Practice-Based Discourse Analysis of InfoSec Policies

Fredrik Karlsson, Göran Goldkuhl, Karin Hedström

Practice-Based Discourse Analysis of InfoSec Policies

Fredrik Karlsson[1], Göran Goldkuhl[2], Karin Hedström[1]

[1] CERIS, Department of Informatics, Örebro University School of Business,
SE-701 82 Örebro, Sweden
{fredrik.karlsson|karin.hedstrom}@oru.se
[2] Department of Management and Engineering, Linköping University,
SE-581 83 Linköping, Sweden
goran.goldkuhl@liu.se

Abstract. Employees' poor compliance with information security policies is a perennial problem for many organizations. Existing research shows that about half of all breaches caused by insiders are accidental, which means that one can question the usefulness of information security policies. In order to support the formulation of practical, from the employees' perspective, information security policies, we propose eight tentative quality criteria. These criteria were developed using practice-based discourse analysis on three information security policy documents from a health care organisation.

Keywords: Information security policy, Discourse Analysis, Communicative Analysis, Quality criteria

1 Introduction

Information and information systems have become key assets in, for example, health care. Here is timely access to correct electronic medical records (EMR) essential in order to provide medical care of high quality. Consequently, the importance of information security increases; the confidentiality, availability and integrity of business information assets need to be kept at the level regulated by laws and public administration policies. It is argued that employees' poor compliance with information security policies is a perennial problem for many organizations [1, 2]. Having said that, existing research also shows that about half of all breaches caused by insiders are accidental [3], which means that one can question how useful today's information security policies are in guiding employees. Despite the importance of information security policies the design of such artefacts is an understudied area of information security research in general [4]. Gaskell [5], one of few who has studied the design process, has characterized the information security policy design process as ad-hoc. The main input that information security managers draw upon during such a design process is elicited information security requirements and international security standards [6]. Standards are general guidelines not addressing the specific context of an

organisation [7], such as the specific needs of healthcare, making the elicited requirements an important complement.

If few studies focus information security policy design, even fewer studies have been carried out on information security policies as communicative objects and what constitutes a useful information security policy from a communicative point of view. Stahl et al. [8] is a notable exception, who based on a discourse analysis of information security policies provide six advices for the development of information security policies. Of course, this is a valuable contribution, but according to Baskerville's and Siponen's [4] taxonomy of information security policies, Stahl et al. [8] mainly focus on high-level policies. With this focus they seem to leave out the problematic aspect that employees often are exposed to several documents that together constitute the information security policy.

We therefore take an explicit starting point in a practice-based perspective. This means that a) we critically assess the role of the information security policy as a *practical tool* in the employee's every day work, including the use of both high-level *and* low-level policy documents, and b) we acknowledge the fact that there exist *multiple practices* in an organisation that *need to interact*. To this end we view information security policy documents as the results of the interaction (or lack thereof) between the information security practice and the health care practice. Information security policy documents are in this setting thus seen as communicative objectives.

The purpose of this paper is a) to illustrate the usefulness of practice-based discourse analysis for understanding information security policy design, and b) to provide a set of tentative quality criteria for information security policy design in health care from a practice-based perspective. For this purpose, we carried out a case study at a Swedish emergency hospital. We employed a *practice-based* discourse analysis on the hospital's information security policy. A practice-based discourse analysis means besides collecting and analysing information security policy texts, that we also have studied the mentioned practices through observations and interviewing. The latter is important in order to interpret the communicative limitations of the policy from the *employees'* perspective. Hence, this research responds to the call for more research on employees' behaviour with respect to information security policies within health care [9] and it focuses communicative aspects of the information security policy artefact, which is an even more understudied area. As far as we know there exist no quality criteria for information security policy design in health care anchored in a practice-based perspective.

2 Information security policy theories

An information security policy is a general rule for directing acceptable behaviour of employees when using an organisation's information assets [10]; they provide information security management with a vehicle for establishing information security practices in organisations [11]. Given the strategic importance of information assets it is nowadays stressed that information security management should be integrated into corporate governance [12]. The executive management at the strategic level outlines a

set of directives to indicate the importance of information assets, which are operationalized through the organisation's information security policy design. While information security governance research fail to offers detailed guidance on how to develop information security policies [e.g. 13], there exists practitioner-oriented literature that do [14, 15]. However, this literature focuses on design guidelines without reflecting on the end products' usefulness from an employee perspective. Scholarly studies about information security policy design exist as well. Gaskell [5] and Sibley [16] have described the information security policy formulation as an ad-hoc process, although, for example, Wood [17] has stressed the importance of a well thought out design process. It is common in information security literature to recommend that this process should be informed by information security standards [5, 18]. However, the use of information security standards has been criticised, since they do not take into account that organisations differ [4, 7], and Wood [17] argued that 'one must understand the special needs of an organization before one attempts to generate specific written management directives'. Knapp et al. [19] provided a more balanced view when proposing that both external and internal aspects of an organisation should influence information security policy work.

Research on techniques for eliciting local information security requirements [e.g. 20, 21] make a valuable contribution in such cases. Although there is a large body of research on information security policy, and much consensus can be found with regard to the importance of information security policies, less attention has been given to how to design the content of these policies. Wood [17] provided guidelines for the information security policy design process, arguing that different audiences often require tailored policies. Baskerville and Siponen [4] explored the design of information security policies, but their conclusions are limited to emerging organisations. Doherty et al. [22] stated that 'there are very few studies that explicitly address how the scope or content of information security policies support the employee in their daily work.' They concluded that there is a wide diversity of disparate policies in use and that they contain a low degree of detail. A somewhat broader take on how to design information security policy content also shows a debate about the ideal number of policies in an organisation and how they should be inter-related [e.g. 4, 23]. However, Lindup [24] has noted that in practice organisations often have one single information security policy.

In summary, existing research stresses the importance of congruent communication, and that information security policies should align both with business strategies and international standards. However, we found few empirical studies that address the communicative quality of information security policies. One exception is the study by Stahl et al. [8] who present six advices on how to design an information security policy, based on a critical discourse analysis of twenty-five information security policies.

3 Research approach

3.1 The study object and its implication on overall research strategy

The research approach taken in this study is discourse analysis [25]. Discourse in an open sense 'cover all forms of spoken interaction, formal and informal, and written texts of all kind' (ibid p 7). An inter-textual analysis is a natural element of discourse analysis. So is also an action perspective: 'Texts … do not just describe things; they *do* things.' (ibid p 6; emphasis in original). A discourse analysis of an information security policy will study how different text elements relate to each other; how well they congruently build up the whole text. The discourse analysis will also focus how the text is intended to influence the regulated practice and how it succeeds to comply with governing statements of higher order (standards and regulations). A discourse analysis of this kind is qualitative and interpretive with the purpose to reveal meanings of inter-textual and efficacious character. As a practice-based discourse analysis, we have besides collection and analysis of the information security policy texts also studied the mentioned practices through observations and interviewing.

3.2 Case study and data collection

This study is as a case study [26], and the analysis is based on a reading of three documents that regulate the information security practice in one medium-size Swedish county council. The information security policy consists of one high-level policy document, and two low-level documents that more in detail describe information security instructions and rules. The findings in these documents were complemented with interviews with three high-level information security managers. The interviews gave us deeper knowledge about the county council's information security policies and how they were designed. In order get an understanding of the type of practice we studied, we selected one hospital within the county council for studies of information security policy compliance and translation in practice. We chose a hospital with about 750 employees, 142 places of treatment that serves around 90 000 citizens. Two clinics at the hospital were chosen as cases based on their different degrees of computerization of patient information: one clinic had manual handling of medical records; the other has used an EMR system for a number of years. This variety was important for providing us with rich data concerning information security in both light and heavy computerized settings, both of which are common in health care. We carried out twenty-four semi-structured interviews with health care staff (e.g., nurses, physicians, administrators) at the two clinics. The interviews lasted between one and two hours and concerned how information security were translated and carried out in practice, together with the reasons for the information security actions. The interviews were tape-recorded and transcribed. We complemented the interviews with 28 hours of observations of the information security practice. The observations were documented by note-taking and, when appropriate, by photographs (for example, how medical record were stored). The interviews and observations taken together gave us deeper knowledge about how information security was integrated in the health care practice.

During observations we focused on the same categories as during the interviews, i.e., areas regulating the information security practice. This resulted in re-interviewing and further probing about the rationality for information security actions in practice.

3.3 A conceptual framework for practice-based discourse analysis

We characterize this type of discourse analysis as practice-based. A practice is considered to be "embodied, materially mediated arrays of human activity centrally organized around shared practical understanding" [27, p 2]. This means that language and discourse is part of a practice. A practice consists of humans and their activities including material and semiotic elements. Thus, a study of documents (as e.g. information security policies) cannot be made without taking into account the practices where these documents are generated and used. Three important influences to be used in discourse analysis have been suggested: a semiotic understanding of different language functions; a speech act-based understanding of utterances; an ethnomethodological understanding of conversation. Consequently, they have stated these demands, but they have not synthesised and operationalised these theoretical orientations into a coherent approach for discourse analysis. Within information systems research there exists several studies that use different linguistic theories, but usually only one such theory at a time. Goldkuhl [28] has presented a socio-pragmatic communication framework adapted to studies in information systems. It is a synthesis of speech act theory [e.g. 29], ethnomethodological conversation analysis [30] and semiotics [e.g. 31]. Goldkuhl's [28] framework consists of nine communicative functions. It emphasises a multi-functional view of language and communication, i.e. we do several things at the same time while communicating. The nine functions are shown in Table 1 together with an explanation of each function, and the analytical questions we have used to assess each function.

Table 1. Goldkuhl's [28] framework of communicative functions

Communicative function	Explanation	Analytical question
Accountable	The message is comprehensible, i.e. include sufficient self-references and arguments to explain its role in the communication process.	What is meant?
Carried	The message is using the features of some medium.	How? By what means?
Constitutive	The message creates changes in social states between communicators and sometimes socially broader.	What is done?
Directed	The message is intended towards one or more addressees.	To whom?
Expressive	The message is an expression of the locutor's (the one who says the speech act) subjectivity (e.g. desires, emotions, values).	By whom?

Referential	The message is saying something about something in the world.	About what?
Pre-situationally compliant	The message is in accordance with general institutions and norms and specific pre-situational grounds.	Why? What reasons there?
Projected future actions	The message is an initiative for further actions.	For what?
Situationally responsive	The message is a response to prior messages and other situational features.	Why? What reasons there?

We have modified the terminology of two functions (carried, constitutive) in order to make them more intelligible. In our discourse analysis we have selected seven of these functions to use for our study of the information security policy. We have not used the functions of carried (since it is sufficient with a general characterization that policies are written documents), or situationally responsive (since the demand to write a policy has been excluded from our analysis).

3.4 Analytical steps

A classical dilemma and choice in empirical social research is how to be open-minded vs. to be informed by previous theories in relation to the data material. In our study we used both strategies. We studied the text in an inductive and open-minded way, and then in the further analysis of the text we applied Goldkuhl's [28] framework in a theory-informed way. We have adopted an inquiry attitude [32], i.e. searched for and recorded what seems problematic in some way from a communicative point of view. In our case these principles meant the following. First, the information security policy has been read through and we have noticed all things that caught our attention as being communicatively problematic. We made an open coding of data through this reading [33], just stating what kind problems or other peculiarities we identified. This means that we have selected a set of policy declarations and made annotations to be used for further analysis.

Second we carried out the theory-informed discourse analysis using the results from the open coding as input. The theory-informed analysis in our case meant employing the analytical questions in Table 1. Furthermore, in order to carry out this step the interviews and observations were necessary background information. We used this information to interpret the policy declarations (when asking the analytical questions) from an employee's point of view, since a practice-based discourse analysis of an information security policy requires taking into account the practice where it is used. For example, we used this background understanding when interpreting what the confidentiality instructions meant for the medical secretaries when they are to fax patient information to another care provider. The information security policy stated that 'Patients should be confident that sensitive information does not reach unauthorized'. A second guideline was the following: 'Whatever form the information has, or the way in which it is transmitted or stored, it must always receive adequate protection.' When reading these statements we concluded that the instructions were directed

(to whom?) towards the medical secretaries. However, the instructions were vague when it came to projected future actions (for what?).

Our interviews and observations revealed that the instructions were interpreted as follows by the staff: First, the medical secretary checked whether or not the care provider requesting the medical record had the patient's consent or not, either documented in the medical records or provided by the inquiring part. Second, the medical secretary removed the social security number from the physical medical record. This was done to anonymise the medical record when sending it via fax. Third, she/he added a temporary code, for example 2020. Finally, after faxing the medical secretary called her/his contact person at the requesting care provider in order to tell the temporary code. However, this set of actions was difficult to understand of from only reading the information security policy.

The third step was carried out to organise the analysed policy declarations into overall themes. These themes, which were inductively generated, are to be seen as broader problem areas based on the detailed analysis. We ended up with four themes of importance for design of practical communicative information security policies: external congruence, goal conflicts, internal congruence, and target group. These themes were used when constructing the tentative quality criteria, which are found in Section 4.2.

4 From discourse analysis to tentative quality criteria

At the hospital the employees had to deal with three different information security policy documents that together constituted the information security policy. One document contained a high-level description of the information security regulations, while additional two documents contained low-level descriptions. The presentation below is structured according to the thematic analysis we carried out. The analysis was brought further through the formulation of eight tentative quality criteria (Section 4.2). Table 2 shows examples from our analysis. The table has three columns. The left-most column contains identifiers referring to the policy documents. Passages from the high-level document are referred to using 1.x, while the two low-level documents are referred to as 2.x and 3.x. The second column shows the policy declarations. Finally, the right-most column contains the analysis. Due to the limited space we only present the communicative functions that were considered problematic when analysing the policy declarations.

4.1 Thematic analysis of information security policy

Internal congruence is our first theme. This theme includes concerns about projected future actions that arise from incomplete explanations and definitions, inconsistent use of terminology, inconsistent communicative function, inconsistent description of the information security mechanisms in use, inconsistent description of the same rule and unclear references between the different information security policy documents. The incomplete explanations and definitions found in the three policy documents can

be exemplified with passage 2.7 in Table 2. This quote refers to 'sensitive information' that must be removed from the hard drive before the computer is handed over to external service. However, none of the three investigated policy documents contains a definition of 'sensitive information'. In addition, the same document also includes the term 'business critical information' which is never defined and the differences between these categories are not accounted for. It results in a lack of guidance of the employees due to lack of definitions.

Passage 1.4 in Table 2 is to some extent related to the use of definitions, however it is an example of inconsistent use of terminology once it is introduced. This passage gives the impression that information security is achieved through 'information security policies, guidelines, and instructions', which means that technical measures are not necessary. However, it contradicts, for example, passage 2.6 and 2.11 that clearly contain references to technical security controls. It is also contradicts other references to the existence of technical security controls, such as password controls: 'Do not reveal your password to others, or lend out your authorization'. Consequently, the first and second policy documents give different impressions of what types of information security measures that are needed, and also how the most fundamental concept in the policy, information security, is defined.

Table 2. Practice-based discourse analysis of information security policy

No	Policy declaration	Analysis
1.2	'Information security must protect patients, employees and the public from harm caused by deficiencies in information management or disruption in information systems. The protection of human life, health and privacy are valued the most.'	*Pre-situational grounds:* Based on health law and security standards. *Accountable:* A goal conflict between health and privacy is built into this policy statement. *Projected future actions:* There is no guidance to users for choice between conflicting goals.
1.3	'Laws and regulations shall constitute the lowest level when specifying security measures and controls.'	*Pre-situational grounds:* Difficulties to know which laws and regulations one is to pay attention to. *Projected future actions:* Risk that laws and regulations are neglected.
1.4	'Information security is achieved by developing and complying with appropriate management tools such as information security policies, guidelines, and instructions.'	*Pre-situational grounds:* Lack of compliance with standards; neglect of technical, physical and informal security. *Accountable:* Contradictory to other statements including technical security. *Projected future actions:* Risk of neglecting measures (e.g. technical).
2.6	'If you leave your work place, you must lock the PC using the "Ctrl-Alt-Del" or log out, even if it is just	*Accountable:* Very clear and detailed instruction implies a shift in the text from abstract explanations to concrete

	for a short while.'	and detailed measures. Hard to understand how and when this type of shift occurs. *Projected future actions:* Very clear measures specified.
2.7	'If your personal computer is handed over - for external services, you must ensure that any sensitive information is removed from the hard drive. It is the organisation's responsibility to ensure that the drives are cleaned before the computer goes to scrapping or another organisation.'	*Directed:* Ambiguous addressee (you vs. organisation). *Accountable:* Sensitive information is. *Constitutive:* Ambiguous responsibility is constituted. *Projected future actions:* Limited guidance for the users to take actions concerning file deletion when the PC is handed over to external parties.
2.10	'Information classification should be performed according to documented rules for classification of information.'	*Directed:* This instruction does not target regular users.
2.11	Examples of advice for management of information: • 'Information shall not be stored on the "own" local disc • Backup should always be taken • Unauthorized access shall be prevented'	*Accountable:* Why are "examples" given; not a complete list? *Constitutive*: What is meant by "advice" in this regulative context? *Directed:* These "advices" are addressed not only to regular users. Unclear who the addressees are. *Projected future actions:* Difficult for users to understand the scope of the instructions.
2.17	The 'Information security policy'-document is referred to as the IT-policy.	*Referential:* the reference to the documents is incorrect. The naming of the document is inconsistent.
3.5	'Do not save patient information or other sensitive information on your local hard drive.'	*Accountable:* Unclear what 'other sensitive information' means. *Projected future actions:* Unclear what information can be saved locally
3.7	'Sensitive information may only in exceptional cases be saved on the local hard drive.'	*Accountable:* Unclear what 'sensitive information' means. In addition, earlier they have stated that you are not allowed to store sensitive information on your local hard drive. Cf. 3.5 *Projected future actions:* Unclear what actions are allowed or not.

The three documents have inconsistent communicative functions. Information security management switches from being regulative to in some parts being educational. As discussed in Section 2 the main purpose of a policy is limiting acceptable behaviour of employees, meaning that its primary communicative function is to be regula-

tive. Of course, it is sometimes necessary to educate employees, but the two types of communicative functions are highly intertwined in the documents, without clear indication which communicative function that is in focus. For example, the detailed instructions on how to lock a workstation (Passage 2.6), is followed by an educational passage on why functionality to log the employees' activities is used: 'Logging of activities and transactions are carried out in order to continuously monitor the security of the IT systems. The purpose is to trace important events if disturbances occur in the systems. Tracing is also used to free the innocent, and discover threats to the information security.' Another educational passage in the document is a discussion on malware: 'code in the form of viruses, trojans, or worms could damage, distort or destroy information, or make sensitive information available to persons not allowed to see the information … Malware can be said to be software'.

In addition, Passage 2.6 is also an example of how the available information security mechanisms are described using an inconsistent level of abstraction. This specific passage is a very clear and detailed instruction compared to a passage similar to the following one, which is found sentences earlier: 'Remember that you are responsible for everything that is registered with your user identity.' Hence, from an employee's point it becomes difficult to understand the role of the document. Passages 3.5 and 3.7 are examples of inconsistent descriptions of the same rule. In this case it concerns if the employee are allowed to store sensitive information on 'the local hard drive'. In passage 3.5 the regular user is not allowed to store sensitive information on the computer. While, passage 3.7 states that such information should only 'in exceptional cases be saved on the local hard drive'. This is an inconsistent description, where the employees are left in the dark on how to act. Finally, as discussed earlier the investigated information security policy consists of three documents, and they contain references to each other. But the naming of the documents is not consistent (2.17), which means that it is difficult for the employees to find the right related document. For example, the 'Information security policy'-document is referred to as the IT-policy in the 'Security instructions for county council IT users'-document.

Target group is the second theme, which covers the problem of ambiguous addressees in three policy documents. Passage 2.7 in Table 2 shows one such case. As discussed above, the example concerns how to handle the computer when it is handed over to a third, external, part for service. However, the regulation is ambiguous. In the first part of the example, there is a focus on 'you' as the addressee: 'If your personal computer is handed over - for external services, you must ensure that any sensitive information is removed from the hard drive'. But in the next sentence it is at the same time the responsibility of the organisation, which means that it is not the employee's responsibility. Finally, the third sentence reads 'IT Support provides software for cleaning and can assist with clean-up', which yet again signals that it is the employee's responsibility. A second example of ambiguous addresses is passage 2.10: 'Information classification should be performed according to documented rules for classification of information.' Information classification is carried out in order to determine the right level of information security measure. It is normally an activity of information security management or general management. If employees would carry out this activity they might start neglecting existing information security measure

based on their own classifications. Consequently, it is not evident who the information security management is actually regulating, which in the end means that an ambiguous responsibility is constituted.

External congruence is the third identified theme. In several occasions the three policy documents reference other documents such as laws, regulation, or standards. However, the congruence with these sources is not clear. Passage 1.4 claims, as discussed earlier, that information security is achieved through 'information security policies, guidelines, and instructions.' Hence it is a focus on administrative routines, neglecting technical, physical and informal information security. The same document refers to the ISO-standard 17799, which does not described information security as something to be addressed by administrative means only. Another problem with the information security policy documents is that information security management references laws and regulations in general, without specifying exactly which laws and regulations (Passage 1.3). Consequently, it is difficult for the employees to know exactly which laws and regulations they are to pay attention to.

Goal conflicts are the fourth and final theme we identified. The three investigated policy documents included a number of goal conflicts. Passage 1.2 concerns the tension between protection of human life and health on one hand, and protection of patient information, i.e. privacy, on the other. In the policy document it is stated that 'protection of human life, health and privacy are valued the most.' Another example of conflicting goals is the following which is found in passage 2.1: 'In addition to legal requirements, there are additional demands from organisations and the public, stating that information must be correct, it must be available and must be handled with respect to privacy or publicity.' In this case the tension is between privacy and publicity. A third example is passage 2.11 gives advises 'for management of information'. However, these advises are not directed towards employees only. From an employee's point of view it is contradictory that information should not be stored on the local disc, but at the same time backup should always be taken. In all these cases the information security management leaves the employees without any guidance on how to choose between the conflicting goals.

4.2 Towards tentative quality criteria

The practice-based discourse analysis of this case material has revealed problems with the information security policy. The analysis has aimed for abstraction and four themes have been formulated. These abstracted themes (designating problematic areas in the information security policy) were used for articulating general expectations on policy features. The underlying assumption in our work is that an information security policy should be functional in regulating employees' actions with respect to information security. The policy documents must be comprehensive and useful in guiding employees' actions. The discourse analysis has been a generative basis for formulation of tentative quality criteria for information security policies in health care. The quality criteria express what is considered a good information security policy in health care, i.e. they express positive design values. We have formulated them as criteria that can be useful both in a design/formulation situation and in an evaluation

situation. Our criteria cover both the whole information security policy (possibly consisting of different documents of both high-level and low-level character) and different parts of such policy documents.

Quality criteria:

1. *The information security policy shall not introduce goal conflicts.* We identified several goal conflicts (1.2, 2.1) that the employees were left to manage. The policy was ambiguous with regard to employee prioritization. Theme: goal conflicts.
2. *External policies shall be translated and transformed to the current work practice when such parts are included in the information security policy.* Our analysis (1.3) showed that parts of laws and international standards were included in the policy without paying attention to the local context, or that only vague references were provide to laws. Theme: external congruence.
3. *The information security policy (or explicit parts thereof) shall have clear and uniformed user groups.* The analysis (2.7) showed that it was unclear who were affected by the instructions. Theme: target group.
4. *The information security policy shall contain congruent guidelines for actions that are well adapted to the current work practice.* The analysis (2.6, 3.5, 3.7) showed that instructions are provided at a general level, which left room for interpretation on how to implement the guidelines in the work practice. Theme: internal congruence.
5. *The information security policy shall have a clear and congruent conceptual framework adapted to the current work practice.* The analysis (1.4, 2.6, 2.11) showed an ambiguous use of concepts, where several concepts were used for the same phenomenon. As a consequence, the policy was ambiguous when referring to phenomena in the work practice. Theme: internal congruence.
6. *The information security policy (in whole and parts) shall have a clear structure.* Our analysis (2.7, 2.17) showed ambiguously structured documents where phenomena concerning the same target group were discussed at multiple places. Thus it was difficult for employees to know when they had assimilated all information concerning a specific phenomenon. Theme: internal congruence.
7. *The information security policy (in whole and parts) shall have clear objectives; implying clear communicative functions of the document.* Our analysis (2.6) showed that the communicative functions of specific parts of the documents were unclear (regulative and educational sections are highly intertwined). Making it difficult to identify regulatory instructions. Theme: internal congruence.
8. *The information security policy shall be constitutively clear; clarifying responsibilities and social commitments and expectations.* The analysis (2.10) showed that the responsibilities of the employees were unclear. Hence, it was difficult to achieve accountability. Theme: target group.

5 Conclusions

An information security policy of high communicative quality has the potential to be a practical and useful tool for information security management. The purpose of this paper was a) to illustrate the usefulness of practice-based discourse analysis for un-

derstanding information security policy design, and b) to provide a set of tentative quality criteria for information security policies in health care from a practice perspective. Based on a practice-base discourse analysis that includes high-level and low-level information security policy documents we suggest eight quality criteria for design of information security policies in health care. Our findings are based on one case study. We therefore see interesting venues for future research to further validate the criteria and make them more precise. Another research task is to investigate if any of these criteria are applicable in other business sectors, and if so to what extent. Our quality criteria have, to some extent, similarities with the criteria presented by Stahl et al. [8]. If we are to highlight one similarity, both studies stress the importance of using a clear and congruent conceptual framework adapted to the current work practice. Otherwise, the policies are not accessible to the employees. However, unlike Stahl et al. [8] our quality criteria also address the importance of the structure of policy documents. This difference is a result from Stahl et al.'s [8] choice to limit their study to high-level policies, whereas we studied both high-level *and* low-level policy documents and their relationships. The criteria presented are all derived from a practice-based perspective. It means that they emphasize information security policies as *useful tools for employees*. This perspective represents an alternative and a contrast to the management perspective. When designing information security policies both perspectives need to be acknowledged in order to create a balanced solution. Our list of quality criteria is one important component in the discussion to find such a balance.

References

1. Ernst & Young: Ernst & Young 2008 Global Information Security Survey. Ernst & Young (2008)
2. Ernst & Young: Borderless security - Ernst & Young's 2010 Global Information Security Survey. Ernst & Young (2010)
3. Vroom, C., von Solms, R.: Towards information security behavioural compliance. Computers and Security 23, 191-198 (2004)
4. Baskerville, R., Siponen, M.: An information security meta-policy for emergent organizations. Logistics Information Management 15, 337-346 (2002)
5. Gaskell, G.: Simplifying the onerous task of writing security policies. In: 1st Australian Information Security Management Workshop. (Year)
6. ISO: ISO/IEC 27002:2005, Information Technology - Secuirty Techniques - Code of Practice for Information Management Systems - Requirements. International Organization for Standardization (ISO) (2005)
7. Baskerville, R.: Information systems security design methods: Implications for information systems development ACM Computing Surveys 25, (1993)
8. Stahl, B.C., Doherty, N.F., Shaw, M.: Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal 22, 77-94 (2012)
9. De Lusignana, S., Chanb, T., Theadoma, A., Dhoula, N.: The roles of policy and professionalism in the protection of processed clinical data: A literature review. International Journal of Medical Informatics 76, 261-268
10. Davis, G.B., Olson, M.H.: Management information systems: conceptual foundations, structure, and development McGraw-Hill, Inc., New York, NY, USA (1985)

11. von Solms, R., von Solms, B.: From policies to culture. Computers and Security 23, 275-279 (2004)
12. von Solms, B.: Corporate Governance and Information Security. Computer & Security 20, 215-218 (2001)
13. von Solms, R., von Solms, S.H.: Information Security Governance: A model based on the Direct–Control Cycle. Computer & Security 25, 408-412 (2006)
14. Peltier, T.R.: Information security policies and procedures - a practitioner's reference. Auerbach Publications, Boca Raton (2004)
15. Wood, C.C.: Information security policies made easy. Information Shield, Huston, Texas (2001)
16. Sibley, E.H.: Experiments in organizational policy representation: resuls to date. In: Proceedings of the International Conference on Systems, Man and Cybernetics. (Year)
17. Wood, C.C.: Writing InfoSec Policies. Computer & Security 14, 667-674 (1995)
18. Janczewski, L.: Managing Security Functions Using Security Standards. In: Janczewski, L. (ed.) Internet and Intranet Security Management: Risks and Solutions, pp. 81-105. IGI Global, Hershey, PA (2000)
19. Knapp, K.J., Morris Jr, R.F., Marshall, T.E., Byrd, T.A.: Information security policy: An organizational-level process model. Computer & Security 28, 493-508 (2009)
20. Fabian, F., Gürses, S., Heisel, M., Santen, T., Schmidt, H.: A comparison of security requirements engineering methods. Requirements Engineering 15, 7-40 (2010)
21. Mellado, D., Blanco, C., Sánchez, L.E., Fernaández-Medina, E.: A systematic review of security requirements engineering Computer Standards and Interfaces 32, 153-165 (2010)
22. Doherty, N., Anastasakis, L., Fulford, H.: The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management 29, 449-457 (2009)
23. Siponen, M.: Policies for construction of information systems' security guidelines. The 15th international information security conference (IFIP TC11/SEC2000), Beijing, China (2000)
24. Lindup, K.: The Role of Information Security in Corporate Governance. Computer & Security 15, 477-485 (1996)
25. Potter, J., Wetherell, M.: Discourse and social psychology. Beyond attitudes and behaviour. Sage, London (1987)
26. Yin, R.K.: Case study research: design and methods. SAGE, Thousand Oaks, CA (1994)
27. Schatzki, T.R.: Introduction: Practice theory. In: Schatzki, T.R., Knorr Cetina, K., von Savigny, E. (eds.) The practice turn in contemporary theory. Routledge, London (2001)
28. Goldkuhl, G.: The many facets of communication – a socio-pragmatic conceptualisation for information systems studies. Proceedings of the Workshop on Communication and Coordination in Business Processes, Kiruna (2005)
29. Habermas, J.: The theory of communicative action1. Reason and the rationalization of society. Polity Press, Cambridge (1984)
30. Sacks, H.: Lectures on conversation. Blackwell, Oxford (1992)
31. Bühler, K.: Theory of language. John Benjamins Publishing, Amsterdam, Netherlands (2011)
32. Dewey, J.: Logic: The theory of inquiry. Henry Holt, New York (1938)
33. Corbin, J., Strauss, A.: Basics of qualitative research. Techniques and procedures for developing Grounded Theory. Sage, Thousand Oaks (2008)