Information Security Management in Picture Archiving and Communication Systems for the Healthcare Industry

Carrison K.S. Tong
Pamela Youde Nethersole Eastern Hospital, Hong Kong

Eric T.T. Wong
The Hong Kong Polytechnic University, Hong Kong

INTRODUCTION

Like other information systems in banking and commercial companies, information security is also an important issue in the health care industry. It is a common problem to have security incidences in an information system. Such security incidences include physical attacks, viruses, intrusions, and hacking. For instance, in the USA, more than 10 million security incidences occurred in the year 2003. The total loss was over $2 billion. In the health care industry, damages caused by security incidences could not be measured only by monetary cost. The trouble with inaccurate information in health care systems is that it is possible that someone might believe it and do something that might damage the patient. In a security event in which an unauthorized modification to the drug regime system at Arrowe Park Hospital proved to be a deliberate modification, the perpetrator received a jail sentence under the Computer Misuse Act of 1990. In another security event (The Institute of Physics and Engineering in Medicine, 2003), six patients received severe overdoses of radiation while being treated for cancer on a computerized medical linear accelerator between June 1985 and January 1987. Owing to the misuse of untested software in the control, the patients received radiation doses of about 25,000 rads while the normal therapeutic dose is 200 rads. Some of the patients reported immediate symptoms of burning and electric shock. Two died shortly afterward and others suffered scarring and permanent disability.

BS7799 is an information security management standard developed by the British Standards Institution (BSI) for an information security management system (ISMS). The first part of BS7799, which is the code of practice for information security, was later adopted by the International Organization for Standardization (ISO) as ISO17799. The ISO 27002 standard is the rename of the existing ISO 17799 standard. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented. The second part of BS7799 states the specification for ISMS which was replaced by The ISO 27001 standard published in October 2005. The Picture Archiving and Communication System (PACS; Huang, 2004) is a clinical information system tailored for the management of radiological and other medical images for patient care in hospitals and clinics. It was the first time in the world to implement both standards to a clinical information system for the improvement of data security.

BACKGROUND

Information security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional. A more proactive definition is the preservation of the confidentiality, integrity, and availability (CIA) of information and information resources. Confidentiality means that the information should only be disclosed to a selected group, either because of its sensitivity or its technical nature. Information integrity is defined as the assurance that the information used in making business decisions is created and maintained with appropriate controls to ensure that the information is correct, auditable, and reproducible. As far as information availability is concerned, information is said to be available when employees who are authorized access, and whose jobs require access, to the information can do so in a cost effective manner that does not jeopardize the value of the information. Also, information must be consistently available to conduct business smoothly. Business con-

tinuity planning (BCP) includes provisions for assuring the availability of the key resources (information, people, physical assets, tools, etc.) necessary to support the business function.

The origin of ISO17799/BS7799 goes back to the days of the UK Department of Trade and Industry's (DTI's) Commercial Computer Security Centre (CCSC). Founded in May 1987, the CCSC had two major tasks. The first was to help vendors of IT security products by establishing a set of internationally recognized security evaluation criteria and an associated evaluation and certification scheme. This ultimately gave rise to the information technology security evaluation criteria (ITSEC) and the establishment of the UK ITSEC scheme. The second task was to help users by producing a code of good security practices and resulted in the *Users Code of Practice* that was published in 1989. This was further developed by the National Computing Centre (NCC) and later a consortium of users, primarily drawn from British industry, to ensure that the code was both meaningful and practical from a user's point of view. The final result was first published as the British Standards guidance document PD 0003, *A Code of Practice for Information Security Management,* and following a period of further public consultation, it was recast as British Standard BS7799: 1995. A second part, BS7799-2: 1998, was added in February 1998. Following an extensive revision and public consultation period in 1997, the first revision of the standard, BS7799: 1999, was published in April 1999. Part 1 of the standard was proposed as an ISO standard via the "fast track" mechanism in October 1999, and then published with minor amendments as ISO/IEC 17799: 2000 on December 1, 2000. A new version of this appeared in 2005, along with a new publication, ISO 27001. BS7799-2: 2002 was officially launched on September 5, 2002 and later replaced by ISO27001 in October 2005.

PACS is a filmless (Dreyer, Mehta, & Thrall, 2001) and computerized method of communicating and storing medical image data such as computed radiographic (CR), digital radiographic (DR), computed tomographic (CT), ultrasound (US), fluoroscopic (RF), magnetic resonance (MRI), and other special X-ray (XA) images. A PACS consists of image and data acquisition and storage, and display stations integrated by various digital networks. Full PACS handles images from various modalities. Small scale systems that handle images from a single modality (usually connected to a single acquisition device) are sometimes called *mini-PACS* The medical images are stored in an independent format. The most common format for image storage is DICOM (Digital Imaging and Communications in Medicine), developed by the American College of Radiology and the National Electrical Manufacturers' Association.

Tseung Kwan O Hospital (TKOH) is a newly built general acute hospital (built in 1999) with 458 in-patient beds and 140 day beds. The hospital is composed of several clinical departments including medicine; surgery; paediatrics and adolescent medicine; eye, ear, nose, and throat; accident and emergency; and radiology. A PACS was built in its radiology department in 1999. The PACS was connected with the CR, CT, US, RF, DSA, and MRI system in the hospital. The hospital has become filmless since a major upgrade of the PACS in 2003.

An ISO 17799/BS7799 ISMS was implemented in the TKOH PACS in 2003. During the implementation, a PACS security forum was established with the active participation of radiologists, radiographers, medical physicists, technicians, clinicians, and employees from the information technology department (ITD). After a BS7799 audit conducted in the beginning of 2004 and later ISO27000 upgrade audit was conducted in 2006, the TKOH PACS was the world's first system with the ISMS certification. In this article, the practical experience of the ISO27000 implementation and the quality improvement process of such a clinical information system will be explained.

MAIN FOCUS OF THE ARTICLE

In TKOH, the PACS serves the whole hospital including all clinical departments. The implementation of ISO27000 was started with the establishment of an ISMS for the PACS at the beginning of 2003. For effective implementation of ISO27000 in general, four steps will be required:

1. Define the scope of the ISMS in the PACS.
2. Make a risk analysis of the PACS.
3. Created plans as needed to ensure that the necessary improvements are implemented to move the PACS as a whole forward toward the ISO27000 objective.
4. Consider other methods of simplifying the above and achieving compliance with minimum effect.