Journal of Strategic Information Systems xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Journal of Strategic Information Systems

journal homepage: www.elsevier.com/locate/jsis

Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method

Ella Kolkowska, Fredrik Karlsson *, Karin Hedström

School of Business, Örebro University, Fakultetsgatan 1, SE-701 82 Örebro, Sweden

ARTICLE INFO

Article history:
Received 1 September 2014
Received in revised form 16 August 2016
Accepted 29 August 2016
Available online xxxx

Keywords:
Information systems security
Compliance
Goals
Value
Rationale
Method
Security policy

ABSTRACT

Employees' poor compliance with information security policies is a perennial problem. Current information security analysis methods do not allow information security managers to capture the rationalities behind employees' compliance and non-compliance. To address this shortcoming, this design science research paper suggests: (a) a Value-Based Compliance analysis method and (b) a set of design principles for methods that analyse different rationalities for information security. Our empirical demonstration shows that the method supports a systematic analysis of why employees comply/do not comply with policies. Thus we provide managers with a tool to make them more knowledgeable about employees' information security behaviours.

1. Introduction

An organisation's information is often one of its most important assets, yet the number of information security incidents, as well as the financial losses relating to such incidents is increasing (Cisco, 2014; ENISA, 2014; European Commission, 2013; Intel Security, 2014; PwC, 2013). For instance, the Global State of Information Security Survey 2014 (PwC, 2013) reported a 25% increase in security incidents compared with 2012. Furthermore, average financial losses relating to security incidents had increased by 18%. Thus, it is not surprising that information security management, aimed at safeguarding an organisation's information assets, has become a key strategic issue for many organisations (Van Niekerk and Von Solms, 2010). Indeed, it is widely argued that information security, which can be defined as "the protection of information" that minimises "the risk of exposing information to unauthorised parties" (Venter and Eloff, 2003), should be an integrated part of organisational governance (McFadzean et al., 2006; von Solms, 2006).

Because of its military and technical origin, information security is sometimes reduced to "the techniques employed to maintain security within a computer system" (Gollmann, 1999). However, information security in the context of organisational governance is much broader. Today, information security includes both technical and non-technical information-handling activities (Dhillon, 2007). Management of information security therefore embraces various technical, operational, and managerial controls (NIST, 2012) for safeguarding information and preventing the misuse of information systems (Baker and Wallace, 2007). One type of management control is the implementation of policies, rules and guidelines for regulating

* Corresponding author.
E-mail addresses: ella.kolkowska@oru.se (E. Kolkowska), fredrik.karlsson@oru.se (F. Karlsson), karin.hedstrom@oru.se (K. Hedström).

http://dx.doi.org/10.1016/j.jsis.2016.08.005
0963-8687/

employees' information security behaviours (Siponen and Vance, 2010). Despite this, the majority of information security breaches are caused by employees who violate information security policies (Herath and Rao, 2009b; Nash and Greenwood, 2008; Siponen et al., 2014; Stanton et al., 2005). Non-compliance, where employees fail to act according to information security policies, is therefore seen as a serious security problem, particularly in practice (ENISA, 2014; PwC, 2014a; Symantec Corporation, 2014). For instance, the Global State of Information Security Survey 2015 (PwC, 2014b) stated that current employees account for 35% of all security breaches within organisations. Furthermore, ENISA's (2014) incident report showed that, in some sectors, incidents caused by employees who, intentionally or unintentionally, violate information security regulations are among the top five causes of large disruptions in organisations.

The seriousness of this problem also means that employees' non-compliance has received significant attention from researchers (e.g. Crossler et al., 2013; Karjalainen, 2011; Siponen and Vance, 2013). Son (2011) has shown that intrinsic motivation, such as value congruence, explains employees' compliance more effectively than security measures that are rooted in extrinsic motivations such as sanctions. Thus, in terms of information security, it is necessary to recognise different goals and values (i.e., rationalities) as important factors when analysing the reasons for non-compliance (Albrechtsen, 2007; Kolkowska, 2009; Son, 2011; Vaast, 2007; Besnard and Arief, 2004). According to these scholars, tensions exist between the values prescribed in information security policies and those that are actually in use.

Kirlappos et al. (2013) and Hedström et al. (2011) have argued for an alternative to the prevailing centralised and uncontextualised "command-and-control" approach to managing employees' information security behaviour. According to them there is a need for an approach that balances organisational goals (e.g., productivity goals) with those of information security management. Currently, the prioritization of different rationalities is left to individual employees (Kirlappos et al., 2013), thus risking security breaches. To improve compliance, information security management needs to understand the different rationalities that come into play in relation to information security (Besnard and Arief, 2004; Mishra and Dhillon, 2006; Renaud and Goucher, 2012; Vaast, 2007). Consequently, information security managers need methodological support to analyse and understand the different rationalities that exist in their organisations. Such support would help them to improve the alignment of information security policies with the organisation's work practices (Hedström et al., 2011).

Many studies have used existing approaches to analyse employees' compliance (e.g. Myyry et al., 2009; Siponen and Vance, 2010; Son, 2011) by examining rationalities related to employees' information security behaviours. However, only a few studies have sought to address the rationality behind the information security policies (e.g. Albrechtsen and Hovden, 2009; Thomson, 2009). Thus, although most compliance studies describe the research method used, few can claim to offer an explicit method that can be used to guide information security managers' efforts to analyse and understand the rationalities behind employees' non-compliance in relation to information security regulations. In order to be a useful tool, an explicit method needs to include not only a clear description of the steps to be taken, but also a set of concepts to create an analytical focus, and a specific form of notation to document the results (Brinkkemper, 1996).

As argued by Kirlappos et al. (2013) and Hedström et al. (2011), few *comprehensive* information security analysis methods (ISAMs) exist which are aimed at supporting information security managers when carrying out a *systematic analysis* of different rationalities in relation to information security within an organisation. Information security managers are therefore not as well informed as they could be when making decisions about resource allocation to counteract security breaches caused by employee non-compliance. The purpose of an ISAM is therefore to provide management with a tool to analyse the current level of security, as well as provide support for prioritising future information security investments (Siponen et al., 2006). For instance, investment decisions are highly dependent on an ISAM's ability to highlight the relevant information security issues.

Against this backdrop, we elaborate on the design of an ISAM, the Value-Based Compliance (VBC) method for analysing different rationalities in relation to information security compliance. This method provides information security managers with a powerful analytical tool to understand why rationality conflicts exist and the impact they have on employees' compliance. We hope that this tool offers an improved basis for strategic decision making on investment in information security by pointing towards more efficient security solutions that are better aligned with organisational goals and practices. Such solutions can change bad practices by creating better information security policies and work procedures. Ultimately, the VBC method can act as a tool that changes the management of employees' information security behaviour.

This paper is organised as follows. The next section presents an overview of related research. This is followed by a section on our design science research approach. The next two sections are devoted to the VBC method. The first of these covers the method itself, whilst the second reports on the lessons learned from using the VBC method in two hospital cases. This is followed by a discussion section in which we address the implications for practice and research. Finally, we present a short conclusion.

2. Related research

The proposed ISAM needs to be based on a theory that acknowledges the existence of several competing rationalities in an organisation. The Value-Based Compliance theory (Hedström et al., 2011; Karlsson and Hedström, 2008) takes a pluralistic perspective on rationalities in organisations. Thus, employees do not simply serve as the instruments of a particular rationality promoted by one category of managers, such as information security managers. Instead, the VBC theory assumes that employees base their actions on different types of rationalities when complying or not complying with information

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

security policies. Consequently, this theory acknowledges the existence of clashes between different types of rationalities. In order to assess whether existing research on ISAMs and compliance takes into consideration the key concepts of the VBC theory we suggest four method requirements based on three complementing kernel theories: the theory of organisational learning (Argyris and Schön, 1996) social action theory (Weber, 1978) and the theory of tacit knowledge (Polanyi, 1983).

2.1. Value-Based Compliance theory

The VBC theory (Hedström et al., 2011; Karlsson and Hedström, 2008) consists of a set of concepts. These concepts are depicted as Unified Modelling Language classes in Fig. 1: information security action (prescribed and actual), actor, goal, and value. The way in which these classes are associated with each other is illustrated through a number of named associations. The VBC theory draws on the theory of organisational learning (Argyris and Schön, 1996) and social action theory (Weber, 1978). According to the latter, all types of information security actions (ISAs) are considered as social actions (Hedström et al., 2013). Consequently, an ISA is always associated with one or several actors. Information security managers design the rules (prescribed ISAs), whilst employees put them into practice (actual ISAs). This distinction is in line with the theory of organisational learning (Argyris and Schön, 1996), and is an operationalisation of the "espoused theory" and "theory-in-use" concepts. Argyris and Schön (1996) argued that actors, such as employees, enact and realise the explicit action strategies of organisations, such as information security policies, rules, and guidelines. However, they adapt these action strategies to fit current situations based on their situational and local knowledge; thus, compliance or non-compliance may occur (illustrated by the compliance association between actual and prescribed ISAs in Fig. 1). Hence, Argyris and Schön (1996) led us to the first method requirement (MR1): *to capture the difference, if any, between prescribed and actual ISAs*.

The key feature of the VBC theory is the attention it pays to the rationale behind prescribed and actual ISAs and *why* an actual action differs from a prescribed action. According to Weber (1978), it is possible to distinguish between two types of social actions: rational and non-rational. However, it is only possible to identify goals related to rational actions. A prescribed ISA, such as an instruction in an information security policy that forbids the sharing of passwords, is the result of a goal-oriented design activity. Hence, it is the result of a rational action. In such an activity, specific design goals are set out (Friedman, 2003). In Fig. 1, these goals are represented as the "design rationale". They are anchored in the underlying information security values of the information security manager responsible for design. This is illustrated as "value rationale".

Weber (1978) distinguished between two types of rational actions: instrumental and value-oriented. Instrumental actions are based on a means-end calculation, where the actor has to accept "given realities and choose a preconceived means to achieving a particular end" (Hedström et al., 2013). For example, an employee's decision to share a password, which leads to non-compliance, may be based on an efficiency goal and value, where the employee wants to reduce the time spent logging on and off the system. Value-oriented actions, on the other hand, are anchored in a context-specific value system. Thus, instead of accepting given realities and choosing from preconceived means, an employee justifies an action by

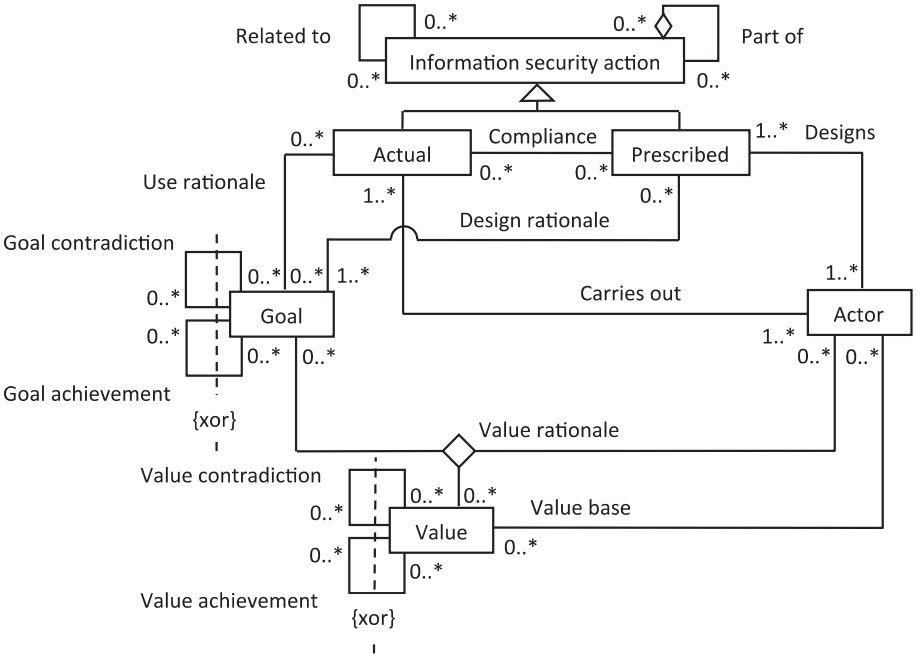

Fig. 1. Value-Based Compliance theory (Hedström et al., 2011).

appealing to a specific value system (Kalberg, 1980). One such example is how university personnel anchor their "right" to freely install software on their computers in the value system of "scientific freedom". According to Weber (1978), these actions are important in themselves, irrespective of the consequences.

An employee's actual ISA can be either rational or non-rational, as shown by the "use rationale" association in Fig. 1. In the case of a rational action, the employee anchors it in one or more goals. As is shown in Fig. 1, the goals that lie behind rational actions can either support or contradict each other; a similar pattern exists for values. Hence, the VBC theory shows potential clashes between the rationalities that underlie prescribed and actual ISAs. Consequently, Weber's (1978) theory of social action led us to the second method requirement (MR2): *to capture the rationale behind prescribed and actual ISAs as (a) goals and (b) values*.

When it comes to non-rational ISAs, it is not possible to identify a "use rationale" or "value rationale" linked to these actions, i.e., they are not associated with any goals or values. Weber (1978) distinguished between two types of non-rational actions: traditional actions and affectual actions. The former "are based on deeply rooted habits, where the actor does not reflect on or even remember why the action is carried out" (Hedström et al., 2013). The latter are linked to the emotional condition of employees. None of these action types involve a rational mental process when carried out, which has a practical management implication: rational and non-rational actions may need to be approached differently in order to mitigate breaches from these actions (Karjalainen, 2011). This led us to the third method requirement (MR3): *to distinguish between rational and non-rational ISAs*.

In addition to the three requirements above, we identified a fourth method requirement (MR4): *the method needs to uncover the tacit dimensions of an ISA in order to convert unarticulated ISAs into articulated ISAs*. This requirement is based on experiences from our empirical work, where we found that it can be difficult for employees to describe everyday work practice and information-handling activities, and, as a consequence, their ISAs (see the section on Lessons learned from applying the Value-Based Compliance Method). Polanyi (1983) has explained how knowledge has a tacit dimension, where tacit knowledge can be "something hidden, which we may yet discover". Thus, it is important to consider tacit as well as non-tacit knowledge in the analysis of rational and non-rational ISAs in order to embrace all dimensions of knowledge in the analysis. Unarticulated ISAs can include tacit knowledge, as well as non-tacit knowledge not previously expressed. Actions, more often than not, embody tacit knowledge. Tacit knowledge is often based in experience and know-how, where observations together with dialogue are one way of capturing this dimension of knowledge. Polanyi (1983) wrote that "[...] we know more than we can tell [...] but that does not mean that we are unable to communicate what we know, given the means to do so". This has a bearing on the type of data collection chosen, because actions can be difficult to describe, remember and recount in detail (e.g. in an interview situation), making observation a valuable source for data collection.

2.2. Existing methods to analyse employees' compliance

In total, we reviewed 54 compliance studies (see Appendix A for how the literature search was carried out) in order to investigate how these studies carried out an analysis of different rationalities in relation to information security within an organisation. We used the four method requirements described in the previous section as our analytical lens. A detailed analysis of existing methods is presented in Table B1 in Appendix B. Below, we present an overview of this analysis.

The existing methods were grouped into four categories. The first category includes traditional ISAMs: checklists and standards. The second addresses methods for minimising computer abuse. These studies are based on the belief that extrinsic motivations, such as coercion and sanctions, have a significant impact on compliance and non-compliance (Parker, 1981). Our third category relates to methods for understanding information security compliance. These studies share the argument that problems associated with non-compliance can be overcome by understanding the reasons for a particular employee's behaviour. Finally, the fourth category focuses on methods for creating a compliance-friendly environment. According to these studies, compliance can be improved if employees internalise information security values in their daily work practices (Thomson, 2009).

2.2.1. Traditional information security analysis methods

Employees' ISAs appear to be a central aspect of compliance studies. However, existing research shows that ISA is not a clear-cut concept. Traditional information security methods (e.g. GASSP, 1999; ISO, 2013) place the emphasis on management's perception of employees' actions, rather than employees' actual actions. Such a perception may be related to the fact that data collections are often based on surveys or interviews with managers. Methods in this category do not capture the goals or values the lie behind identified ISAs.

2.2.2. Methods for minimising computer abuse

Methods for minimising computer abuse tend to focus on intentionally malicious ISAs, such as the abuse or misuse of computers. According to these methods, employees' malicious actions may be discovered accidentally or by detective activity (Straub and Nance, 1990). In this category, employees' intended ISAs are commonly investigated through surveys (e.g. Lee et al., 2004; Hu et al., 2011; Hovav and D'Arcy, 2012). Furthermore, in a number of survey studies it was only managers who were asked about employees' malicious behaviours (e.g. Straub, 1990; Straub and Nance, 1990).

Also within this category are studies (D'Arcy and Hovav, 2007b, 2007a; D'Arcy et al., 2009; Hu et al., 2011) that examined employees' intentions for misuse using scenarios. Consequently, studies in this category either look at management's

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

perception of employees' ISAs or at the employees' perception of their ISAs. These studies do not focus on the rationalities that underlie information security policies or employees' actual ISAs; in other words, they do not consider the goals or values that form the basis of these actions.

2.2.3. Methods for understanding information security compliance

Most methods for understanding information security compliance capture employees' ISAs or intentions to act using questionnaires and/or questionnaires using hypothetical scenarios. These studies measure employees' perceptions of their ISAs and/or their intentions to comply with policy (e.g. Siponen and Vance, 2010; Pahnila et al., 2007a). These perceptions or intentions to act may differ from actual ISAs. An exception among these is a study by Rhee et al. (2009), in which actual ISAs were systematically investigated. A significant number of studies in this category are not focused on specific ISAs, but rather on a general intention to comply with organisational information security policies or actual compliance with such policies (e.g. Bulgurcu et al., 2010; Chan et al., 2005; Herath and Rao, 2009a; Pahnila et al., 2007a). A few studies (e.g. Adams and Sasse, 1999; Albrechtsen, 2007; Huebner and Britt, 2006; Karjalainen, 2011) used interviews to identify employees' ISAs; however, the methods in these studies do not support a systematic analysis and comparison of prescribed and actual ISAs.

Most studies in this category focus on the reasons for employees' compliance and non-compliance in an attempt to find out why people act in a certain way. Few researchers have explicitly focused on the goals and values that underlie these actions. One notable exception is a study by Myyry et al. (2009). These scholars proposed a model for the way in which different value priorities are related to compliance actions. Son (2011) studied how value congruence and legitimacy influence employees' compliance. Albrechtsen (2007), Besnard and Arief (2004), and Huebner and Britt (2006), have also discussed behaviours, values and goals to varying degrees. However, none of these studies focused explicitly on methodological aspects; thus, they fall short on how to capture and track these concepts.

2.2.4. Methods for creating a compliance-friendly environment

Regarding methods for creating a compliance-friendly environment, their emphasis is often on the importance of value correspondence and the cultivation of an information security culture. However, the methods themselves do not support the capture of ISAs; nor do they distinguish between prescribed and actual ISAs. According to these studies, compliance can be improved if employees internalise information security values in their daily work practices (e.g. Thomson et al., 2006; Vroom and von Solms, 2004). Hence, these studies focus on the rationality that underlies employees' ISAs. Many focus on information security culture using Schein's (1999) model of organisational culture (e.g. Da Veiga and Eloff, 2010; Thomson, 2009; Thomson and von Solms, 2006; Vroom and von Solms, 2004).

The methodological limitation of these studies is that they do not incorporate the data collection techniques needed to populate the suggested conceptual frameworks. One exception is a study by Schlienger and Teufel (2003). Here, the scholars used questionnaires, interviews, document analysis and auditing to collect data about information security culture according to Schein's (1999) organisational culture model. However, their study focused on employees' values related to prescribed ISAs, and did not captured rationality behind employees' actual ISAs.

2.2.5. Summary – existing methods

Only a few studies (Karjalainen, 2011; Stanton et al., 2005) have stressed the importance of differentiating between various kinds of employees' non-compliant ISAs and the importance of approaching these kinds of actions in different ways. Vance et al. (2012) and Pahnila et al. (2007a) studied unconscious ISAs, such as habits, which are performed without a conscious decision to act. These scholars concluded that habits have a significant influence on compliance. However, none of these studies have offered any methodological support for distinguishing between conscious and unconscious types of ISAs.

To date, compliance studies have only weakly supported the conversion of unarticulated ISAs to articulated ones. In addition, existing studies lack the ability to trace both the rationale (i.e. goals and values) that underlies employees' ISAs and the rationale behind information security policies. Consequently, existing methods do not provide the necessary support to gain an understanding of the different rationalities that come into play in relation to information security in organisations.

3. Research design

The aim of this research is to develop the VBC method and solve a practical problem: the lack of ISAMs for analysing the different rationalities associated with employees' information security compliance or non-compliance. Consequently, the aim is to change the toolbox available to information security managers. Thus, the research approach applied in this study can be characterised as design science research (DSR) (Hevner et al., 2004). Our research process was structured according to the DSR process model put forward by Peffers et al. (2008). According to this model, DSR cycles contain six phases: (1) problem identification, (2) requirements elicitation, (3) design and development, (4) demonstration, (5) evaluation and (6) communication.

The study is carried out in three different organisations during six DSR cycles, of which the final two cycles are presented in this paper. Although our study indicates the usefulness of the VBC method, we do not claim that our findings are valid beyond the cases investigated. Indeed, some researchers have argued for the use of a nomothetic approach, because case

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

studies are seen to be too context-specific to offer the possibility of generalisation (Benbasat et al., 1987). However, in order to evaluate the VBC method's usefulness we needed to apply the method in real settings, similar to those in which it will be applied in future. Here, case studies provide such settings (Yin, 1994), making case study-based research a relevant choice when combined with DSR.

3.1. Design science research process in this study

The complete research process spanned eight years, from 2004 to 2012. The first four DSR cycles covered the years 2004–2007 and the intermediate results from these cycles were published earlier (Kolkowska, 2005, 2006, 2009, 2011; Kolkowska and De Decker, 2012), along with a description of the VBC theory (Hedström et al., 2011). The fifth and sixth DSR cycles took place between 2008 and 2012 and included a redefinition of the VBC method, the VBC theory and the design principles.

DSR cycle 5 (spring 2008 – spring 2009) and DSR cycle 6 (autumn 2009 – winter 2012) were carried out at a Swedish emergency hospital in central Sweden. The hospital serves approximately 90,000 citizens. Two clinics at the hospital were chosen as cases based on the extent to which their patient information was computerised: the surgical clinic practiced manual handling of medical records, while the medical clinic used an electronic medical record (EMR) system. This variety was important for demonstrating the VBC method in both light and heavy computerised settings. The research process of DSR cycles 5 and 6 is summarised below, structured according to the six phases put forward by Peffers et al. (2008).

3.1.1. Phase 1: Problem identification

The lessons learned from DSR cycles 1–4 were used as the starting point for the fifth DSR cycle; lessons learned from the fifth cycle were fed into the sixth, final DSR cycle. During DSR cycles 5 and 6 the main problem was defined as follows: How do we design a method to support information security managers' analysis of the multiple rationalities that come into play in an information security practice?

3.1.2. Phase 2: Requirements elicitation

In the second phase we derived the VBC method's requirements from the problem definition, the VBC theory and the lessons learned. Three method requirements were elicited during DSR cycle 5 and another one was elicited during DSR cycle 6 (see the section on Value-Based Compliance Theory).

3.1.3. Phase 3: Design and development

During the third phase we designed the VBC method based on the kernel theories. Moreover, we carried out updated literature reviews on ISAMs and compliance research to inform our design (see Appendix A for details). As described in the section on Value-Based Compliance Theory, we used social action theory (Weber, 1978) and the theory of organisational learning (Argyris and Schön, 1996) as a starting point for our design of the VBC method. Based on these two theories, three design principles were defined to meet the method requirements for the redesign of the VBC method in DSR cycle 5:

(1) The principle of espoused theory and theory-in-use. The method should explicitly support an acknowledgement of the differences that exist between: (a) prescribed ISAs and (b) actual ISAs.
(2) The principle of rational and non-rational ISAs. The method should support the distinction between: (a) instrumental and value-oriented ISAs and (b) traditional and affectual ISAs.
(3) The principle of information security rationale. The method should explicitly support the capture of: (a) ISAs, (b) goals, and (c) values.

During the fifth DSR cycle, we identified the need to convert non-articulated ISAs into articulated ISAs; this need was addressed during DSR cycle 6. The theory of tacit knowledge (Polanyi, 1983) was used to define the fourth design principle for the redesign of the VBC method:

(4) The principle of tacit knowledge. The method should explicitly support the conversion of non-articulated ISAs into articulated ISAs.

3.1.4. Phase 4: Demonstration

In the fourth phase, the current version of the VBC method was demonstrated to assess the method's ability to support an analysis of different rationalities in relation to information security. During DSR cycle 5 we carried out the demonstration at the hospital's surgical clinic, and during DSR cycle 6 at the hospital's medical clinic. In both cases the demonstration focused on information security related to patient information, because treating patients is the hospital's main activity. We collected data during the demonstration, as prescribed by the current version of the VBC method. See Appendix C for details about the data sources.

3.1.5. Phase 5: Evaluation

During the evaluation phase, we evaluated the ability of the method to support the analysis of the different rationalities in relation to information security. The following data sources were used during evaluation: (1) The project members'

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

experiences from using the method in the demonstration, together with feedback from the research community on publications, (2) Notes from design workshops, with a focus on the analysis of the collected material, and (3) Panel discussions with members of the studied organisations, with a focus on the results of the analysis and the main concepts. Two expert panels were convened in relation to the fifth DSR cycle and two in relation to the sixth DSR cycle. One of the expert panels consisted of administrative staff, physicians, and nurses from the clinic (in total, five experts). The second expert panel consisted of four high-level managers at the county council level. All panel participants received results from the analysis before the discussions so that they were able to reflect on the results and prepare questions. The discussions with the experts were structured around the method requirements. The results are presented in the section: Lessons learned from applying the Value-Based Compliance method.

3.1.6. Phase 6: Communication

During the last phase of each cycle the results were presented at several workshops to both researchers and practitioners. For example, the final method was presented at a workshop organised by the Swedish Civil Contingencies Agency to which Swedish information security researchers were invited. The method was also presented to information security managers at a conference organised by the Swedish Standard Institute. Approximately one hundred practitioners participated in the conference. A practitioners' version of the VBC method was published at informationssakerhet.se, a website managed by the Swedish Civil Contingencies Agency, and which is aimed information security practitioners.

We received many positive comments on the results from both practitioners and researchers. For example, practitioners from the health care sector recognised the problem situations and gave us positive feedback on the results. The VBC theory developed during the fifth and sixth DSR cycles was communicated to the research community in a study by Hedström et al. (2011). The final version of the VBC method, used during the sixth DSR cycle, is published in this paper.

4. The Value-Based Compliance method

This section is a hands-on description of the VBC method. In relation to each step we also present examples of the method's demonstration in the hospital setting. Hence, we show snapshots of our empirical grounding. The VBC method consists of nine steps, as illustrated in Fig. 2.

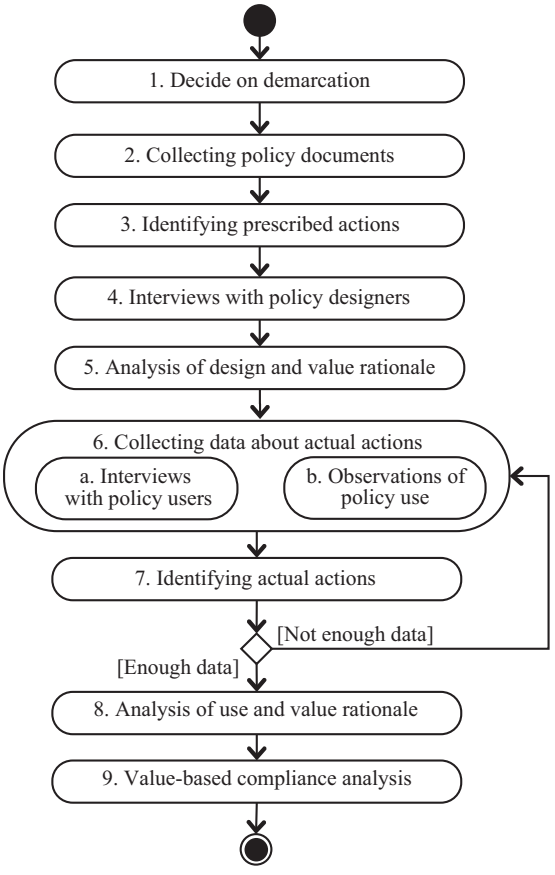

Fig. 2. The Value-Based Compliance method.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

4.1. Step 1: Decide on demarcation

This step is aimed at determining the project's scope. First, the team members have to select those aspects of information security that should be in focus. This step is carried out by:

(a) defining what the project team means by information security;
(b) defining the organisational boundaries of the study;
(c) informing employees affected by the project.

For example, during our demonstration at the hospital we decided to focus our study on information security aspects that are related to patient information because treating patients is the hospital's main activity. In addition, we used the county's overall definition for information security as our working definition, and subsequently as the demarcation for our analysis: "Correct information to the right people, right on time, and to the right place". The organisational boundary for the study consisted of the hospital's medical and surgical clinics.

4.2. Step 2: Collecting policy documents

This step is aimed at collecting background material on the prescribed ISAs. By the end of this step, a set of information security documents will have been collected; these documents relate to the management of information security in an organisation.

Documents should be collected within the project's demarcated boundaries. These official documents for information security management can exist on several levels. They can include policies, rules, guidelines and instructions. Such documents can be found by asking managers and users in the organisation the following question: "What documents are used to manage information handling here?"

When we applied the VBC method at the two clinics, a number of relevant information security documents were collected. These regulate information security practice (e.g. information security policy, IT strategy and routines for handling medical records) at the county council level as well as at the hospital level. From the start of the project, we chose information security policy as the main source for identifying information security rules. The other documents were suggested during interviews with information security managers and also during interviews with health care staff. The health care staff suggested documents that were used to manage information and information security at the clinics. See Appendix C for a list of all the reviewed documents during our two cases.

4.3. Step 3: Identifying prescribed actions

This step is aimed at creating a list of prescribed ISAs based on the collected policy documents. A prescribed ISA is one that regulates the handling of information and information assets, including what one is allowed or not allowed to do with this information. During the operationalisation of ISAs it is necessary to acknowledge that prescribed ISAs in the policy documents have different granularity and exist on various levels. Hence, abstract and detailed descriptions about the same ISA are grouped together in order to reduce the number of action statements that need to be worked on in the on-going analysis.

At the hospital, the prescribed ISAs were described in terms of different granularity and on different levels in the various documents. Thus, it was necessary to group together similar ISAs. During our demonstration, approximately 200 prescribed actions were identified at each clinic; these were categorised into 25 groups at the surgical clinic and into 36 groups at the medical clinic. For example, one group was related to prescribed ISAs on the secure handling of passwords, while another was related to actions on the secure handling of patient information. Table 1 illustrates how prescribed ISAs were identified from the documents during our demonstration.

4.4. Step 4: Interviews with policy designers

This step is aimed at deepening the understanding of policy design and the design rationale. Hence, the focus of the interviews is on: (1) the goals that the policy designers want to achieve with the prescribed ISA and (2) why these goals are important and the values on which they are based. In addition, the interviews are used to verify the importance of the actions elicited. In this step, the list of prescribed ISAs identified in the previous step, is used as an information source for the interviews.

First, it is necessary to clarify the purpose of the interviews and explain what is meant by information security. Such clarification is carried out in order to determine the scope of the interview. After defining the scope, the process of identifying the design rationale can begin; goals and values found in the policy documents are used as a starting point.

Policy documents and the prescribed ISAs they include are viewed as the chosen design from among a range of alternatives in the design process. Questions are thus asked about why certain prescribed ISAs are included, and what influenced the design. In doing so, it is possible to identify goals and values, as well as associations with standards, professional practices and legislation. The identification of associations with other information sources is important if one is to elicit further goals

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

Table 1
Example of the identified prescribed ISAs and analysis of design and value rationale.

Prescribed ISA	Source	Goal	Value
p1. "Medical records should be handled and kept so that unauthorised people cannot access them."	s1. Routines for handling manual medical records s2. Routines for using EMRs	g1. To protect patient information against disclosure	v1. It is important that patient information is confidential
p2. "Information concerning a patient's social, medical and other sensitive information must be carefully protected against disclosure."	s3. Information security policy		
p3. "Medical records [paper] shall be kept in a locked box or document cabin. Documents in use can be kept in a binder at the nurses' office."	s1. Routines for handling manual medical records		

and values. The interviews are conducted as semi-structured interviews, and are ordered according to the prescribed ISAs. The interviews should be recorded to bring traceability to the data during analysis.

When demonstrating the VBC method at the two clinics the information security managers were asked to explain the rules, what they wanted to achieve with a specific rule, and why they had chosen to work with that specific rule. For example, the information security manager explained that p1 (''Medical records should be handled and kept so that unauthorised people cannot access them") was included in the hospital's routines (s1) because it is important to protect patient information against disclosure (see Table 1). The protection of patient information is emphasised in the Patient Record Act and in the Secrecy Act, and Swedish hospitals have to comply with both pieces of legislation. Each interview lasted approximately two hours, and was recorded and subsequently transcribed. A list of all interviewees can be found in Appendix C.

4.5. Step 5: Analysis of design and value rationale

This step is aimed at elaborating the design and value rationale of the prescribed ISAs. Goals and values are elicited from the collected documents and from the interviews with information security policy designers by paying attention to the areas in which the prescribed ISAs are explained. To find goals and values in the collected material, particular attention should be paid to actions or words that show approval or disapproval, actions intended to achieve a certain goal or result, and actions showing a consistent tendency to choose a specific direction. The analysis results in a list of: (a) goals and (b) values. Within each list, similar goals/values are grouped together, and the categories are labelled. Table 1 offers a brief example of the analysis carried out, based on the data collected during our demonstration.

4.6. Step 6: Collecting data about actual actions

The aim of this step is to gather data about the actual ISAs in the organisation. This step consists of two sub steps that are carried out in an iterative pattern: (a) interviews with employees in their role as policy users, and (b) observations of employees in their role as policy users. The step results in a list of actual ISAs.

During an initial interview session the policy users are asked to identify the important tasks they carry out in their daily work. In addition, they are also asked what they want to achieve with these actions and why they see them as important. The aim is to capture the use rationale behind these actions. This interview session is followed by observations. It is valid to carry out these observations after conducting the interviews for two reasons. First, it gives an opportunity to learn more about the workplace before starting the observations. Second, a larger number of people can be observed at the same time, which can be more efficient in organisations in which a lot of teamwork takes place.

The interviews are conducted as semi-structured interviews and are ordered according to the prescribed ISAs identified in previous steps. Each interview should be recorded in order to be able to refer back to the collected data during the analysis.

Eleven semi-structured interviews were carried out with health care staff during our demonstration at the surgical clinic. Thirteen interviews were carried out at the medical clinic. Each interview lasted between one and two hours. A list of the interviewees is presented in Appendix C. The interviews were recorded and transcribed. They were complemented by observations of information security practice in the medical clinic. We observed daily health care work at both clinics over the course of seven days (four hours of observation/day).

4.7. Step 7: Identifying actual actions

This step is aimed at creating a list of actual ISAs. An actual ISA is an action that is carried out by the policy user, during which he or she handles information as part of their daily work. These actions can be identified in the collected data (transcribed interviews and notes from the observations). As with prescribed ISAs, policy users can describe actions with different granularity. Hence, in this step, abstract and detailed descriptions of the same ISA are grouped together in order to reduce the number of action statements that require on-going analysis.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

During the demonstration, we identified approximately 350 actual ISAs at the surgical clinic and 360 at the medical clinic. Table 2 illustrates the kind of actions that were identified during interviews and through observations.

4.8. Step 8: Analysis of use and value rationale

This step is aimed at identifying the use and value rationale associated with actual ISAs. During this step, goals and values are derived from the reasons that underlie the actual ISAs. First, actual actions are identified by reading through staff interview transcripts and notes from the observations. Then, values and goals that relate to these actions are derived from the collected data. To find goals and values in the collected data, attention is paid to approvals or disapprovals of rules and actions that show a consistent tendency to choose a specific direction. The analysis results in a list of: (a) goals and (b) values associated with actual ISAs. Within each list, similar goals/values are grouped together, and the categories are labelled.

During this analysis, it might not be possible to identify a use and value rationale behind an ISA. In this situation, it is necessary to investigate the action further to find out if the action is non-rational, i.e., traditional or affectual. More interviews might be needed to identify corresponding goals and values. If after additional interviews it is still not possible to find values and goals that are consciously acted on behind the actual ISA, the action is classified as non-rational (see, for example, action a5 in Table 2).

Table 2 shows examples from our demonstration of when the hospital staff anchored their actions in three values: efficiency, quality of health care and availability. For example, when we asked the nurses why they used paper notes to record sensitive patient information (a1), they explained: "We have new patients and new ordinations every day so we do not have time to read all information in the medical record [digital]. We want to ensure individual efficient care for each patient, because of that we use paper notes."

All identified values were structured into value categories. Nine value categories were identified in relation to actual ISAs: awareness, integrity, confidentiality, availability, traceability, privacy, quality of health care, efficiency, and self determination.

4.9. Step 9: Value-Based Compliance analysis

This step is aimed at analysing the rationale behind compliance and non-compliance. Compliance analysis is carried out in two parts. First, the prescribed and actual ISAs are compared in order to find compliance and non-compliance situations. Then, a comparison is made between the rationality (values and goals) that underlies the prescribed ISA and the actual ISAs. In this way, it is possible to distinguish between the goals and values (rationality) that underlie prescribed ISAs and actual ISAs. Since individual actions are related to goals and values it is possible to analyse the rationale behind compliant and non-compliant ISAs.

The graph shown in Fig. 3 illustrates value conflicts relating to the routines that protect patient information at the hospital. The prescribed actions (p1, p2, p3) ensure that only authorised people have access to patient information (g1). The prescribed actions, which are related to protecting patient information, state that patients' information must be carefully protected (p1, p2). Among other things, this means that paper medical records should be kept in locked document cabinets (p3).

Table 2
Example of actual ISAs and of analysis of use and value rationale.

Actual ISA	Source	Goal	Value
a1. The nurses use paper notes that include sensitive information about the patients, selected from medical records	s4. Observation at the medical clinic	g3. To be efficient g4. To ensure individualised care	v3. It is important to be efficient (efficiency). v4. It is important to ensure high quality of health care (quality of health care)
a2. "In the evening, before closing, medical records for patients coming for consultation the next day are put on the desk."	s5. Interview with nurse at surgical clinic	g3. To be efficient	v3. It is important to be efficient (efficiency)
a3. Lists containing sensitive information [names, security numbers] about patients coming for consultations during the day were put up on the wall	s4. Observation at the medical clinic	g2. To have easy access to information	v2. It is important to have easy access to information (availability)
a4. "We put the medical records in a special place close to the fax machine. It is not possible to lock this room."	s5. Interview with nurse at surgical clinic	g2. To have easy access to information	v2. It is important to have easy access to information (availability)
A5. Emergency alarm goes off. A nurse working with a medical record runs out. The computer stays logged on with the medical record on the screen	s4. Observation at the medical clinic	–	–

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

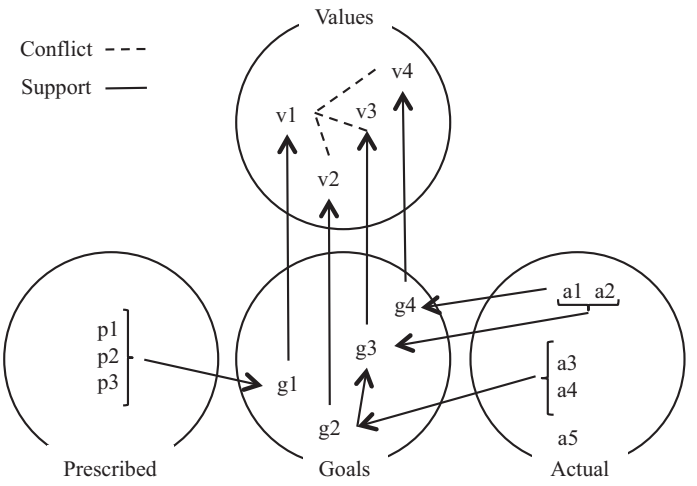

Fig. 3. Value conflicts regarding the protection of patient information.

The graph illustrates how hospital employees' ISAs (a1–a5) came into conflict with prescribed ISAs that were designed to protect patient information. We observed lists containing sensitive patient information being put up on the wall (a3). Hospital staff also put paper medical records on the desk, where they were visible (a2), as well as beside the fax machine, even though it was not possible to lock the room (a4). We also found that nurses wrote patient information on small notes that they kept in the pockets of their uniforms (a1). Finally, computers were left logged on when nurses rushed off to attend emergency situations (a5). As a consequence, there was a risk that unauthorised people could access patient information on several occasions, which is in conflict with prescribed rules (p1, p2, p3).

In their daily work, health care professionals have to spend as much time as possible with the patients and ensure high quality (individualised) care. Consequently, it is time consuming to log on and read an EMR every time the nurse needs to take care of a specific patient. It is considered much more efficient to look at a paper note that gives a summary of the most important information about the patient. In our case, the nurses wrote small paper notes in order to have easy access to patient information (g2), because, in this setting, it is important to be efficient (g3) and to ensure high quality (individualised) health care (g4).

At the hospital, it is very important to protect patient information in order to ensure confidentiality (v1). However, for health care staff three values were revealed as being important: availability of information (v2), efficiency (v3), and high quality care (v4). The pressure to treat as many patients as possible and the lack of technical solutions to support the prescribed ISAs means that staff felt justified in developing their own information-handling routines. As in the example above, the medical records can only be accessed from desk top computers located in special rooms; meanwhile, the nurses work in another part of the ward, taking care of patients. It is seen to be important to spend as much time with patients as possible and to offer individualised health care; thus, the nurses need easy and efficient access to patient information. To be able to do this, they use paper notes. They would not need to use paper notes if they could access information in the EMRs using, for example, mobile devices. This example illustrates how information security values that are based on the design rationality of information security management come into conflict with health care values that are based on the use rationality of the health care practice, as seen by the health care staff.

5. Lessons learned from applying the Value-Based Compliance method

In this section we present lessons learned from demonstrating the VBC method in the hospital setting. The section is structured according to the four method requirements (MR) presented in the section: Value-Based Compliance theory.

5.1. MR1 - the method needs to capture the difference, if any, between prescribed and actual ISAs

The VBC method supports the identification of both prescribed and actual ISAs. Prescribed ISAs were identified through documents, while actual ISAs were identified through observations and interviews. We identified approximately 550 ISAs (both prescribed and actual) at the surgical clinic and approximately 560 ISAs at the medical clinic. As shown in the examples, prescribed ISAs both restrict and guide information security practice at the hospital (e.g. "Medical records should be handled and kept so that unauthorised people cannot access them" and "Do not borrow passwords").

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

The VBC method supports the identification of actual ISAs through interviews with policy users and observations of information security practice. A mix of interviews and observations offered effective support for the identification of actual ISAs. It was clearly the case that actions identified from the interviews sometimes did not correspond to actions observed. This means that our respondents sometimes told us how they should behave and not how they actually behaved. For instance, one respondent told us: "We always lock up the medical records [paper] when we do not use them". However, we could observe that patients' medical records (paper-based records) were often left in unlocked rooms, even when no one was sitting in these rooms. Thus, observation served to verify our hypotheses on non-compliance.

By comparing the prescribed ISAs and the actual ISAs, we were able to identify both compliance and non-compliance situations. For example, we identified compliance with prescribed actions on how to make copies of medical records and how these actions were to be carried out. One part of the prescribed ISAs states that: "You must document to whom you send a copy of the medical record". Our observations and one of the interviewees confirmed this procedure in practice: "It must be clearly documented where you send it [the medical record] and why". Several examples of non-compliance were illustrated in the previous section.

5.2. MR2 - the method needs to capture the rationale behind prescribed and actual ISAs as (a) goals and (b) values

In relation to MR2 we focused on how the VBC method supports an analysis of the rationality that underlies prescribed and actual ISAs. The VBC method supports such an analysis. By following this method, ISAs can be associated with goals and values. These goals and values can then be traced back to actions in compliance and non-compliance situations, thus making it possible to compare rationalities in these situations.

Above, we exemplified compliance through actions that prescribe how medical records should be copied and the way in which these actions are carried out. When tracing the goals we found that the prescribed ISA is based on the Swedish Patient Data Act. The protection of patient information against disclosure is an important goal in Swedish hospitals; it can be traced back to a confidentiality value ("It is important that patient information is confidential"). When we studied compliance in hospital settings, we found that, in relation to copying and sharing medical records, the policy users were aware of and shared this value. Examples of rationality conflicts behind non-compliance have been given in the previous section. The VBC method allowed us to identify a number of value conflicts at the two clinics (a total of nine conflicts at the surgical clinic and ten at the medical clinic) that could explain the identified non-compliance situations.

During discussions at an experts' panel, the participants told us that identifying the rationale behind non-compliance situations helped to increase their understanding of these actions. One high-level manager said: "I thought that non-compliance was always an expression for ignorance and carelessness, I did not realise that users actually have a solid reason for why they do not comply". Hence, the results from using the VBC method created a deeper understanding of the rationality of non-compliance.

5.3. MR3 - the method needs to distinguish between rational and non-rational ISAs

The VBC method allowed us to identify actual ISAs that are non-rational. As discussed earlier, such actions are not associated with any goals or values. Thus, it is not possible to identify any use rationale; nor is it possible to carry out a value conflict analysis on these actions, because there is no rational explanation behind them. However, the analysis can still reveal important information about these non-compliant behaviours. Following the VBC method, we were able to identify several examples of actions that could not be associated with any goals or values. These actions are often based on tradition or emotional stress.

For example, we could observe that when an emergency alarm sounded, nurses working with medical records ran out of the room, leaving the computer logged on with the medical record on the screen (a5). This was a non-compliant action (violation of p2) that left patient information at risk of disclosure or uncontrolled changes. From our analysis, we learned that hospital staff were aware of the rule and shared the rationality behind this rule; however, in such a stressful situation they acted effectually. This means that, in all probability, the information security risk related to this situation could not be reduced through the use of additional awareness programs because this action was non-rational. In this situation, the best solution would be to install an automatic log-off system.

5.4. MR4 - the method needs to uncover the tacit dimensions of an ISA in order to convert unarticulated ISAs into articulated ISAs

By using observation as a data collection technique we were able to reveal ISAs that no one mentioned during the interviews. For example, at the surgical clinic during the fifth DSR cycle we were able to observe that the computer in the local office was always logged on to the registration system. One person logged on in the morning and the computer stayed logged on all day. At the later interviews, we discussed this observation with the users. When we asked why they had not mentioned this action at the earlier interviews, one nurse explained that she had just not thought about it. Thus, we realised that some of the actions were not articulated during the interviews because they were deeply rooted habits, and that we should pay more attention to non-articulated actions in the next DSR cycle, when performing step 7.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

The importance of non-articulated ISAs became so significant that we introduced the fourth design principle (the principle of tacit knowledge) to our set of design principles. Consequently, during the sixth DSR cycle we were able to convert more non-articulated ISAs into articulated ones. For example, and as discussed earlier, we discovered that the nurses used paper notes to record patient information. These observations were later discussed during the interviews. When we asked why it had not been mentioned during the earlier interviews, they said that they did not realise that it was important enough to be brought up. According to the nurse it was just "a piece of paper with notes that make the work easier and not a medical record". This modification of the VBC method was important because it made it possible to identify a greater number of non-compliant actions as well as rationality conflicts. These actions would probably have been missed in traditional compliance analysis.

6. Discussion

Employees' lack of compliance with information security policies is a perennial problem for many organisations. Currently, information security managers lack an ISAM to analyse the different rationalities that exist in relation to information security. Below, we discuss the implications of our results on practice and research.

6.1. Implications for practice

Many recent compliance studies (Bulgurcu et al., 2010; Herath and Rao, 2009b; Pahnila et al., 2007b; Son, 2011; Ifinedo, 2012; Hu et al., 2012) have emphasised the importance of considering value congruence, and subjective norms and beliefs in managing the information security behaviours of employees. However, in practice, most organisations still rely on traditional ISAMs. This means that they base their information security management on an outmoded command-and-control approach that promotes the enforcement of information security rules and disciplinary procedures for non-compliance (Hedström et al., 2011). Kirlappos et al. (2013) argued that this occurs because of a lack of alternative approaches for managing employees' security behaviours in practice.

The predominance of the command-and-control approach has a serious consequence when working with employees' information security behaviours. Employees are still seen as the biggest obstacle to information security. In many cases, their security behaviours are directed by poorly designed information security policies (Stahl et al., 2012). Moreover, most methods focus on changing employees' behaviours because they consider these behaviours to be irrational and wrong, while the information security policies themselves are "correct" and unchangeable. However, various studies (e.g. Mattia and Dhillon, 2003; Corbin, 2013) have shown that the inability of policy to reflect current work practices is one of the biggest reasons for non-compliance.

Traditional ISAMs, such as GASSP (1999) and ISO (2013), are easy to access and easy to use; thus, it is not surprising that these methods are still used by practitioners regardless of criticism in the information security literature (e.g. Dhillon and Backhouse, 2001; Kirlappos et al., 2013; Siponen, 2005b). These methods were developed by practitioners and are often formalised in books or other prescribed formats. Usually, tools that support a method's implementation are also available to its users. On the other hand, new ISAMs are usually not as well formalised as traditional ISAMs. Consequently, practitioners find them difficult to use (Siponen, 2005a).

Our research contributes to practice by offering a formalised method for the analysis of compliance and non-compliance. More importantly, however, it enables practitioners to analyse the multiple rationalities that come into play in terms of employees' compliance and non-compliance. In this way, the method can inform management about new "unseen" aspects of information security levels in their organisations and point towards possible alternative solutions and rules. This is evident from the demonstration at the hospital, where the high-level manager realised that the employees had "solid reasons" for their non-compliance. In this case the results from using the VBC method created a deeper understanding of the rationality for non-compliance. Hopefully, it can influence the future design of information security policies at the hospital.

In addition, this research proves that it is possible to devise a method to support a structured analysis of the different rationalities that come into play in information security compliance and non-compliance situations. This is important because, even if a particular organisation chooses not to adopt the VBC method, the very fact that this method has proved useful should encourage any similar endeavour. In such a case, the design principles presented are an important contribution, because they constitute a general point of departure for devising an ISAM similar to the VBC method.

6.2. Implications for research

In the Related research section, we showed that most recent compliance studies have focused on understanding the reasons behind compliance and non-compliance. Many of these studies emphasised the significant role of norms, values and beliefs, which influence employees' compliance and non-compliance (e.g. Albrechtsen, 2007; Myyry et al., 2009; Son, 2011). However, none of them have offered a methodological support for a comprehensive and systematic analysis of the rationality that underlines compliance and non-compliance actions. In other words, they do not act as a guide to carrying out an analysis that focuses on the rationale behind employees' compliance and non-compliance.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

In addition, most of the current compliance research that focuses on the underlying reasons for employees' non-compliance does it without questioning or analysing the rationality behind information security policies (e.g. Huebner and Britt, 2006; Myyry et al., 2009; Son, 2011). In research, design rationale is generally considered as part of information security policy development (Dhillon and Torkzadeh, 2006); however, in such research the employee dimension and user rationale are not considered. Hence, current research gives little practical guidance on how to capture and analyse the different rationalities that come into play in information security compliance. Consequently, current compliance research is hampered because of a lack of analytical tools that can elicit conflicting rationalities. Our proposed ISAM can help researchers explore the conflicting rationalities that exist in an organisation, thus helping to build new theories or refine existing ones.

The VBC method contributes to research by suggesting data collection techniques for actual ISAs. Identifying actual ISAs is seen to be one of the greatest challenges for behavioural information security researchers (Crossler et al., 2013). Most of the traditional ISAMs (e.g. GASSP, 1999; ISO, 2013) identify employees' actions based on questions to IT administrators and high-level managers. Consequently, these methods capture perceptions of actions, rather than actual ISAs. Elsewhere, researchers (e.g. D'Arcy and Hovav, 2007a; Pahnila et al., 2007a; Siponen and Vance, 2010) have studied employees' intended actions or perceived actions using surveys and scenarios. Crossler et al. (2013) concluded that these actions might differ from employees' actual ISAs. According to the VBC method, interviews with policy users can be complemented with observations when collecting data about actual ISAs. Our findings from using the VBC method in practice have shown that, based on multiple data sources, it was possible to capture additional ISAs that would have been missed if only one data collection technique was used. It was also possible to distinguish between rational and non-rational ISAs, which Karjalainen (2011) has put forward as an important analytical distinction in research on employees' compliance. Thus, the VBC method contributes to the field by providing practical guidance on how to improve data collection and the analysis of rational and non-rational ISAs.

Finally, the set of design principles presented also contributes to the research community. These principles can also act as a starting point for further elaboration of the VBC method when devising research tools that are similar to the VBC method.

6.3. Limitations and future research

An obvious limitation in this study's research design is validation. We can conclude that the process and steps included in the VBC method support the systematic analysis of different rationalities in relation to compliance and non-compliance. The method is internally congruent, which means that its concepts and steps are free from ambiguities and are anchored in explicit requirements and design principles. Our review of existing ISAMs and compliance studies shows that the method is also externally congruent; the VBC method builds on and does not contradict existing wisdom in the information security field.

So far, only the method's developers have actually used the VBC method. Thus, there is a risk that the method's success depends on the researchers being present when applying the method in practice. It is therefore necessary to carry out an additional validation of the method, this time under the leadership of people who were not involved in the method's development. However, future method users should be aware that the need for further validation means that it is also necessary to:

(a) find out if policy users are willing to reveal their actual ISAs when information security managers collect the data instead of researchers.
(b) find out if observation is a supportable data collection technique. To date, it has not been frequently used in the information security field. Hence, the effects of using this technique have not been fully explored.
(c) reveal any steps that are insufficiently described. External experts have reviewed the method description and the description of the steps has been found sufficient; however, further use by people other than the method developers may reveal the need for additional details.
(d) determine how and to what extent the method is transferable to other contexts.
(e) evaluate the long-term effects of information security managers using the analytical results of the VBC method for management decision making. This would reveal the true value of the method, as the aim is to create a tool for organisational change. This type of validation would require a longitudinal study, where the VBC method is used at different points in time to identify changes (if any) in policy users' information security compliance.

Given the above limitations, there are ample opportunities for future research. Another future research topic is to develop a computerised tool to support the method. Such a tool is probably a necessity if the VBC method is to be widely enacted by practitioners. Working with the method needs to be both effective and efficient; otherwise, it will not be used in practice. On a general level, such a tool would also improve the quality of the analysis, because it would help to keep track of data.

7. Conclusions

In this paper we have addressed the practical problem of how to analyse the multiple rationales that come into play in an organisation's information security work. Currently, information security managers lack a method for such analyses. To this

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

end, we have proposed the Value-Based Compliance (VBC) method. Our empirical demonstration shows that the method supports a *systematic* analysis of different rationalities in relation to compliance and non-compliance. Thus, we provide managers with a tool that can make them more knowledgeable about *why* employees comply or do not comply with information security policies.

On a more general level, we have also provided a set of design principles; these can be used both by practitioners and researchers to construct similar analysis methods, or extend existing ones. If we were to highlight one design principle that was important for achieving useful analysis in practice, it is the principle of rational and non-rational actions. This principle made us rethink why employees carry out actions in general, and ISAs in particular. In turn, this led us to develop a theoretical framework, the VBC theory, which acknowledges that employees often act according to their own values; such values can have different origins. Within this framework, any improvements to an organisation's information security would require reflection on, and a re-examination of existing rationales in the organisation.

Acknowledgement

This research has been funded by the Swedish Civil Contingency Agency.

Appendix A

A literature review informed each of the design science research cycles. Hence, six literature reviews were conducted during the whole research process in order to keep the design process updated with the current body of knowledge in the area of information security. Five principles guided our searches in the SCOPUS database.

The first principle, which investigates the existence of information security analysis method (ISAMs), focused on identifying methods that support managers with the task of systematically analysing different rationalities in relation to information security within an organisation. Hence, searches based on this principle identified methods that had the potential to solve the existing problem. The keywords used to search for ISAMs were: information security methods, standards, checklists, methods for information security management, frameworks for information security management, information security metrics, security measurement method/model, security evaluation methods, security maturity model and information security management metrics.

The second principle focused on how information security policy compliance has been studied in more general terms. Because of the lack of suitable ISAMs, we took a broader approach to look at existing studies on information security compliance. At the start of the research project such studies were scarce, but the existing body of knowledge in this area has increased over the years. We wanted to look at these studies to see the extent to which ideas used in research studies could be used as input to our design process. The keywords used to search within the area of information security compliance were: information security compliance, policy violations, policy compliance, behavioural aspects within information security, employees' behaviours, and user security behaviour.

The third principle is related to the extent to which the emerging method requirements could be found in ISAM and information security compliance literature. Hence, this principle was driven by the method requirements that we developed and the exact searches depended on the method requirements of the current DSR cycle. During the last two cycles reported on in the paper we used the following keywords in combination with information security: goal, value, tacit knowledge.

The fourth principle is an implementation of Webster and Watson's (2002) "go backward"-principle. Thus, we reviewed the citations for the papers identified by our three first principles to ensure we did not miss earlier research that we felt should be acknowledged in our design process or as reference work.

The fifth principle is the principle of saturation. This means that we stopped our search when we could no longer identify any additional ways of analysing compliance, i.e. additional references did not add anything new to our design work or to our knowledge on existing way of analysing compliance. Based on this principle we ended up with 54 articles in the literature review carried out during the last DSR cycle.

Appendix B

Our analysis of existing research on information security analysis methods and compliance is summarised in Table B1, which contains five columns. The leftmost column shows the reviewed studies, and the remaining columns contain an evaluation of the four method requirements respectively. Three symbols are used to show how the method requirements are supported: "+" means that the method/research supports the method requirement, "–" shows that the method/research does not support the method requirement, while "∗" illustrates that the method/research partly supports the method requirement. With regard to the third method requirement, three letters are used to show which concepts are focused on/supported by the studies/methods: "A" means ISAs, "G" means goals, and "V" means values.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

Table B1
Analysis of existing research on information security compliance methods.

Example of compliance methodology/study	MR1	MR2	MR3	MR4
Category 1: Traditional information security methods				
ISO (2005)	*	*(A)	–	–
GASSP (1999)	*	*(A)	–	–
NIST (2006)	*	*(A)	–	–
Moulton and Moulton (1996)	+	*(A)	–	–
Wood et al. (1987)	+	*(A)	–	–
Category 2: Methods for minimising computer abuse				
Straub (1990)	–	*(A)	–	–
Straub and Nance (1990)	–	*(A)	–	–
Lee et al. (2004)	+	*(A)	–	–
D'Arcy et al. (2009)	+	*(A)	–	–
D'Arcy and Hovav (2007a)	+	*(A)	–	–
D'Arcy and Hovav (2007b)	+	*(A)	–	–
Hovav and D'Arcy (2012)	+	*(A)	–	–
Harrington (1996)	+	*(A)	–	–
Hu et al. (2011)	+	A*	–	–
Category 3: Methods for understanding of information security compliance				
Adams and Sasse (1999)	*	*(A)	–	–
Albrechtsen (2007)	–	*(AGV)	–	–
Besnard and Arief (2004)	–	*(G)	–	–
Albrechtsen and Hovden (2009)	–	*(V)	–	–
Boss and Kirsch (2009)	–	–	–	–
Bulgurcu et al. (2010)	–	–	–	–
Chan et al. (2005)	–	–	–	–
Furnell (2006)	–	–	–	–
Karjalainen (2011)	–	–	*	–
Gonzalez and Sawicka (2002)	–	–	–	–
Herath and Rao (2009a)	–	–	–	–
Herath and Rao (2009b)	–	–	–	–
Hu et al. (2012)	–	–	–	–
Huebner and Britt (2006)	–	*(V)	–	–
Ifinedo (2012)	–	–	–	–
Johnston and Warkentin (2010)	*	*(A)	–	–
Leach (2003)	–	*(V)	–	–
Li et al. (2010)	–	–	–	–
Liang and Xue (2010)	*	*(A)	–	–
Myyry et al. (2009)	+	*(AV)	–	–
Ng et al. (2009)	*	*(A)	–	–
Pahnila et al. (2007a)	–	–	–	–
Rhee et al. (2009)	+	A	–	–
Sasse et al. (2001)	+	*(A)	–	–
Siponen et al. (2007)	–	–	–	–
Siponen and Vance (2010)	+	*(A)	–	–
Siponen et al. (2010)	–	–	–	–
Son (2011)	*	*(V)	–	–
Stanton et al. (2005)	–	–	*	–
Vance et al. (2012)	+	*(A)	+	–
Warkentin et al. (2011)	–	–	–	–
Zhang et al. (2009)	–	–	*	–
Category 4: Methods for creating a compliance-friendly environment				
Da Veiga and Eloff (2010)	–	*(AV)	–	–
Furnell and Thomson (2009)	–	*(AV)	–	*
Ramachandran et al. (2013)	–	*(V)	–	–
Schlienger and Teufel (2003)	–	*(AV)	–	–
Thomson (2009)	–	*(V)	–	*
Thomson et al. (2006)	–	*	–	*
Thomson and von Solms (2006)	–	–	–	*
Vroom and von Solms (2004)	–	*(V)	–	–

Appendix C

Table C1 offers a summary of data collection during the demonstration of the VBC method in the fifth and sixth design science research cycles. The table contains three columns. The leftmost column shows the type of data collection technique. The second column shows the part of the organisation from which the data was collected. The third column shows a description of the specific data collected; for example, if the interview was carried out with a nurse.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

Table C1
Summary of data collection.

Data collection technique	Part of organisation	Description
Documents	Hospital-wide	Information security policy
		Information to county council staff about information security
		Policy for information and communication
		Security instructions for county council IT users
		IT policy
		IT strategy
	Surgical clinic	Routines for handling manual medical records
	Medical clinic	Routines for using the electronic medical record.
		Routines for using Infomedix – an IS for communication between municipalities and the clinic.
Interview	Hospital-wide	1 × Information security manager
		1 × IT manager
		1 × Quality manager
	Surgical clinic	5 × Administrative staff
		1 × Assistant nurse
		4 × Nurse
		1 × Physician
	Medical clinic	5 × Administrative staff
		1 × Assistant nurse
		2 × Counsellor
		4 × Nurse
		1 × Physician
Observations	Surgical clinic	3 observations over four hours
	Medical clinic	4 observations over four hours

References

Adams, A., Sasse, M.A., 1999. Users are not the enemy. Commun. ACM 42, 41–45.
Albrechtsen, E., 2007. A qualitative study of user's view on information security. Comput. Secur. 26, 276–289.
Albrechtsen, E., Hovden, J., 2009. The information security digital divide between information security managers and users. Comput. Secur. 28, 476–490.
Argyris, C., Schön, D.A., 1996. Organizational Learning II. Theory, Method, and Practice. Addison-Wesley Publishing Company, Reading, Mass..
Baker, W.H., Wallace, L., 2007. Is information security under control? Investigating quality in information security management. IEEE Secur. Priv. 5, 36–44.
Benbasat, I., Goldstein, D.K., Mead, M., 1987. The case research strategy in studies of information systems. MIS Q. 11, 369–388.
Besnard, D., Arief, B., 2004. Computer security impaired by legitimate users. Comput. Secur. 23, 253–264.
Boss, S.R., Kirsch, L.J., 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control and information security. Eur. J. f Inf. Syst. 18, 151–164.
Brinkkemper, S., 1996. Method engineering: engineering of information systems development methods and tools. Inf. Softw. Technol. 38, 275–280.
Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34, 523–548.
Chan, M., Woon, I., Kankanhalli, A., 2005. Perceptions of information security in the workplace: linking information security climate to compliant behavior. J. Inf. Privacy Secur. 1, 18–41.
Cisco, 2014. Cisco 2014 Annual Security Report.
Corbin, K., 2013. Federal Security Breaches Traced to User Noncompliance. CIO.
Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Wartentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. Comput. Secur. 32, 90–101.
D'Arcy, J., Hovav, A., 2007a. Deterring internal information systems misuse. Commun. ACM 50, 113–117.
D'Arcy, J., Hovav, A., 2007b. Towards a best fit between organizational security countermeasures and information systems misuse behaviors. J. Inf. Syst. Secur. 3, 3–30.
D'Arcy, J., Hovav, A., Galletta, D., 2009. User awareness of security countermeasures and its impact on information security misuse: a deterrence approach. Inf. Syst. Res. 20, 79–98.
Da Veiga, A., Eloff, J.H.P., 2010. A framework and assessment instrument for information security culture. Comput. Secur. 29, 196–207.
Dhillon, G., 2007. Principles of Information Systems Security: Text and Cases. John Wiley and Sons, New York.
Dhillon, G., Backhouse, J., 2001. Current directions in IS security research: towards socio-organisational perspectives. Inf. Syst. J., 11
Dhillon, G., Torkzadeh, G., 2006. Value-focused assessment of information security in organizations. Inf. Syst. J. 16, 293–314.
Enisa, 2014. ENISA Threat Landscape 2014. Overview of Current and Emerging Cyber-Threats. European Union Agency for Network and Information Security.
European Commission, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.
Friedman, K., 2003. Theory construction in design research: criteria, approaches, and methods. Des. Stud. 24, 507–522.
Furnell, S., 2006. Malicious or misinformed? Exploring a contributor to the insider threat. Comput. Fraud Secur. 9, 8–12.
Furnell, S., Thomson, K.-L., 2009. From culture to disobedience: recognising the varying user acceptance of IT security. Comput. Fraud Secur., 5–10
Gassp, 1999. Generally Accepted System Security Principles (GASSP) Version 2.0. Information Systems Security, 8.
Gollmann, D., 1999. Comput. Secur. UK, Wiley, Chichester.
Gonzalez, J.J., Sawicka, A., 2002. A framework for human factors in information security. In: WSEAS International Conference on Information Security. Rio de Janerio, Brazil.
Harrington, S., 1996. The effects of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. MIS Q. 20, 257–277.
Hedström, K., Karlsson, F., Kolkowska, E., 2013. Social action theory for understanding information security non-compliance in hospitals: the importance of user rationale. Inf. Manage. Comput. Secur. 21, 266–287.
Hedström, K., Kolkowska, E., Karlsson, F., Allen, J.P., 2011. Value conflicts for information security management. J. Stra. Inf. Syst. 20, 373–384.
Herath, T., Rao, H.R., 2009a. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47, 154–165.
Herath, T., Rao, R., 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125.
Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design science in information systems research. MIS Q. 28, 75–105.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

Hovav, A., D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Inf. Manage. 49, 99–110.
Hu, Q., Dinev, T., Hart, P., Cooke, D., 2012. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis. Sci. J. 43, 615–659.
Hu, Q., Zhengchuan, X., Dinev, T., Ling, H., 2011. Does deterrence work in reducing information security policy abuse by employees? Commun. ACM 54, 54–60.
Huebner, R.A., Britt, M.B., 2006. Analyzing enterprise security using social networks and structuration theory. J. Appl. Manage. Entrep. 11, 68–77.
Ifinedo, P., 2012. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31, 83–95.
Intel Security, 2014. Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies.
Iso, 2005. ISO/IEC 27002:2005, Information Technology – Secuirty Techniques – Code of Practice for Information Management Systems – Requirements. International Organization for Standardization (ISO).
Iso, 2013. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. International Organization for Standardization (ISO).
Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34, 549–566.
Kalberg, S., 1980. Max Weber's types of rationality: cornerstones for the analysis of rationalization processes in history. Am. J. Sociol. 85, 1145–1179.
Karjalainen, M., 2011. Improving Employees' Information Systems (IS) Security Behavior - Toward a Meta-Theory of IS Security Training and a New Framework for Understanding Employees' IS Security Behavior. PhD. University of Oulu.
Karlsson, F., Hedström, K., 2008. Exploring the conceptual structure of security rationale. AIS SIGSEC Workshop on Information Security & Privacy, WISP 2008. Paris, France.
Kirlappos, I., Beautement, A., Sasse, M.A., 2013. "Comply or Die" Is Dead: Long live security-aware principal agents. In: Adam, A.A., Brenner, M., Smith, M. (Eds.), Financial Cryptography and Data Security – FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers. Springer-Verlag, Berlin Heidelberg.
Kolkowska, E., 2005. Value Sensitive Approach to Information System Security. Americas Conference on Information Systems 2005, August 11–August 14, 2005. Omaha, Nebraska, USA.
Kolkowska, E., 2006. Value Sensitive Approach to Information System Security - A Pilot Study. 12th Americas Conference On Information Systems (AMCIS) August 4–6, 2006. Acapulco, Mexico.
Kolkowska, E., 2009. A Value Perspective on Information System Security – Exploring IS Security Objectives, Problems and Value Conflicts Licentiate Thesis. Orebro University.
Kolkowska, E., 2011. Security subcultures in an organization-exploring value conflicts. In: 19th European Conference on Information Systems (ECIS 2011), 2011 Helsinki, Finland. AIS Electronic Library, Paper 237.
Kolkowska, E., De Decker, B., 2012. Analyzing value conflicts for a work-friendly ISS policy implementation. In: Gritzalis, D., Furnell, S., Theoharidou, M. (Eds.), Information Security and Privacy Research – 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4–6, 2012. Proceedings.. Springer, Berlin, Heidelberg.
Leach, J., 2003. Improving user security behaviour. Comput. Secur. 22, 685–692.
Lee, S.M., Lee, S.-G., Yoo, S., 2004. An integrative model of computer abuse based on social control and deterrence theories. Inf. Manage. 41, 707–718.
Li, H., Zhang, P., Sarathy, R., 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. Decis. Support Syst. 48, 635–645.
Liang, H., Xue, Y., 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J. Assoc. Inf. Syst. 11, 394–413.
Mattia, A., Dhillon, G., 2003. Applying double loop learning to interpret implications for information systems security design. In: IEEE International Conference on Systems, Man and Cybernetics, 2003.. IEEE, Washington DC.
Mcfadzean, E., Ezingeard, J.-N., Birchall, D., 2006. Anchoring information security governance research: sociological groundings and future directions. J. Inf. Syst. Secur. 2, 3–48.
Mishra, S., Dhillon, G., 2006. Information systems security governance research: a behavioral perspective. In: 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, 2006 New York.
Moulton, R.T., Moulton, M.E., 1996. Electronic communications risk management: a checklist for business management. Comput. Secur. 15, 377–386.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A., 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Eur. J. Inf. Syst. 18, 126–139.
Nash, K.S., Greenwood, D., 2008. The Global State of Information Security. CIO Magazine (reprinted by PriceWaterhouseCoopers).
Ng, B., Kankanhalli, A., Xu, Y., 2009. Studying users' computer security behavior using the health belief model. Decis. Support Syst. 46, 815–825.
Nist, 2006. Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology, Gaithersburg, USA.
Nist, 2012. NIST Special Publication 800-30 - Revision 1: Guide for Conducting Risk Assessments Gaithersburg, MD: National Institute of Standards and Technology (NIST), U.S. Department of Commerce.
Pahnila, S., Siponen, M., Mahmood, A., 2007a. Employees' behavior towards IS security policy compliance. In: 40th Annual Hawaii International Conference on System Sciences (HICSS'07). IEEE CS Press, Big Island, Hawaii, pp. 1561–1571.
Pahnila, S., Siponen, M., Mahmoodb, A., 2007b. Employees' behavior towards IS security policy compliance. In: 40th Hawaii International Conference on System Sciences (HICSS 2007). IEEE, Waikoloa, Big Island, Hawaii, p. 156.
Parker, D.B., 1981. Computer Security Management. Englewood Cliffs, NJ, Prentice-Hall.
Peffers, K., Tuunanen, T., Rothenberger, M., Chatterjee, S., 2008. A design science research methodology for information systems research. J. Manage. Inf. Syst. 24, 45–77.
Polanyi, M., 1983. The Tacit Dimension. Gloucester, MA, Peter Smith.
Pwc, 2013. Defending Yesterday – Key Findings from The Global State of Information Security Survey, 2014.
Pwc, 2014a. The Information Security Breaches Survey - Technical Report. Department for Business, Innovation and Skills (BIS), London, UK.
Pwc, 2014b. Managing Cyber Risks in an Interconnected World - Key findings from The Global State of Information Security Survey 2015. PriceWaterhouseCoopers.
Ramachandran, S., Rao, C., Goles, T., Dhillon, G., 2013. Variations in information security cultures across professions: a qualitative study. Commun. Assoc. Inf. Syst. 33, 163–204.
Renaud, K., Goucher, W., 2012. Health service employees and information security policies: an uneasy partnership? Inf. Manage. Comput. Secur. 20, 296–311.
Rhee, H.S., Kim, C., Ryu, Y.U., 2009. Self-efficacy in information security: its influence on end users' information security practice behavior. Comput. Secur. 28, 816–826.
Sasse, A., Brostoff, S., Weirich, D., 2001. Transforming the weakest link – a human/computer interaction approach to usable and effective security. BT Technol. J. 19, 122–131.
Schein, E.H., 1999. The Corporate Culture Survival Guide. Jossey-Bass Publishers, San Francisco.
Schlienger, T., Teufel, S., 2003. Analyzing information security culture: increased trust by an appropriate information security culture. In: The 14th International Workshop on Database and Expert Systems Applications (DEXA'03). IEEE CS Press, Prague, Czech Republic, pp. 405–410.
Siponen, M., 2005a. Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Inf. Organ. 15, 339–375.
Siponen, M., 2005b. An analysis of the traditional IS security approaches: implications for research and practice. Eur. J. Inf. Syst. 14, 303–315.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005

Siponen, M., Baskerville, R., Heikka, J., 2006. A design theory for secure information security design methods. J. Assoc. Inf. Syst. 7, 725–770.
Siponen, M., Mahmood, A., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inf. Manage. 51, 217–224.
Siponen, M., Pahnila, S., Mahmood, A., 2007. Employees' adherence to information security policies: an empirical study. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., Von Solms, R. (Eds.), IFIP International Federation for Information Processing, New Approaches for Security, Privacy and Trust in Complex Environments. Springer, Boston.
Siponen, M., Pahnila, S., Mahmood, M.A., 2010. Compliance with information security policies: an empirical investigation. Computer 43, 64–71.
Siponen, M., Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. MIS Q. 34, 487–502.
Siponen, M., Vance, A., 2013. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. Eur. J. Inf. Syst. 23, 289–305.
Son, J.Y., 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf. Manage. 48, 296–302.
Stahl, B.C., Doherty, N.F., Shaw, M., 2012. Information security policies in the UK healthcare sector: a critical evaluation. Inf. Syst. J. 22, 77–94.
Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J., 2005. Analysis of end user security behaviors. Comput. Secur. 24, 124–133.
Straub, D., 1990. Effective IS security: an empirical study. Inf. Syst. Res. 1.
Straub, D., Nance, W., 1990. Discovering and disciplining computer abuse in organizations: a field study. MIS Q. 14, 45–60.
Symantec Corporation, 2014. Internet Security Threat Report 2014, vol. 19. Symantec Corporation World Headquarters, Mountain View, CA.
Thomson, K.-L., 2009. Information Security Conscience: a prediction to an Information Security Culture. In: 8th Annual Security Conference, April 15–16, 2009. Las Vegas, Nevada, USA.
Thomson, K.-L., Von Solms, R., 2006. Towards an information security competence maturity model. Comput. Fraud Secur. 2006, 11–15.
Thomson, K.-L., Von Solms, R., Louw, L., 2006. Cultivating an organizational information security culture. Comput. Fraud Secur. 2006, 7–11.
Vaast, E., 2007. Danger is in the eye of the beholders: social representations of Information Systems security in healthcare. J. Strat. Inf. Syst. 16, 130–152.
Van Niekerk, J.F., Von Solms, R., 2010. Information security culture: a management perspective. Comput. Secur. 29, 476–486.
Vance, A., Sipponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manage. 49, 190–198.
Venter, H., Eloff, J.H.P., 2003. A taxonomy for information security technologies. Comput. Secur. 22, 299–307.
Von Solms, B., 2006. Information security – the fourth wave. Comput. Secur. 25, 165–168.
Vroom, C., Von Solms, R., 2004. Towards information security behavioural compliance. Comput. Secur. 23, 191–198.
Warkentin, M., Johnston, A.C., Shropshire, J., 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur. J. Inf. Syst. J. 20, 267–284.
Weber, M., 1978. Economy and Society. University of California Press, Berkeley, CA.
Webster, J., Watson, R.T., 2002. Analyzing the past to prepare for the future: writing a literature review. MIS Q. 26, 13–22.
Wood, C.C., Banks, W.W., Guarro, S.B., Garcia, A.A., Hampel, V.E., Sartorio, H.P., 1987. Computer Security: A Comprehensive Controls Checklist. John Wiley & Sons, New York.
Yin, R.K., 1994. Case Study Research: Design and Methods. Thousand Oaks, CA, SAGE.
Zhang, J., Reithel, B.J., Li, H., 2009. Impact of perceived technical protection on security behaviors. Inf. Manage. Comput. Secur. 17, 330–340.

Please cite this article in press as: Kolkowska, E., et al. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inform. Syst. (2016), http://dx.doi.org/10.1016/j.jsis.2016.08.005