The Adoption of IT Security Standards in a Healthcare Environment

Rui GOMES\textsuperscript{a,c} and Luís Velez LAPÃO\textsuperscript{b,c} \textsuperscript{1}

\textsuperscript{a} Hospital S. Sebastião – Sta. Maria da Feira, Portugal, \textsuperscript{b} Healthcare Systems Group, Instituto Nacional de Administração, Portugal, \textsuperscript{c} CINTESIS-Faculdade de Medicina, Universidade do Porto, Portugal

Abstract. Security is a vital part of daily life to Hospitals that need to ensure that the information is adequately secured. In Portugal, more CIOs are seeking that their hospital IS departments are properly protecting information assets from security threats. It is imperative to take necessary measures to ensure risk management and business continuity. Security management certification provides just such a guarantee, increasing patient and partner confidence. This paper introduces one best practice for implementing four security controls in a hospital datacenter infrastructure (ISO27002), and describes the security assessment for implementing such controls.

Keywords: ISO 27002, Security standards, CIO, Healthcare Information Management.

Introduction

Healthcare services aims at serving people well. In this regard, the need for IS standards is recurrent since every year thousands of people died as the result of clinical errors caused by fatigue or inaccuracy that could have been prevented with proper technology \cite{1}. Most of the problems have to do with lack of coordination between systems due to the use of different standards \cite{2}. Anybody waiting for the standards bodies before implementing IS will be waiting such long time, but information security must stay manageable and able to let preventing threats, reduce vulnerabilities and risks. Hospital S. Sebastião (HSS) is aware of the significance of information security issues and the relevance of standards and frameworks such as Committee Of Sponsoring Organizations of the Treadway Commission (COSO) \cite{3} for financial processes control, COBIT \cite{4} for information technology (IT) control, “Health Insurance Portability and Accountability Act” (HIPAA) \cite{5} to insurance protection and promoting communications standards and ISO 27002 \cite{6} to manage the information security. Our approach here will focus on healthcare IT security issues. The COSO is a group of standards that includes different financial and auditing institutions’ functions, while COBIT, Control Objectives for Information and related Technology is a good

\footnote{1 Corresponding Author: Prof. Luís Velez Lapão, Healthcare Systems Group, Instituto Nacional de Administração, Palácio dos Marqueses do Pombal, 2784-540 Oeiras, Portugal, email: luis.lapao@ina.pt.}

framework for assessing, managing and reducing IT risks. We aim at applying the ISO27002 standards to HSS taking advantage of its comprehensiveness in implementation details. One must recognize that each framework has its own weaknesses and strengths; e.g. ISO27002 has a complete level of security, but does not contain product-oriented measures, such as those used on COBIT [4].

1. The IT Security Standards in the Healthcare Environment

The use of standards can be viewed from legal and IT architecture perspectives [7]. From the legal perspective, there are ranges of standards that either recommend general or specific scenarios in healthcare. In the USA, HIPAA is a legal requisite and comprehensive health information protection policy, which promotes the development of electronic healthcare transactions and specifically addresses the issues of privacy and security for health related information [5]. The security element specifically distinguishes the innate problems in using electronic forms of records keeping and the changing nature of the technology upon which such records are recorded, used and stored. HIPAA has suffered many delays but it had a clear impact on services feasibility [8]. From IT standards perspective, we refer to ISO27002 (former British Standard Institute (BSI) 7799-1:1999) to assist in the development of security plans. It is a “Code of Practice” purposeful on high-level security management, revised in 2005 to cover current technology and business practices. ISO 27002 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices based on 11 main sections. As a code of practice it cannot be used for certification, so another standard has been developed ISO 27001 (information security management system requirements) which is certifiable [9]. This standard specifies the requirements for security implementation that is customizable for individual organizations. ISO standards are only a starting point, as they do not contain widespread information on how security measures should be implemented or maintained. Other standards exist for specific proposes of health information, particularly for use in e-health information exchange, like HL7 [10] developed as a standard for clinical information exchange and based predominantly on the HIPAA guiding principles. In addition, the CEN (European Committee for Standardization) is putting significant effort into development of healthcare information systems security in Europe. However, this has resulted in an assorted range of standards being developed for specific instances of technology use. Many standards do not include sufficient security-related provision and given the complex nature of standards, it has resulted in a large number of providers selling security management solutions for interpretation of the standards and also to explore its implementation.

2. The Process of Adoption of IT Security Standards: The role of the CIO

It is now accepted that healthcare is one of the most complex businesses with a large diversity of types of interactions [11, 12]. The possibility of using IS to support the services delivery also opens new opportunities. Smith [13] and others [14] have proposed that only Information Systems (IS) could bridge the information "chasms". Interoperability of healthcare systems can play a critical role in this process. The Institute Of Medicine reports [14, 15] identified weaknesses in the design and safety of
healthcare IS whereas interoperability rules’ utilization can provide additional pressure to help the proper use of technology in that regard [16]. Both technical and semantic interoperability require a wide organizational agreement on standards. Both represent huge tasks to be accomplished and require people in the organization to deal with it. Specialized groups such as IHE are pushing the debate and developing interoperability profiles to tighten areas of ambiguity en route to stronger interoperability. The HL7’s Electronic Health Record (EHR) group has produced many reports and other materials to guide technology managers towards interoperability. But before going into this sophisticated processes there are many other basic areas that need to be properly covered, being security issues one of them. The human and organizational side of the interoperability has been mostly forgotten [17, 18]. For a long time healthcare process engineering was also not taken very seriously [19]. In order to take advantage of an IS it is necessary a leadership to promote the alignment of business with IS. In this complex environment the role of the Chief Information Officer (CIO) is critical to ensure good focus on organizational specificities. It was recognized that best performing HIS departments were related with department heads that matched CIO attributes [12], like openness to suggestions and excellent relationship with other healthcare professionals; leadership skills, which help them to address challenges; meaningful negotiation skills which are used in their relationships with the vendors, openness to bolder projects with new technologies; etc. Healthcare CIOs are a kind of “special people” that push the organization further through an innovative use of technology [18, 20]. They know that pushing for interoperability will allow the organization to be more productive and less inefficient. Interoperability in an organization can also mean data access safety and security.

3. The Hospital S. Sebastião Information Security Case

HSS is integrated in the National Health Service providing tertiary health care services for all citizens of its geographical area. Built in 1999, it covers an area with 367 000 inhabitants. HSS was chosen to become involved in an innovative management framework, supported by the Ministry of Health, to show the evidence of the improving efficiency of the new framework.

3.1 HSS Information System Architecture

Hospital owns today a unified IS platform that aims to serve not only administrative and management purposes but mainly patients needs, helping professionals doing their job correctly. This middle management application provides approximately 320 physicians and 510 nurses with an integrated view of all clinical information related with the patients, from exams to surgery reports. Since 1999, those physicians create and stores medical records through the hospital’s datacenter storage bank. The IS architecture is showed below (Figure 1.), where all the exclusively solutions contribute to grow the datacenter databases on consolidate and concentrated philosophy.
The architecture definition was a long working process. The hospital board have recognized that a huge effort was carried out to minimize risks concerning the information management, data privacy and protection. This level of maturity was achieved in 2003, though these good principles are still not enough. These first successes encouraged the CIO, the IT personnel and top managers to be more focused on the improvement of the information security management.

3.2 CIO Role in the HSS IT Security Approach

The CIO created a team to address the IT security at the HSS. After relevant literature and practices review, it was selected the ISO27002 rather than COBIT. COBIT’s entirety would make implementation onerous and if one compared it with ISO27002, it is easy to see that it focuses more on efficiency and effectiveness of IT environment rather than information security linked to business issues. It was recognized that ISO27002 represents a good mix of international acceptance level and full comprehensiveness, as well as it is dedicated most exclusively for information security practices built around policy and process management. However, in the future it could be necessary to implement some COBIT measures to accomplish ISO27002 good practices. The applications servers and databases are all concentrated and beneath a controlled physical habitat, and what concerns securing and managing information, the prerequisites surround ISO27002 were recognized as an excellent point of reference to starting managing the information security. Some of controls of this standard have been implemented over a hospital datacenter infrastructure area and the focus has been IT and security policies as a best practice for information security management in the daily basis procedures operation. ISO27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems. 11 main sections border physical and logical preservation of confidentiality, integrity and availability properties. Making analogy with ISO quality standards and their way of managing and improving hospital made process of ISO27002 implementation as easy as possible. Analogically to quality manager, information security manager observes situation, gives regular assessments, and then recommendations for improvement, afterwards business managers determine to what issues investments should be put in as well as their priority. All 11 ISO27002’s control chapters have subset elements. To
provide performance measurement HSS rated the 39 main security categories, based on ISO27002 structures and according to a simple level of risk scale H-M-L (High-Medium/Moderate-Low/Tolerable). The following table 1., concisely shows the risk levels for each control area helping the CIO to rapidly overview the whole picture of information security and to identify priority actions.

Table 1. Risk Levels in the ISO 27002

<table>
<thead>
<tr>
<th>#</th>
<th>ISO 27002 Section</th>
<th>Risk Level (control objective)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>H</td>
</tr>
<tr>
<td>1</td>
<td>Security Policy</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Organizing Information Security</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Asset Management</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Human Resources Security</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Physical and Environmental Security</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Communications &amp; Operations Management</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Access Control</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>Information Systems Acquisition, Development and Maintenance</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Information Security Incident Management</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Business Continuity Management</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Compliance</td>
<td>0</td>
</tr>
</tbody>
</table>

The application of this framework has been quite successful at HSS. For instance, section 3, 5, 6 and 7 were well accomplished in the datacenter infrastructure whereas the security assessment sections were based on the most relevant high-risk level control objective.

3.3 IT Security Project Issues

CEO and CIO have assumed the project and the relevance of a security auditing and it’s implications: for instance, the obligation to up-grade, both physically and logically, the datacenter, and to change the daily modus operandi. The hospital board decided to hire an auditor (named by SINFIC, a BSI certificated partner). The auditor applied a Gap Analysis with five major steps: 1. Project planning, to ensure that expectations, timelines and deliverables are appropriately managed. 2. During the Information-gathering phase many players were interviewed to determine the business environment and current security management and system administration processes through in-depth discussions with key players in the organization. 3. At the Review and Analysis stage Security Policies, Procedures and Practices were addressed to evaluate the existing security policies, procedures and practices, and compare it with the ISO27002 international security standard and industry best practices. 4. The Review and Analysis stage results help to write down a concise, detailed technical and ISO27002 Security Assessment Executive Summary Report. 5. External and Internal vulnerability scanning to discover all devices and applications across the datacenter, and to identify and eliminate the security threats that make datacenter infrastructure attacks possible.
4. Conclusions

From the case presented one should conclude that rules code of practice or standards are essential to ensure the delivery of benefits to the patient and healthcare providers in information interoperability. This is only part of a bigger effort to implement a comprehensive strategy that allows consistency of information collection and sharing within the healthcare sector. This effort will establish a secure infrastructure between organizations over which to share patient secure information. It is required a comprehensive set of standards that define practical guidelines for the healthcare community, for which ISO27002 is a good benchmarking. Its area of application is a set of diverse and heterogeneous organizations like public hospitals, private, specialists and general practitioners. It means that specific targeted standards should be developed or established for the protection of sensitive information, and not left to individual interested parties to build up. It also means that we are facing a rather new field yet to be proven, implying that the CIO responsible for the implementation of an IS security framework will have to deal with its many variables and barriers. The CIO role and understanding of the organization’s environment is key to deliver real interoperability potential to the organization to patients’ benefit.

References

[4] COBIT. Control Objectives for Information and related Technology", control focuses on IT.