Evaluating Information Security Effectiveness with Health Professionals

Robin Krens[1], Marco Spruit[2], and Nathalie Urbanus[1]

[1] University Medical Center Utrecht, Heidelberglaan 100, Utrecht, The Netherlands
rkrens@umcutrecht.nl
[2] Department of Information and Computing Science, Utrecht University, Padualaan 8, Utrecht, The Netherlands
m.r.spruit@cs.uu.nl

Abstract. This paper outlines an alternative view on the information security discipline. We argue that information security is, in general, viewed from a technological and means-end oriented perspective. Our approach can be seen as an initial attempt to approach information security in a broader, more holistic, sense. For this purpose, we approach information security from a health professional's perspective. An instrument, The Information Security Employee's Evaluation (ISEE), is presented to evaluate and discuss information security with health professionals. The ISEE instrument consists of seven dimensions: priority, responsibility, incident handling, functionality, communication, supervision and training and education. The ISEE instrument can be used to better understand health professional's perception, needs and problems when dealing with information security in practice. Following the design science approach, the ISEE instrument was validated within a focus group of security experts and pilot tested as workshops across five hospital departments in two medical centers. Although the ISEE instrument has by no means the comprehensiveness of existing security standards, we do argue that the instrument can provide valuable insights for both practitioners and research communities.

Keywords: information security, evaluation, human perspective

1 Introduction

Information security is involved with guaranteeing the availability, integrity and confidentiality of information [18]. In health care, correct and in-time medical information is needed to provide high quality care. Unavailable or unreliable information can have serious consequences for patients, such as incorrect or delayed treatment. Also, since this type of information is uttermost sensitive, protecting the patient's privacy is another major security objective. From a health professional's point of view, information security aspects concern issues such as in-time access to medical information during consultation, fast recovery during system downtime and assurance of data integrity.

1.1 Narrow and Holistic Definition

There is no clear definition of information security in the health care domain: this alone would be sufficient for a research on its own. We see, however, two types of definitions most frequently. One is a narrow definition, while the is more of a holistic definition. The narrow definition could be best defined as the protection of information against unauthorized disclosure, modification and withholding [6]. One could argue that this view is almost synonymous with computer security. Identity and Access management is, for example, a discussed theme by authors who use this type of definition. Referring to the aspects of information security, in this type of definition there seems to be a tendency towards the confidentiality aspect, overshadowing the other two: availability and integrity. Barber notices this tendency and states that "the issues of integrity and availability will probably deserve more attention than the issues of confidentiality as medical information systems became more inter-twined with clinical practice" [2].

In contrast, a holistic definition of information security could be defined in terms of quality of care or safety of patients. If for example, information is not available at a given time in a health care environment, would this just be solely an issue for the safety and quality of care, or is this an issue for information security as well? To give another example, if information in an electronic health record is altered unauthorized, would this just be solely an issue for information security, or has this an impact on safety and quality of health care as well? We argue that it involves both domains and thereby use a holistic definition: information security can not be seen as a distinct discipline.

1.2 Effectiveness of Information Security?

Practitioners are most interested in the effectiveness of information security in an organization. They question (1) whether or not security controls (i.e. continuity management) have a positive effect and (2) whether more (or less) security control are needed.

Roughly, methods to test the effectiveness of security could be divided in:

1. Compliance with standards, checklists and legislation.
   The general idea is that, as long as an organization is compliant with a certain standard (i.e. ISO/IEC 27002 [9]), security is considered sufficient. Of course, compliance is a useful method to test if certain processes of information security are implemented. An objection, however, is clearly stated by Siponen [17]:

   > "[T]he fact that an organization has in place a certain security process or security activity prescribed by the information security standards does not imply the ultimate goal of this process (or security activity) is therefore achieved. It does not mean the organization's systems are secured according to this objective."

So in this view, for example, a process conducting end-user training, no matter the quality, would be concerned as effective security.

2. Usage of performance indicators.
   Clearly, an indicator has more focus on the quality of a process. The COBIT control objectives framework, for example, describes a few indicators for security, such as the number of incidents damaging the organization's reputation with the public and the number of violations in segregation of duties. The discussion, however, arises if a complex subject as information security, can be systematically mapped down by a few indicators.

3. Perception by the end-user.
   This view focuses on the perceived effectiveness of security by end-users. User-related issues and needs are central in this view. Examples of user-related type issues are problems with retrieving data when needed and lack of knowledge on security procedures. Recent research subscribes the need for a more social approach to information security [3] [16]. Part of this approach is to enlighten on the human and cultural elements of information security [21] [7] [1] . Another part is, since the increase in vulnerabilities and complexity to health information systems nowadays, to involve health professionals actively within the domain of information security.

1.3 Outline of Paper

This paper takes the later approach and focuses on all aspects of medical information security seen from a health professional's point of view. The aim of the research is to build an instrument to evaluate and discuss information security with health professionals. The developed instrument, named ISEE (Information Security Employee's Evaluation), can be used to better understand user's perception, needs and problems. The paper is structured as follows. After this introduction, the second section reviews related work. The third section describes the research approach and the development of the ISEE instrument. Subsequently, the fourth section describes the use of ISEE. The fifth and final section discusses contributions, limitations and future research for this study.

2 Related Work

It is widely recognized that information security is much more than technology. Williams [21] states that information security is not a technical problem but mostly a human one. Williams identifies poor implementation of security controls, lack of relevant knowledge and inconsistencies between principles and practice as key issues. Williams also states that a trusting hospital environment undermines the need for proper supervision. In a culture of trust, confidence in medical practice staff is high, resulting in little scrutiny of Internet usage, no policy on changing passwords and unmonitored access to clinical records. Fernando

and Dawson [4] show similar findings: poor quality training and the hospital environment are constraints on effective information security. Additionally, they argue that wrongly implemented security controls can result in workarounds such as the sharing of passwords or the usage of written clinical notes in case of systems downtime. Security controls often take time from patient care (i.e. logging out of a system). Health professionals are skeptic about such controls that form a constraint on their daily work and that could, in the worse case, harm the patient. In a complex environment were sensitive information is routinely recorded, spread and used it is a challenge to guarantee the availability, confidentiality and integrity of information. As indicated in the introduction, most evaluation approaches of information security are technical and risk based. Our aim is to evaluate information security with health professionals and for this purpose we desire a different type of evaluation. In the discipline of information security such a comprehensive type of evaluation does not exist yet. Most existing instruments are prescriptive (i.e. how should end-user perform?) and focus strongly on the confidentiality aspect. We, therefore, adapt an instrument from the health care domain. The instrument, named the Manchester Patient Safety Framework [19] is used to discuss the physical safety of patients with health professionals. The following subsection gives a short overview of this Patient Safety evaluation instrument.

2.1 The MaPSaF Instrument

The Manchester Patient Safety Framework (MaPSaF) is an instrument to help health care teams assess the safety of patients. Assessment with the instrument is usually carried out in workshops, led by a facilitator from a health care department. A workshop starts by letting each health professional individually rate dimensions of the patient safety instrument. Dimensions of this instrument are, for example, staff education and the investigation of patient safety incidents. The dimensions are given a score according to a maturity framework (we discuss this framework in detail in the next section). If, for example, a nurse thinks that staff education is lacking to 'safely' perform her daily job, she can fill out a low score.

A sample evaluation form and manual is given in Fig. 1. The evaluation form is the compact version of the instrument, the manual contains an explanation of each dimension and textual illustrations for each level that a user can rate.

The Maturity Framework MaPSAF is based on a maturity framework. This framework was originally developed by Westrum [15], and was later extended by Reason [15] and Parker and Hudson [13]. The framework identifies five levels an organization can have: pathologic, reactive, bureaucratic, proactive and generative. Pathologic is defined as a situation where safety practices are the barest industry minimum. There is no top level commitment to the pursuit of safety goals. Reactive is a attitude where changes are implemented after incidents or problems occur. Bureaucratic is a situation where a lot is formalized, on paper,

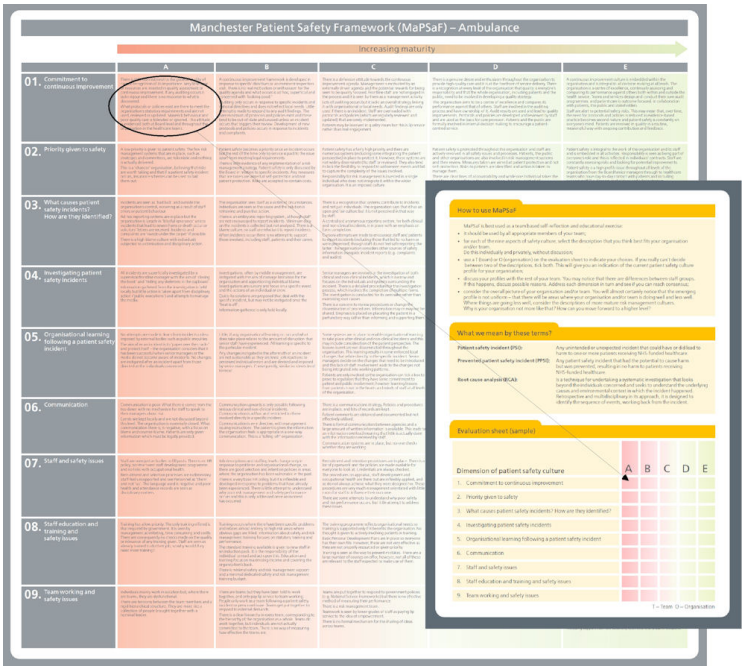

Fig. 1. Evaluation sheet and manual

but practically a lot is failing. In contrast, proactive and generative form complete opposite and the positive view of this situation. Table 1 shows the MaPSaF safety framework.

Table 1. MAPSAF safety levels

Pathologic	Why waste our time on safety?
Reactive	We act when we have an incident.
Bureaucratic	We have systems in place to manage risks.
Proactive	We are alert on safety related risks.
Generative	Safety is a part of everything we do.

The Dimensions Health professionals can, as already shortly explained, rate safety dimensions according to the maturity framework. Table 2 shows a sample of a dimension combined with this framework. Each level contains a description with examples on what stereotypical department is like at that particular maturity.

Table 2. A dimension combined with the framework. Illustrative description are given for each level.

Dimension	Pathologic	Reactive	Bureaucratic	Proactive	Generative
Staff education	Training has a low priority. The only training offered is that required by government.	Training occurs where there have been specific problems and relates almost entirely to high risk areas where obvious gaps are filled.	The training program reflects organizational needs so training is supported only if it benefits the organization.	There is an attempt to identify the training needs of the organization, and of individuals, and to match them up.	Individuals are empowered and motivated to undertake their own training needs analysis and negotiate their own training program.

Workshop Set-up The instrument is typically used practically in workshops. A workshop involves two facilitators and around six to ten participants. MaPSaF encourages to involve a "crosscut" of a department, involving physicians, nurses, management and supportive staff. This will stimulate discussion from different perspectives. Workshops were conducted by a scheme. The following list shows the sequence of steps:

1. Individual evaluation: participants fill out the evaluation individually.
2. Work in pairs: participants discuss their perceptions with other participants. They are encouraged to explain their ratings and exchange anecdotes and personal experiences.
3. Group discussion: general discussion about strength, weaknesses and differences in perceptions.
4. Action planning: the creation of an action plan for weak safety issues.

We have adapted MaPSaF for the purpose of evaluating information security. The next section describes what methods we followed to translate MaPSaF to information security.

3 Development of Information Security Employee's Evaluation (ISEE)

To adapt MaPSaF for evaluating medical information security, we used the design science approach [8]. The design science approach consists of two main steps, namely (1) the development and (2) the validation of the instrument.

3.1 Literature Review

The security dimensions were initially based on a literature review. At first we identified over 30 user-related (i.e. lack of knowledge, poor security implementation, unusable security controls, workarounds) security issues. Since it was not feasible to include each of these issues individually in this type of evaluation, we decided to increase the level of abstraction. We provide a list of seven dimensions:

Table 3. Information Security Employee's Evaluation (ISEE) dimensions.

Dimension	Information security issues
Priority	Lack of time [4] [11] [21], cost [21], the hospital environment [4], conflicting demands [7] and productivity [4]
Handling of incidents	Lack of incident reporting and handling [11] and response [12]
Responsibility	Attitude and ignorance [21] [7], lack of awareness and responsibility [11] [12], skepticism [4], data fragmentation [4] and underestimation of threats [11]
Functionality	Usability [4] [5], Workarounds [4], poor implementation [21], inadequate systems [7] and security design [12]
Communication	Communication [11], communication and feedback [10] and inconsistent policies and communication [7]
Supervision	Audit and supervision [4], trust [21], ethics [12], reward, punishment and hiring practices [10]
Training and education	Training shortcomings [4] [10], lack of knowledge [21], capability and education [21], [11]

priority, responsibility, incident handling, functionality of security, communication, supervision and training and education. Table 3 provides a general overview of these dimensions. The table also shows how we mapped various security issues from our literature study to a dimension. Though security involves many more topics than discussed within the evaluation (i.e. network control or protection against viruses), our perspective is restricted to those security issues that were relevant to health professionals.

3.2 Expert Review

Consequently, the dimensions were reviewed and approved by security experts from the health care discipline. The first review round was performed in a focus group with nine security experts. A focus group was chosen to stimulate discussion between experts. Focus groups encourage people to talk to one another, ask questions, exchange anecdotes and comment on each others' experiences and points of views. By these means, focus groups are considered to have high face validity [14]. The group consisted of security auditors, security officers and IT executives. The data collected during this session was used to develop descriptions for each of the seven dimensions of information security, at each of the five levels. A second interview round was performed with these experts to revalidate

Table 4. The ISEE instrument with abbreviated examples.

Dimension	1: Pathologic	2: Reactive	3: Bureaucratic	4: Proactive	5: Generative
Priority: how important is security (availability, integrity and confidentiality of patient information?	Risks are not recognized	After incidents there is an increase in priority	Now and then plans are made for improvements	Plans are made and evaluated	Employees are involved, security is a management cycle
Incident handling: is the importance of reporting incidents (system failure, confidentiality breaches, unsafe systems) recognized?	It is not clear how and where incidents should be reported	Incidents are handled unstructured and on ad-hoc basis	There is a formal reporting systems, but is not fully implemented	Incidents are handled swiftly.	Trend analysis takes place to prevent incidents for future happenings
Responsibility: who or what is responsible for medical information security?	Information security is not my responsibility	Security is something management does	Security is about defining roles and responsibilities	Security is everybody's concern.	Employees know how to enhance security
Functionality: do systems support security in daily working routines?	Functionality comes with the systems	Temporary solutions are constructed	Needed system security functionality is planned	Systems work correctly and new improvements are considered	Systems fully support the process of care!
Communication: how is the communication about medical information security?	There is no possibility to discuss concerns	Communicatio is one way	Communicatio is paper work	Communicatio is a two-way process	Employees are aware and have a questioning attitude
Supervision: is the correct usage of medical information examined?	Incorrect usage has no consequences	Sanction are taken by severe shortcomings	Most of procedures are in place	Evaluation of behavior is done on periodic basis	Management and employees are widely involved on this topic
Training and education: do health care professionals know how to act?	Employees should not be bothered with security	Training is done if it is an absolute necessity	Training is highlighted, but not enforced	Employees are encouraged to participate	Training is part of the day-to-day job

these descriptions. Table 4 shows the constructed and validated instrument (a bit abbreviated due to paper size constraints).

Table 5. An overview of the participants and associated scores of one of the workshops.

Department and participants	P	I	R	F	C	S	T
Radiotherapy							
Manager Quality Assurance	3	4	3	3	4	4	1
Manager Department	3	5	3,5	2,5	2	3	2
Physician	4	3,5	3	2	3	1	2
Head of Laboratory	3,5	3,5	3	3	2	3	2,5
Laboratory worker	2	3	4	2	4	2	2
Laboratory worker	3	2	2,5	3,5	2,5	3	2
Front Office / secretary	4	3	4	3	3	2	2
P=priority, I=incident handling R=responsibility, F=functionality, C=communication, S=supervision, T=training and education 1=pathologic, 2=reactive, 3=bureaucratic, 4=proactive, 5=generative							

Table 6. Workshop at a radiotherapy department (statistics are based on seven participants).

INSTR. Dimensions	Mean (1-5)	Std	Range (1-5)	Floor (x)	Ceiling (x)
Priority	3,21	0,69	2-4	0	0
Handling of incidents	3,42	0,93	2-5	0	1
Responsibility	3,29	0,57	2,5-4	0	0
Functionality	2,71	0,57	2-3,5	0	0
Communication	2,93	0,84	2-4	0	0
Supervision	2,57	0,98	1-4	1	0
Training and education	1,93	0,45	1-2,5	1	0

4 Use of the ISEE

How is ISEE perceived in a practical context? For this purpose we conducted a pilot study at five hospital departments in two medical centers in the Netherlands. The goal of the workshops was to test if ISEE is applicable in a practical setting. For each workshop the face validity and utility of the instrument were investigated. We asked the participants if they found the evaluation useful and if they thought the scope of information security was covered. Feasibility concerned boundary conditions such as the amount of time. Since the instrument is not a pure measurement instrument validation was kept qualitative. The original instrument, MaPSaF, was also constructed in this nature. We will discuss one of these workshops in more detail below.

4.1 One Workshop Highlighted

One of the workshops was held at a Radiotherapy department. There was a total of seven participants. See Table 5 for an overview of participants and Table 6 for the descriptive statistics over the scores. The lowest scoring dimensions were *Supervision* and *Training and education*. The highest scoring dimensions were

Responsibility and *Handling of incidents*. Most standard deviations of the dimensions indicate an acceptable distribution of responses. Handling of incidents and supervision show the highest variance. Management of the radiotherapy department was very positive on handling of security incidents, which explains the variance. The range of scores on supervision is also broad. Management was also more positive towards this dimension then direct health care workers. The difference in perception brought to light that access control mechanism were not fully implemented.

Most participants prioritize the availability and sharing of information. This may have consequences on the confidentiality aspects. Most participants agreed that more awareness on confidentiality of patient information is desirable. Some even came up with a proposal, such as introducing privacy concerns to new employees or to make 'confidentiality and electronic medical records' a recurrent theme. The discussion also brought forward that many security issues (such as automatic logging out of systems) can be easily implemented. However, a reactive attitude causes that this does not happen. As one participants stated: "things should go wrong, before something eventually happens".

Furthermore, a variety of contemporary issues were discussed. Amongst these were:

- Unavailability of patient's status information.
- Slow security incident handling according to some health care workers.
- Poor integration with another system which made it impossible to write down medical information.
- The transition towards electronic medical records systems made that information was scattered (partly digital and partly on paper).

Based on these differences between experiences regarding the supervision and functionality dimensions the department created an action plan. Participants considered the workshop useful to discuss information security. Most participants encouraged the multidisciplinary setup to discuss different perceptions on information security.

5 Contributions, Limitations and Future Research

Health professionals are the first in line to experience disturbances with the availability and integrity of medical information. Furthermore, concerning the confidentiality of information, they play an important role in the protection of such information. Based on the MaPSaF instrument, that discusses the safety of patients, we constructed the Information Security Employee's Evaluation (ISEE) to evaluate information security with health professionals.

Overall, the pilot study showed that ISEE is useful to:

- Discuss medical information security within a hospital department.
- Identify and discuss weak and strong points.
- Discuss different perceptions on information security between employees.

A workshop can best be held at one single department (i.e. an outpatient clinic or nursing department). At one workshop two departments participated. Some security issues that were problematic at one department (availability of electronic nursing records) were never heard of at the other department. It was interesting to see such differences between departments. It is, however, hard to discuss and identify single points for improvements with such diverse groups. We, therefore, recommend using the evaluation within a single department.

The multidisciplinary set-up of participants highlighted various perceptions on information security. For instance, at one workshop management indicated that they had a very positive view on incident handling. Further discussion however, showed that staff had no idea how to report problems, and even when they did, they were not pleased with the department's solving skills. At another workshop the multidisciplinary set-up even took care of some quick fixes: A physician indicated that during night shift, magnetic resonance information about patients was not available. An employee of the IT supportive staff argued that this was an unknown issue, yet provided a quick solution.

Reflecting on all five workshops of the pilot study, we found that the dimensions priority and responsibility show the least amount of variance and range of scores. These dimensions, since they relate to attitude, might suffer social desirability bias. Floor effects occurred most frequently at the dimensions functionality and supervision. A majority of these low scores was explained by the participants. Ceiling scores were only given by management staff. Overall, management gave relatively higher scores than direct health care workers which might indicate a too optimistic view by management.

For future purposes, it might be interesting to further develop the instrument and apply it as a measurement instrument in a survey-format. Dimensions can be further defined with specific characteristics. To give an example, the dimension training and education could be further defined on the issues 'knowledge of privacy legislation', 'knowledge of information security' and 'knowledge on how to use security controls'. Such refinement makes the instrument more applicable for actual measurement within a hospital environment. Further work, then, will be needed to address these characteristics specifically. Also, such a measurement instrument, gives opportunities to examine in greater depth the instrument's psychometric properties including measures of internal consistency, reliability and construct validity.

This research has shown that the ISEE instrument can effectively assist health professionals in their efforts to improve information security within their hospital departments. The ISEE instrument has by no means the comprehensiveness and completeness of existing standards or other security checklists. We do, however, argue that the instrument and the human perspective can provide additional insights. Implementing secure systems does involve health care workers, both in respect of functional security controls as in human characteristics such as awareness, responsibility and knowledge.

References

1. Ashenden, D.: Information security management: A human challenge? Information Security Technical Report 13(4), 195-201 (2008)
2. Barber, B.: Patient data and security: an overview. International Journal of Medical Informatics 49(1), 19-30 (1998)
3. Dhillon, G. and Backhouse, J: Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 11(2), 127-154 (2001)
4. Fernando, J. I. and Dawson, L. L.: The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics 78(12), 815-826 (2009)
5. Ferreira, A., Antunes, L., Chadwick, D., and Correia, R.: Grounding information security in healthcare. International Journal of Medical Informatics 79(4), 268283 (2010)
6. Gollman D.: Computer Security. 1st edition: John Wiley & Sons (1999)
7. Gaunt, N.: Practical approaches to creating a security culture. International Journal of Medical Informatics 60(2), 151-157 (2000)
8. Hevner, A. R., March, S. T., Park, J., and Ram, S: (2004) Design science in information systems research. MIS Quarterly 28(1), 75-105 (2004)
9. International Organization for Standardization. Information technology security techniques code of practice for information security management. Technical Report ISO/IEC 27002:2005, (2005)
10. Kraemer, S. and Carayon, P.: Computer and information security culture: Findings from two studies. In: Human factors and the Ergonomics Environment, pp. 1483-1487. Human Factors and the Ergonomics Society, Orlando (2005)
11. Nosworthy, J. D.: Implementing information security in the 21st century do you have the balancing factors? Computers & Security 19(4), 337-347 (2000)
12. OECD: Guidelines for the security of information systems and networks: Towards a culture of security. Technical report, Organization for Economic Cooperation and Development, Paris (2002)
13. Parker, D. and Hudson, P. T.: HSE: Understanding your culture. Shell International Exploration and Production EP 2001 - 5124 (2001).
14. Pope, C., Mays, N., and Kitzinger, J., (eds): Qualitative research in health care, chapter Focus Groups. pages 21-31. Blackwell Publishing, Oxford, 3rd edition (2006)
15. Reason, J.: The identification of latent organizational failures in complex systems. In J.A. Wise, V.D. Hopkin, P. S. (eds.), Verification and identification of complex systems: human factor issues, pp. 223-237. Springer-Verlag, New York (1993)
16. Siponen, M. T.: An analysis of the traditional IS security approaches: implications for research and practice. European Journal of Information Systems 14(3), 305-315 (2005)
17. Siponen, M. T.: Information security standards focus on the existence of process, not its content. Communications of the ACM, 49(8), 97–100 (2006)
18. Stamp, M.: Information security: principles and practice. John Wiley & Sons, Hoboken, 2nd edition (2006)
19. University of Manchester and National Patient Safety Agency: Manchester Patient Safety Framework MaPSaF, http://www.nrls.npsa.nhs.uk
20. Westrum, R.: Cultures with requisite imagination. In J.A. Wise, V. D. Hopkin, P. S. (eds.) Verification and Validation in Complex Man-machine Systems, pp. 401416. Springer-Verlag, New York (1993)

21. Williams, P. A. H.: When trust defies common security sense. Health Informatics Journal 14(3), 211-221 (2008)