ISO 17799 AND AUSTRALIAN HEALTHCARE ORGANISATIONS

W.J.Brooks¹, M.J.Warren¹ and W.Hutchinson²

¹Deakin Univeristy, Australia and ²Edith Cowan Univeristy, Australia

Abstract: Information security is now recognised as critical factor within the healthcare industry. With the gradual move from paper-based to electronic information there is an even greater need for protection. However, financial and operational constraints often exist which influence the practicality of developing a secure system. A new baseline security standard has been drafted which applies specifically to the unique information security requirements of the healthcare industry. The aim of this paper is to look at the effectiveness of the health information security standard and the development of information security within the Australian healthcare industry.

Key words: Security Healthcare, Baseline Security, AS/NZS ISO/IEC 17799.

1. INTRODUCTION

The Australian healthcare industry has undergone significant changes over the past 10 years. To deal with the issues of security within healthcare, the Health Information Security Management Implementation Guide (Deloitte Touche Tohmatsu 2002) was drafted. This is based on the Australian and New Zealand Standard (AS/NZS) 17799 (Standards Australia, 2000 & 2001), to apply specifically to the interests and unique information security requirements of the Australian healthcare industry. This standard provides a comprehensive set of controls comprising of current best information security practices that will provide assistance with the initiation, implementation, and maintenance of information security measures within a health business (Deloitte Touche Tohmatsu, 2002). Once a business has implemented the standard they can be certified against that

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35691-4_52](https://doi.org/10.1007/978-0-387-35691-4_52)

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

© IFIP International Federation for Information Processing 2003

standard by a certification authority. But will this standard actually offer a set of controls and safeguards that are suitable for the healthcare industry; is the healthcare industry willing to conform to the development of a national health information network? To answer these questions the Health Information Security Management Implementation Guide was critically analysed and a survey sent out to Victorian health establishments to determine the views of information security in the healthcare industry. The results of this survey will be discussed in this paper.

2. RESULTS OBTAINED FROM SURVEY

The survey objectives are to heighten awareness of the development of information security management systems; to seek an understanding of information security trends and issues; and, to determine the reactions and intention regarding certification against an information security standard, particularly the AS/NZS ISO/IEC 17799:2001, throughout health organisations in Victoria, Australia. The overall rate of response for the survey was 20% (similar rate of return to AusCERT and CSI/FBI security surveys) which included public and private hospitals, day procedure centres, bush nursing hospitals and other health services facilities; each response has been carefully reviewed.

Over 80% of the respondents rated the security of their health organisation's information as highest priority but this level of importance for security was contradicted by a number of answers to other questions within the survey, such as:

- 93% of the organisations that responded allow internet access to staff but only 62.5% of these organisations have a formal written policy concerning staff internet usage;
- 40% of respondents have performed a formal risk assessment to determine potential areas of risk, 49% have not performed a formal risk assessment but plan to in the future, and the remaining 12% have not performed a formal risk assessment and do not plan to. Of those organisations that have performed a formal risk assessment many chose to hire security consultants outside of their organisation, or other healthcare bodies.
- With regards to each organisation's current state of their information security policy the majority of respondents (26%) are still gaining information about security standards and considering action. Second to this, 24% of respondents are agreeing on internal standards, and only

14% of respondents are ready to implement their information security policy.

The majority of health organisations perceive the protection of business information to be the main benefit of implementing an information security policy, with secondary benefits of raising security awareness among staff, and, the development of an internal information security framework. The vast majority of organisations surveyed believe computer viruses to be the main risk to their information, closely followed by lack of security awareness among staff. Other risks noted were failure of data backups, lack of direct control due to using another hospital’s network, staff’s willingness to ‘upgrade’, and the financial issues of implementing an information security policy in smaller health organisations. Table 1 illustrates the results obtained.

Type of Security Risk	Percentage of Respondents
Computer Viruses	74%
Hackers	21%
Disgruntled Employees	12%
Data Integrity	54%
Corruption	
Human Failure	63%
Technical Failure	63%
Natural Disasters	14%
Denial of Service	9%
Lack of Security	65%
Awareness	
Other	9%

Table 1. The perceived security risks

Figure 1. Awareness of AS/NZS and its implementation

Even though computer viruses are a major concern among Victorian hospitals, only 62% of respondents that allow staff Internet access have a formal written policy on internet usage in place. Within the health industry AS/NZS ISO/IEC 17799:2001 and certification against this standard is still in its early stages but there is clear evidence of gradual acceptance. It was a case that 41.9% of respondents are aware of the standard but only 5.9% have implemented AS/NZS ISO/IEC 17799:2001. The majority of organisations are planning to take action in the future as shown by figure 1.

3. CONCLUSIONS

The Australian healthcare industry handles very sensitive information, whether it is a patient's health record or scientific test data it is imperative to maintain data integrity as well as adhering privacy laws and legislation. This is particularly the case as more health information is being stored and transmitted in electronic format, and the simplicity of distribution of information has increased dramatically. A recent Australian computer crime and security survey jointly produced by AusCERT discovered 67% of respondents suffered a computer security incident in 2002, twice the level of 1999, and 35% of these experienced six or more incidents (AusCERT et al., 2002). These results provide enough evidence to suggest that it is imperative for health businesses to implement a set of security controls and safeguards that satisfy the very distinctive requirements of the healthcare industry. The survey has shown that, within Victoria, the Australian healthcare industry is not ready to certify itself against any information security standard.

REFERENCES

AusCERT, Deloitte Touche Tohmatsu, and NSW Police (2002) *2002 Australian Computer Crime and Security Survey*, The University of Queensland, Australia.

Deloitte Touche Tohmatsu (2002) *Health Information Security Management Implementation Guide to AS/NZS 17799.2*, Australia.

Standards Australia (2001) *Information Technology – Code of practice or information security management*, AS/NZS ISO/IEC 17799:2001, Standards Australia & Standards New Zealand.

Standards Australia (2000) *Information security management – Specification for information security management systems*, AS/NZS 7799.2:2000, Standards Australia & Standards New Zealand.