Equipment-as-Experience: A Heidegger-Based Position of Information Security

Completed Research Paper

Dan Harnesk
Luleå University of Technology
97187 Luleå, Sweden
Dan.Harnesk@ltu.se

Devinder Thapa
University of Agder
4630 Kristiansand S, Norway
Devinder.Thapa@uia.no

Abstract

Information security (InfoSec) has ontologically been characterised as an order machine. The order machine connects with other machines through interrupting mechanisms. This way of portraying InfoSec focuses on the correct placement of machine entities to protect information assets. However, what is missing in this view is that for the InfoSec we experience in everyday practice, we are not just observers of the InfoSec phenomena but also active agents of it. To contribute to the quest, we draw on Heidegger's (1962) notion of equipment and propose the concept of equipment-as-experience to understand the ontological position of InfoSec in everyday practice. In this paper we show how equipment-as-experience provides a richer picture of InfoSec as being a fundamental sociotechnical phenomena. We further contend using an example case to illustrate that InfoSec equipment should not be understood merely by its properties (present-at-hand mode), but rather in ready-to-hand mode when put into practice.

Keywords: Information Security, Equipment-as-experience, Ontology, Heidegger.

Introduction

Engagement with information security (InfoSec) requires knowledge of three types of equipment: technical (e.g. firewall), formal (e.g. policies) and informal (e.g. security culture) (Dhillon 2007). These equipment have distinct characteristics and yet they are not stand-alone, but rather engage with human entities to form a cohesive structure of InfoSec (Baskerville and Dhillon 2008; Siponen and Oinas-Kukkonen 2007). To this end, Vuorinen and Tetri (2012) argue that there is a lack of ontological understanding of InfoSec, and recommend the order machine metaphor in the form of relational ontology using Deleuze and Guattari's (2004) philosophical concepts of machine, coupling, interruption and territory. In this metaphor, InfoSec is portrayed as a machine that connects with various entities to maintain order in what the authors call 'data territories'.

In this paper, we interpret the ontology of the order machine as a classification of facts about InfoSec properties rather than presenting the ontology of InfoSec, even though it references specific ontological direction. The ontological direction that manifests in the order machine is the same as that which considers entity in a universal manner, i.e. as within Cartesian representationalism (see e.g. Mingers 2001; Riemer and Johnston 2014). In this direction, the revealing of InfoSec is, as Heidegger (1977, p.322) puts it, about 'the challenge that sets upon man to order the actual as standing-reserve in accordance with the way it shows itself', and is indeed the same ontology that explains the existence of computers and other technological artefacts. Being nothing but the order of standing-reserve inevitably puts man in a position to regulate the revealing, insofar as it stays in the position of securing the characteristics of the machine. Here we see signs of what Heidegger calls concealment—the machine conceals itself in terms of what and how it is. The machine, represented as a standing-reserve are,

according to Heidegger made disposable in the sense that it is easily ordered and arranged. Within the InfoSec landscape, machines can be replaced with other more efficient machines when new security regulations appear. The machine reveals itself to us humans when we have gained knowledge about its purpose of existence. Heidegger suggests a structure that contains three ways of revealing technology. Present-at-hand mode in which humans have to explicitly encounter the properties of the technology, ready-at-hand mode in which humans already have knowledge how the technology function, and third as human engagement with other humans and technology. The revelation, in Heidegger's view, is thus that the machine is what it can become—a socio-technical constitution that involves technology, human agents, and organisational practices. Admittedly, the advantage of the order machine is the network with connected entities that it presents as a venture in conceptual modeling. The machine ontology however overlooks humans' experience and their role as active security producers, which is a cornerstone in socio-technical perspectives on InfoSec. Hence, the question arises: What would be the characteristics and structure of a relational ontology of InfoSec that incorporate human experiences?

To contribute to the ontological understanding of InfoSec, we reconceptualised InfoSec in relational to human experience rather than entity terms. This required a shift in our thinking to Martin Heidegger's notion of equipment (Heidegger 1962; Heidegger 1977). Equipment, as per Heidegger, is not just a specific tool, but a system of tools in use in a particular context. It is in context that things make sense to us and fit into our lives. 'It is the overall scheme in which we can act, produce, think and be' (Polt 1999, p.52). The relevance of Heidegger's philosophy to the information systems field has been suggested previously (Whitley and Introna 1998). Several attempts have been made to expand on Heidegger's relational view using his terminologies, including 'anxiety', 'familiarity', 'gestell', 'enframing' and 'worldliness'. The most recent attempt is the article 'Rethinking the place of the artefact in IS using Heidegger's analysis of equipment' (Riemer and Johnston 2014). This insightful and critical account of philosophy's importance to the field conceptualises IT as equipment interwoven with other equipment, user practices and individual identities. Interestingly, while Heidegger's thoughts have been problematised in information systems research, we find no studies focusing on Heidegger's relevance in InfoSec research.

In this paper, by applying Heidegger's philosophy and following (Riemer and Johnston 2014), we argue for the understanding of InfoSec as *equipment-as-experience*. This approach to InfoSec means revealing it through an understanding of equipment as a basic experience. According to Heidegger (1962), experiences emerge deliberately and non-deliberately through everyday engagement with equipment. We propose that equipment-as-experience consists of experience variance, rather than a unified configuration, and that these variances are made obvious in the enactment of InfoSec equipment Experience variance in our view refers to the different, inconsistent and controversial positions of InfoSec as a phenomenon that both requires special attention and simultaneously creates experiences during the use of InfoSec equipment. Our view is thus distinct from the common strategy in explaining variance as a formalisation of human behaviour based on the assumption that a causal relationship exists between technological and mental properties (Riemer and Johnston 2014). Our argument is further that configuration unity employs a configuration perspective that centres on the analysis of possible configurations of information technologies (Henfridsson and Bygstad 2013), and is the result of the view of conceptual modelling as a representation of a real-world system. For instance, Weber (2003) use the example of a email system that represents states and events that relate to the sender of the message. Similarly, InfoSec contains states and events that regulate computer users access to information bases. We consider configuration unity and experience variance as two fundamental characteristics of InfoSec. These two characteristics stress the socio-technical constitution of InfoSec by guiding technical performance and shaping organisational InfoSec practises (Almusharraf et al. 2015; Hedström et al. 2010; Kolkowska and Dhillon 2013; Siponen and Willison 2009; Siponen and Oinas-Kukkonen 2007; Warkentin et al. 2011). Using the notion of equipment-as-experience, we reconcile the characteristic of Infosec and argue that the reconciled view can reveal the nature of InfoSec better than the Cartesian position can (Riemer and Johnston 2014).

The rest of the paper is organised as follows: we first embed equipment-as-experience within Heidegger's philosophy. Next, we review the InfoSec literature to provide a basis for an ontological discussion. Subsequently, we describe and analyse equipment-as-experience using one example case. Finally, we discuss our reconceptualisation of InfoSec and conclude the paper.

Positioning equipment-as-experience

To examine InfoSec's ontological status, we must situate it within three ways of revealing equipment-as-experience (Heidegger 1962): first, the present-at-hand mode of using a tool; second, the ready-at-hand mode, in which the equipment explicitly points to a purpose; and third, as human engagement wherein the human is not an observer but an active agent, skilfully coping with the equipment.

The main question that Martin Heidegger (1962) asked in his seminal work *Being and Time* was, 'what is the meaning of being of any entities'. He proposed that understanding the meaning of being of something means to reveal it. Likewise, in order to reveal the 'being of something' more clearly, we have to place that thing within a particular context. Heidegger stated that understanding the meaning of being doesn't mean enquiring about entities; rather, we have to pay attention to equipment as it reveals itself in use. Heidegger asserts that 'entities are, quite independently of the experience by which they are disclosed, the acquaintance in which they are discovered, and the grasping in which their nature is ascertained' (Heidegger 1962, p.251). For example, studying a firewall and analysing its properties does not mean one has uncovered its being; however, when we put this device into use in a particular context, it becomes part of its experiences (i.e. the equipment is given meaning through its performance in a network, switch or router). As Heidegger puts it, 'the less we just stare at the hammer-thing, and the more we seize hold of it and use it, the more primordial does our relationship to it become, and the more unveiledly is it encountered as that which it is—as *equipment*' (Heidegger 1962, p.98).

Heidegger refuted the Aristotelian notion of 'being' in terms of substance with properties, just as he rejected the Cartesian notion of 'being' as thinking substance (human subjects) and extended substance (non-human objects). Instead, he proposed three modes of being: *Dasein* (human), *present-at-hand* (objects) and *ready-to-hand* (equipment). The Dasein (our) mode of existence is different from that of other entities because we involve ourselves in activities, are social and 'inhabit a world, we are capably engaged in a meaningful context. Our world is the context in terms we understand ourselves, and within which we become who we are' (Polt 1999, p.30). Heidegger expressed that *being-in-the-world* means we are thrown into a context where we have a place in a meaningful whole; here we deal or encounter with equipment and other Daseins. Regardless of our personal and cultural differences, we continuously actively engage in the world by generating experiences in our struggle for identity.

To encounter equipment in ready-to-hand mode means that we understand something not by observation but by use. We use the equipment *'in-order-to'*; we get something done for the sake of *'towards-which'* someone (a Dasein). For example, if we consider security controls (both technical and organisational) as equipment, InfoSec is meant to protect information assets for the sake of securing the continuity of business activities, so that stakeholders (Dasein) can maintain their business identity (in its widest meaning). In ready-to-hand mode, all entities involved form the 'referential totality' and do not remain as individual items of equipment, but rather as a referential whole without parts (Harman 2010). We can deal with entities in present-at-hand mode as well. This involves the reflective observation of any object. For example, we observe the properties of different technical and organisational controls from a distance rather than from its use in practice. Objects can be present-at-hand when broken, and become obtrusive once they no longer function effectively. Breakdown does not always refer to permanent breakdown (obstructive), however (one could, for example, simply be unable to find a tool); it also refers to temporary breakdown (obstinate) such as when a part of a tool is missing or malfunctioning (conspicuous), or the tool is not appropriate (Dreyfus 2001). As such, 'breakdowns' in InfoSec should not be taken as technical failures only, as they can also be failures of formal and informal controls.

It is important to carefully recognise that present-at-hand and ready-to-hand are not two different types of entities. 'Instead, all entities oscillate between these two separate modes: the cryptic withdrawal of readiness-to-hand and the explicit accessibility of present-at-hand' (Harman 2010, p.3). According to Heidegger, 'the present-at-hand way of being in which entities are encountered as objects with properties is a derivative way that humans can relate to the world (for example to reflect mindfully) that is grounded ultimately in our practical understanding of the work (for example through using equipment)' (Riemer and Johnston 2014, p. 277). In this context, we can say that ready-to-hand and present-at-hand are both different modes of InfoSec. However, the present-at-hand mode is derived from ready-to-hand and not the other way round.

In summary, as shown in Figure 1, we are always engaged with other Dasein and equipment (ready-to-hand entities) in our everyday existence to construct or reconstruct our 'world'. We are already thrown into the world as 'being-in-the-world' and have a pre-understanding (familiarity) of this context through our involvement in everyday practice; however, this understanding can be vague. Therefore, any entity we encounter takes on meaning based on its familiarity to our existing practice. However, if we encounter entities that are unfamiliar to us (or defined by context-independent properties) (Riemer and Johnston 2014), then the entities are simply present-at-hand entities and not equipment for us. Consequently, we cannot comprehend their practical meaning. For example, when we find security controls designed without an understanding of practical context, it is difficult for us to know what they are and what they are for. We must examine the tangible properties of the security controls against our own familiarity. This leads to ambiguity in placing the controls within any practices that we know; the controls may turn out to be unsuitable in our particular context. The implications of Heidegger's analysis to the security practitioners is that the entity we deal with is not defined by its properties (present-at-hand mode), but is understood by its place in practice (ready-to-hand). 'That makes intelligible the object (i.e. equipment) and influences which properties show up for us as meaningful in a situation. The being of such objects (what they are) is thus grounded in intelligibility (how we understand them practically) and not in substantiality (their material properties)' (Riemer and Johnston 2014, p.279). Through this engagement in practice with other Daseins and equipment, we maintain our identity and keep on exploring the possibilities of Dasein's reality. The meaning in this context is that of either security personnel or users will not experience the equipment in totality if they cannot see how it serves to preserve their identity.

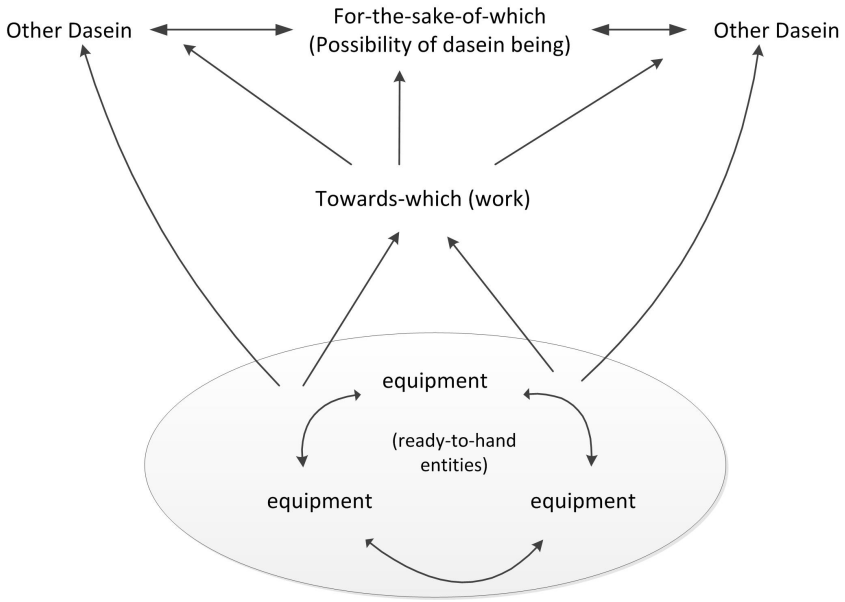

Figure 1.Equipment (adopted from Richard Polt 1999, p. 54)

InfoSec in an equipment-as-experience perspective

InfoSec has been conceptualised in socio-technical terms. The technical level consists of the specific performance of the security equipment, and the socio-organisational level that both shapes and is shaped by this performance (Almusharraf et al. 2015; Hedström et al. 2010; Kolkowska and Dhillon 2013; Siponen and Willison 2009; Siponen and Oinas-Kukkonen 2007; Warkentin et al. 2011). As the socio-technical account of InfoSec centres around interactions between security technology and people (c.f. Cordella 2006; Latour 1987; Orlikowski 2007), the abundance of technical, formal and informal security equipment will generate distinct experiences that are co-constructed relationally through direct engagement in daily activities (D'Aubeterre et al. 2008; Dhillon 2007; Siponen and Vance 2014; Siponen and Oinas-Kukkonen 2007; Warkentin and Willison 2009).

Note that equipment has a strong association with experiences. Experiences envision a way forward in the shaping of a comprehensive security practice within an organisation (Dhillon and Backhouse 2001; Siponen 2001). This shaping is dependent on revealing, however, and revealing is challenging; the effort required of equipment—in our case the InfoSec technology—is unreasonable, so says Heidegger in 'The question concerning technology' (Heidegger 1977). This is because the in-built capacity of InfoSec technology is not sufficient to secure access to the layers below and to other artefacts within IT infrastructures, nor to shape the InfoSec culture of the organisation. It is against this setting of challenges that Vuorinen and Tetri's (2012) order machine operates. Independent machines are connected by way of covering their controlling attributes through the act of interrupting. It is in this mode of operation that the order machine reveals itself through its performance. It is a kind of mechanised performance of covering that in Heidegger's view means the unlocking of protected information bases and the exposure of resources. Heidegger (1977) formulates the challenge in the following:

> *Unlocking, transforming, storing, distributing and switching about are ways of revealing. /.../ The revealing reveals to itself its own manifold interlocking paths, through regulating their course. This regulation itself is, for its part, everywhere secured. Regulating and securing even become the chief characteristics of the revealing that challenges (p.322).*

In literature wherein technical security equipment is at the centre of attention, a number of machines function as standing-reserves in the regulation and security of the IT domain within an organisation. Vuorinen and Tetri (2012) recognised that organisations are occupied with several different machines and present a structural view accompanied by a flowchart that sequences connections between different machines. These connections are part of a configuration logic that seeks to unify the machines towards a single goal—to protect data territories. The order machine metaphor is however not a fixed position of InfoSec as would have been the case if it was presented as an autonomous tool. Through connections the order machine is part of an on-going relationship with humans and other entities. Furthermore, when they turned to the material content, Vuorinen and Tetri (2012) discovered that a single machine is indeed multiple machines. Where Vuorinen and Tetri (2012) see multiple entities, we see functional features of the machine. For example, in order to secure communication, a cipher machine functions by interconnecting categories of cryptographic algorithms to ensure data confidentiality or data integrity (Siponen and Oinas-Kukkonen 2007). Similarly, a firewall is a flow detection machine that applies its regulative functionality to control data traffic (Hedström et al. 2010).

How is the efficiency of these machines monitored? The effective operations of technical security equipment are typically explained as a function of rule-based structures and their associated role-based responsibilities (i.e. formal security equipment) (Dhillon 2007). The formal equipment is characterised by the support and management of the resources needed to govern technical equipment (Stahl et al. 2008). While the formal security equipment includes tools such as checklists, risk analysis and standard security frameworks (Dhillon and Backhouse 2001; Saleh et al. 2007), its practise is that of technical systematisation in the sense that it tends to reinforce present-at-hand equipment. Several security management techniques have been proposed with the purpose of controlling and creating stable security environments. These include security management models (Dhillon 2007; Wylder 2004), information security governance (Moulton and Coles 2003), security policy compliance (Thomson and von Solms 2006) and agile security design (Siponen et al. 2005). Given the ultimate objective of the proposed techniques—to ascertain the integrity of strategic information resources—we frame formal security equipment as a reconnaissance machine (Mookerjee et al. 2011; Ransbotham and Mitra 2009). Essentially, the responsibility of the reconnaissance machine is to execute descriptive accounts with prescribed management-in-action protocols to render secure IT milieus. It is argued that such descriptions are meant to better facilitate the utilisation of security tools (Hsu 2009; Kolkowska and Dhillon 2013; Siponen and Vance 2010; Vance et al. 2012).

While technical and formal equipment help clarify the setting-upon challenges, we still need to reconcile the subordinate role of users and the distortion that the order machine brings upon them. Turning to the literature for examples may shed some light on this particular gap. The user is subjected to the orderability of InfoSec, but order may never be actualised. Faced with the quest for order, users may develop expectations that conflicts with the expectations of those (e.g. InfoSec managers) who possess the authority to enforce InfoSec regulation in the workplace. These expectations (sometimes perceived

expectations) leave little room for users to comprehend the InfoSec frameworks they face every day. The literature describes this lack of understanding as a potential source of malicious security behaviours. It is acknowledged in the received literature that this problem occurs as users' intention to obey to given security frameworks largely depends on their motivation to comply with the frameworks (Myyry et al. 2009). These programmes have been criticised as delivering weak content (Lacey 2010). Puhakainen and Siponen (2010) suggest that compliance can be achieved if users systematically utilise the cognitive processing of information received through training activities. Interestingly, despite the possible impact of training programmes, Stanton et al. (2005) maintain that improvement in these areas also brings a greater likelihood of writing down one's password, or even sharing passwords, which indicates a lack of InfoSec awareness (Dinev and Hu 2007). Hence, users may develop misaligned InfoSec use patterns in the course of enacting InfoSec regulation because of discrepancies between emerging experiences and expected experiences (Backhouse and Dhillon 1996).

In their attempt to clarify the ontological position of the order machine, Vuorinen and Tetri (2012) unfortunately regard the human agent more as a source of distortion than an active agent of InfoSec. In their view, the machine can foster good security behavior and in that respect the machine are assigned the task to influence the human self. For example, by interrupting information access it is expected that human agents will internalise password policies and avoid compromising the integrity of information systems. Technology is, however, a mode of revealing according to Heidegger, and so is the order machine. But what does it reveal that is relevant to the status of InfoSec. It reveals, in accordance with Cartesian representationalism, a structure of entities which Heidegger (1977) refers to as 'the basis of the ordering of the orderable' (p.323). In Heidegger's view such a structure of entities is similar to what Vuorinen and Tetri (2012) call assemblage of order machines. This position represents the context of interlocking processes pertaining to the orderly disposition of InfoSec that appears to be something at human command.

In our view of InfoSec, the human (an active agent) cannot be excluded from the picture. A precise organisation of order invites decidedly rational approaches to InfoSec by assuming that it is possible to deterministically match technology with human intentions. Such a prescriptive approach is likely to manifest InfoSec as a predictable and stable entity. We propose that when we engage with InfoSec equipment, different experiences will emerge. For example, when security engineers are occupied with configuring InfoSec equipment, they are attuned to the present-at-hand mode. When the same engineer explains why and how that equipment functions within the overall InfoSec practice without turning to its material content, he or she is undergoing a ready-to-hand experience. So, in the pathway of unitary actions, engineers could develop a unifying experience. The same analogy holds for the user as well. When the login process to systems is interrupted due to password problems, the user is forced to direct his or her attention to the present-at-hand mode. When the password works, the user can engage in work-related activity. Experiences thus emerge in oscillation between these two separate modes of engagement because the actors have developed familiarity with pathways of action (Harman 2010).

A narrative and interpretation of equipment-as-experience

For this project, we examined a published case study in which behavioural security (BSec) technology was introduced in a nursing home (Harnesk and Lindström 2012), to illustrate how equipment-as-experience can inform the study of InfoSec ontology. The research design in the original case was qualitative and data collection method was in-person interviews. Data analysis had a focus on how organizational actors made sense of BSec and how they engaged in the emerging relationship between organizational security objectives, technology, and users. Our approach in reinterpreting the case was to identify the emergent experiences among stakeholders and how these experiences oscillate between present-at-hand mode and ready-at-hand mode and how stakeholders engaged with each other during the introduction phase. The decision to introduce the security technology was taken by the elderly care unit in the municipality of Luleå, Sweden. The municipality sponsored the introduction of the new security application to this facility in response to undesirable security behaviour. Four different work roles were involved in the narrative: IT manager, local IT manager, care unit manager and care staff. Table 1 illustrates examples of the managers' experiences in pursuing the goal of configuring InfoSec (Con_Exp) and the users' experiences of engaging with it (Use_Exp).

In the case, security managers reported that their main goal was to ensure secure behaviour while using the department's computer resources. The initiators of the introduction, the IT manager at the social

department and the IT manager at the IT service unit in the organisation, stressed that their privacy regulations in elderly care necessitated a change in security behaviour. Accordingly, the users were informed of the privacy issues and were asked to sign a confidentiality agreement when employed. While the involved managers contended that awareness of privacy matters was high in the organisation, there was still a risk of computer abuse due to an observed reluctance to complete logout procedures, which enabled people to use the computers under someone else's user credentials.

With the introduction of the BSec platform, security management wanted to substantially improve the protection of patient records. Compliance with legal and regulatory frameworks is of outmost importance in organisations of this type. The technical justification for moving from traditional subject-object security approaches to BSec was the possibility of automated authentication. The BSec technology in question also featured effective monitoring and control of user behavioural patterns by producing performance statistics. Monitoring before BSec involved the manual checking of log files, including cross-checking the logs for breaches. The intention was to use the new technology to collect and analyse behavioural data during run-time [Con_Exp 1]; however, the technology was also expected to raise security awareness among the staff. Interestingly, the latter was more or less taken for granted due to an understanding that the software was self-instructive. Along with this basic assumption about BSec's perceived utility, the managers strongly believed its mechanisms could protect computer resources and secure the privacy of care receivers [Con_Exp 2]. Indeed, the BSec technology substantially improved monitoring activity through an automated authentication process across all care applications [Con_Exp 3].

Besides the obvious technical leverage, there was also an anticipation of the usefulness of the security technology. The nursing staff anticipated substantial impact from BSec on work performance, productivity and effectiveness [Use_Exp 1] as they previously had complained about the significant number of computer-related problems affecting the use of healthcare applications. One major issue was that a single computer had to serve up to 40 people on reporting days. Considering the overall computer situation in the nursing home as explained by the user group, there were clear signs of potential maladaptive security behaviour. For example, when having trouble with passwords, employees were expected to call local support for further assistance. However, this was not efficient according to the staff because of long response times to get a new password from the support function. The nursing staff 'solved' this by sharing user credentials between each other [Use_Exp 2]. There was indeed a need for better security policy compliance among the staff.

With the introduction of BSec, the security system remained invisible in the sense that employees were not intruded upon by system properties. It was agreed that the usefulness of security procedures had indeed increased after the introduction of BSec [Use_Exp 3]. Once enrolled, the employees confirmed that their experience of the system was better than expected prior to introduction. Two of the employees even expected that the general service level of the new system would increase after some time of use. This was due to high expectations among employees that the system would, more or less, entail changed and improved work processes. While managers uniformly distributed responsibilities to prepare for the new security system, employees initially expected other benefits from the system, which in reality the technology could not deliver upon.

One interesting aspect is that although the three managers agreed that the organisation had suffered from maladaptive security behaviour, they exhibited conflicting views in preparing for the security software's introduction. This in turn affected the communication of instructions to work groups. While the initiators of the security software introduction used a push approach when persuading the work group to participate in the project, there were no interactions between management levels and employees after the decision for the introduction was made. It was anticipated that the identification and verification features of the BSec security platform would be sufficient to render a change in security behaviour.

Table 1. Equipment-as-experience
Configuration domain (Con_Exp) 1. BSec can automatically collect, store and continuously analyse data about employees' computer behaviour 2. BSec can be configured to immediately signal computer abuse 3. BSec reduces InfoSec administrative tasks due to lesser control of authentication character
User domain (Use_Exp) 1. Improvement in work performance, productivity and effectiveness 2. Sharing passwords make work easier 3. Work life became easier as the single sign-on authentication procedure in BSec resulted in seamless identification and less intrusive security controls

Table 1. Equipment-as-experience

After some time using BSec, the nursing staff acknowledged their intention to continue using the security software over alternative means such as having colleagues enter healthcare information in the security software on their behalf. BSec thus encouraged new security patterns among employees.

Interpreting equipment-as-experience

In the configuration domain, equipment-as-experience exists as a roadmap for goal-directed action at any security event occurring within the IT infrastructure. In regard to the user domain, we have defined experience variance as the different, inconsistent and controversial positions of InfoSec, a phenomenon that demands explicit attention while being coped with and simultaneously creates experiences during use. Here, the order machine regards configuration only as goal-directed action, whereas equipment-as-experience subsists as a significant whole of connections between present-at-hand and ready-at-hand items. If we bring instances of formal, informal and technical equipment into a meaningful web of experiences, they will make sense in an organisation. As Heidegger tells us, 'our using or manipulating of any individual item of equipment remains oriented towards some equipmental context' (Heidegger 1962, p.403). Therefore, equipment is either usable or in use and involved in a certain activity; in Heidegger's terms, the towards-which *why* and for-the-sake-of-which *who*. Those involved with BSec in the examined case study experienced InfoSec differently, but always in a way that was relevant to their respective work tasks; this is obvious in the two kinds of experiences displayed in Table 1. For security managers, the introduction of InfoSec in the nursing home was justified by the support it brought to securing the enactment of software applications, IT infrastructures and networks (i.e. the functional objects that represent the present-at-hand status of InfoSec). For computer users, the introduced InfoSec was simply a means to complete work tasks and support care receivers' overall safety and security.

The equipment-as-experience position of InfoSec revealed inconsistencies between groups, as there was no strategy in place to identify assumptions about BSec within the nursing staff group. An interesting controversy to InfoSec is the assumption that the BSec introduction would lead to improvements in work performance, which was never intended by the decision makers. The nursing staff reconciled this with sharing passwords continuously between each other. As it was clear that the BSec introduction required staff to begin behaving in accordance with new InfoSec regulations, the introduction was essentially a change project. While the two characteristics, configuration unity and experience variation help clarify the basic configuration role of InfoSec, and the different, inconsistent and controversial positions of InfoSec, these characteristics also manifest experiences that emerge in the enactment of InfoSec. Thus experiences emerge in both the configuration domain and in the user domain. The experiences emerged

in our case through the identification of improved technical equipment, i.e better protection trough BSec, and that the nursing staff adapted to BSec and eventually accepted BSec as the technical security foundation within their nursing practice.

In the course of implementing InfoSec, professionals must demonstrate how computer users can utilise InfoSec within their own contexts. Security equipment is intertwined with user practices in the continuation of business activities. As such, InfoSec properties appear to users as meaningful in actual use situations. The identity of such experiences (what they are) is thus grounded in the way we understand them practically and not in their material properties. The use of equipment-as-experience to understand InfoSec is related to but differs in important ways from the order machine metaphor. While both metaphors are consistent with safeguarding organisational information assets, the order-machine focuses on rules, boundaries and limitations through its neutral appearance in the regulation and control of data territories. To achieve this, Vuorinen and Tetri (2012) suggest that territories with order machines that connect to each other are visible patterns of distinct InfoSec goals. Whatever these goals may be in practice, they always involve three fundamental security processes: identification, authentication and authorisation. In this case, the security technology performs these processes with present-at-hand equipment that, without association to a web of meaning, will be seen as features of connectivity (i.e. it will carry out a precise organisation of order). In order for the association to take hold, the present-at-hand equipment must instead connect to continuous activity rather than specific entities. Thinking in terms of equipment-as-experience enables the exploration of different equipment and how they become intertwined to shape InfoSec over time. In Heidegger's view, this represents the skilful coping with equipment that professionals use in making sense of a flow of a directed activity (Dreyfus 2001). The sense-making of directed activities leads to knowing what others are doing in the process of securing and safeguarding organisational information assets, without explicitly knowing the purpose of all types of security measures.

Discussion

We began this paper to understand the ontology of InfoSec. We observed that Vuorinen and Tetris' (2012) idea of InfoSec is oriented towards computational entities to safeguard data territories. Vuorinen and Tetri suggest their conceptualisation of InfoSec should be regarded as relational ontology. Our examination of their approach to InfoSec in the form of the order machine reveals InfoSec by existence rather than InfoSec *as* existence, namely in present-at-hand mode, with explicit attention towards the configuration of assemblages of connected entities. The order machine thus takes priority over security professionals and users' actual experiences when InfoSec comes into everyday activity. We found the irresistibility of ordering intriguing and elaborated on some limitations of the order machine by drawing on Heidegger's notion of equipment. To that end, we propose equipment-as-experience as a concept to understand the relationship between experiences generated from engagement with technical, formal and informal security equipment. One fundamental limitation with the order machine metaphor that our approach overcomes is its neutrality towards singular actors' conceptions about InfoSec. For example, the being or nature of InfoSec is defined as an interrupter that maintains order in the security chaos that comes from inside or outside. We find the order machine to represent a foundation of entities needed to provide the secure interactive base to human agents. Once again, we see this relationship *as* existence; i.e. the engagement with equipment that will generate distinct experiences co-constructed relationally in daily activities. Our understanding of InfoSec is thus distinct from not only the order machine but also from InfoSec as a 'business enabler' (Sherwood et al. 2005), 'security-insulator' (Pieters 2011), 'security-by-experiment' (Pieters et al. 2015) and 'emancipator' (Talib and Dhillon 2010; Thapa and Harnesk 2014), as these approaches may conceal the way InfoSec generates comprehensive experiences of technical, formal and informal equipment.

Besides the neutrality towards human agents, another shortcoming of the order machine ontology is the vagueness in which different modes of equipment are treated. The order machine focuses more on *towards-which* (in this context, information protection), and the human aspect gives less attention to *for-the-sake-of-which* (for whom). To understand both aspects, we need to comprehend how people experience InfoSec in practice. The example case illustrates how similar phenomena can be experienced in different modes (e.g. Con_Exp and Use_Exp). As Heidegger states, the essence of technology is in the revealing or double revealing of a designer's intention and user experience. In this context, the double

revealing can work as a feedback loop to the configuration domain in terms of understanding how users appropriate the technology, and to the users' domain in identifying the latent affordances of the technology.

This study also dissects the sociotechnical phenomena in general, and InfoSec in particular. For example, some scholars argue that InfoSec holds a strong association between socio-technical elements in that the integrity of an organisation as a whole is the main focus (Hedström et al. 2010; Kolkowska and Dhillon 2013; Siponen and Vance 2014; Siponen and Willison 2009; Siponen and Oinas-Kukkonen 2007; Warkentin et al. 2011). It is also suggested that where the technological frames (assumptions, expectations and knowledge) backed by values, cultures and beliefs in key groups (managers, technologists and users) within an organisation are significantly different, difficulties and conflict around the development, use and change of technology may arise (Orlikowski and Gash 1994). We argue that the ontological positioning of InfoSec as equipment-as-experience reveals experiences in different levels that can have different effects on the phenomena, as illustrated in the example case. In this example, the same InfoSec instance was experienced differently across the configuration and user domains in terms of how the experiences reframed the InfoSec system.

Conclusion

In this paper, we investigated a previously overlooked phenomenon; namely, the everyday understanding (equipment-as-experience) of InfoSec. By drawing on well-acknowledged InfoSec concepts (technical, formal and informal), we provided an alternative understanding of the nature and scope of InfoSec. The concepts proved to be a suitable and appropriate basis on which to suggest that a relational ontology has the capability to cultivate a holistic understanding of the area. The findings illustrate that the 'being' of security entities should not be understood merely by their properties (present-at-hand mode), but rather that when put into practice (ready-to-hand mode), information security reveals itself. The notion of equipment-as-experience thus provides a way to handle the challenge of maintaining the benefit that a wider scope of InfoSec can generate in organisational InfoSec practices. The implications of the equipment-as-experience perspective to security practitioners is that the entity they deal with is not defined by its properties (or present-at-hand mode), but rather requires skilful coping with security equipment to understand its place in practice (or ready-to-hand mode).

References

Almusharraf, A., Dhillon, G., and Samonas, S. 2015. "Mismatched Understanding of Is Security Policy: A Repgrid Analysis," *21th American Conference on Information Systems*, Puerto Rico.

Backhouse, J., and Dhillon, G. 1996. "Structures of Responsibilities and Security of Information Systems," *European Journal of Information Systems* (5:1), pp. 2-10.

Baskerville, R., and Dhillon, G. 2008. "Information Systems Security Strategy: A Process View," in *Information Security: Policy, Processes, and Practices,* D.W. Straub, S. Goodman and R. Baskerville (eds.). Armonk, New York: Sharpe, ME.

Cordella, A. 2006. *Information Infrastructure in Action*. London School of Economics and Political Sciences, Department of Information Systems.

D'Aubeterre, F., Singh, R., and Iyer, L. 2008. "Secure Activity Resource Coordination: Empirical Evidence of Enhanced Security Awareness in Designing Secure Business Processes," *European Journal of Information Systems* (17:5), pp. 528-542.

Dhillon, G. 2007. *Principles of Information Systems Security: Text and Cases*. Wiley New York.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in Is Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.

Dinev, T., and Hu, Q. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the AIS* (8:7).

Dreyfus, H. L. 2001. "How Heidegger Defends the Possibility of a Correspondence Theory of Truth with Respect to the Entities of Natural Science," *The practice turn in contemporary theory*, pp. 151-162.

Harman, G. 2010. "Technology, Objects and Things in Heidegger," *Cambridge Journal of Economics* (34:1), pp. 17-25.

Harnesk, D., and Lindström, J. 2012. "Materializing Organizational Information Security," *Nordic Contributions in IS Research: Third Scandinavian Conference on Information Systems,* C. Keller, M. Wiberg, P. Ågerfalk and J. Eriksson Lundström (eds.): Springer Verlag, pp. 76-94.

Hedström, K., Dhillon, G., and Karlsson, F. 2010. "Using Actor Network Theory to Understand Information Security Management," in *Security and Privacy–Silver Linings in the Cloud*. Springer, pp. 43-54.

Heidegger, M. 1962. *Being and Time* (First English Edition). Blackwell Publishing Ltd.

Heidegger, M. 1977. *The Question Concerning Technology and Other Essays*. New York: Harper and Row.

Henfridsson, O., and Bygstad, B. 2013. "The Generative Mechanisms of Digital Infrastructure Evolution," *Mis Quarterly* (37:3), pp. 907-931.

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

Kolkowska, E., and Dhillon, G. 2013. "Organizational Power and Information Security Rule Compliance," *Computers & Security* (33), pp. 3-11.

Lacey, D. 2010. "Understanding and Transforming Organizational Security Culture," *Information Management & Computer Security* (18:1), pp. 4-13.

Latour, B. 1987. "Science in Action: How to Follow Engineers and Scientists through Society," *Cambridge: Harvard UP*).

Mingers, J. 2001. " Combining Is Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3).

Mookerjee, V., Mookerjee, R., Bensoussan, A., and Yue, W. T. 2011. "When Hackers Talk: Managing Information Security under Variable Attack Rates and Knowledge Dissemination," *Information Systems Research* (22:3), pp. 606-623.

Moulton, R., and Coles, R. S. 2003. "Applying Information Security Governance," *Computers & Security* (22:7), pp. 580-584.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules[Quest] an Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Orlikowski, W. J. 2007. "Sociomaterial Practices: Exploring Technology at Work," *Organization Studies* (28:9), pp. 1435-1448.

Orlikowski, W. J., and Gash, D. C. 1994. "Technological Frames: Making Sense of Information Technology in Organizations," *ACM Transactions on Information Systems (TOIS)* (12:2), pp. 174-207.

Pieters, W. 2011. "The (Social) Construction of Information Security," *The Information Society* (27:5), pp. 326-335.

Pieters, W., Hadziosmanovic, D., and Dechesne, F. 2015. "Security-by-Experiment: Lessons from Responsible Deployment in Cyberspace," *Science and engineering ethics*, pp. 1-20.

Polt, R. 1999. *Heidegger. An Introduction*. Cornell University Press.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Throgh Information Systems Security Training an Action Research Study," *MIS Quarterly* (34:4), pp. 767-793.

Ransbotham, S., and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research* (20:1), pp. 121-139.

Riemer, K., and Johnston, R. B. 2014. "Rethinking the Place of the Artefact in Is Using Heidegger's Analysis of Equipment," *European Journal of Information Systems* (23:3), pp. 273-288.

Saleh, M. S., Alrabiah, A., and Bakry, S. H. 2007. "A Stope Model for the Investigation of Compliance with Iso 17799-2005," *Information Management & Computer Security* (15:4), pp. 283-294.

Siponen, M., Baskerville, R., and Kuivalainen, T. 2005. "Integrating Security into Agile Development Methods," *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, Hawaii.

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS quarterly* (34:3), p. 487.

Siponen, M., and Vance, A. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations," *European Journal of Information Systems* (23:3), pp. 289-305.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp. 267-270.

Siponen, M. T. 2001. "An Analysis of the Recent Is Security Development Approaches: Descriptive and Prescriptive Implications," *Information Security Management-Global Challenges in the Next Millennium, Idea Group*), pp. 101-124.

Siponen, M. T., and Oinas-Kukkonen, H. 2007. "A Review of Information Security Issues and Respective Research Contributions," *The DATA BASE for Advances in Information Systems* (38:1), pp. 60-80.

Stahl, B. C., Shaw, M., and Doherty, N. F. 2008. "Information Systems Security Management: A Critical Research Agenda," in: *Association of Information Systems SIGSEC Workshop on Information Security and Privacy (WISP2008)*. Paris.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of End User Security Behaviors," *Computers & Security* (24:2), pp. 124-133.

Talib, Y. A., and Dhillon, G. 2010. "Invited Paper: Employee Emancipation and Protection of Information," *5th Annual Symposium on Information Assurance (ASIA'10)*, p. 10.

Thapa, D., and Harnesk, D. 2014. "Rethinking the Information Security Risk Practices: A Critical Social Theory Perspective," *System Sciences (HICSS), 2014 47th Hawaii International Conference on*: IEEE, pp. 3207-3214.

Thomson, K.-L., and von Solms, R. 2006. "Towards an Information Security Competence Maturity Model," *Computer Fraud & Security* (2006:5), pp. 11-15.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3), pp. 190-198.

Vuorinen, J., and Tetri, P. 2012. "The Order Machine–the Ontology of Information Security," *Journal of the Association for Information Systems* (13:9), pp. 695-713.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems* (20:3), pp. 267-284.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18), pp. 101-105.

Weber, R. 2003. "Conceptual Modelling and Ontology: Possibilities and Pitfalls," *Journal of Database management* (14:3), p. 1.

Whitley, E. A., and Introna, L. D. 1998. "Special Issue: Heidegger and Information Technology," *Information, Technology and people* (11:4).

Wylder, J. 2004. "Towards Enforcing Security Policy: Encouraging Personal Accountability for Corporate Information Security Policy," *Information Security Management Handbook*), pp. 945-952.