**A comparative review of information security risk assessment methodologies for health care**

N. Hazelhoff Roelfzema

Institute for Informatics & Digital Innovation, Edinburgh Napier University

10 Colinton Road, Edinburgh EH10 5DT, United Kingdom

# ABSTRACT

Health care organizations face major compliance challenges as they need to secure patient information. An important compliance requirement is the performance of regular risk assessments and the implementation of controls to secure data. In theory, any state of the art risk assessment technique could be employed to facilitate the prevention and/or management of potential information risks. Health care environments are, however, quite unique when compared to other automated environments and different sectors do not experience similar kinds of information security attacks. Where security issues have been researched in health care, there is a strong emphasis on the development of technological measures for data protection but the ‘human’ or professional side of ensuring data security is equally important in everyday practice. In this paper, seven methodologies for risk assessment are compared in a framework with specific health care requirements. It is concluded that improvements could be made in comparative frameworks to support the selection process for a suitable risk assessment approach. Furthermore, the available methods show several weaknesses in their ability to quantify risks or to include human risk factors. The presentation of threat events and their interaction is often oversimplified. Data aggregation is not possible in order to allow regulators to gain insight in trends and high level security threats. An integration of existing techniques is proposed to facilitate reliable and repeatable risk assessments that contribute to compliance to governance codes, and costs savings by making informed -sector wide- decisions to invest in the development of new systems and security controls.

KEYWORDS

Risk assessment, information security, health care, governance.

1. INTRODUCTION

Health care organizations face major compliance challenges as they need to secure patient information. Standards and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the US, the Information Governance Framework for the NHS in the UK, or the Health Care Governance Code in the Netherlands, require the performance of regular risk assessments and the implementation of controls to secure data. In the UK, the Department of Health recommends that the Boards of NHS organizations should ensure that the effort and resources that are spent on managing risk are proportionate to the risk itself. Therefore, it is essential that risks are valued according to the likelihood and damage they can cause and that the risk assessment leads to a quantified value for the risk. There are many different methods and tools for information security and risk assessment available and this paper aims to compare methodologies for their suitability in a health care environment. In theory, any state of the art risk assessment technique could be employed to facilitate the prevention and/or management of potential information risks. Health care information systems are, however, quite unique when compared to other information systems, with the result that they require a different approach to risk management (Smith and Eloff, 1999). Furthermore, it seems not true to assume that different sectors experience similar kinds of information security attacks (Kjaerland, 2006). A recent study by Appari and Johnson concluded that despite the growing stream of research on information security, very limited research has focused on studying information security risks in the health care sector, which is heavily regulated and calls upon business models quite different from other industries (Appari and Johnson, 2010). Where security issues have been researched in health care, there is a strong emphasis on the development of technological measures for data protection. However, the ‘human’ professional side of ensuring data security is equally important in everyday practice (de Lusignan, Chan et al., 2007). In large health care organizations, the number of people moving through operational areas is significant. By their nature, health care organizations operate in an environment where visitors and the public at large can never be totally excluded. Any risk assessment approach used in health care should evaluate a combination of technological, human and organizational risks. The approach should also be dynamic and future proof: health care organisations and their information technology are complex adaptive systems, thus requiring adaptive decision making processes and adaptive risk assessment approaches (Rasmussen, 1997). In the next section, several risk assessment techniques are compared against a set of characteristics that are specifically relevant to health care environments.

1. Comparative Framework

A list of commonly known information security standards, tools and methods in Europe is maintained by Enisa (2010). Five Health care specific information security methods have been identified: Odessa, RiMaHCof, Octave, NHS toolkit and IEC 80001, and these methods will be discussed in the next section. In order to provide a structured review, a number of know information security methods were compared using a framework of characteristics. The characteristics were partially inspired from other comparative frameworks for information security methods (Vorster and Labuschagne, 2005; Sunyaev et al., 2009). Only methodologies that include risk assessment techniques as part of the risk management process were assessed against the framework. Several information security methods or standards describe a management framework; they deliver a set of processes to manage information security in an organization. However, the scope of this review does not include the question how responsibilities and procedures are to be embedded within the organization. This review only compares the risk measurement techniques. The comparative framework was set up to deliver answers to the following questions:

* Are the threats provided for in the current risk analysis methodologies also representative of the threats occurring in the health care environment?
* Are the methods used to perform the actual risk analysis modelling scientific and well suited to health care environments?
* Does the methodology effectively model and evaluate both the technical and human aspects of information security in a health care environment, taking into account dynamics of organisational and technological changes?

With the help of the framework, the methodologies were assessed on the following characteristics:

**Sector**: The market sector that it was designed for or developed in. Was it developed for health care?  
**Standard**: Formal method or industry standard that it refers to.  
**Year**: Available for public use since.  
**Aggregation**: Is it possible to analyse results and aggregate data from individual assessments to organizational or regional level?  
**Scope**: Information systems focus, human, process focus or combined?   
**Measurement method**: Is risk measured with a quantitative or a qualitative approach?  
**Presentation and risk description**: How are risks presented and described in words?  
**Key feature**: What makes this method special?  
**Research activity**: Are there published case studies in health care organizations or evaluations available?

Available documentation and manuals were reviewed for these characteristics. A literature search on databases with journals related to computing, health care, nursing and medical informatics was performed to find case studies or reviews relating to the use of a specific method in a health care environment.

1. methodologies and their characteristics

**3.1 Information security risk assessment methodologies designed for health care**

A study in the US amongst 250 health care organizations concluded that Health Care organizations are actively taking steps to ensure that patient data is secure. However, hospitals appear to be focusing on how to handle a breach after it has taken place, rather than focusing on prevention through risk assessments (Kroll-Fraud-Solutions, 2010). Risk management for health care organizations can be defined as an organized effort to identify, assess, and reduce, where appropriate, risks to patients, visitors, staff, and organizational assets (Kavaler and Spiegel, 2003). Risk management in Health care includes the whole spectrum of things that could and can go wrong. It includes slips, trips and falls involving staff, patients and the public, administrative errors that impact on patient care and clinical incidents that have a direct effect on the outcome of patient care. It also includes the management of the business risks associated with running a health care organization or hospital including financial, ethical and information technology risks. Risk assessment methods for health care organizations include Health care Failure Mode and Effect Analysis (developed by the US Department of Veterans Affairs) and PRISMA-medical. Prisma stands for Prevention and Recovery Information System for Monitoring and Analysis (Eindhoven University of Technology). Furthermore, there is a variety of risk assessment methods available for public health, disease risk assessment and workplace Health and Safety. Surprisingly enough, not many widely implemented approaches to information risks exist. The literature search found only five information security risk assessment methods for health care and 2 independent methods that are currently being used in health care environments. These seven approaches were reviewed in the framework of characteristics. A summary of these characteristics is illustrated in table 1.

**Odessa** is a methodology that provides health care data security, developed in the UK in 1997 (Warren et al., 1997). However, the database search did not find any published case studies or reviews or other evidence of this approached being used or having evolved since. Odessa could not be evaluated in depth as no detailed documentation was available.

Risk management in health care – using cognitive fuzzy techniques (**RiMaHCoF**) is a prototype for assessing information technology risks in health care (created in South Africa) (Smith and Eloff, 2002). This approach is a qualitative assessment with the focus on technical aspects and human aspects are not in scope of this model, which is considered a major shortcoming. The database search did not find any published case studies or reviews.

A well-documented approach comes from **CORAS** (Lund, 2011): a methodology that bases itself on: hazard and operability (HazOp), fault tree analysis (FTA), failure mode and effect criticality analysis (FMECA), Markov analysis, CCTA risk analysis and management methodology (CRAMM). CORAS was a European Research & Development project that run from 2001 to 2003. The aim was to develop an integrated framework for model-based risk analysis of security critical systems within telemedicine and e-commerce. CORAS has further evolved since, and now provides a customized language, the CORAS diagrams, for threat and risk modelling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis (Hogganvik 2007). A successful case study has been published for a cardiology eHealth service in Crete (Stathiakis et al, 2003), but no further implementations have been published.

The **NHS Information Governance** toolkit knowledge base is an online list of good practice guides, standards and templates for NHS organizations in the UK. The risk matrix for managers guidance has been developed for the purpose of assisting NHS risk managers in implementing an integrated system of risk assessment. It can be adapted, depending on the needs of individual NHS trusts. This guidance can be used on its own as a tool for introducing risk assessments in an NHS organization, or for improving consistency or scope of risk assessments already in place in NHS organizations and for training purposes (NPSA, 2008). The risk matrix could be used for any risk: financial, safety, environmental, quality and so on. No examples are included that relate to information security risks. The toolkit also contains an ISMS risk assessment template. This template is provided to “assist NHS organisations and General Practices to identify, assess and evaluate the treatment of risk that is appropriate to their local business needs” (NHS, 2007). The template describes a high level procedure, but gives no detailed guidelines to evaluate risk scores. The toolkit does not give any further information about risk assessments. The Department of Health Informatics Directorate considers CRAMM to be the standard for risk analysis for NHS information systems (NHS Connecting for Health, 2010). Siemens, the supplier of CRAMM, advises on their website the availability of a NHS toolkit for CRAMM. The NHS IG Governance toolkit does not provide further references to this specific toolkit.

The NHS Information Policy Unit and NHS Information Authority had developed an Information Security Officers’ Toolkit based on **CRAMM**. In CRAMM the information is gathered through interviewing the owners of assets, the users of the system, the technical support staff, and the security manager. In this manner, CRAMM is more like a review of the security of a product, conducted during the system development or for an already running system. Physical assets are valued in terms of the replacement cost. Data and software assets are valued in terms of the impact that would result if the information were to be unavailable, destroyed, disclosed or modified. There is not much focus on risks in operational processes or human factors. The risk assessment again is qualitative, but the supporting software provides the advantage of generating the appropriate controls and countermeasures for each risk. The documentation produced during a CRAMM review uses a standardized format, mostly in the form of tables. The documentation is compliant with the mandatory documentation needed to achieve ISO 27001 certification.

**Octave** is a method aligned to the HIPAA standard. It is a well-documented methodology from the US with a strong presence on conferences and publications in journals. Although it was developed for manufacturing, it has been tailored for health care since 2002. Several publications describe case studies in health care environments. Coleman published a report on the use of Octave in 3 health care organizations of different size and geographical location (Coleman, 2004) and reported that the method is usable in different health care environments. The method documents the risk findings in tables and creates threat trees using a simple graphical tree-structure. The approach is quite similar to the one used in CORAS.

Currently a new risk approach is under development: the **IEC 80001** Application of risk management for IT-networks incorporating medical devices. The IEC 80001 addresses how accumulated and residual risks from medical and nonmedical equipment and applications should be managed in a heterogeneous networked environment, how controls and monitors should be identified and affected, and how remaining risk should be documented, communicated, and approved by senior management all before the technologies are deployed. It aims to address the key properties of safety, effectiveness, data and system security. The publication of this standard is expected by the end of 2010. It will be evaluated in this framework as soon as it becomes available.

**4.2 Methodologies for other sectors**

A quick review of the other information security methods shows that most of them use a table or a list of possible threats to assess risks. However, a list of terms is not sufficient; there should be description of how the various threats relate to each other. A security breach is more likely to be caused by a chain reaction or combination of events than just by one single threat picked from a list. Furthermore, a threat on its own does not have to cause a risk, if there are no vulnerabilities to exploit at that time. Any security incident often forms part of more complex landscape of external threats, managerial and regulatory failure, of poor technical design and of operational inadequacies (Johnson, 2006). Mackie (1993) uses the term ‘causal complex’ to describe this causal landscape. Each individual factor in a causal complex may be necessary for an incident to occur but an attack may only be successful if they happen in combination. Several different causal complexes can lead to the same outcomes even though only one may actually have caused a particular incident. A repeating difficulty in risk assessment seems to be the risk estimation. Risk estimation is concerned with determining the likelihood of occurrence and a quantification of the consequences. Evaluating the severity of the consequences (impact) is often difficult for immaterial assets. Often, the participants in a risk assessment are unable to estimate the likelihood of risk in terms of an exact numeric value. Most methods give no guidelines on how to quantify a risk. The BSI-standard 100-3 has decided not to consider the likelihood of occurrence in their method because “keine Grundlagen für verlässliche Schätzungen vorhanden sind” (BSI, 2008). The most commonly used approach is a qualitative technique with a nominal scale of potentiality of risks. Raz and Hillson reviewed, amongst others, the 6 risk management standards illustrated in the left circle in figure 1 for qualitative techniques and their conclusion that most tools that are used to identify risks are descriptive and qualitative in nature, and that there are very few tools based on statistical or mathematical techniques (Raz and Hillson, 2005). This further supports the conclusion that there is gap in knowledge for information risk quantification.

1. CONCLUSIONS

The review of information risk assessment methods and security breach databases in this paper has shown that health care organizations are not presented with many options when it comes to the selection of an information security risk assessment methodology. Octave in the US and CRAMM in the UK seem the most commonly advised approaches, but CRAMM is considered to be more a ISO 27001 compliance tool than a risk evaluation method. CORAS has been tested, but not widely implemented as a standard approach in information security policies and governance standards. Governance standards require performing risk assessments, but there are no clear guidelines on how to select a risk assessment approach.

Popular methods generally use pick-lists for the risk assessor to describe threats, but in reality a security risk is more likely to be caused by a combination of events than just by one single threat or source and could therefore better be presented in tree-like diagrams. The CORAS’ presentation of risks in diagrams improves the understanding of how events are related and could lead to a data security breach. Further enhancement of these diagrams by using health care specific terminology will make them even more user-friendly and appealing to the professionals participating in the assessments.

Many information security risk assessment approaches have a technology focus and assess the risks of a system, a database, an application or a network on a given point in time. This delivers incomplete results, but there is no set of guidelines on how to assess the risks to information security caused by a patient, administrative employees, nurses, volunteers or specialists. Studies in human factor engineering, criminology and human behaviour studies could add valuable knowledge to the understanding of threats to information security. Further value could be added from risk assessment methods in environmental studies or the financial sector, where adaptive risk management for complex situations has been researched and applied.

It is essential that risks can be rated in a common currency, allowing financial, operational and clinical risks to be compared against each other and prioritized (NPSA, 2008). This comparison should include information security as a risk category. This currency or measurement could be improved by implementing quantitative risk scoring mechanisms, which is not impossible, as can be learned from the risk models in the banking and insurance industry (Hubbard, 2002).

Individual health care organization and the sector in general could benefit from a knowledge base of common security risks. None of the above methods support a central database to analyse risks and trends and to benchmark similar environments. Individual risk assessments lead to individual investments in countermeasures to control the risks. If health care practises and their partners were provided with the knowledge from others, investments could be shared or specific solutions could be copied and there will be a better understanding of each other’s key risks and priorities. Trend analysis would make it possible for regulators and individual practices to target the main risk areas quicker and more cost-effective. Regulators and public administration could also use this knowledge to adjust and maintain their policies and compliance requirements. For regulators and public administration, the management of risk and trust is crucial and it is critical that they receive high quality information about issues and communicate more effectively about them (Lips et al, 2005).

An integrated and adaptive risk management approach is needed for health care to meet their compliance requirements. Information risks should not be approached from a technology point of view as information risks include human and organisational threats and should be part of the entire enterprise risk management framework. The risks should be presented in understandable language, and be quantified in order to better map those risks to countermeasures. The development of a cross-organisational integrated risk management system will allow organisations to respond to their partner(s)’ key risks as they do to their own. Risk assessment results should not be kept within individual organizations; knowledge should be shared in a central system that enables a benchmarking and trend analysis for the whole sector, which could further contribute to policy improvement and cost reductions.

REFERENCES

Appari, A. and M. E. Johnson, 2010. Information security and privacy in Health care: current state of research. *International Journal Internet and Enterprise management.* Volume 6, issue 4, pp 279-310.

BSI, 2008. BSI-Standard 100-3: *Risikoanalyse auf der Basis von IT-Grundschutz*. Bundesamt fur Sicherheit in der Informationstechnik, Bonn, Germany.

Coleman, J., 2004. Assessing information security risk in Health care organizations of different scale. *Computer Assisted Radiology and Surgery*, Chicago, USA, pp 125-130.

De Lusignan, S. et al., 2007. The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International Journal of Medical Informatics,* Vol. 76, No. 4, pp 261-268.

ENISA, 2010. *Inventory of Risk Management/Risk Assessment Tools*. Retrieved 6 January 2010, from <http://www.enisa.europa.eu>.

Hazelhoff Roelfzema, N., 2010. A novel security risk assessment method for personal health data. [*PerAda workshop on Privacy, Security & Trust*](http://www.perada.eu/perada-activities/18-current-events/133-media-resources-perada-rome-november-2010). 22-23 November 2010. Rome.

Hogganvik, I., 2007. *A graphical approach to security risk analysis*. Faculty of mathematics and natural sciences. Oslo, University of Oslo. PHD: 154.

Hubbard, D. W., 2002. *How to measure anything: finding the value of "intangibles" in business*. Wiley & Sons, Hoboken, New Jersey.

Johnson, C. W., 2006. *V2: Using violation and vulnerability analysis to understand the root-causes of complex security incidents*. Glasgow, University of Glasgow.

Kavaler, F. and A. D. Spiegel, 2003. *Risk Management in Health Care Institutions. A strategic approach.* Jones and Bartlett Publishers.

Kjaerland, M., 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, Vol. 25, pp 522-538.

Kroll-Fraud-Solutions, 2010. *2010 HIMSS Analytics report: security of patient data*, Kroll Fraud Solutions.

Lips, M. et al, 2005. Public administration in the inforamtion society: essays on risk and trust. Editorial. *Information policy*. Vol. 10, pp 1-9.

Lund, M.S., et al, 2011. *Model-driven risk analysis. The CORAS approach*. Springer-Verlag, Berlin Heidelberg.

Mackie, J.L., 1993. Causation and conditions. In E. Sosa and M. Tooley (eds.), *Causation and Conditions*, pages 33-56. Oxford University Press, Oxford, 1993.  
NHS, 2007. *NHS Information Governance: Guidance – ISMS Risk Assessment Template*. Retrieved 16 October 2010, from [www.igt.connectingforhealth.nhs.uk](http://www.igt.connectingforhealth.nhs.uk).

NHS Connecting for Health, 2010. *Standards and methods*. Retrieved 3 December 2010 from <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/standards>.

NPSA (National Patient Safety Agency), 2008. *A risk matrix for managers.* London.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. *Safety Science,* Vol. 27, No. 2/3, pp 183-213.

Raz, T. and D. Hillson, 2005. A comparative review of risk management standards. *Risk management: an international journal,* Vol*.* 7, No. 4, pp 53-66.

Smith, E. and J. H. P. Eloff, 1999. Security in health-care information systems--current trends. *International Journal of Medical Informatics,* Vol. 54, No. 1, pp 39-54.

Smith, E. and J. H. P. Eloff, 2002. A prototype for assessing information technology risks in health care. *Computers & Security*, Vol. 21, No. 3, pp 266-284.

Stathiakis, N., et al, 2003. Risk Assessment of a cardiology eHealth servcie in HYGEIAnet. *Computers in Cardiology,* Vol. 30, pp 201-204.

Sunyaev, A., et al, 2009. Characteristics of IS Security approaches with respect to Health care. *Americas Conference on Information Systems (AMCIS)*, San Francisco, California.

Vorster, A. and L. Labuschagne, 2005. A framework for comparing different information security risk analysis methodologies. *Proceedings of South African Institute for Computer Scientists and Information Technologists*. Mpumalanga, South Africa.

Warren, M. J., et al, 1997. ODESSA: a new approach to Health care risk analysis*. Proceedings of the IFIP TC11 13 international conference on Information Security (SEC '97) on Information security in research and business*. Copenhagen, Denmark.

Table 1. Overview of characteristics of the compared methodologies

| **Characteristic** | **Odessa** | **RiMaHCof** | **NHS IG toolkit** | **IEC 80001** | **OCTAVE** | **CORAS** | **CRAMM** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sector** | Health care, developed within UK University | Health care organisations in South Africa | Health care, NHS in the UK | Health care | Manufacturing, but tailored for health care since 2002 in the US. | CORAS is a European R&D project, aims to develop an integrated framework for model-based risk analysis of security critical systems within telemedicine and e-commerce. | CRAMM (CCTA Risk Analysis and Management Method) was created in 1987 by the Central Computing and Telecommunications Agency (CCTA) of the United Kingdom government |
| **Year** | 1997 | 2002 |  | December 2010 | 2003 | 2003 | 1987 |
| **Standards used** |  |  | AS/NZS 4360:1999 Risk Management,  BS 7799 | Does not address regulatory or legal requirements | SP800-30 | AS/NZS 4360:1999 Risk Management, hazard and operability (HazOp), fault tree analysis (FTA), failure mode and effect criticality analysis (FMECA), Markov analysis, CRAMM. | ISO 27001 |
| **Scope** | Medical information systems | IT risks for each phase in a patient route. Technical aspects of securing patient information. Human aspects are not the primary focus of the model. | Provides the Information Governance standards and guidance for the NHS and partner organisations. | It defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address safety, effectiveness and data and system security. | Risk-based information security strategic assessment and planning | Applicable to security critical systems to aid the early discovery of security vulnerabilities, inconsistencies and redundancies and will provide methods to achieve the assurance of the security policy implementation | Providing a structured and consistent approach to computer security management for all systems. |
| **Data aggregation** |  |  |  |  |  |  | Some |
| **Focus** |  | Information systems | Systems and Enterprise risks |  | Assets | All types. | Physical, software, data and location assets. |
| **Measurement method** |  | Qualitative, using cognitive fuzzy-logic approach. | Qualitative |  | Qualitative | Qualitative | Qualitative |
| **Presentation** |  | Scenario. | Table. |  | Scenario, threat trees. Limited use of graphical modelling. | Scenario, UML graphical presentation | Common risk based tables. |
| **Key feature** |  |  | The approach is suitable for different types of risks. |  | Maps threat trees to risk profiles and scores impacts (although qualitative). | Graphical threat and risk modelling | Supporting tool generates countermeasures for the risks |
| **Research activity** |  |  |  |  | Several conference presentations and a case study | Several conference presentations and a case study |  |