive board.

Table 2. MachineryCorp's InfoSec policy development periods.

	Period 1	**Period 2**	**Period 3**	**Period 4**	**Period 5**
Timeline	2 months	5 months	2 months	5 months	1 month
Participation	CTO, Head of risk management, Compliance officer, Head of R&D, CISO	InfoSec professionals, CTO	CTO, Head of risk management, Compliance officer, Head of R&D, InfoSec professionals	Various organisational actors, InfoSec professionals	CIO, CIO Board, Executive Board, InfoSec professionals
Description	Initial discussions around policy	First policy draft	Amendments to policy draft, approval for organisation-wide consultation	Organisation-wide consultation, major amendments to policy draft	Policy approval
Dominant theme in policy development		Policy content derived from external sources	Policy content adjusted based on organisational demands	Policy content adjusted based on organisational demands	

Thirdly, we read the chronological description, field notes, documents, and extant literature to make sense of what was happening during the discovered periods (Klein & Myers, 1999). This

analysis led us to appreciate a dialectical view of organisations (Benson, 1977, 2013), as the organising around the policy development seemed to unfold through contradictions, tensions, and moments of settlement. We further came to understand that top-down and bottom-up approaches to policy development are not opposing poles but are dialectically interrelated. This understanding led us to further analyse the data in terms of their interrelationship, which evolved into a dialectic interpretation of their relationship and the identification of three phases of the InfoSec development process:

(1) Deductive adoption: making sense of InfoSec best practices and forming interpretations of their local application;

(2) Inductive adjustment: evaluating the interpretations of the best practices against local contingencies and idiographic practices to jointly construct possibilities to implement the developed ideas locally; and

(3) Synthetic innovation: coming up with locally innovative (administrative and technological) measures to reconcile emergent tensions.

As the process consisted of phases of developing interpretations from the best practices and then evaluating the interpretations against the jointly constructed organisational (and idiographic) possibilities, it seemed to follow abductive reasoning, which is often used by innovators when they face (complex) problems (Dunne & Dougherty, 2016). Thus, we called the three-phase process *abductive innovation.* When presenting the findings, we analytically separate the phases as three distinct phases although they overlapped and unfolded partly simultaneously. The three phases reflect both as categories and as a sequence abductive processes more generally (Staat, 1993).

Fourthly, we analysed the empirical material across the three phases to understand what drove the process towards the innovation. This analysis revealed tensions between the abstract (best practices) and the particular (local practices) that were part of the dynamics of the development process that gave rise to innovation as a problem-solving activity. By tensions, we mean situations

that emerge from contradictions between best practices and local contingencies (Benson, 1977). We were interested in understanding how the participants socially constructed (Benson, 1977) and gave meaning to best practices and local organisational constraints rather than in discovering an "objective" truth behind those constructions. That is, we relied on the participants' joint construction of the tensions during the process for developing the InfoSec policy, when the participants were reflexive and explicated their views on the mismatch between what ought to be done and what they viewed could be done. We analysed these participants' "first-order" constructs (e.g., words and statements in the field notes that indicate tensions, such as "trade-off," "frustration," "they demanded," "what ideally should be done…what is done in this case") to uncover "second-order" constructs (Klein & Myers, 1999; Walsham, 1995). By moving between first- and second-order constructs, we uncovered three categories of tensions: infrastructure affordances, economic realities, and social arrangements.

Next, we present the findings of the analysis. Presenting findings of ethnographic studies includes a trade-off between showing the rich data upon which the findings are founded and being constrained by the page limitations of an article (Walsham, 1995). Therefore, we draw on suggestions proposed by Jarzabkowski et al. (2014), and provide the findings as vignettes. The vignettes describe illustrative events, and the related actors and situations, through which the process unfolded, and tensions surfaced. As short but detailed descriptions, the vignettes provide vivid, authentic, and evocative accounts of the events and seek to increase the truthfulness, plausibility, and credibility of the findings as measures of ethnographic reliability and validity (Golden-Biddle & Locke, 1993; Guba, 1981; Walsham & Sahay, 1999). We carefully selected the vignettes from different policy development periods, to progressively illustrate how the development of the policy occurred. The findings and data presented are consistent with the entire data corpus. The names of the company and participants, as well as key technical details, have been disguised to protect the confidentiality of the research site and its members.

Abductive innovations for the development of an information security policy at MachineryCorp

In this section, we report the findings for the three tensions and illustrate the process of abductive innovation in three vignettes. At MachineryCorp, the development of the InfoSec policy unfolded during five periods (see Table 2) over 15 months. The company aimed at widening the scope of InfoSec from IT security to organisational InfoSec, ensuring implementation of the policy across the global corporation and alignment with industry InfoSec best practices. The main challenge in developing the policy was how to ensure that the policy was aligned with the best practices and mindful of the infrastructure affordances, economic realities, and social arrangements of the corporation.

Reworking and working around infrastructure affordances

At MachineryCorp, policy-makers felt a tension between their current *infrastructure affordances* and the new infrastructure demands the best practices mandated. By infrastructure affordances, we mean the participants' construction of what could be possibly implemented with the installed IT base (Leonardi, 2011). Implementing what was mandated by the best practices was perceived to induce significant costs or was otherwise deemed unfeasible, but leaving best practices unimplemented could expose MachineryCorp's information assets to threats that could be alleviated if they were carefully attended to and resolved. Thus, the policy-makers were keen to find ways to work around the infrastructure inertia (Star & Ruhleder, 1996) through innovative InfoSec practices that would still use and reflect the best practices. We illustrate some of the infrastructure tensions and the resulting innovations in policy development in Table 3 and discuss them next.

Table 3. Innovation emanating from infrastructure affordances.

Phases of abductive innovation	**Illustrations of policy requirements' development**	
Deductive adoption	ISO/IEC 27001 best practice states: "Detection, prevention, and recovery controls to protect against	ISO/IEC 27001 (2005) best practice

	malicious code and appropriate user awareness procedures shall be implemented" (ISO/IEC, 2006, p. 43). InfoSec best practice concretised into three requirements in the policy draft: (1) installation of protection software; (2) installation of intrusion detection and prevention (IDS) capabilities; and (3) installation of security logging capabilities.	gives only generic guidance on device security. No particular consideration for mobile devices derived from best practices in the policy draft.
Inductive adjustment	Policy requirements adjusted due to the organisation's existing infrastructure: (1) no adjustment for the protection software as the infrastructure provided capabilities; (2) the requirement adjusted as the infrastructure did not provide capabilities for IDS; and (3) the requirement adjusted as IT systems did not include capabilities for security logging.	Requirements for mobile device security came to the fore during workshops due to the extensive use of mobile devices and best practice to control against malicious code.
Tension	Mismatch between best practices and infrastructure affordances.	
Synthetic innovation	Include required IDS capabilities and security monitoring in new service contracts. Contracts will shape the infrastructure. Revise policy to include requirements for mobile devices.	

Deductive adoption

In the second period of the policy development (Table 2), InfoSec professionals crafted the first policy drafts based on InfoSec best practices they adopted from ISO/IEC 27001 and ISO/IEC 27002 standards (the 2005 and 2013 versions). Many of the best practices pertained to MachineryCorp's IT infrastructure. The prescribed practices and processes included, for example, documentation and formal approval of operational processes, protection against malicious code, and systematic processes for detecting and controlling vulnerabilities. When adopting the best practices in the policy, the InfoSec professionals sought to concretise the best practices from abstract and general requirements to several specific requirements. For example, regarding controlling against malicious software that was described in the ISO 27001 standard as one requirement, the list of adopted requirements included not one but three requirements. These requirements detailed that formally approved malware protection software must be installed on all MachineryCorp's IS, IDS capabilities must be deployed,

and security logging capabilities must be established. When the CISO felt that all the required practices were included, she reviewed them with InfoSec consultants. They began with almost 60 requirements that all related to MachineryCorp's IT infrastructure but ended up with 52 requirements. The changes also included modifications to the proposed responsibility and accountability requirements to align them with the corporation and its processes. The adoption of requirements from InfoSec standards resulted in a selection of requirements similar to but not the same as the requirements in InfoSec best practices. What resulted was the InfoSec professionals' understanding of what was required to secure MachineryCorp's IT infrastructure.

Inductive adjustments

After the InfoSec professionals had made sense of and adopted best practices in the policy draft, the professionals arranged several workshops (periods 3 and 4) in which the policy draft was shown to organisational members. A senior InfoSec consultant explained this approach and the benefits of involving organisational members in policy crafting as follows:

> We will select the suitable practices from different [InfoSec] standards and then have them approved by, for example, head of risk management. Then we will arrange workshops to discuss the practices with different people. This way they can comment on them [the practices] and we can ensure that the practices are relevant for the company. …It's great and important that people participate from the very beginning, because it means that implementation [of the policy] also begins immediately. (Excerpt from field notes)

One of the workshops was about MachineryCorp's IT infrastructure, and participants included the CTO, COO (who was responsible for IT operations), and CISO (period 4). This workshop was very important for the development and implementation of the InfoSec policy as many of the InfoSec requirements were directly related to or had implications for the IT infrastructure and IT operations. The COO was in the position of deciding whether the requirements would be implemented. Therefore, the CISO had to find ways to obtain the COO's agreement with and approval of the requirements as

otherwise they would never be implemented. In contrast, the CTO—the policy project's sponsor—had already shown interest and now was seemingly excited. For him, the policy project, and this workshop, was a means of demonstrating that something "big" was happening to MachineryCorp's InfoSec. Demonstrating this to the COO was important for the CTO personally as the COO—known for his deep understanding of IT and InfoSec—had previously raised concerns about the state of InfoSec across the corporation, and that was now being taken care of. The CTO was so eager to assure positive results from the workshop that he had taken the COO to play a round of golf before the workshop to have an informal occasion to promote the project.

In the workshop, the CTO, COO, and CISO discussed how MachineryCorp's IT infrastructure had evolved over the years and had become more effective in supporting the corporation's business but had also become more complex, unpredictable, and difficult to govern. The infrastructure included an amalgam of in-house, customised, and purchased applications, a variety of IS, hundreds of servers running different operating systems, several data centres on different continents, and a growing number of mobile devices. The COO explained, and the CTO and the CISO repeated, that the heterogeneity of the infrastructure meant that all these components had different features that possibly included InfoSec vulnerabilities which might cause incidents that put MachineryCorp's information assets at risk. The three executives were particularly worried about the InfoSec state of the software developed in-house used in the IoT solutions. Much of the software had been developed for function and not for InfoSec. InfoSec was not part of the product development processes. In addition, the workshop participants expressed concerns about the growing number and diversity of mobile devices used. Mobile devices could be taken out of the office spaces whilst storing and processing sensitive information but still be left accidentally in public spaces or stolen, and the confidentiality of the information breached, or the information lost all together. Consequently, the CTO and the COO expected the CISO to incorporate these considerations in the policy, because the draft did not include specific requirements for mobile devices, and the requirements for software

vulnerabilities were vague at best. The lack of requirements for mobile security was due to the InfoSec professionals' initial understanding that mobile devices were not a major threat to MachineryCorp and due to the limited attention the ISO/IEC 27001 (2005) pays to mobile threats but was now complemented by the participants' expertise.

The workshop revealed that complying with some of the proposed requirements would require changes in the IT infrastructure. A requirement for controlling against malicious software stated the following: "Standardized and approved malware protection software shall be installed, configured and maintained on all [MachineryCorp's] information systems" (PowerPoint presentation). Without the technical capabilities provided by the security technology, detecting and protecting against malware would not be possible. Similarly, the requirement related to IDS (i.e., an activity that aims at finding hackers' attempts to break into an organisation's network or IS) prescribed that technical systems should be in place. Complying with this requirement meant MachineryCorp had to acquire technical tools as they were lacking in the current infrastructure. In addition, a requirement to monitor and report the InfoSec status of organisational IS implied changes in the technological and social fabric. Technical tools for automated monitoring of the status and aggregating of the findings of the monitoring, as well as a social arrangement to report the findings to the organisation's management and relevant stakeholders, were needed. In addition, IS properties that support such technology were required. The workshop participants seemed to be well aware of the constitutive role of IT in the defined requirements and discussed how the antivirus software, IDS, and monitoring needed could be accomplished to the extent stated in the policy. Only antivirus software was part of the current IT infrastructure.

Innovation

The workshop drew the InfoSec professionals' attention not only to the material implications the new InfoSec policy would have—to the changes required in the existing IT infrastructure—but also to the amendments required in the InfoSec policy draft. The workshop revealed contradictions between the

draft and the realities of MachineryCorp's IT infrastructure. The professionals faced a difficult choice: Should they try to change the infrastructure, or should they change the policy draft? Solving the problem required finding innovative ways that could be taken neither directly from the best practices, nor from local practices. Firstly, as the InfoSec professionals perceived that the InfoSec best practices provided only limited help regarding mobile devices, the professionals wrote new requirements specifically for these devices. The requirements were not part of the adopted best practices, and did not reflect the corporation's current practices; rather, the requirements emerged from local expertise. Secondly, the InfoSec professionals defined new risk management procedures for in-house applications. Although the best practices did not specifically address in-house software development, they included requirements for risk management that provided the foundation for a local solution. Thirdly, as new InfoSec technology was necessary to fulfil the requirements for IDS and security monitoring and reporting, the CISO proposed that the requirements for such technology should be included in the IT service contracts under negotiation at the time. By including these requirements in the contracts, MachineryCorp moved the responsibility for implementing the policy's requirements to the firm's service providers.

Framing the economics of the information security investment

Determining the return on investment for an InfoSec investment is a difficult task as "accurate inputs to an economic analysis are difficult to estimate because success in protecting information equals to 'nothing happened,' and thus the potential outcomes (benefits or loss) are often intangible" (Kwon & Johnson, 2014, p. 452). At MachineryCorp, the difficulty of determining the economic rationale for implementing certain best practices with a limited organisational budget gave rise to a tension and necessitated finding innovative ways to work around it. Focusing purely on best practices could induce monetary costs beyond what was organisationally feasible. Although MachineryCorp did not perform rational calculus for their InfoSec investments, they deemed certain best practices "too" expensive to fully implement and sought alternative ways of framing the best practice and its local

variant. Thus, the participants jointly constructed an *economic reality* within which certain investments became overly expensive and others affordable. The jointly constructed economic reality importantly shaped policy development as participants sought ways in which to implement the best practices within the constructed economic space. We exemplify this economic tension and its relation to policy development in Table 4 and discuss this tension next.

Table 4. Innovation arising from economic concerns.

Phases of abductive innovation	**Illustrations of policy requirements' development**
Deductive adoption	ISO/IEC 27001 prescribes five controls for business continuity management (BCM) (e.g., developing and implementing continuity plans for business processes; ISO/IEC, 2006). InfoSec best practice adopted as four requirements in the policy draft. Considering global implementation led "all processes" to be reduced to "important processes".
Inductive adjustment	Workshops revealed business units were accountable for BCM and responsible for funding it. BCM was perceived to be unrelated to InfoSec. Requests to remove BCM from the InfoSec policy due to economic considerations. Workshops revealed a general concern for implementation costs of the whole policy that required leaving more conditionality and openness for interpretation of the policy.
Tension	Imbalance between the expected benefits of implementing best practice against the assumed expenses of the required organisational investments.
Synthetic innovation	Narrow the policy requirements such that they relate only to InfoSec. Exclude most BCM requirements from the policy. Encourage risk-based approach and empower employees in policy implementation. Appoint a coordinator and a steering board for global implementation to ensure implementation oversight.

Deductive adoption

MachineryCorp's CISO was mindful of the corporation's economic reality when she made sense of and formed ideas about adopting requirements from best practices in the new InfoSec policy. She carefully considered whether it was realistic to expect the corporation to invest in implementing the

requirements. The global implementation in particular worried her. Therefore, she and a consultant, for example, modified the best practice of business continuity management (BCM) substantively from what the ISO/IEC 27001 standard prescribed. They lessened and lowered the requirements for BCM by removing the word "all" from all BCM requirements (e.g., the requirement "BCM should cover all processes" became "BCM should cover important processes" (excerpts from policy drafts)). They predicted that including "all processes" would only evoke objections and counterarguments across the organisation and thus, were better left out. Given the corporation's global presence and the number of processes, the CISO and the consultant expected "all processes" would introduce costs the company could not, or would not be willing to, bear.

Inductive adjustments

A workshop that included employees from different organisational functions (such as enterprise risk management, compliance, IT, and R&D) brought to the fore the considerations of the economic realities and boundaries within which the policy implementation unfolded. The head of risk management, compliance officer, head of R&D, CTO, and CISO started the workshop in a cheerful atmosphere. The participants clearly had anticipated the opportunity to comment on the policy draft. The CISO projected the policy draft on a screen, and the workshop participants reviewed the policy draft carefully from top to bottom, even word by word. Although the InfoSec professionals had already softened the BCM requirements from those prescribed by the best practices, the workshop participants saw that the BCM requirements had to be amended. The participants demanded that the BCM responsibilities be separated from the InfoSec policy because they perceived BCM as unrelated to InfoSec. At MachineryCorp, BCM and InfoSec were organisationally under different departments, and thus, this separation had to be reflected in the InfoSec policy. Participants argued that traditionally the business units were accountable for BCM and were responsible for funding it. Introducing BCM in the InfoSec policy could mean that the business units would start requesting directives and funding from the corporate functions. The workshop further brought to the fore that the CTO was very

concerned that the whole policy project might fail if the estimates of the implementation expenses presented to the executives were too high. Other participants expressed similar views. The higher the number and the more specific the new requirements, the higher the implementation costs. Consequently, the workshop participants faced a dilemma between what could be mandated in the policy and what could be achieved in practice. The participants requested more conditionality and openness for interpretations of the policy to allow for dissimilar implementation efforts in different countries.

Innovation

Creative solutions were required to find a balance between the expected alignment with best practices and the costs of implementing the policy. Given the framed economic realities that the workshops during periods 3 and 4 revealed, the policy draft had to be modified. At first, the InfoSec professionals were vexed about the demand to remove BCM from the policy. Fortunately, consultation of the latest version of ISO 27001 (2013) standard revealed that in contrast to the previous standard, the standard now included only InfoSec aspects of BCM as part of the standard's best practices (ISO/IEC, 2013). The InfoSec professionals felt that alignment could be maintained even if most of the BCM requirements were removed from the policy. Finding a balance between strict enough requirements that would assure sufficiently uniform implementation globally and the requests to make the practices in the policy more conditional and to leave room for interpretation was more difficult to achieve. The head of risk management proposed a solution to the challenging situation. He proposed that the CISO's responsibilities be broadened in the policy by appointing her as the coordinator of the global implementation. As a coordinator, she could detect early if countries or organisational units sought to circumvent the intent, the *geist*, of the policy and provide steering and guidance. Additional measures included describing in the policy the responsibilities of an InfoSec steering board and making the board responsible for overseeing and prioritising the implementation efforts, which was assumed to alleviate the risk of too loose an implementation. Furthermore, the CISO introduced more

conditionality in and room for interpretation in some of the requirements. In practice, she allowed a more risks-based approach to implementation that provided more freedom for the local units to consider their budget when they implemented the requirements. For example, one of the requirements for human resources security that in the adopted form stated "Information security awareness training must be provided during induction" (policy draft) was amended to "Information security awareness training must be provided during induction when relevant" (policy draft). Through these local innovations, the participants resolved the tension between the economic realities and best practices.

Converging with social and structural organisational arrangements

Although InfoSec best practices have a history (and reflect that history; see Backhouse et al., 2006), best practices, once abstracted, documented, and disseminated, are acontextual and ahistorical. Organisations, in turn, always reflect their history and the past choices through which the organisation's specific characteristics were borne out (Benson, 1977). This acontextuality of best practices and the local organisational context at MachineryCorp created a tension and gave rise to local innovation to converge the best practices and the local *social arrangements*. Implementing the best practices without the organisational considerations could lead to decoupling the InfoSec policies from the organisational reality or to InfoSec policies that employees cannot enact in their work. However, creating policies from current arrangements, for example, by documenting accountability structures, could omit the assignment of important InfoSec responsibilities and roles. We illustrate the social tensions and their relation to policy development in Table 5 and discuss them next.

Table 5. Innovations in social and structural arrangements.

Phases of abductive innovation	**Illustrations of policy requirements' development**

Deductive adoption	ISO/IEC 27001 best practice states that risk management forms the foundation of InfoSec. The scope of the best practice prescribed risk management narrowed to a reference to the organisation's enterprise risk management to avoid social conflict.	ISO/IEC 27001 prescribes the organisation of InfoSec (e.g., allocation of InfoSec responsibilities). Best practice contextualised as high-level roles and responsibilities of policy implementation and a general requirement to define the organisation for InfoSec.	ISO/IEC 27001 prescribes requirements for IS development and development processes. 17 practices for IS development derived from best practices. Practices referenced the organisation's project management methodology.
Inductive adjustment	Workshops confirmed the narrowing of the risk management scope without further adjustment.	Workshops revealed the need to include more InfoSec responsibilities in local units and requests to reduce the ambiguity considering responsibilities and the need for alignment with the organisation's practices.	Workshop revealed that incorporating InfoSec practices in the organisation's methodology was prohibited by a powerful actor.
Tension	Contrast between best practices and prevailing organisational arrangements.		
Synthetic innovation	Facilitate adoption of new roles and responsibilities by providing advice and appointing a coordinator for the implementation. Extract practices from the InfoSec policy and integrate them in existing processes. Include a general statement in the policy.		

Deductive adoption

Organisational and social arrangements shaped the deductive adoption of best practices in MachineryCorp's InfoSec policy. One requirement concerned information risk management. Although best practices required implementation of formal processes for managing information risk, the InfoSec professionals narrowed the scope of information risk management to a simple reference to MachineryCorp's enterprise risk management. By narrowing the scope from that prescribed in the standard (ISO/IEC 27001), they avoided treading on the toes of the head of risk management. Proposing a risk management methodology or defining how risk management should be

accomplished at MachineryCorp would have been beyond the InfoSec professionals' mandate. As a result, the adopted requirement about InfoSec risk management in the policy draft was written to state only that InfoSec risks should be managed as part of the organisation's enterprise risk management.

Inductive adjustments

The need for more profound adjustments due to social and organisational demands appeared during periods 3 and 4. The involvement of organisational functions in the development of the policy uncovered situated practices and social affairs not anticipated in the interpretation of the best practices. In one of the workshops with representatives from organisational functions (head of risk management, compliance officer, head of R&D, CTO), the CISO acted as a facilitator and as a secretary. She noted the issues that participants thought needed clarification, but also made changes to the wording of the requirements as requested by the participants. Lively discussion about the InfoSec roles and responsibilities proposed in the draft soon began; the main questions seemed to be whether the roles and responsibilities were stated clearly enough to avoid conflicting interpretations during implementation of the policy. The head of risk management and the compliance officer demanded more responsibilities for local units and countries and alignment of the InfoSec policy to the existing ways of working. For instance, instead of using the generic statement "documented system development methodologies," the two executives demanded the name of the corporation's formal project methodology be included in the policy. The head of risk management explained that local units and countries must be made accountable and committed to implementing the policy. He suspected struggles and rough negotiations would occur regarding the implementation. Participants were further concerned whether the policy would be understood unambiguously across the corporation, and to ensure uniform understanding, proposed adding words that were assumed to reflect language with which employees were more familiar.

The need for fundamental changes in the policy due to organisational practices was revealed by a workshop that delved into secure IS development and in which MachineryCorp's CFO and

CISO, and an InfoSec consultant participated. In addition to financial responsibilities, the CFO was responsible for corporate-wide and standardised project management methodology. InfoSec professionals had derived 17 practices for IS development when they adopted requirements from best practices. The professionals' plan was to refer to the project management methodology in the requirements and integrate the practices in the methodology. In their view, this would ensure implementation of the InfoSec policy regarding all IS development. For the InfoSec professionals, this was significant as the software developed in-house was considered a weak point of MachineryCorp's InfoSec. The CFO was about 15 minutes late when he suddenly appeared at the workshop. Without even sitting down and before the CISO had a chance to say anything, the CFO urgently stated that he clearly understood that "this information security is very important topic, and of course, it must be included in the methodology" (excerpt from field notes). However, he then urged the participants to emphasise that the new project methodology must be light, and as lean as possible, and thus, anything excessive could not be included. The CISO and the consultant merely nodded as the CFO talked as if he was on fire. Suddenly, he ended as abruptly as he had started by saying:

> I think this information security can have at most two checkpoints in the project methodology. One at the beginning and one at the end. Nothing more. I clearly see that this is important, but two is enough. (Excerpt from field notes)

He then turned to the CISO as if he were asking, "It is enough, right?" This seemed more a rhetorical gesture than encouragement to look for other solutions. The CISO felt she had no choice but to quickly agree that InfoSec could be integrated in the methodology's existing checkpoints. The CFO then abruptly announced he had to leave, and left the CISO and the consultant bedazzled.

Innovation

The social and organisational issues of the policy draft were revealed by the organisational members' involvement in crafting the policy. Without such involvement and without surfacing of the issues, the policy would never have been approved or implemented. The contradictions between the InfoSec

professionals' best practices–based approach to policy development and the situated practices had to be resolved. The InfoSec professionals had to manage the tension between the defined roles and the organisational members' expectations for more strictly defined responsibilities. For the workshop participants, stating "InfoSec must be organised" as suggested by ISO/IEC 27001 was not strong enough. This statement was seen to "leave loopholes in the policy," as the CTO put it, and would enable MachineryCorp's local units to ignore the policy. Participants wanted to introduce more responsibilities and accountability for local units but were afraid that the units would oppose the responsibilities. The CISO's previous appointment as the coordinator for global implementation was seen as a solution for overseeing the implementation. This shows how the abstract requirement of the best practice "InfoSec must be organised" was contextualised mindful of the situated realities.

Addressing the CFO's intervention was a great challenge for the InfoSec professionals. They had documented 17 practices for IS development in the policy draft but now faced a situation in which their plans had unexpectedly vanished. However, they understood that to get the new InfoSec policy approved it was imperative to follow the CFO's recommendation. They agreed that they could not just remove all the InfoSec requirements as this would have significant consequences for the InfoSec of product development. The CISO and the InfoSec consultant pondered what to do. Finally, they decided to move the requirements from the InfoSec policy as part of the project methodology's existing checkpoints. Thus, they could incorporate the requirements as part of the development process, honour the CFO's request not to introduce additional checkpoints, and improve MachineryCorp's InfoSec. The CISO and the consultant were satisfied with the result as they did not have to seek approval for those requirements as part of the InfoSec policy, and they thought it offered a better chance for the requirements to become implemented throughout the organisation. In the InfoSec policy, they wrote only a general statement that stated IS development must be conducted through a documented methodology and that the methodology must include requirements for InfoSec

measures. This illustrates the creativity required from InfoSec professionals to find a balance between InfoSec best practices and local demands.

Discussion

This study was motivated by a dilemma we identified in the extant literature on the development of InfoSec policies. The tendency in the literature to depict the process for developing an InfoSec policy as a top-down or bottom-up approach has left managers with, at least partly, conflicting arguments. We tried to narrow the chasm by examining how an innovative corporation dealt with this dilemma in practice when they revised their InfoSec policy.

Through the application of the lens of the dialectical theory of organisations (Benson, 1977, 2013), the findings suggest the development of the InfoSec policy unfolded through recurrent processes of *abductive innovation* (Figure 1). In abductive innovation, policy-makers set out to make sense of InfoSec best practices to construct interpretations of what ought to be done in terms of security (deductive adoption). When these tentative ideas are discussed within an organisation, considerations of local contingencies emerge as policy-makers construct possibilities for local implementation (inductive adjustment). The contradictions between the best practice imperatives of what should be done (Siponen, 2005b) and the possibilities for a local implementation give rise to tensions in an effort to align the policy with the totality of the goals and the organisational arrangements that constitute the organisation (Benson, 1977; Hargrave & Van de Ven, 2017). The policy remains under negotiation as provisional statements until an innovative local resolution is discovered that creatively reconciles the contradictory elements between best practices and local contingencies (synthetic innovation). Only then does the open-ended becoming (Benson, 1977) of the policy development stabilise, and the innovation materialises as a (new) part of the InfoSec policy. In other words, the contradictory elements of what ought to be done (in terms of best practices) and what can be (locally) implemented engender tensions that function as facilitative and limiting conditions for the creativity involved in synthetic innovations to occur that are necessary for the local

appropriation of best practices (Baskerville & Pries-Heje, 2014) and thus, for effective policy development.

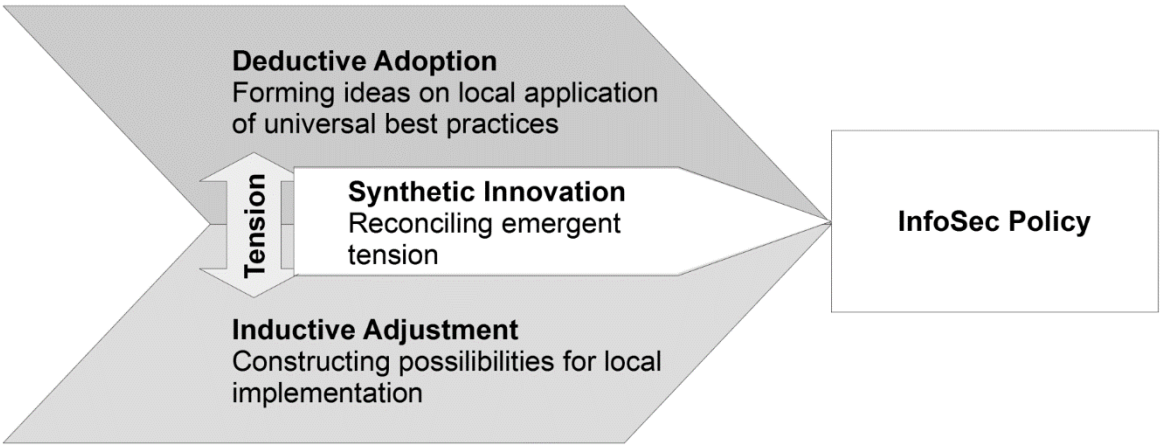

Figure 1**.** Phases of abductive innovation in the development of the InfoSec policy.

Next, we elaborate the theoretical and research implications of abductive innovation for the development of an InfoSec policy and provide critical reflections. Last, we present practical implications as seven provisional maxims for the development of InfoSec policies that aim to support organisations in their effort to take emancipatory approaches to this process.

Implications of abductive innovation for information security policies

As documented in literature, top-down development may lead to policies that are impractical in practice and in which the "users' knowledge, relevant for securing systems, is not exploited properly" (Siponen, 2005a, p. 313). A bottom-up approach may lead to policies that become disconnected from and omit the expert knowledge documented in InfoSec best practices. In contrast, abductive innovation suggests that policy development likely involves phases that resemble top-down and bottom-up approaches—which we refer to as deductive adoption and inductive adjustments, respectively—but requires a creative leap to come up with a local innovation that seeks to sustain the connection to good InfoSec practices whilst meeting the local contextual requirements and utilising local expertise. Thus, we contribute to the development of the "fifth generation" of InfoSec methods that should incorporate user participation and empirical development along with practice (Siponen,

2005a). Further, our conceptualisation of the process for developing InfoSec policies contributes to providing a sought-for alternative to strict top-down InfoSec management (Kirlappos et al., 2013).

The present findings are in line with those of Hsu et al. (2012), who emphasised the innovative nature of InfoSec management. Their study provides important insights into the popularity of and the reasons companies build on "administrative innovations," that is, why they adopt international InfoSec management standards.,We extend this insight by showing *how* MachineryCorp transformed the international standard into local InfoSec practices. Further, in line with Njenga and Brown (2012), who stress the improvised nature of InfoSec management, the present study provides further evidence that the development of InfoSec policies includes a moment of creativity. Improvisation is characterised by strict time constraints and a pressing need to solve the issue at hand quickly (Ciborra, 1999). Innovation is less time critical, collective, and evolutionary and to which it is possible to return during a later phase and rethink, and to tinker. Nevertheless, the present findings support the broad idea present in Hsu et al.'s (2012) and Njenga and Brown's (2012) work that managing InfoSec demands local innovations—adapting ideas and developing practices that are new and novel to a particular community or group (Hsu et al., 2012)—which implies that InfoSec management cannot be based solely on externally stipulated requirements.

Tensions as facilitators for local innovations

The present findings indicate that the process for developing InfoSec policies is driven by various dialectical tensions that give the process a forward momentum and a thrust (Carlo, Lyytinen, & Boland, 2012; van de Ven & Poole, 1995). This dialectical relationship between the general (best practice) and the particular (local context) proceeds towards synthesis through local innovations. Thus, "[i]f we think of a developmental process as a dialectical development, it means it does not go forward in straight line, but moves more in a spiral, perhaps coming back to the same point but at a different level" (Benton & Craib, 2001, p. 108). Progress does not proceed along a predictive trajectory as development *towards* some certainty but instead as development *from* somewhere. That

is, whilst the development process at MachineryCorp proceeded towards a goal of crafting an "InfoSec policy," the end maintained a constant openness and unpredictability regarding what the documented practices would be like and what shape they would take in practice due to the inherent and ever-present conflict that characterises organising (Benson, 1977). What this implies is that although InfoSec best practices are universal, their local appropriation is always idiographic due to the highly idiographic and contextual nature of local practices. Through the synthetic innovation, the ahistorical best practices become situated in the historical flow of the previous choices that make up an organisation. That is, "at each stage arguments are different from but related to the ones that went before" (Benton & Craib, 2001, p. 108). The development of InfoSec policies is not an isolated task separate from the rest of the organisation but is inherent in the flow of the totality of the practices, structures, procedures, and technologies that constitute organising (Benson, 1977).

The analysis suggested a triangle of tensions were particularly strong and gave rise to synthetic innovations at MachineryCorp: economic realities, infrastructure affordances, and social arrangements. Likely, these tensions occur and are salient in other cases. Firstly, the economic realities reflect the tension that arises from jointly constructed economic constraints and from the estimated expenditures of implementing best practices locally. As best practices are often universal (Siponen & Willison, 2009), they tend to lead to the problem of "one size does not fit all" (Botha & von Solms, 2004). Although one solution would be to come up with frameworks that are sensitive to organisational characteristics (such as staff size and the field of business), we suggest another option is to promote local organisational innovativeness. As the present findings show, innovations emerged as MachineryCorp faced several difficulties in implementing certain best practices with a certain budget. Thus, best practices are useful as "tools for thinking" to the extent the practices facilitate and support organisations' ability to innovate local InfoSec practices.

Secondly, the infrastructure affordances tension relates to the mismatch between the perceived local IT infrastructure capabilities and the assumed implications of implementing best practices. Such

tensions arising from the "relationship between the material and the social result in often unpredictable security outcomes" (Coles-Kemp, 2009, p. 182). Occasionally, then, it is possible that the development of InfoSec policies is not merely a matter of changing employees' intentions to comply with the set policy (Herath & Rao, 2009; Johnston & Warkentin, 2010), but requires a change in practices that are tightly anchored to and restricted by the organisation's material fabric (Orlikowski, 2010; Zammuto, Griffith, Majchrak, Dougherty, & Faraj, 2008). By focusing on enforcement of rule following, important material aspects shaping user behaviour and possibilities of rule following may become omitted or ignored and seen as "user ignorance or misconduct" (Hedström et al., 2011, p. 381). However, this does not imply that such tensions always necessitate innovations that change the organisational material fabric. Instead, as we observed at MachineryCorp, innovation may take a different form from the tension. However, the tension is not merely negative. Although an infrastructure's history limits the possible future development trajectories (Hanseth & Lyytinen, 2010; Venters, Oborn, & Barrett, 2014), shifting organisational goals (e.g., demands to improve organisational InfoSec) engender tension which may create conditions that drive organisations to innovative local resolutions.

Thirdly, the social arrangements tension arises from the social accountability reflected in the organisational structure and the generality and acontextuality of the best practices (Almklov & Antonsen, 2014). The tension encouraged MachineryCorp to address it through local innovation in a way that is mindful of the social change implied by the best practices and the stability of the organisational social arrangements (i.e., the organisational "status quo"). By focusing on *what* rather than on *how* (Siponen & Willison, 2009), best practices leave room for contextual appropriation that is a necessary feature of broad applicability, but also leave room for local negotiation. Although solving the tension necessitates social change, it may, naturally, have economic and material consequences (for instance, increasing someone's area of responsibilities may also require salary increases). Failure to effectuate local social change will likely engender non-compliance by

decoupling documented organisational practices from social practices. For instance, documenting new responsibilities as part of the InfoSec policy is straightforward, but without actual change effectuated in organisational responsibilities, the implementation will fall short. When policies fail to effectuate changes, the policies may easily fade into the background and become overshadowed by the more immediate concern of finding ways in which policy compliance can be enforced (Pahnila, Karjalainen, & Siponen, 2013). However, as indicated by the economic and material tensions we observed at MachineryCorp, what is easily perceived as employee resistance and reluctance to follow policies may actually have more complex origins that cannot be anticipated from the psychological antecedents of compliant behaviour alone. Similarly, solving social tensions, such as those caused by value conflicts between best practices and work practice, through bottom-up management (Hedström et al., 2011) may lead to suboptimal InfoSec practices as alignment between employees' values and security practices does not guarantee those values result in good InfoSec practices. Thus, best practices may become overshadowed by local social considerations and consensus practices. As the present findings suggest, the development of InfoSec policies cannot be a purely consensus practice but rather an *informed* consensus practice that reconciles the general knowledge of best practices with particular knowledge, and vice versa. Despite the many shortcomings (Backhouse et al., 2006; Siponen, 2005a, 2006; Siponen & Willison, 2009), we see great risk to organisational InfoSec management if the codified expert knowledge the best practices contain (Baskerville & Pries-Heje, 2014) becomes lost.

The innovative local appropriations that took place at MachineryCorp in response to the dialectical tensions may explain more broadly some of the variation in and the diversity of InfoSec implementations across organisations (and sectors)—widely acknowledged by practitioners and scholars (Butler & Gray, 2006)—despite the popularity of the best practices (Hsu et al., 2012). Thus, although best practices seek to homogenise organisational InfoSec practices, these practices are unlikely to engender *identical* practices across organisations due to the contextual specificity involved

in the process of the practices' local appropriation. Nevertheless, local appropriation has to preserve some form of recognisable connection to best practices; otherwise, for instance, InfoSec auditing and accreditation would turn out to be impossible. Thus, we speculate that in lieu of being identical, a "family resemblance" (Monteiro, Jarulaitis, & Hepsø, 2012) might exist between InfoSec practices across organisations that build on the same set of best practices. The present findings also suggest that organisations may need to balance between fidelity to best practices with innovativeness in their InfoSec policies—how to adopt and innovate a best practice in its local form but sustain the intended connection to the best practice. Although implementations that leap too far from the prescriptions of best practices may create unintentional holes in InfoSec practices, a direct "'cut and paste' effort that does not truly reflect the culture of the organisation...does not result in an effective direction-giving document for information security within the organisation" (Höne & Eloff, 2002, p. 403).

Towards ethical and democratic information security management practices

More broadly, we argue that engaging employees actively in the process for developing InfoSec policies will not only lead to policies that are more likely to be enacted by the employees, but also increase their awareness of those policies (Siponen, 2000). As we observed at MachineryCorp, through the development process, the employees became more knowledgeable about the organisational InfoSec policies (James, 1995). The policy development process at MachineryCorp indicates that approaching policy development as abductive innovation makes it easier for employees to understand the rationale for their compliance. The employees can also understand the origins of the InfoSec policies as the employees have helped craft policies which we expect to lead to greater degrees of compliance (Hedström et al., 2011; James, 1995; Spears & Barki, 2010). Ideally then, awareness and compliance are not wholly separate and consecutive tasks, but a matter of ways in which innovative local practices can be developed in conjunction and in cooperation with employees so that they can and will enact and incorporate the resulting policies in their respective work tasks.

Researchers have recently indicated that empowering employees by giving them the opportunity to override defined access rules may increase policy compliance (Jeon et al., 2018). Although such empowerment is a step towards more inclusive InfoSec management, we argue more attention should be devoted in research and practice to where the policies originate and how they are formed. By engaging employees in workshops, meetings, and other focus group–like settings, InfoSec policies should reflect not only management values (Stahl, Doherty, & Shaw, 2012), or create conflicting perceptions (Albrechtsen, 2007; Niemimaa et al., 2013), but also a consensual and shared view. This may not only benefit organisational InfoSec, but also move organisations towards more ethical InfoSec management. Much of the literature on InfoSec policies focuses on imposing pseudo-natural constraints (i.e., rules of acceptable behaviour) on employees which is always counter-emancipatory (Brooke, 2002; Hirschheim, Klein, & Lyytinen, 1995; Klein & Hirschheim, 1993). Thus, how the InfoSec policies come into being is—or at least should be—an ethical concern.

When the development of InfoSec policies is approached as abductive innovation, management and employees must interact and come up with a common view, which encourages the use of emancipatory development methods (Stahl, Tremblay, & Lerouge, 2011) rather than top-down enforcement. Such management approaches founded on a dialectical view of the organisation advance "a praxis of liberation or emancipation of people from systems of domination" (Benson, 2013, p. 4) that provides opportunities for IS research to fulfil its potential to "contribute to the process of reconstruction, to the liberation of human potential through the production of new social formations" (Benson, 1977, p. 6). What may result is "a qualitatively different form of management: one that is more democratically accountable to those whose lives are affected in so many ways by management decisions" (Alvesson & Willmott, 1996, p. 40).

Managerial implications

We derive seven practical InfoSec maxims (rules of conduct) from the findings that are intended to be general guidelines for managers to guide them in developing InfoSec policies (Table 6). These

maxims reflect our theorising, analysis, and learning gained through the in-depth ethnographic field work as participant observers proficient in InfoSec management. More specifically, reflecting Benson's (1977) *praxis* (i.e., the interplay between practical interests and scholarship), the maxims aim to support managers in crafting InfoSec policies whilst empowering employees to participate in the process. Given that these maxims were derived from a large company, it is likely that they are more suitable to similar contexts that have more resources to invest in policy development than to smaller companies or governmental organisations.

Although IS scholars have criticised industry best practices for lacking empirical foundations and traceability (Ma et al., 2005; Siponen, 2005a, 2006; Siponen & Willison, 2009), scholars have yet to provide alternatives that would meet their own criteria; conceptual papers on the topic abound in the literature (Cram et al., 2017; Siponen & Willison, 2007). The maxims address these concerns and are an addendum to the existing body of InfoSec best practices. The maxims are provisional in the sense that they are likely to change and be refined as empirical work in the area progresses. Nevertheless, we are confident that others can use the maxims in their organisations to surface tensions and innovate local solutions that may result in not only better InfoSec policies but also policies that are more just and fair to those whose work they affect in so many ways. When the maxims fail to do so, the authors should lay out their criticism of why and where the maxims did not provide the expected outcome. Thus, we contribute to building a cumulative tradition for developing best practices (Siponen, 2006; Siponen & Willison, 2009).

Table 6. Seven information security policy development maxims.

1. Make use of the technical expert knowledge contained in InfoSec best practices but be mindful that their adoption requires local innovation. There are likely to be several tensions between the best practice requirements and the local context—such as budgetary constraints, infrastructure limitations, and restrictive social structures—that require innovative solutions.
2. Recognise that employees' expert knowledge in information systems and local ways of working is as important for developing InfoSec policies as InfoSec best practices. Knowing general InfoSec best practices can never substitute for knowing minute and particular organisational practices—only supplement them. Employees are not only sources of potential

misconduct, but also contributors with often good intentions. However, be mindful that malicious employees exist.
3. Accept that a degree of misalignment is likely to exist between an InfoSec best practice and its local implementation. Innovative local practices are never identical to best practices; they always require going from "what" to "how" that is never simply adoption but requires a degree of innovativeness.
4. Seek informed consensus amongst InfoSec, business, and organisational practices. In contrast to popular thought, even in InfoSec, there is room for consensual practices. Be innovative and seek consensus within the plasticity of best practices. It is also an ethical choice to engage employees in deciding upon matters concerning their work conditions and behaviour rather than imposing rules upon them.
5. Recognise that InfoSec policy awareness and compliance begin at policy development—not at policy implementation. Although it is generally accepted in practitioner and scholarly frameworks that awareness and compliance are separate parts of an InfoSec management program, they start during the policy development phase.
6. Do not only seek to change employees' behaviour by enforcing the InfoSec policy, but also be willing to change the policy. Consider and be sensitive to alternative explanations for non-compliance other than employee resistance or reluctance to follow rules.
7. Be mindful that the development of an InfoSec policy is not only a managerial and strategic task but also an operational and tactical task. Despite the common emphasis on managerial processes and management frameworks (such as the ISO/IEC 27001), the effectiveness of InfoSec is dependent on what takes place in practice. Thus, it is as important to be aware of what takes place at the organisational "grassroots" as it is to be strategic.

Conclusions

Through ethnographic research, we studied the process for developing InfoSec policies in the context of a large, multinational, innovative engineering company, MachineryCorp. The main contribution of this research is the conceptualisation of the process for developing InfoSec policies as abductive innovation that involves phases of deductive adoption, inductive adjustment, and synthetic innovation. We found a triangle of tensions related to the infrastructure affordances, economic realities, and social arrangements driving the process at MachineryCorp that originated neither from the InfoSec best practices guiding the development, nor from the organisational context, but from their interaction. Solving these tensions pushed the organisation to seek innovative ways to come up with local InfoSec practices. Thus, the development surfaced as a consensus-seeking practice, which surprised us somewhat. However, InfoSec best practices were an essential part of the consensus

seeking, in that the consensus was informed and governed by the flexibility afforded by the best practices. From this end, the InfoSec management surfaces in a different light from what seems to be the general perception: InfoSec practices are much more dependent on the organisation's collective ability to innovatively appropriate and come up with local InfoSec practices than on management's ability to enforce predefined policies. Employees seemed to express a readiness and willingness to enact in their work the policies they had helped form. Nevertheless, readers should bear in mind that the study represents one ethnographic study at a specific organisation which encourages further studies on the topic to uncover the broadness and applicability of these findings across contexts. Hopefully, with time "it might be possible to develop more general models of the meaningful contexts of various aspects of business organizations" (Myers, 2009, p. 99).

When organisations approach the development process as abductive innovation, they empower their employees and emancipate them from the role of mindless rule-following that previous research and practice have largely designated for them, and instead, encourage employees to participate in defining the rules and work conditions under which they have to work. This process simultaneously drives the employees towards secure practices.

References

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289.

Almklov, P. G., & Antonsen, S. (2014). Making work invisible: New public management and operational work in critical infrastructure sectors. *Public Administration, 92*(2), 477–492.

Alvesson, M., & Willmott, H. (1996). *Making sense of management: A critical introduction.* London, England: Sage.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.

Av-Test Institute. (2017). *The Av-Test security report 2016/2017*.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, 30(Special Issue), 413–438.

Baskerville, R., & Pries-Heje, J. (2014). Diffusing best practices: A design science study using the theory of planned behavior. In B. Bergvall-Kåreborn & P. Nielsen (Eds.), *Creating value for all through IT* (pp. 35–48). Berlin, Germany: Springer.

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

Benson, J. K. (1977). Organizations: A dialectical view. *Administrative Science Quarterly, 22*(1), 1–21.

Benson, J. K. (2013). Dialectical theory of organizations. In E. H. Kessler (Ed.), *Encyclopedia of management theory* (pp. 190–193). London, England: Sage.

Benton, T., & Craib, I. (2001). *Philosophy of social science: The philosophical foundations of social thought.* Hampshire, England: Palgrave.

Botha, J., & Von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security, 12*(4), 328–337.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R.W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*, 151–164.

Brooke, C. (2002). What does it mean to be "critical" in IS research? *Journal of Information Technology, 17*(2), 49–57.

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly, 30*(2), 211–224.

Carlo, J. L., Lyytinen, K., & Boland, R. J., Jr. (2012). Dialectics of collective minding: Contradictory appropriations of information technology in a high-risk project. *MIS Quarterly, 36*(4), 1081–A3.

Cho, S., Mathiassen, L., & Robey, D. (2006). The dialectics of resilience: a multilevel analysis of a telehealth innovation. In B. Donnellan, T. J. Larsen, L. Levine, & J. I. Degross (Eds.), *The Transfer and Diffusion of Information Technology for Organizational Resilience - IFIP TC8 WG 8.6 International Working Conference* (pp. 339–357). Galway, Ireland: Springer Link.

Ciborra, C. U. (1999). Notes on improvisation and time in organizations. *Accounting, Management and Information Technologies, 9*(2), 77–94.

Ciborra, C. U., & Hanseth, O. (1999). Introduction: From control to drift. In C. Ciborra, K. Braa, A. Cordella, V. Hepsø, B. Dahlbom, A. Failla, & O. Hanseth (Eds.), *From Cnotrol to Drift: The Dynamics of Corporate Information Infrastructures* (pp. 1–11). New Yor, USA: Oxford University Press.

Constantinides, P., & Barrett, M. (2014). Information infrastructure development and governance as collective action. *Information Systems Research, 26*(1), 40–56.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report, 14*(4), 181–185.

Corbitt, B. (2010). Developing intraorganizational electronic commerce strategy: An ethnographic study. *Journal of Information Technology, 15*(2), 119–130.

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems, 26*(6), 605–641.

Crespi, V., Galstyan, A., & Lerman, K. (2008). Top-down vs bottom-up methodologies in multi-agent system design. *Auton Robot, 24*, 303–313.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127–153.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449–457.

Duclos, V. (2016). The map and the territory: An ethnographic study of the low utilization of a global eHealth network. *Journal of Information Technology, 31*(4), 334–346.

Dunne, D. D., & Dougherty, D. (2016). Abductive reasoning: How innovators navigate in the labyrinth of complex product innovation. *Organization Studies, 37*(3), 131–159.

EY. (2018). *Cybersecurity regained: Preparing to face cyber attacks – 20th Global Information Security Survey 2017-2018*.

Farjoun, M. (2016). Contradictions, dialectics, and paradoxes. In A. Langley, & H. Tsoukas (Eds.), *The SAGE Handbook of Process Organization Studies* (pp. 87–105). Thousand Oaks, California, USA: SAGE.

Feldman, M. S., & Orlikowski, W. J. (2011). Theorizing practice and practicing theory. *Organization Science, 22*(5), 1240–1253.

Geertz, C. (1973). *The interpretation of cultures*. New York, NY: Basic Books.

Golden-Biddle, K., & Locke, K. (1993). Appealing work: An investigation of how ethnographic texts convince. *Organization Science, 4*(4), 595–616.

Guba, E. (1981). Criteria for assessing the trustworthiness of naturalistic inquiries. *Educational Technology Research and Development, 29*(2), 75–91.

Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: The case of building internet. *Journal of Information Technology, 25*(1), 1–19.

Hargrave, T. J., & Van De Ven, A. H. (2006). A collective action model of institutional innovation. *Academy of Management Review, 31*(4), 864–888.

Hargrave, T. J., & Van De Ven, A. H. (2017). Integrating dialectical and paradox perspectives on managing contradictions in organizations. *Organization Studies, 3*(4-4), 319–339.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems, 20*(4), 373–384.

Hellström, T. (2004). Innovation as social action. *Organization, 11,* 631–649.

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

Hirschheim, R., Klein, H., & Lyytinen, K. (1995). *Information systems development and data modeling: Conceptual and philosophical foundations.* Cambridge, England: Press Syndicate of the University of Cambridge.

Höne, K., & Eloff, J. H. P. (2002). Information security policy - What do international information security standards say? *Computers & Security, 21*(5), 402–409.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security innovations. *Information Systems Research, 23*(3-Part-2), 918–939.

Ingold, T. (2014). That's enough about ethnography! *HAU: Journal of Ethnographic Theory, 4*(1), 383–395.

International Organization for Standardization/International Electrotechnical Commission. (2005). ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements. Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization/International Electrotechnical Commission. (2006). ISO/IEC 27001:fi Information technology - Security techniques - Information security management systems – Requirements. Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization/International Electrotechnical Commission. (2013). ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements. Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization/International Electrotechnical Commission. (2014). ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Geneva, Switzerland: International Organization for Standardization.

James, H. L. (1996). Managing information systems security: A soft approach. *Proceedings of Information Systems Conference of New Zealand* (pp. 10–20). IEEE Society Press.

Jarzabkowski, P., Bednarek, R., & Lê, J. K. (2014). Producing persuasive findings: Demystifying ethnographic textwork in strategy and organization research. *Strategic Organization, 12*(4), 274–287.

Jeon, S., Hovav, A., Han, J., & Alter, S. (2018). Rethinking the prevailing security paradigm: Can use empowerment with traceability reduce the rate of security policy circumvention?. *DATA BASE for Advances in Information Systems, 49*(3), 54–77.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–A4.

Kaplan, S., & Orlikowski, W. J. (2013). Temporal work in strategy making. *Organization Science, 24*(4), 965–995.

Kappelman, L., Mclean, E., Johnson, V., & Torres, R. (2016). The 2015 SIM IT issues and trends study. *MIS Executive, 15*(1), 55–83.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security, 24*(3), 246–260.

Kirlappos, I., Beautement, A., & Sasse, M. A. (2013). “Comply or die” is dead: Long live security-aware principal agents. In A. A. Adams, M. Brenner, & Smith, M. (Eds.), *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013* (pp. 70–82). Okinawa, Japan: Springer.

Klein, H. K., & Hirschheim, R. (1993). The application of neohumanist principles in information systems development. In D. E. Avison, J. E. Kendall, & J. I. DeGross (Eds.), *Human, organizational, and social dimensions of information systems development: Proceedings of the IFIP WG 8.2 Working Group, Information Systems Development—Human, Social, and Organizational Aspects* (pp. 263–280). North Holland, the Netherlands: Noordwijkerhout.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*(1), 67–93.

Knapp, K. J., Morris, R. F. J., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security, 28*(7), 493–508.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security noncompliance: Devising a value-based compliance analysis method. *Journal of Strategic Information Systems, 26*(1), 39–57.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451–471.

Laaksonen, A., Niemimaa, M., & Harnesk, D. (2013). Influences of frame incongruence on information security policy outcomes: An intepretive case study. *International Journal of Social and Organizational Dynamics in IT, 3*(3), 33–50.

Langley, A. (1999). Strategies for theorizing from process data. *The Academy of Management Review, 24*(4), 691–710.

Lapke, M., & Dhillon, G. (2008). Power relationships in information systems security policy formulation and implementation. *Proceedings of the European Conference on Information Systems.*

Leonardi, P. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly, 35*(1), 147–167.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Beverly Hills, CA: Sage.

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273.

Lyytinen, K. (2009). Data matters in IS theory building. *Journal of the Association for Information Systems, 10*(10), 715–720.

Lyytinen, K., Yoo, Y., & Boland, R. J. (2016). Digital product innovation within four classes of innovation networks. *Information Systems Journal, 26*(1), 47–75.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251–270.

Monteiro, E., Jarulaitis, G., & Hepsø, V. (2012). The family resemblance of technologically mediated work practices. *Information and Organization, 22*(3), 169–187.

Myers, M. (1999). Investigating information systems with ethnographic research. *Communications of the Association for Information Systems, 2*(23), 1–20.

Myers, M. (2009). *Qualitative research in business & management*. London, England: Sage.

Nasution, F. M., & Dhillon, G. (2012). Shaping of security policy in an Indonesian bank: Interpreting institutionalization and structuration. *Proceedings of the European Conference on Information Systems.*

Niemimaa, M., Laaksonen, E., & Harnesk, D. (2013). Interpreting information security policy outcomes: A frames of reference perspective. *Proceedings of the 46th Hawaii International Conference on System Sciences* (pp. 4541–4550).

Niemimaa, M., & Laaksonen, A. E. (2015). Enacting information security policies in practice: Three modes of policy compliance. In F.-X. de Vaujany, N. Mitev, G. F. Lanzara & A. Mukherjee (Eds.), *Materiality, rules and regulation: New trends in management and organization studies* (pp. 223–249). Hampshire, UK: Palgrave Macmillan.

Niemimaa, A. E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems, 26*(1), 1–20.

Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems, 21*(6), 592–607.

Orlikowski, W. J. (2010). The sociomateriality of organisational life: Considering technology in management research. *Cambridge Journal of Economics, 34*(1), 125–141.

Orr, J. E. (1996). *Talking about machines: An ethnography of a modern job*. Cornell, NY: ILR Press/Cornell University Press.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information security behavior: Towards multi-stage models. *Proceedings of the Pacific Asia Conference on Information*.

Ponemon Institute. (2017). *2017 cost of data breach study: Global overview*.

PwC. (2015). *2015 information security breaches survey*.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121–139.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM, 46*(7), 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), 469–487.

Safa, N. S., Von Solms, R., & Furnella, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70–82.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60–66.

Sarker, S., & Sahay, S. (2004). Implications of space and time for distributed work: An interpretive study of US–Norwegian systems development teams. *European Journal of Information Systems, 13*, 3–20.

Schultze, U. (2000). A confessional account of an ethnography about knowledge work. *MIS Quarterly, 24*(1), 3–41.

Schultze, U. (2017). Ethnography in information systems research. In R. D. Galliers, & M.-K. Stein (Eds.), *The Routledge Companion to Management Information Systems* (pp. 103–120). London: Routledge.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.

Siponen, M. (2005a). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems, 14*(3), 303–315.

Siponen, M. (2005b). Analysis of modern IS security development approaches: Towards the next generation of social and adaptable ISS methods. *Information and Organization, 15*(4), 339–375.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM, 49*(8), 97–100.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445–472.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

Smets, M., Morris, T., & Greenwood, R. (2012). From practice to field: A multilevel model of practice-driven institutional change. *Academy of Management Journal, 55*(4), 877–904.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly, 34*(3), 463–486.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–A5.

Staat, W. (1993). On abduction, deduction, induction and the categories. *Transactions of the Charles S. Peirce Society, 29*(2), 225–237.

Stahl, B., Doherty, N., & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal, 22*(1), 77–94.

Stahl, B. C., Tremblay, M. C., & Lerouge, C. M. (2011). Focus groups and critical social IS research: How the choice of method can promote emancipation of respondents and researchers. *European Journal of Information Systems, 20*(4), 378–394.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111–134.

Straub, D. W., Goodman, S., & Baskerville, R. L. (2008). Framing the information security process in modern society. In D. W. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information security: Policy, processes and practices* (pp. 5–12). Armonk, NY: Sharpe.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

Svahn, F., Henfridsson, O., & Yoo, Y. (2009). A threesome dance of agency: Mangling the sociomateriality of technological regimes in digital innovation. *Proceedings of International Conference on Information System.*

Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online.*

Utesheva, A., Simpson, J. R., & Cecez-Kecmanovic, D. (2016). Identity metamorphoses in digital disruption: A relational theory of identity. *European Journal of Information Systems, 25,* 344–363.

Van De Ven, A. H., & Poole, M. S. (1995). Explaining development and change in organizations. *The Academy of Management Review, 20*(3), 510–540.

Van Maanen, J. (2011a). Ethnography as work: Some rules of engagement. *Journal of Management Studies, 48,* 218–234.

Van Maanen, J. (2011b). *Tales of the field: On writing ethnography*. Chicago, IL: University of Chicago Press.

Venters, W., Oborn, E., & Barrett, M. (2014). A trichordal temporal approach to digital coordination: The sociomaterial mangling of the CERN grid. *MIS Quarterly, 38*(3), 927–949.

von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security, 7*(1), 50–57.

von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*(2), 99–104.

von Solms, S. H. (2005). Information security governance: Compliance management vs operational management. *Computers & Security, 24*(6), 443–447.

von Solms, R., Thomson, K.-L., & Maninjwa, M. (2011). Information security governance control through comprehensive policy architectures. *Information security South Africa* (pp. 1–6).

von Solms, B., & von Solms, R. (2004a). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371–376.

von Solms, R., & von Solms, B. (2004b). From policies to culture. *Computer & Security, 23*(4), 275–279.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*(2), 74–81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320–330.

Walsham, G., & Sahay, S. (1999). GIS for district-level administration in India: Problems and opportunities. *MIS Quarterly, 23*(1), 39–65.

Warkentin, M., & Johnston, A. C. (2008). IT governance and organizational design for security management. In D. W. Straub, S. E. Goodman, & R. Baskerville (Eds.), *Information security: Policy, processes and practices* (pp. 46–68). Armonk, NY: Sharpe.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*(1), 43–57.

Whitman, M. E. (2008). Security policy: From design to maintenance. In D. W. Straub, S. E. Goodman, & R. Baskerville (Eds.), *Information security: Policy, processes and practices* (pp. 123–151). Armonk, NY: Sharpe.

Whittington, R. (2006). Completing the practice turn in strategy research. *Organization Studies, 27*(5), 613-634.

Wittell, L., Snyder, H., Gustafsson, A., Fombelle, P., & Kristensson, P. (2016). Defining service innovation: A review and synthesis. *Journal of Business Research, 69*(8), 2863–2872.

Zammuto, R. F., Griffith, T. L., Majchrak, A., Dougherty, D., & Faraj, S. (2008). Information technology and the changing fabric of organization. *Organization Science, 18*(5), 749–762.