Stakeholder Perceptions and Standards for Information Security Risks : a case study at a Dutch Health Care Organization

Bartel Van de Walle
Tilburg University, the Netherlands
bartel@uvt.nl

Ronald Spanjers
Tilburg University, the Netherlands
ronald.spanjers@iae.nl

Dirk de Wit
Tilburg University, the Netherlands
dirk@dwit.nl

ABSTRACT

With the increased use of electronic patient files in Health Care Organizations (HCOs), addressing the risks related to the storage and use of patient information has become increasingly important to avoid intentional or unintentional disclosure, damage to or abuse of patients' personal health records. This has lead governments from various countries to introduce and impose information security standards for HCOs. The Dutch government introduced the NEN 7510 national information security standard; a standard derived from the international ISO 17799 norm. Preceding the implementation phase of NEN 7510 standard at a Dutch HCO, we conducted a field study to identify the information security risks as perceived by the main stakeholder groups in the HCO. We present the differences in the perceived information security risks and threats by end users, management and suppliers, and the degree to which these identified risks will be addressed by the implementation of the NEN 7510 standard.

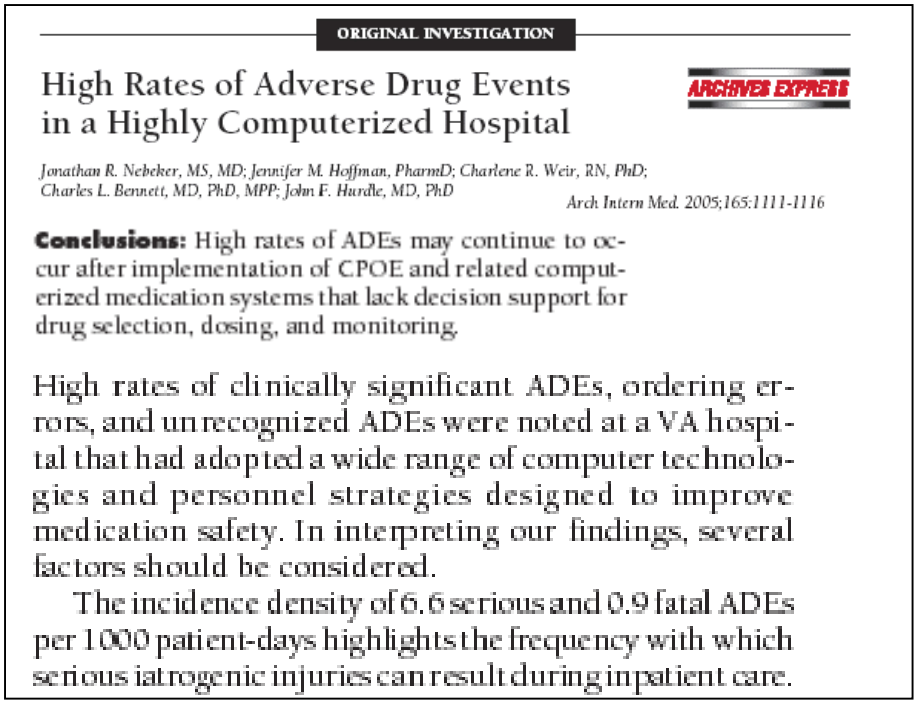
Keywords

Information security; stakeholders analysis; risk perception, NEN 7510.

INTRODUCTION

"At this moment HCOs give insufficient attention to the risks involved with the application of IT, causing possible danger to the patient. This danger has now limited impact, because of the restricted application of IT. But times are changing, the electronic patient file is introduced almost everywhere and within a short time the application of IT will increase enormous, leading to considerably more danger." (Dutch Healthcare Inspection DHI 2004).

Quality is a matter of vital importance in healthcare. According to an estimate of the DHI, between 1,500 and 6,000 Dutch patients die annually as a result of medical mistakes or accidents (DHI 2005). An significant number of mistakes and accidents can be prevented through the use of an Electronic Patient File (EPF), providing healthcare professionals with access to reliable information at the right time. However, the use of electronic information may in turn lead to new errors (see Figure 1).



ORIGINAL INVESTIGATION

High Rates of Adverse Drug Events in a Highly Computerized Hospital

ARCHIVES EXPRESS

Jonathan R. Nebeker, MS, MD; Jennifer M. Hoffman, PharmD; Charlene R. Weir, RN, PhD; Charles L. Bennett, MD, PhD, MPP; John F. Hurdle, MD, PhD

Arch Intern Med. 2005;165:1111-1116

Conclusions: High rates of ADEs may continue to occur after implementation of CPOE and related computerized medication systems that lack decision support for drug selection, dosing, and monitoring.

High rates of clinically significant ADEs, ordering errors, and unrecognized ADEs were noted at a VA hospital that had adopted a wide range of computer technologies and personnel strategies designed to improve medication safety. In interpreting our findings, several factors should be considered.

The incidence density of 6.6 serious and 0.9 fatal ADEs per 1000 patient-days highlights the frequency with which serious iatrogenic injuries can result during inpatient care.

Figure 1 Illustration of problems caused by increased use of IT in HCO

Examples of IT related risk are (DHI 2004):

- IT products use obsolete code tables, which make recordings incorrect;
- IT products contain incorrect or obsolete protocols which results in incorrectly interpreted recordings;
- IT products use several terminologies and code tables, which makes exchange of information unreliable;
- Instructions for IT products are not clear for the user(s), which results in recurrence of errors;
- Medical data entered incorrectly leads to recurrence of errors;
- Mistakes in or theft of patient identity;

Information security is used to create a well-informed sense of assurance that information risks and controls are in balance (Anderson, 2003). To reach this level of assurance in Dutch HCOs, the government has introduced the NEN 7510 information security standard. The NEN7510 standard aims to guarantee the availability, integrity and confidentiality of all information required to offer patients proper and safe care. In addition, the standard demands that the information security measures are organized in a verifiable way (NEN 7510, 2004)

The remainder of this paper is organized as follows. First, the paper identifies the risks preceding the actual implementation of the NEN 7510 standard as perceived by the different key stakeholders in a Dutch HCO. Second, the differences in the perceived information security risks and threats between stakeholders are identified by creating individual cognitive maps from which collective or group cognitive maps for each of the stakeholder groups are derived. Third, the degree to which the risks are perceived to be addressed by the implementation of the NEN 7510 standard is evaluated. The paper concludes with observations from this study and recommendations for risk management contributing to the implementation of NEN 7510 standard in the HCO.

CASE STUDY ENVIRONMENT

The HCO

The HCO where this field research is conducted is a general teaching hospital, innovation and high quality care are core values. Besides basic care, the HCO offers top clinical care in several areas, such as cardiology and oncology.

- Annual budget: 200 million Euro (240 all-inn)
- Employees: 3.000, 150 physicians
- Capacity: 700 beds, 25.000 admissions , 170.000 nursing days, 19.000 short stay, 350.000 ambulatory care
- Patient files: 360.000 paper, 1.3 million microfiche
- IT infrastructure, 125 file-servers, 250 terabytes storage, 300 applications, 2.250 personal computers, 650 printers

In the HCO, the IT-department is responsible for the information and communication technology. The IT department facilitates technical as well as functional areas. The department handles the introduction of patient-oriented systems, the production of various general and technical support services and the implementation of the HCO information system (HIS).

Until recently, information security received ample structured attention at the HCO. As a prelude on the introduction of a nationwide EPF in 2007 HCOs need to structure their information security in compliance with the NEN 7510 standard.

INFORMATION SECURITY DEFINITION AND NORMS

Information Security Definition

Information exists in many forms and media, for instance electronically or paper-based, in oral conversation or even shown in films. In whatever form the information is exchanged or stored, it should always be appropriately protected (ISO 17799, 2005). Information security is a discipline that seeks to promote the proper and robust use of information in all forms and in all media (Allan, 2004). The objective of information security is to ensure business continuity and minimize business damage by preventing and minimizing the impact of security incidents (von Solms, 1998). It is a well-informed sense of assurance that information risks and controls are in balance (Anderson, 2003). According to Parker (Parker 1998) is information security the preservation of confidentiality and possession, integrity and validity and availability and utility of information. While no 'standard' definition of information security exists, the definition used in the NEN 7510 standard is as follows: *Information security is a set of controls to minimize business damage by preventing and minimizing the impact of security incidents (Nen7510, 2004).* This definition is derived from the definition in the ISO 17799 standard (2005) and accepted by many information security experts. Nevertheless, this definition is rather abstract as it only focuses on how to achieve information security and preventing information incidents, and does not clarify anything about information risks, the kind of information (Allan, 2004) or the sense of assurance (Anderson, 2003).

NEN 7510 Information Security Norm

The development of information security baselines has started in 1995 with the British Code of Practice for Information Security Management (BS 7799). This code gained widespread recognition when the International Standards Organization (ISO) adopted it. The ISO 17799 is defined as a comprehensive set of controls comprising best practices in information security and its scope is to give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization (ISO 17799, 2000; Radu et al., 2004). The ISO 17799 has been adopted for use in many countries around the world including the UK, Ireland, Germany, the Netherlands, Canada, Australia, New Zeeland, India, Japan, Korea, Malaysia, Singapore, Taiwan, South Africa, and others. The NEN 7510 describes 125 controls that can be

considered as good guiding principles for implementing information security in HCOs. These controls are categorized in eleven security baselines, which correspond to existing areas of responsibility (NEN 7510, 2004).

Healthcare Information Security Framework

Like other security baselines, the NEN 7510 has many advantages in the implementation of information security management in an organization, such as being simple to deploy and using baseline controls, easy to establish policies, maintain security consistency, etc. However, such a set of baseline controls addresses the full information systems environment, from physical security to personnel and network security.

Not all controls listed in NEN 7510 will be applicable to every IT environment, because a HCO may not operate in certain areas. As a set of universal security baselines, one of the limitations associated with NEN 7510 is that it cannot take into account the local technological constraints or be present in a form that suits every potential user in the HCO. There is no guidance on how to choose the applicable controls from the listed ones that will provide an acceptable level of security for a specific organization, which can create insecurity when an organization decides to ignore some controls that were actually required. Therefore, it is necessary to develop a comprehensive framework to ensure that the message of commitment to patient privacy and information security is pervasive and implemented in policies, procedures and everyday behaviour, both within the HCO and across the health sector (Janczewski & Shi, 2002). This framework should include an effective set of security controls that should be identified, introduced and maintained (Barnard & von Solms, 2000). Elements of those security controls are: baselines assessment, risk analysis, policy development, measure implementation, and monitoring and reporting action. Figure 1 provides an overview of the security controls as well as the critical steps of the health information security framework (Janczewsk and Shi, 2002).

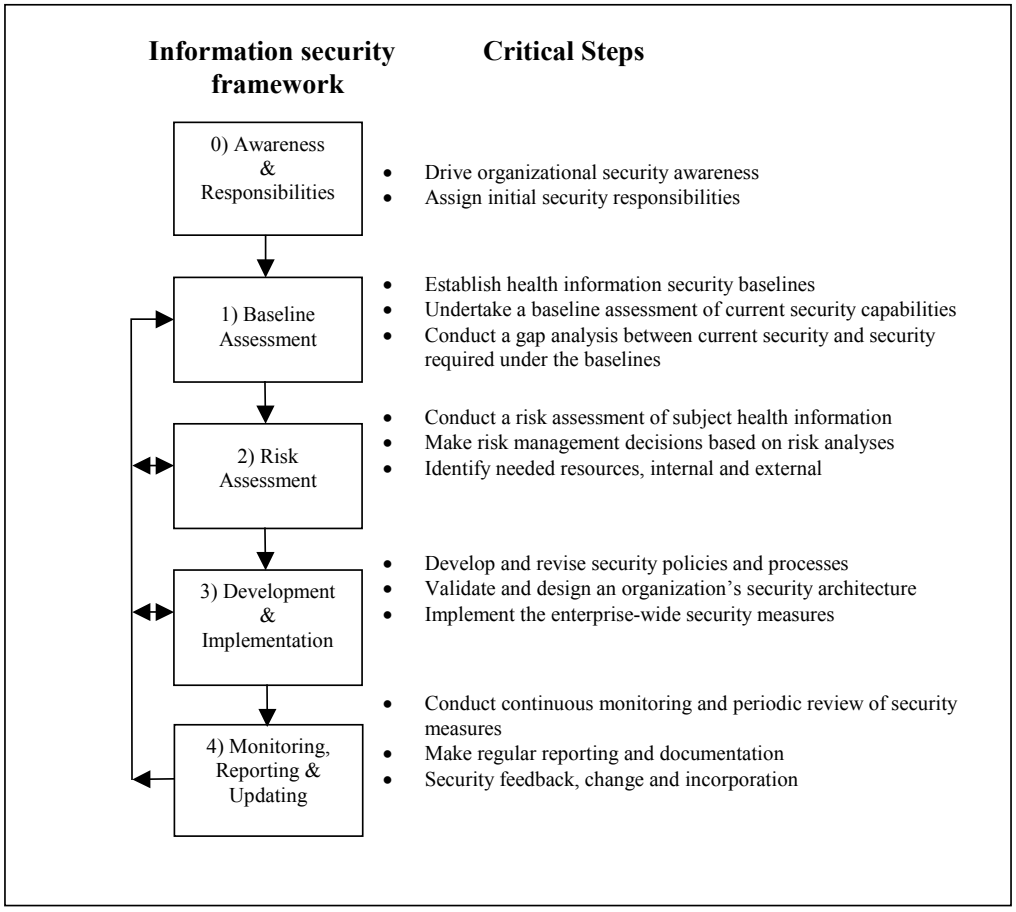


Figure 2 Information Security Framework (Janczewski & Shi, 2002)

RESEARCH METHOD

This research aims to identify and model users' perceptions of risks in HCOs. Similar to research methodologies used in previous security studies (Fléchais, 2005; Rutkowski, 2005; Siponen, 2002), action research is adopted for this research. In particular, we follow the research method developed earlier research by Rutkowski et al. (2005) which consists of the following steps:

1. Define participants and stakeholder groups;
2. Identify concepts (i.e., threats, risks & solutions) using interviews;
3. Model concepts using cognitive maps.

Participants

Table 1 presents the sectors and functional groups of the participants in this study, divided over three groups: *top-management*, *IT-suppliers* and *end users (Hasselbring, 2000)*. The group of IT-suppliers consists of three departments that are involved in the implementation of the NEN 7510 standard.

The top-management group is responsible for information security within the HCO and therefore also selected.

Table 1 Participants and stakeholder groups

Stakeholder Group	Division	Department
End users (7)	Medical support	General clinical lab
		Radiology
	Treatment centre	First aid
		Short-stay
		Intensive care
		Operating theatre
	Surgery	General surgery
IT-suppliers (6)	Finance & Information	IT department (3x)
		Medical administration
	Medical support	Medical instruments
	Quality department	Document management
Top-management (2)	Board of directors	Board of directors
	Surgery	Management
Total number of participants: 15		

Concept Identification

Interviews are conducted based on the protocol developed by Rutkowski et al. (2005), extended with questions on the NEN 7510 (Ma and Pearson 2005). General questions are asked to allow participants to provide details of importance. It allows the interviewees to freely associate concepts (e.g. threat, risk and solution) to events and situations that had happen in the organization. Nelson et al. (2000) emphasize that free association is a good predictor of performance whenever the task involves similar representations and/or processes. The free association method is based on the retrieval of a personal cognitive architecture, stored in a persons' memory. This architecture

is composed of concepts encoded over time and linked to one another. The interview protocol contains six categories:

- *Background questions:* general questions concerning the function, how they are working with the HCO and their affinity with IT.
- *People management:* questions concerning training, responsibility, motivation and morale.
- *Culture:* questions concerning the culture in the HCO, is it a safety culture?
- *Incident management:* questions are asked concerning the experiences with incidents and crisis management.
- *Procedures:* questions concerning the procedures that are in place.
- *Registration:* questions concerning the registration and handling of incidents.
- *NEN 7510:* specific questions from the NEN 7510 standard, which were not incorporated in the categories above.

Not all categories are included in every interview; for instance *Registration* is only included in the interviews for IT-suppliers as they are the single group responsible for the registration of incidents.

Concept Modeling using cognitive maps

To model the concepts identified during the interviews, cognitive mapping is used. Cognitive mapping is a technique that captures an individual's view of a particular issue in a graphical representation. It is a formal modeling technique with rules for its development. "*The formal basis for cognitive maps derives from personal construct theory which proposes an understanding of how humans ''make sense of'' their world by seeking to manage and control it*" (Eden, 2004). A cognitive scheme is the representation of thinking about a problem that follows from the process of mapping. The maps are a network of nodes and arrows as links, where the direction of the arrow implies believed causality. Maps are intended, as a representation, to get close to the problem situated world of the interviewee. However, the quality of the representation depends upon the quality of the interviewer as listener and interpreter. Maps are not just a graphical description of what is said; rather they are interpretations of what is meant by the interviewee (Eden, 2004). In developing the individual maps, the researcher is an active participant who questions group members and adds concepts to the map, with the goal of guiding participants to the "right" strategy (Eden & Ackerman, 1998). Based on the individual cognitive maps of the interviewees, we have created "group maps" for each of the stakeholder groups of end users, suppliers and management. A group map is a collective map that is created by merging individual maps. "*Group mapping creates the ability to conduct a formal analysis of one group, which is meaningful to the client group*" (Eden, 2004).

RESULTS

End Users

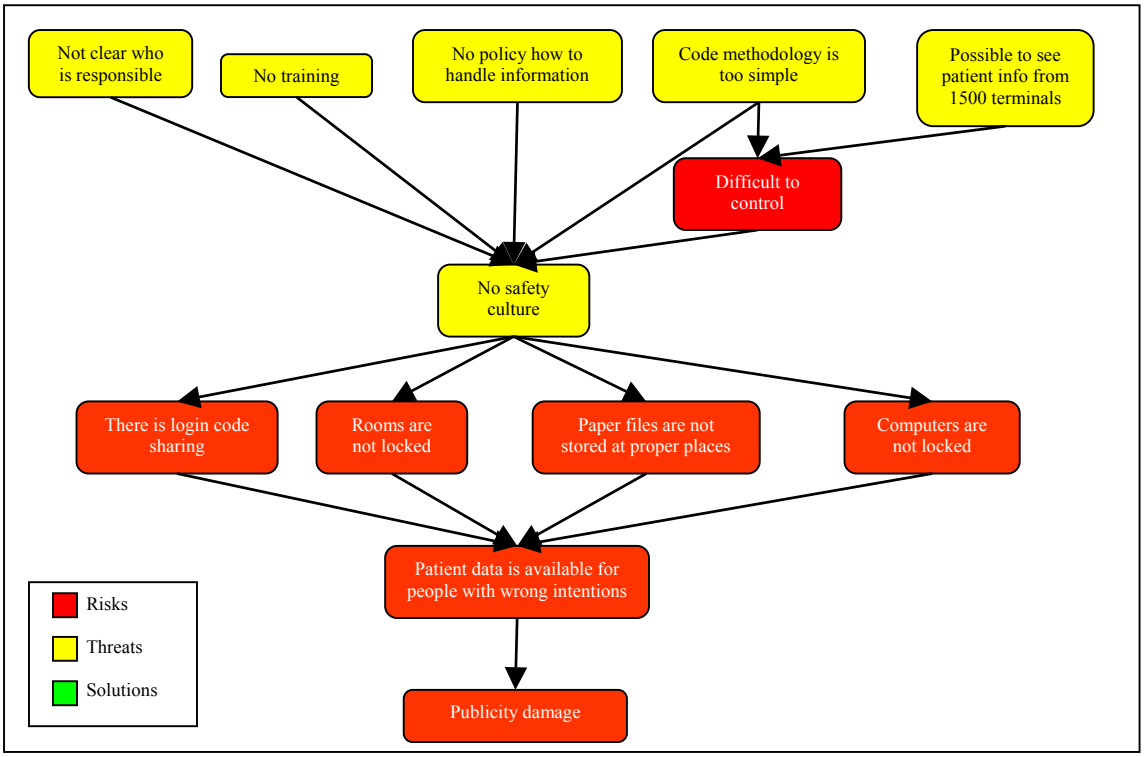


Figure 2a End Users group map (part 1)

Part 1 of the End Users group map (Figure 2a) visualizes this group's view on threats and incidents concerning security policy, organizational security, asset classification and control, personnel security, and system access control. As seen in figure 2a end users perceive five threats and one risk which all influence the treat "no safety culture". "No safety culture" has to do with the way employees see information security and how they handle the (valuable) information. It is a key process in this figure; five risks are influenced by this threat. Those five risks are again influencing the risk "patient data is available for people with the wrong intensions". An interesting note is that end users did not identify any solutions.

Part 2 of the map (figure 2b) visualizes the end users' group view on threats and incidents concerning organizational security, physical and environmental security, communication and operations management, system development and maintenance, business continuity planning, compliance and security incidents.
In figure 2b it is clear that the end users' view focuses on communication and operations management. The risks "network down", "HIS down", "PACS down" (radiology images), and "Mipsys down" (laboratory results) play a central role in this figure. These risks influence other risks, threats and solutions. As opposed to figure 2a end users did identify some solutions.

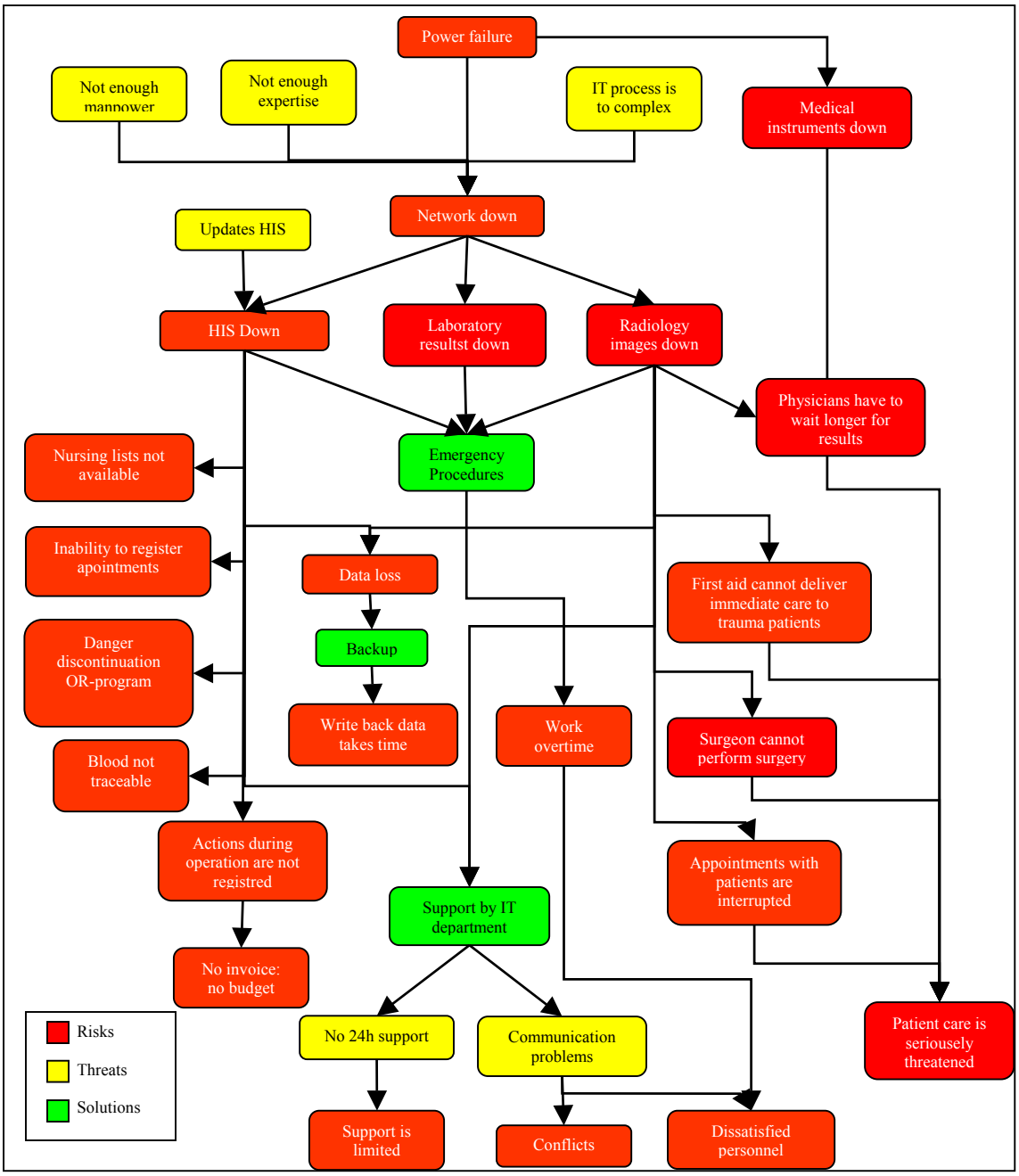


Figure 2b End Users group map (part 2)

Organizational security is a wide topic, it concerns the company culture and the internal security organization, therefore this topic is visible in both parts of the end users' group map. As shown by part 2 of the map, end users are well aware of the numerous consequences of a threat in terms of patient care and procedural problems. For example; images and laboratory results are crucial to most OR procedures, that is why there is danger of discontinuity of the OR program and thus patient care.

IT-**Suppliers**

Part 1 of the map (figure 3a) indicates the view of suppliers on threats and incidents concerning security policy, organizational security, asset classification and control, personnel security and system access control. It has a clear structure where the two concepts "no safety culture" and "patient data available for outsiders" are dominant. "No safety culture" is as with figure 2a important in the hierarchy Two threats can cause "no safety culture" and "no safety culture influences again two risks and two threads. Finally all risks and threats can cause patient data to be available for outsiders. IT-suppliers have, as opposed to the end users, numerous solutions to solve this risk.

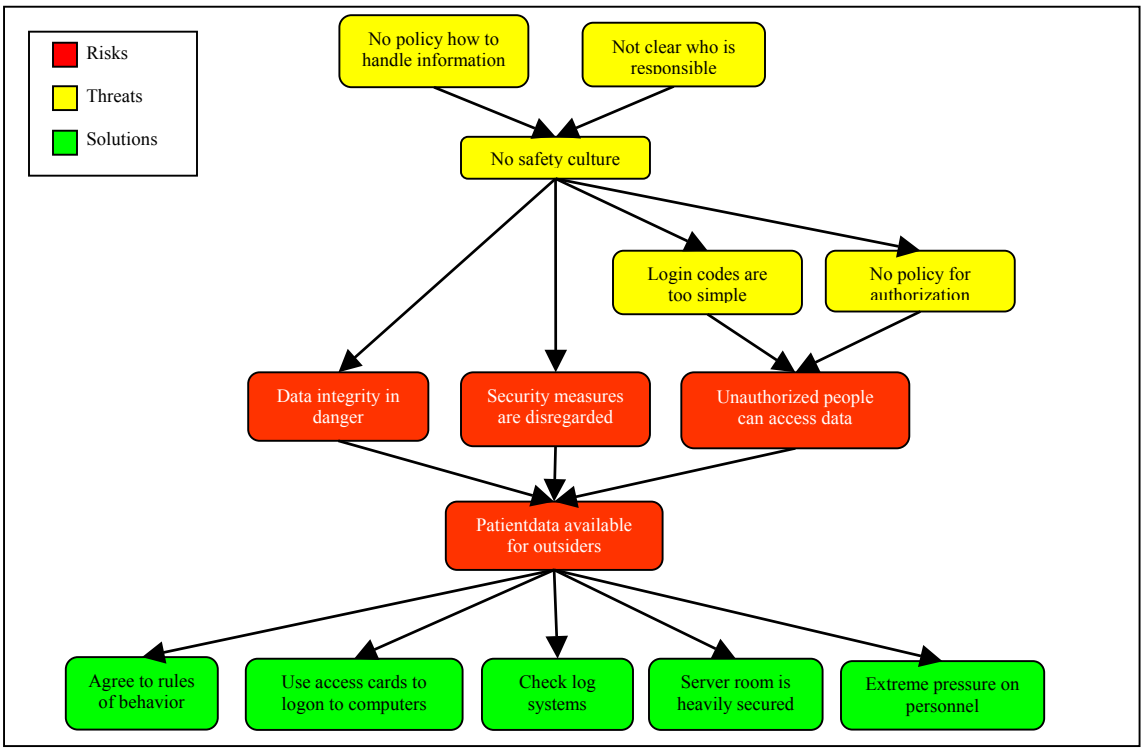


Figure 3a IT Suppliers group map (part 1)

Part 2 of the map (Figure 3b) indicates the suppliers view on threads and incidents concerning the following topics: organizational security, asset classification and control; physical and environmental security, communication and operations management, system development and maintenance, business continuity planning, compliance and security incidents. This figure differs a lot from figure 2b. Suppliers as opposed to end users think more in IT threads and risks, where the end users focused more care processes. In addition, suppliers mentioned more solutions and especially more resourceful solutions. However the upper part of the figure is largely the same, communication and operations management dominates again. Almost all risks and threats start with the risks "systems down"and "systems not stable".

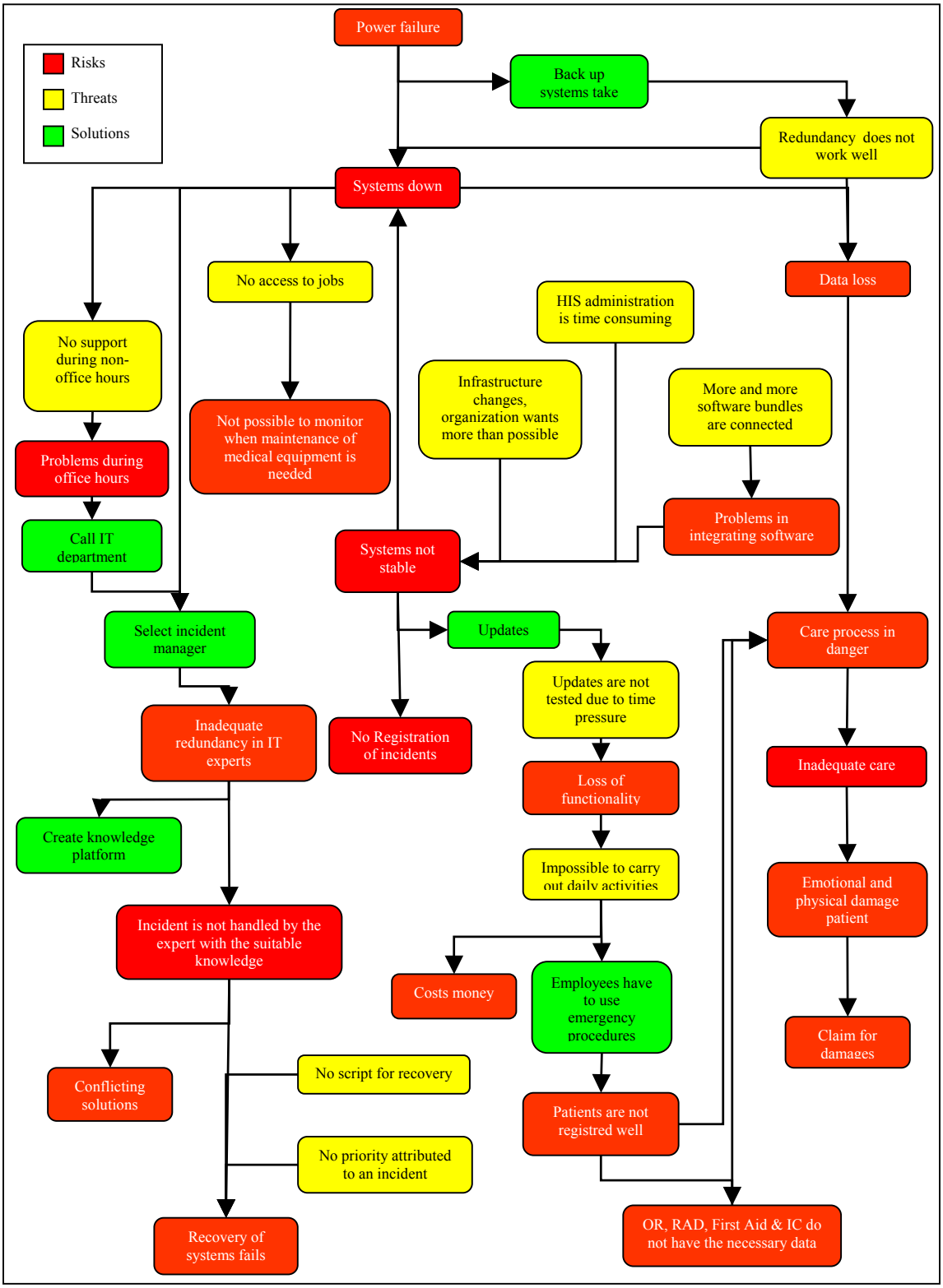


Figure 3b IT Suppliers group map (part 2)

Organizational security and asset classification and control are in both parts of the suppliers cognitive map. As shown in part 2 of the suppliers group cognitive map, suppliers as well as end users identify risks in communication and operations management. Although the risks given by the suppliers focus more on technical details. "Problems integrating software" and "loss of functionality" are examples of these risks.

Management

Figure 4 covers all the baselines of the NEN 7510 standard. Management did identify threats and risks, with communication and operation management again as a dominant factor. As opposed to the figures of the suppliers and end users, management made a connection between the two risk categories. The threat "EPF is not working well" connects "no safety culture" with "system down". Also, note that "power failure" and "system down" were

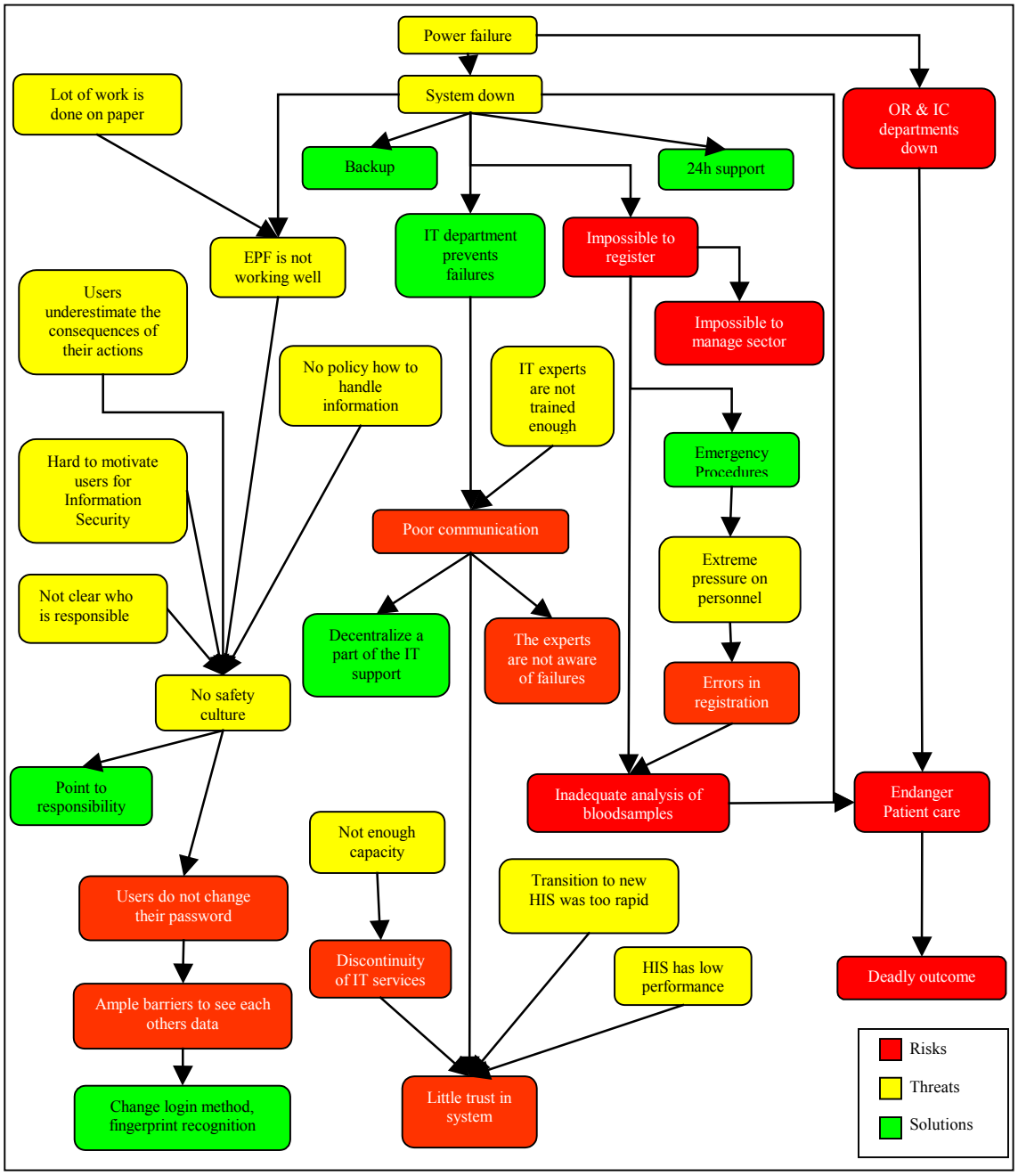


Figure 4 Management group map

identified by the end users and suppliers as a risk, where management identified these concepts as threats.

Clearly, the top-managent has a helicopter view of the organization. Compared to IT-suppliers and end users, top-management does not identify risks in terms of IT failure and inadequate patient care to the same extend. The solutions, risks and threats given by the management are mostly of a organizational nature.

DISCUSSION

Security Policy

As seen in Table 2, end users, suppliers and management have similar perceptions on the baseline security policy. At this moment there is no integrated security policy in place at the HCO, therefore it seems logical the three groups identify the same general threat. Only the suppliers see a risk; "security measures are disregarded". Suppliers are discontent with the fact that the few security measures that have been introduced are disregarded.

Table 2 *Perceived threats, risks and solutions concerning the baseline security policy*

	End users	IT-Suppliers	Top-Management
Threats	• No policy how to handle (valuable) information.	• No policy for information security	• There is a policy for information privacy, but not for information security
Risks		• Security measures are disregarded	
Solutions			

Organizational Security

Many threats, risks and solutions were identified for the baseline organizational security.

Table 3 Perceived threats, risks and solution concerning the baseline organizational security

	End users	IT-Suppliers	Top-Management
Threats	• No safety culture • IT department has not enough expertise • IT process is too complex • Communication with IT department is poor;	• No safety culture • Inadequate redundancy in IT experts	• No safety culture • IT department experts are trained inadequate • Lot of work is done on paper
Risks	• Dissatisfied personnel	• Problems during non-office hours • Incidents are not handled by experts with the suitable knowledge	• Communication with IT department is poor • IT experts are not aware of failures • Discontinuity of IT services due to capacity problems
Solutions	• 24 hour support is needed	• 24 hour support is needed	• 24 hour support is needed • Decentralize a part of the IT support

The overall perception per group is similar, although the classifications differ. For example; end users see "communication with IT department is poor" as a threat while top-managers see it as a risk. Concepts which are widely supported are the solution "24 hour support is needed" and the threat "no safety culture". Furthermore, management and end users have a lot of comments on the IT department regarding security policies.

Communications and Operations Management

In 2003 the HCO changed from a tailor-made to a confection HCO information system to be able to keep up with the rapidly changing specifications as a result of the implementation of a nationwide diagnosis registration and billing system. This caused mayor inconvenience in functionality, therefore many concepts where identified for communication and operation management. The threat given by the management group "Transition to new system was too rapid" illustrates this. During the process of this rapid implementation, frequent updates were needed, which caused system downtime, disturbances in the network-infrastructure, and loss of functionality. As a result of which there trust in the system as a whole diminished temporarily.

Table 4 Perceived threats, risks and solutions concerning the baseline communication and operations management

	End users	IT-Suppliers	Top Management
Threats	• Updates cause disturbances in applications	• Redundancy function of network is not working well	• HIS has low performance • Transition to new system (HIS) was too rapid
Risks	• Many network disturbances, network is often down • Laboratory / Radiology / EPF down • Loss of data • Writing back all data takes a lot of time	• Systems often down • System is not stable • Loss of data • Data integrity is in danger • Updates cause loss of functionality	• System down • Reduced trust in system
Solutions	• Backup	• Backup systems take over in case of failures	• Backup

System Development and Maintenance

While system development and maintenance goes in detail in the NEN 7510 standard, interviewees only identified a few broad concepts like updates which cause problems. Suppliers identified one very interesting threat, which can be identified as the cause of many risk and threats: "Infrastructure changes, organization has too high expectations".

Table 5 Perceived threats, risks and solutions concerning the baseline system development and maintenance

	End users	Suppliers	Management
Threats	• Updates cause disturbances	• Infrastructure changes, organization has too high expectations	• Transition to new system was too rapid
Risks		• Updates cause loss of functionality • Problems integrating software bundles	
Solutions			

CONCLUSION

The objective of the field research reported here was to gather the views of stakeholders in a Dutch HCO on information security threats, their effect on patient care and the role of the NEN 7510 standard. In addition to gathering input, the interviewing sessions we organized did create awareness and encouraged the acceptance of the implementation of the NEN 7510 standard among the stakeholder groups.

A benefit of the cognitive map technique used here is that stakeholders can freely associate concepts with events that happened in their organization. This has allowed stakeholders who do not have the technical know-how to specify their views on security in a simple manner. Clearly, our research has limitations. One of the main concerns is the small population: while the end user group consists of seven participants and the supplier group of six participants, management only consisted of two participants. Also, in the supplier group an IT-vendor was not included. Furthermore, the group mapping technique used can introduce bias from the researchers interpreting and matching the associations..

The group maps show that views of information security vary quite considerably between end users, IT-suppliers and top-management. Neither group is aware of all threats and risks. A consensus was reached for the threats; "no policy how to handle information", "no safety culture", "not clear who is responsible for information security", the risk "system down" and the solutions "24 hour support is needed", "backup" and "emergency procedures". These results will be used by the IT department to help with the implementation of the NEN 7510 standard. The results have been shared in a discussion meeting of the NEN 7510 implementation project group at the HCO. In future research sharing the differences in perceptions amongst stakeholders and the actual use of the use of the findings to facilitate the implementation of the NEN 7510 standard will be addressed.

ACKNOWLEDGMENTS

We are grateful to Mr. Niels Minderman at the HCO's Information and Automation department for his support of our research. We would like to thank two anonymous reviewers for their constructive comments on a previous version of this paper. One of the authors' (Van de Walle) research is supported by the European Commission under the Sixth Framework Programme through a Marie Curie Intra-European Fellowship.

REFERENCES

1. Anderson, J.M. ,2003. Why We Need a New Definition of Information Security, *Computers & Security*, vol 22, no. 4, *308-313*.
2. Allan, A, 2004. Security Matters, *june 2005 at* http://homepage.mac.com/antallan/overview.html
3. Barnard, L., Von Solms, R., A Formalized approach to the Effective Selection and Evaluation of Information Security Controls, *Computers & Security*, vol 8, no. 3, *185-194*

4. Dutch Healthcare Inspection (DHI), 2004. Rapport: ICT in ziekenhuizen, beveiliging van informatie nog onvoldoende voor een betrouwbare papierloze patiëntenzorg.
5. Dutch Healthcare Inspection (DHI), 2005. Rapport: Jaarbericht 2004
6. Eden, C.L., 2004. Analyzing cognitive maps to help structure issues or problems, *European Journal of Operational Research,* vol. 159, *673–686*
7. Eden C.L., Ackerman F. (1998) Making Strategy: The Journey of Strategic Management. *Sage Publication Ltd, London,* ISBN 0-7619-5224-1.
8. Fléchais, I. 2005. Designing Secure and Usable Systems, University of London
9. Hasselbring, W.; Peterson, R.; Smits, M.; Spanjers, R., 2000. Strategic Information Management for a Dutch University Hospital, Technology and Informatics 77, Medical Infobahn for Europe, Proceedings Medical Informatics Europe 2000, A. Hasman et al (Eds.), ISBN 1-58603-63-9, Page(s) 885-888, 4 pp., IOS Press, Amsterdam
10. ISO 17799, 2005. Information technology - Security techniques - Code of practice for information security management August 2005 at *http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html*
11. ISO 17799, 2000. The ISO 17799 Directory. *August 2005 at http://www.iso-17799.com/*
12. Janczewski, L., Xinli Shi, F. 2002. Development of Information Security Baselines for Healthcare Information Systems in New Zealand, *Computers & Security*, Vol. 21, No. 2, *172-192*
13. Johnsen H. G., 2004. Knowledge-generation through Action Research: some reflections on limitations and possibilities, *Kingston University*.
14. Ma, Q., Pearson M., 2005. ISO 17799: "Best practices" in information security management?, *Communications of the ACM*, Vol 15, *577-591*
15. Nelson, D. L., McEvoy, C. L., & Dennis, S. (2000). What is free association and what does it measure?, *Memory & Cognition*, vol. 28, *887-899*
16. Nen 7510, 2004. Informatiebeveiliging in de zorg. *May 2005 at http://www.nen7510.org*
17. Parker, D. B., 1998. Fighting Computer Crime, A New Framework for Protecting Information, *John Wiley & Sons New York*, ISBN 0-471-16378-3
18. *http://healthcare.isixsigma.com/library/content/c040901a.asp#author*
19. Radu, S., Chimirel, C., Mircea S, 2004. Information security assurance – condition for metering operator business sucess, *WEC Regional Energy Forum*, Neptun
20. Rutkowski, A-F., van de Walle, B.A., Groenendaal, W.J.H. van, Pol, J., 2005. When Stakeholders Perceive Threats and Risks Differently: the Use of Group Support Systems to Develop a Common Understanding and a Shared Response, *Journal of Homeland Security and Emergency Management*, vol 2, no 1, *1-15*.
21. Siponen M., 2002. Desiging secure information systems and software, Critical evaluation of the existing approaches and a new paradigm, *University of Oulu.*
22. Van den Eede, G., D. Kenis and B. Van de Walle, "*Combining flexibility and reliability for mainstream organisational learning*", Proceedings of the 5th European Conference on Knowledge Management ECKM2004 (Paris, France, September 2004), pp. 851 – 860.
23. Von Solms, B., 2001. Information Security – A Multidimensional Discipline, *Computers & Security*, vol 20, no. 6, *504-508*
24. Von Solms, R., 1998. Information security management (3): the Code of Practice for Information Security Management (BS 7799), *Information Management & Computer Security*, vol 6, no 5, *224-225*