Please quote as: Sunyaev, A.; Atherton, M.; Mauro, C.; Leimeister, J. M. & Krcmar, H. (2009): Characteristics of IS security approaches with respect to healthcare. In: Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS), San Francisco, USA.

Americas Conference on Information Systems (AMCIS)

AMCIS 2009 Proceedings

Association for Information Systems *Year* 2009

Characteristics of IS Security Approaches with Respect to Healthcare

Ali Sunyaev* Mariana Atherton† Christian Mauro‡
Jan Marco Leimeister** Helmut Krcmar††

*Technische Universitat Munchen, sunyaev@in.tum.de
†Technische Universitat Munchen, merian_z@yahoo.de
‡Technische Universitat Munchen, mauro@in.tum.de
**Universitat Kassel, leimeister@uni-kassel.de
††Technische Universität München,, krcmar@in.tum.de

Characteristics of IS Security Approaches with Respect to Healthcare

Ali Sunyaev
Technische Universität München, Germany
sunyaev@in.tum.de

Mariana Atherton
Technische Universität München, Germany
merian_z@yahoo.de

Christian Mauro
Technische Universität München, Germany
mauro@in.tum.de

Jan Marco Leimeister
Universität Kassel
leimeister@uni-kassel.de

Helmut Krcmar
Technische Universität München, Germany
krcmar@in.tum.de

ABSTRACT

In this paper, we provide a detailed overview of specific characteristics required to evaluate IS security approaches with regard to their applicability in the healthcare domain. The future of integrated treatment is enabled by e-health solutions that comprise health services and information delivered or enhanced through communication and information technologies. This is based on the communication between medical information systems involving all healthcare stakeholders. Thus, the implementation of e-health requires not only the establishment of IS communication infrastructures and the appropriate reorganization of current processes, but also requires the deployment of adequate security approaches concerning information systems in healthcare. Due to the special requirements that need to be met to ensure the security of personal health information and due to the healthcare processes that directly affect the care and service delivered to the patients, there is a strong need for clear, concise and healthcare specific IS security approach characteristics.

Keywords

IS Security, Healthcare Information Security, Healthcare Security Characteristics.

INTRODUCTION

Current developments in the field of an integrated treatment, e.g., in Germany (i.e., the healthcare telematics infrastructure (Blobel and Pharow, 2007)), show the need for IS security approaches within the healthcare domain. In the next years in Germany an electronic Health Card (eHC) will replace the present health insurance card, as requested by law (Marschollek and Demirbilek, 2006), and apply IS to administrate medical data of the insured. This leads to the question of whether these systems are secure enough to satisfy requirements such as privacy, safety, security and availability (Sunyaev, Göttlinger, Mauro, Leimeister and Krcmar, 2009). Medical data are strictly confidential and, due to the ethical, judicial and social implications in case of data loss, such data require extremely sensitive handling (Huber, Sunyaev and Krcmar, 2008). It is of general agreement that security issues should be considered very early in an e-health development process in order to avoid risks and to facilitate the achievement of the overall e-health system. Addressing these special information security needs of the health sector, a security approach should accordingly take the unique operating environment in healthcare into consideration (ISO/FDIS 27799:2007(E), 2007). By their nature, health organizations operate in an environment where visitors and the public at large can never be totally excluded (LeRouge, Mantzana and Wilson, 2007). In large health organizations, the number of people moving through operational areas is significant (ISO/FDIS 27799:2007(E), 2007). These factors increase possible vulnerabilities within healthcare information systems not only due to physical threats, but threats arising from personnel and administrative issues. The other unique healthcare characteristic is the array of factors to be considered when assessing these threats and vulnerabilities (ISO/FDIS 27799:2007(E), 2007). These aspects emphasize the need for an IS security approach which evaluates both the technical and organizational aspects within the healthcare domain (Brooks and Warren, 2004). In order to identify a suitable security approach among a set of candidates, an evaluation of an objective comparative framework which considers the healthcare specifics is needed (Bornman and Labuschagne, 2004). To fill this gap, this paper identifies detailed characteristics of IS security approaches with respect to healthcare.

In order to assess the relevance of security approaches for healthcare, we first introduce three different kinds of classification areas: (1) general IS Security Approach Characteristics, (2) General IS Security Approach Characteristics with Reference to Healthcare and (3) Healthcare Specific IS Security Approach Characteristics. These three categories then can be sub classified into groups of characteristics which should be evaluated in order to estimate a relevance of an IS security approach according to its suitability to the healthcare domain.

It is not the intention of the general IS Security Approach Characteristics to write a guideline on computer security, nor is it to restate what has already been written. There are many requirements that are common to all computer-related systems and therefore related standards, whether used in financial services, manufacturing, industrial control, or indeed in any other organized endeavor (ISO/FDIS 27799:2007(E), 2007). The general IS Security Approach Characteristics intend to personalize the profile of the researched security approach.

The rest of this paper is organized as follows: Section 2 overviews the research approach taken for the study. Section 3 presents a summary of different kinds of characteristics of IS security approaches and deals with the detailed description of three different categories. The last section summarizes findings and proposes an outlook for future research.

RESEARCH APPROACH

In order to provide healthcare security characteristics, we examined healthcare IS security issues currently receiving attention in the literature. The literature review was based upon the approach by Webster and Watson (Webster and Watson, 2002). A search was performed by spanning the IS security, information management, information systems, healthcare informatics, risk- and security analysis and management literature[1]. After the identification of relevant journals, the appropriate articles were examined.

Accordingly, a search based on a full-text electronic search[2] of selected keywords was carried out to identify relevant articles. The number of articles analyzed amounted to 1007. By examining the title and abstract of each article, a total number of 145 articles were found to be relevant. A further in-depth review resulted in an assortment of 25 articles that were relevant and of importance for the research. Table 1 assigns identified articles to the relevant scientific field.

Scientific Field	References
Security Analysis, Risk Management, Security / Risk Evaluation, Information Systems Security Evaluation Criteria	(Standards Australia International, 2003); (Hamdi and Boudriga, 2005); (Huber et al., 2008); (Beham, 2004); (BITKOM, 2006); (Bornman et al., 2004); (Brooks et al., 2004); (ENISA, 2006); (Initiative D21, 2001); (Vorster and Labuschagne, 2001); (Schlichtinger, 2005); (Janczewski and Xinli Shi, 2002)
Information Systems Standards, Information Systems in Healthcare	(Anderson, 1996); (Blobel et al., 2007); (Standards Australia International and Standards New Zealand, 2001); (Haas, 2006); (Hildebrand, Pharow, Engelbrecht, Blobel, Savastano and Hovstø, 2006); (ISO/FDIS 27799:2007(E), 2007); (ISO/IEC, 2005); (LeRouge et al., 2007); (Mantzana, Themistocleous, Irani and Morabito, 2007); (Marschollek et al., 2006); (Müller, 2005); (Schweiger, Sunyaev, Leimeister and Krcmar, 2007); (Toyoda, 1998)

Table 1. Scientific Fields of Analyzed References

[1] All issues of the following journals were searched in an effort to include top journals in the selected disciplines: *Accounting; ACM Computing Surveys; ACM Transactions Journals; BioHealth; British Medical Journal; Computers & Security; European Journal of Information Systems; Health Affairs; IEEE Software; IEEE Transactions Journals; IM Information Management & Consulting; Information & Management; Information and Organisation; Information and Software Technology; Information Management and Computer Security; Information Systems; Information Systems Journal; Information Systems Management; Information Systems Security; International Journal of Communication Systems; International Journal of Information Management; International Journal of Information Security; International Journal of Medical Informatics; Journal of Biomedical Informatics; Journal of Management Information Systems; Journal of the American Medical Informatics Association; Management & Information Technologies; Methods of Information in Medicine; MIS Quarterly; New England Journal of Medicine*.

[2] The following databases were used: Business Source Premier, Science direct, JSTOR archive, INSPEC.

OVERVIEW OF IS SECURITY APPROACH CHARACTERISTICS

This section provides an overview of different types of characteristics (Table 2). We use the term "approach" to refer to a published document describing an information systems security method, process or standard concerning the healthcare domain.

General IS Security Approach Characteristics		
	Name	Short Description
1	*Name of the approach* (ENISA, 2006)	The full name of the IS security approach.
2	*Vendor name* (ENISA, 2006; Schlichtinger, 2005)	Company or cross-frontier organization that provides the IS security approach.
3	*Current version*	The version during the case study period.
4	*Availability*	Are there any costs or is it available free of charge?
5	*Languages available* (ENISA, 2006)	Which languages are supported by the IS security approach?
6	*Research activity*	Extent, scope, transparency, independency of the review verification of the active research undertaken.
7	*Skills needed / Time and effort* (ENISA, 2006; Initiative D21, 2001)	The skills needed to understand, maintain or perform the IS security approach in the organization.
8	*Consultancy support* (ENISA, 2006)	Is it necessary to use external help (consultancy) in order to apply the IS security approach?
General IS Security Approaches Characteristics with Reference to Healthcare		
9	*Identification of the IS security approach* (ENISA 2006; Schlichtinger 2005)	Type of the IS security approach concerned, which can be a standard, a norm, a method, regulation, guideline, etc.
10	*The country of origin* (ENISA 2006)	The origination from a company or national organization.
11	*Level of reference of the IS security approach* (ENISA 2006; Schlichtinger 2005; BITKOM 2006)	Details about the type(s) of initiator(s) of the IS security approach.
12	*Geographical spread* (ENISA 2006; Initiative D21 2001)	Whether the IS security approach is also established outside of its original field i.e., the degree of its internationality, e.g., if the IS security approach is used in EU or non-EU member countries.
13	*Lifecycle / Actuality* (ENISA 2006; Initiative D21 2001; Beham 2004)	A short historical overview in order to gain insight into the IS security approach lifecycle (the degree of the actuality).
14	*Fundamental objectives and IS security approach scope* (ENISA 2006)	Intention regarding IS security approach targets to be achieved, expected results, improvements and requirements.
15	*Completeness* (Initiative D21 2001; Schlichtinger 2005)	How comprehensive, abstract, detailed is the IS security approach?
16	*Level of detail* (ENISA 2006; BITKOM 2006)	Who should read and use the IS security approach.
17	*Scalability* (Initiative D21 2001; Beham 2004)	Scalability for the size and complexity of health care organizations.
18	*Target organizations* (ENISA 2006; Initiative D21 2001; BITKOM 2006; Beham 2004)	The most appropriate type of health organizations the IS security approach aims at.

19	*Security Analysis* (Beham 2004; ISO/FDIS 27799:2007(E) 2007; ISO/IEC 2005b)	Is there an appropriate security analysis approach included?
20	*Supporting heterogenic, decentralized information systems* (ISO/FDIS 27799:2007(E) 2007)	Taking heterogenic, decentralized information systems into consideration.
21	*Process oriented evaluation method* (ISO/FDIS 27799:2007(E) 2007)	Process oriented and not asset or system oriented method focused on the health care telematics processes.
22	*Organizational Focus* (Hamdi/Boudriga 2005)	Organizationally focused assessment is targeted at organizational risks which are derived from the interaction with the people with the information systems and consider the implication of the technical failure of the information systems on the patient security.
23	*Pro-active security analysis* (Hamdi/Boudriga 2005)	Is there a separation between preventative/pro-active and reactive security analysis, especially in the health care domain (Hamdi/Boudriga 2005)?
24	*Comparable and reusable results* (ISO/IEC 2005b)	The security assessment methodology selected shall ensure that security assessments produce comparable and reproducible results.
25	*Maturity level* (Initiative D21 2001; ENISA 2006)	Measurement of the maturity of the information system security.
26	*Available tools* (ENISA 2006; Beham 2004; Initiative D21 2001)	Existing of a list of tools that support the IS security approach.
27	*Certification scheme* (Initiative D21 2001; ENISA 2006)	Existence of a certification scheme: a health organization may obtain a certificate that it has fully and correctly implemented the IS security approach on its information systems.
28	*Optimal investment sum* (ENISA 2006)	The amount of the optimal effort related to a risk management project.
29	*Organizational integration* (ENISA 2006)	Interfaces to existing processes within the health organization.
Healthcare Specific IS Security Approaches Characteristics		
30	*Branch* (BITKOM 2006)	Industry sector and the line of business of organizations the IS security approach aims at.
31	*Target audience in the health care branch* (Standards Australia International 2003)	The intended target group in the health care branch the IS security approach aims at: health consumers, health care providers, health funders, the state, the health care telematics infrastructure.
32	*Compliance* (ENISA 2006; Initiative D21 2001; ISO/IEC 2005b)	Compliance to a law and regulations, e.g., several commonwealth and state acts impact the health sector and must to be complied with (Standards Australia International/Standards New Zealand 2001).
33	*Hazard list relevant to health care* (ISO/FDIS 27799:2007(E) 2007)	Proposal of health care generic hazards.
34	*Security requirements relevant to health care* (ISO/FDIS 27799:2007(E) 2007)	Proposal of health care security requirements.
35	*Security measures relevant to health care* (ISO/FDIS 27799:2007(E) 2007)	Proposal of health care security measures.
36	*Risk valuation guidelines relevant to health* (ISO/FDIS 27799:2007(E) 2007)	Proposal of health care valuation of risk explain the risk value specific for health care.

37	*Security measures point of view* (ISO/FDIS 27799:2007(E) 2007)	Are the security measures provided according to the patient's point of view as well or only according to the IS security point of view?
38	*Requirements for confidentiality, privacy, integrity, availability of information* (Anderson 1996b)	Is the protection and security of information ensured with the offering of these requirements? Further security elements of information systems in health care are authenticity, commitment, use regulation, accuracy, utility, possession, legal liability, legal certainty, enforceability, suitability for daily use and anonymity (Müller 2005).
39	*Data quality requirements* (ISO/FDIS 27799:2007(E) 2007)	Requirements for completeness, validity, consistency, timeliness and accuracy of the data.
40	*Physical and environmental security* (Standards Australia International/Standards New Zealand 2001; ISO/IEC 2005b)	Physical security of the information systems.

Table 2. Overview of the IS Security Approaches Characteristics

General IS Security Approach Characteristics

The general IS Security Approach Characteristics contain basic information which helps to identify and personalize the profile of the researched IS security approach and needed skills to use the IS security approach. The basic information that should be provided comprises: the *name of the IS security approach* (ENISA, 2006), the *name of the company or cross-frontier organization that provides the IS security approach* (ENISA, 2006; Schlichtinger, 2005), and *the current version of the IS security approach* during the case study period and information about the existence of any costs – e.g., licenses, fees for upgrades etc. – related to the IS security approach or whether it is *available* free of charge. Possible *languages* are English or German. The first occurrence or other occurrences of the IS security approach could include one of these languages in which the IS security approach is available (ENISA, 2006). In order to define how much *active research* is still being undertaken and to ascertain whether the research activities are transparent and conducted so that research methods can be subjected to peer review and independent verification by others, we take the characteristic activity of the research into consideration as well. The scope of the research activity is also a subject, in particular its limitation, as well as whether it is connected to a long-term goal.

Taking the *needed skills* (ENISA, 2006; Initiative D21, 2001), *time and effort* into consideration (ENISA, 2006) in order to understand, maintain or perform the IS security approach in the health organization, there are three types of skills of relevance to this paper: (1) to introduce, (2) to use and (3) to maintain. While the first type of skills demands is just a general understanding of the dependencies among the specific details of the IS security approach, the second and the third types accordingly require specific qualifications in order to perform current work and to maintain the life cycle of the IS security approach. For each of these types, the level of skills is classified according to the following scale: the basic level as common sense and experience, the standard level indicating that a few days or weeks of training are sufficient, and the specialist level specifying that thorough knowledge and experience is required (ENISA, 2006; Initiative D21, 2001). Sometimes, apart from the skills needed within the organizations, it is necessary to use external help (*consultancy*) in order to apply the IS security approach (ENISA, 2006). In such cases, the IS security approach can be open to any consultant on the market or it is bound to a specific category of consultants (e.g., licensed) (ENISA, 2006).

General IS Security Approaches Characteristics with Reference to Healthcare

Information systems researchers first have to understand the healthcare environment before they can appropriately apply information systems (Mantzana et al., 2007). Hospitals, emergency rooms and laboratories are very different from the "normal" business environment, and "healthcare users" vary considerably in the role that they play (Mantzana et al., 2007). This section thus describes general IS Security Approach Characteristics with reference to the healthcare domain in order to provide a better understanding of the specifics of healthcare.

Type of the IS security approach

The first characteristics extend the personalization of the profile of the researched approach. *Identification of the IS security approach* (ENISA, 2006; Schlichtinger, 2005) is the first aspect since it defines the types of IS security approaches concerned and the differences between them. An IS security approach type can be a standard, a norm, method, regulation, guideline, etc.

Awareness of the type is very important in the healthcare domain because any violation of existing regulations or norms could result in a litigation process and could have high liability implications. Healthcare clearly carries potentially high risks, especially in areas such as laboratories, emergency departments and operating theatres (ISO/FDIS 27799:2007(E), 2007). There are 4 different types of IS security approaches considered in this paper: *Method* (ENISA, 2006), *Standard* (ENISA, 2006), *Regulation* and *Guideline*.

General characteristics

Due to the specific local laws concerning security and privacy of health related data, *the country of origin* (ENISA, 2006) and the *level of reference* of a IS security approach (BITKOM, 2006; ENISA, 2006; Schlichtinger, 2005) are important to also be identified. The level of reference provides more details about the type(s) of initiator(s) of the IS security approach such as: National standardization body (BITKOM, 2006; ENISA, 2006), ANSI, European standardization body (BITKOM, 2006; Hildebrand et al., 2006), CEN/ISSS (Information Society Standardization System), International standardization body (BITKOM, 2006; ENISA, 2006), ISO, Private sector organization / association (ENISA, 2006), institute for one world health, drugs for neglected diseases Initiative etc. and Public / government organization (ENISA, 2006), UK national health service, and medicare Australia, etc.

As soon as we know where the IS security approach and its initiator come from, the next step of interest is the *geographical spread* (ENISA, 2006; Initiative D21, 2001) of the IS security approach, i.e., the degree of its internationality. It should be made clear that internationality per se is not equated to internationality in terms of academic journal publications where in particular, publications in prestigious international journals are used as important quality indicators (Buela-Casal, Perakakis and Taylor, 2006). In this case, the establishment in terms of usability and implementation of the IS security approach within organizations outside of its original field is an important quality indicator. In the healthcare domain, many IS security approaches are available on a regional, national or international level, but they often differ from and compete with each other (Hildebrand et al., 2006).

In order to gain insights into the IS security approach *lifecycle* (Beham, 2004; ENISA, 2006; Initiative D21, 2001) and the degree of the actuality, a short historical overview is important to be defined. It concerns itself with the state-of-the-art level of the IS security approach and the revision on a periodical basis. Topics such as the frequency of updates or how often and how revisions take place are covered in this characteristic. In the healthcare domain this information is important to be identified, for example, the specific and over time changing local laws concerning security and privacy of health related data. The basic information that should be provided is comprised of the date of the first edition / release, date and number of current updated versions, whether the IS security approach has originated from other IS security approaches (i.e., has been complemented to other IS security approaches), which general milestones (i.e., changing the name of the IS security approach) exist, and if it is currently or planned in the future to be covered by new IS security approach(es).

After gaining insights into the IS security approach lifecycle, we then describe characteristics which provide requirements concerning the content of the IS security approach. It is important first to know more about the IS security approach, namely its fundamental *objectives* and especially those which concern the analysis of the security (ENISA, 2006), its scope and, more concretely, its intention regarding its targets to be achieved, expected results, improvements and requirements. So a short and clear description of the IS security approach's focus can help to identify the coherences, derive clear differentiation between the IS security approaches and give a general overview of their relevance to the healthcare.

In order to provide the sufficiency of any given scope or generally speaking to indicate whether the IS security approach content is *complete* (Initiative D21, 2001; Schlichtinger, 2005), all components concerning the analysis of the security should be provided. One elementary question is whether the scope has been extensively and thoroughly examined. Another question is, for example, whether catalogues are encompassed and supported, such as catalogues of healthcare related security measures, catalogues of healthcare related hazards consisting of best practice threats, security policy catalogues taking the healthcare requirements into consideration, etc. Finally, is there just a plain recommendation of healthcare related countermeasures or is there also support for their implementation?

Next, it is essential to identify the *target reader group* of the document (BITKOM, 2006; ENISA, 2006). For instance, the IS security approach could be intended for those responsible for overseeing healthcare IS security and for healthcare organizations and other custodians of health information seeking guidance on this topic, together with their security advisors, consultants, auditors, vendors and third-party service providers (ISO/FDIS 27799:2007(E), 2007). For a clear differentiation, different types of level of details are defined which imply the target user group in the health organization. The targeted kinds of users are (ENISA, 2006): Management level, Operational level and Organizational level.

Other important characteristics are also the *scalability* (Beham, 2004; Initiative D21, 2001) of the IS security approach and the kind of target organizations (Beham, 2004; BITKOM, 2006; ENISA, 2006; Initiative D21, 2001). During the change of

technology, scalability is one of the most commonly affected parameters. Ineffective scalability can reduce the popularity of the IS security approach. Therefore, adequate care to ensure that the incorporation of the new technology doesn't affect the scalability of the IS security approach should be taken. This means that the IS security approach should be technology-neutral with scalability for size and complexity (ISO/FDIS 27799:2007(E), 2007). Thanks to the definition of the *target organizations* (Beham, 2004; BITKOM, 2006; ENISA, 2006; Initiative D21, 2001), it becomes obvious what type of health organizations the IS security approach aims at (ENISA, 2006): Governments, agencies, Large health organizations, Small and Medium Size health organizations, Commercial health organizations, Non-profit, and Specific sector.

Methodology

Healthcare organizations wanting to conduct information security analysis may find selecting a methodology problematic (Vorster et al., 2001). Currently, there are numerous security methodologies available, some of which are qualitative, while others are more quantitative in nature (Vorster et al., 2001). These methodologies have the common goal of estimating the overall risk value (Vorster et al., 2001). But healthcare organizations must select the most appropriate methodology due to its specific needs. This paper addresses the problem by presenting characteristics for the appropriate security approach within the healthcare domain in case the researched IS security approach offers one.

Security analysis (Beham, 2004; ISO/FDIS 27799:2007(E), 2007; ISO/IEC, 2005) approach should provide a structured methodology based on a set of concepts that comprises, for example, a scope definition (ISO/FDIS 27799:2007(E), 2007; ISO/IEC, 2005), security policy (ISO/IEC, 2005), vulnerability analysis (ISO/IEC, 2005), threat analysis (ISO/FDIS 27799:2007(E), 2007; ISO/IEC, 2005), business impact analysis (ISO/IEC, 2005), scenario analysis (ISO/IEC, 2005), security measures evaluation (ISO/IEC, 2005), cost-benefit analyses and/or gap analysis (ISO/FDIS 27799:2007(E), 2007).

Part of the *security analysis's scope* should be the evaluation of *heterogenic, decentralized information systems* which is also of great importance in the healthcare domain. The increased interconnection of health information systems due to the integrated future e-health makes security approaches in healthcare especially challenging, as few health organizations can act as if their systems were isolated islands of information (ISO/FDIS 27799:2007(E), 2007).

The security approach should be *process-oriented* and not asset or system oriented due to the healthcare processes that directly affect the care and service delivered to the patient (ISO/FDIS 27799:2007(E), 2007). Therefore, the scope of the analysis of the security is the healthcare telematics processes, concerning the information systems, a patient emergency visit, a patient ambulatory visit, prescribing of an electronic prescription, etc., which should be clearly defined.

The focus of the security approach should be targeted at *organizational risks* (Hamdi et al., 2005). The organizational risks are derived from the interaction of people with the information systems and consider the implication of the technical failure of the information systems on the patient.

From the methodological point of view, the existing security approach should be *pro-active* and not reactive. Preventative and reactive security approaches exhibit many differences. The former needs a priori reasoning about security (before the occurrence of a security incident), while the latter requires a posterior intervention after a security incident has occurred (Hamdi et al., 2005).

The selected security methodology should ensure that security assessments produce *comparable and reproducible results* (ISO/IEC, 2005), provide IS security approach guidance on how an organization, through the use of metrics, measurements, and appropriate measurement techniques, can assess its security management status in order to compare it to the previous one. This is part of the continuity of the improvement of the IS security of healthcare, which is of great importance because of the high liability impact.

After conducting a security approach, the measurement of the *maturity* of the information system security should be possible (e.g., through a reasoned best practice document). In healthcare the estimation of the level of maturity is of great importance due to the high liability implications (ENISA, 2006; Initiative D21, 2001).

Surrounding conditions

The characteristic *Available Tools* (Beham, 2004; ENISA, 2006; Initiative D21, 2001) provides a list of tools that support the IS security approach (commercial tools as well as non-commercial ones) (ENISA, 2006). If the IS security approach is supported by a tool: supporting of the complete approach or only part of it (e.g.: tool only for security assessment, tool for process modeling). In the healthcare domain, tool supporting means that appropriate protection is maintained (Standards Australia International, 2003) e.g., easier identification of the health information assets and processes requiring stronger protection i.e., what assets and processes does a health business own (Standards Australia International, 2003).

Certification scheme (ENISA, 2006; Initiative D21, 2001) concerns itself with topics such as whether a health organization may obtain a certificate that it has fully and correctly implemented, and whether the IS security approach to its information systems for the health organization is compliant to specifications, policy, standards or laws that have been clearly defined. This means that a health organization of any size, sector or function can seek independent third party verification of its information management performance. The professional certification is a vital step toward improving patient care, reducing costly mistakes and addressing healthcare disparities.

The last two characteristics of this chapter are the *optimal investment sum* and the *organizational integration* (ENISA, 2006). By establishing the healthcare telematics in Germany, several improvements, such as cost savings, better ways of communication in the healthcare sector or the self-determination of the insured person concerning medical data, are supposed to be achieved (Huber et al., 2008). Taking the target of cost reduction into consideration and regarding the fact that security planning itself causes costs to the health provider that conducts it, the amount of an optimal investment sum related to a security project should be conveniently predicted. After calculating the optimal sum, it is important to know if the IS security approach provides interfaces with existing processes within the health organization (e.g.: hospital logistics process, business continuity planning in healthcare, change management, information system management, project management etc.) in order to measure its degree of customization.

Healthcare Specific IS Security Approaches Characteristics

The information security paradigm within the health industry has special requirements that need to be met, such as added emphasis on the protection and safeguarding of patient information (Brooks et al., 2004). Due to their great importance, this section provides a precise overview of these characteristics and explains them in detail.

In order to estimate the IS security approach's relevance for the healthcare *branch* (BITKOM, 2006), the first most important characteristics are whether the IS security approach aims at heath care, and whether its advice is tailored to healthcare. For further details, we need to see what the target audience is in the healthcare branch (Standards Australia International, 2003). This is the intended *target group* that the IS security approach aims at. Furthermore, this information helps to get an overview of the scope and especially which parties are involved within the organizational processes in the healthcare. We have identified the following different kinds of groups:

- **Health consumers**: patients demand high quality, accessible care, etc. (Standards Australia International, 2003; Standards Australia International et al., 2001).
- **Healthcare providers**: public and private hospitals, physician offices, health professionals, pharmacies, medical centers (Standards Australia International, 2003).
- **Health funders / health agencies**: the rate of funding and payment has not kept pace with the demand for care, which narrows the margin for error and inefficiency. The organization's financial status and assets need to be protected (Standards Australia International, 2003; Standards Australia International et al., 2001).
- **The state**: new pressures for increased accountability create a new demand to know if things are getting better, worse or staying the same (Standards Australia International et al., 2001).
- **Information repositories**: healthcare telematics infrastructure (Standards Australia International, 2003).

One of the specifics in the healthcare branch is that there are several commonwealth and state acts which impact this sector, to which the healthcare organizations must *comply* (ENISA, 2006; Initiative D21, 2001; ISO/IEC, 2005; Standards Australia International et al., 2001). Thus, it is very important to know whether there is a given compliance of the IS security approach to a law or to international or national regulations.

Another of the specifics in the healthcare is that this branch clearly carries relatively high risks, especially in areas such as laboratories, emergency departments and operating theatres (ISO/FDIS 27799:2007(E), 2007). The detection of low risks in health information activities that support such areas ought therefore to be questioned, although the trap of assuming that every health information activity directly relates to care delivery would be equally wrong (ISO/FDIS 27799:2007(E), 2007). In order to help the security assessment, it is important not only to provide proposals of healthcare *generic hazards list* (ISO/FDIS 27799:2007(E), 2007), of *healthcare security requirements* (ISO/FDIS 27799:2007(E), 2007) and of *healthcare security measures* (ISO/FDIS 27799:2007(E), 2007), but it is also of great importance to provide, due to this environment, a carefully designed *risk valuation guidelines relevant to health* (ISO/FDIS 27799:2007(E), 2007). Such valuation guidelines recognize the importance of patient security**,** uninterrupted availability of emergency services**,** professional accreditation and clinical regulation (ISO/FDIS 27799:2007(E), 2007).

A further unique healthcare characteristic is the array of factors to be considered when *assessing these threats* and vulnerabilities (ISO/FDIS 27799:2007(E), 2007) with special emphasis on the provision of the security measures which should take into consideration not only the IS security point of view, but also the patient's point of view. The healthcare sector is more than a decade behind other high risk industries in its attention to ensure information systems security from the patient's point of view. Security in this sense is the first critical step towards improving the quality of care (Standards Australia International et al., 2001).

The protection and security of information is of prime importance to all individuals, government agencies and firms. For the health sector, there is added emphasis on the requirements for *confidentiality*, *privacy*, *integrity*, *availability*, authenticity, commitment, use regulation, accuracy, utility, possession, legal liability, legal certainty, enforceability, suitability for daily use and anonymity (Anderson, 1996; ISO/FDIS 27799:2007(E), 2007; ISO/IEC, 2005; Müller, 2005; Standards Australia International, 2003).

Data quality requirements (ISO/FDIS 27799:2007(E), 2007) are characteristics affirming that medical data must have a state of completeness, validity, consistency, timeliness and accuracy that makes them appropriate for the specific use within the healthcare domain. Due to this fact, data quality requirements should be part of the IS security approach in order to help the security assessments. *The physical security* (ISO/IEC, 2005; Standards Australia International et al., 2001) of the information systems within the healthcare is very important due to the high liability impact. Environmental security (ISO/IEC, 2005) is also an important issue. Organizations processing personal health information should use security perimeters to protect areas that contain information processing facilities supporting such health applications. These secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

CONCLUSION AND OUTLOOK

With the trend going from paper-based towards digital communication, the health industry is relying more and more on IS technology to maintain and advance the treatment of patients (Schweiger et al., 2007). Such reliance on IS technology requires protection from unwanted technological disasters (Anderson, 2000). Research shows that current security approaches lack techniques to analyze not only technical, but especially the social aspects of security within the healthcare domain (Brooks et al., 2004). After having conducted an in-depth literature review and using a structured research approach, we identified a lack of specific security requirements of the healthcare domain based, amongst others, on its unique operating environment, where the security is seen as a people problem and users remain its greatest threat (Schneier, 2008) and based on the specific laws concerning security and privacy of health related data. We then addressed this problem with the presentation of specific information systems security characteristics in healthcare. The focus of the introduced characteristics is the improvement of healthcare based security approaches. The introduced characteristics can be used to estimate the relevance of almost any security approach with respect to the healthcare domain. This knowledge can help to evaluate IS security approaches with regard to their applicability in the healthcare domain, develop new healthcare IS security approaches and to reconstruct existing approaches in order to adapt them to the healthcare situation at hand. By the time of the conference we hope to provide an exemplary application of the presented characteristics.

REFERENCES

1. Anderson, J.G. (2000) Security of the distributed electronic patient record: a case-based approach to identifying policy issues, *International Journal of Medical Informatics*, 60, 111–118.
2. Anderson, R. (1996) A Security Policy Model For Clinical Information Systems, *1996 IEEE Symposium on Security and Privacy*, 1996, Oakland, California, USA, IEEE Computer Society, 30-43.
3. Beham, G. (2004) Corporate Risk and IT-Security Application Method im Vergleich mit anderen IT Security Management Basiswerken, Fachhochschule Hagenberg, Hagenberg, 2004.
4. BITKOM (2006) Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Berlin-Mitte.
5. Blobel, B., and Pharow, P. (2007) A model driven approach for the German health telematics architectural framework and security infrastructure, *International Journal of Medical Informatics*, 76, 2-3, 169-175.
6. Bornman, W.G., and Labuschagne, L. (2004) A Comparative Framework for Evaluating Information Security Risk Management Methods, *Information Security South Africa Conference*, 2004.
7. Brooks, W., and Warren, M. (2004) Health information security evaluation: continued development of an object-oriented method, 2*nd Australian Information Security Management Conference*, 2004, Perth, Western Australia, 135-150.

8. Buela-Casal, G., Perakakis, P., and Taylor, M. (2006) Measuring internationality: Reflections and perspectives on academic journals, University of Granada (Spain) and University of Madrid (Spain).
9. ENISA (2006) *Inventory of risk assessment and risk management methods* ENISA ad hoc working group on risk assessment and risk management,.
10. Haas, P. (2006) Standards für die Gesundheitstelematik, in: *Gesundheitstelematik*, Verlag Springer, Berlin Heidelberg, 2006, 293-378.
11. Hamdi, M., and Boudriga, N. (2005) Computer and network security risk management: theory, challenges, and countermeasures, *International Journal of Communication Systems*, 18, 8, 763-793.
12. Hildebrand, C., Pharow, P., Engelbrecht, R., Blobel, B., Savastano, M., and Hovstø, A. (2006) BioHealth - The Need for Security and Identity Management Standards in eHealth, *Stud Health Technol Inform.*, 121, 327-336.
13. Huber, M., Sunyaev, A., and Krcmar, H. (2008) Security Analysis of the Health Care Telematics Infrastructure in Germany, in: *10th International Conference on Enterprise Information Systems*, Vol. ISAS-2, pp. 144-153, Barcelona, Spain, 2008.
14. Initiative D21 (2001) IT-Sicherheitskriterien im Vergleich.
15. ISO/FDIS 27799:2007(E) (2007) Health Informatics - Information security management in health using ISO/IEC 27002.
16. ISO/IEC (2005) Information technology — Security techniques — Information security management systems — Requirements.
17. Janczewski, L., and Xinli Shi, F. (2002) Development of Information Security Baselines for Healthcare Information Systems in New Zealand, *Computers & Security*, 21, 2, 172-192.
18. LeRouge, C., Mantzana, V., and Wilson, E.V. (2007) Health care information systems research, revelations and visions, *European Journal of Information Systems*, 16, 6, 669-671(663).
19. Mantzana, V., Themistocleous, M., Irani, Z., and Morabito, V. (2007) Identifying healthcare actors involved in the adoption of information systems, *European Journal of Information Systems*, 16, 91-102.
20. Marschollek, M., and Demirbilek, E. (2006) Providing longitudinal health care information with the new German Health Card—a pilot system to track patient pathways, *Computer Methods and Programs in Biomedicine*, 81, 3, 266-271.
21. Müller, J.H. (2005) Gesundheitstelematik und Datenschutz, *Bundesgesundheitsbl - Gesundheitsforsch - Gesundheitsschutz*, 48, 629-634.
22. Schlichtinger, A. (2005) Standards of the IT-Governance: COBIT, ITIL etc. - description, confrontation and classification, *Abteilung für Informationswirtschaft* Wirtschaftuniversität Wien Wien, Austria 2005, 29.
23. Schneier, B. (2008) The Psychology of Security *Communications of the ACM*, 50 5, 128.
24. Schweiger, A., Sunyaev, A., Leimeister, J.M., and Krcmar, H. (2007) Information Systems and Healthcare XX: Toward Seamless Healthcare with Software Agents, *Communications of the Association for Information Systems*, 19, 33, 692-709.
25. Standards Australia International (2003) *Information security management — Implementation guide for the health sector* Standards Australia International Ltd,, Sydney.
26. Standards Australia International, and Standards New Zealand (2001) *Guidelines for managing risk in healthcare sector: Australian/New Zealand handbook* Standards Australia International, Sydney.
27. Sunyaev, A., Göttlinger, S., Mauro, C., Leimeister, J.M., and Krcmar, H. (2009) Analysis of the Applications of the Electronic Health Card in Germany, *WI 2009 - Proceedings of Wirtschaftsinformatik 2009 - Business Services: Konzepte, Technologien und Anwendungen*, Vienna, Austria, 25-27 February 2009, Band 2, pp. 749-758.
28. Sunyaev, A.; Leimeister, J.M.; Schweiger, A.; Krcmar, H. (2008): IT-Standards and Standardization Approaches in Healthcare, *Encyclopedia of Healthcare Information Systems*, Publisher: Idea Group, 2008, pp. 813-820.
29. Toyoda, K. (1998) Standardization and security for the EMR, *International Journal of Medical Informatics*, 48, 57-60.
30. Vorster, A., and Labuschagne, L. (2001) A Framework for Comparing Different Information Security Risk Analysis Methodologies, University of Johannesburg.
31. Webster, J., and Watson, R.T. (2002) Analyzing the past to prepare for the future: writing a Literature Review., *MIS Quarterly*, 26, 2, xiii-xxiii.