Chapter 5

Analyzing Information Security Goals

Ella Kolkowska
Örebro University School of Business, Sweden

Karin Hedström
Örebro University School of Business, Sweden

Fredrik Karlsson
Örebro University School of Business, Sweden

ABSTRACT

One of the problems highlighted within the area of information security is that international standards are implemented in organisations without adopting them to special organisational settings. In this chapter the authors analyse information security goals found in hospital settings. They found that the CIA-triad fails to cover organisational specific information security goals in hospital settings. They found also that information security goals held by information security managers and business managers are not the same, implying that both these groups should be involved in designing of information security goals, in order to find information security goals relevant for the organisation. Finally, the authors found goal maps used in this study for analysis of empirical data, to be a useful tool for analysis and communication of information security goals in an organisation.

INTRODUCTION

A strong trend in information security management in organisations under the last decade has been standardization, certifications and development of best practices (B. von Solms, 2000). Consequently, information security management standards are seen as a basis for successful security management in organisations and have become widely used for security management (Siponen, 2006). The most known and widespread standard today is the ISO/IEC 17799 – Information Security Code of Practice (Freeman, 2007; ISO/IEC 17799, 2005).

Although there are obvious advantages of using international standard for security management, various researchers point out that applying such standards without enough consideration to the specifics of the organisation may be detrimental.
to effective management of information security (e.g. Hsu, 2009; Höne & Eloff, 2002; Siponen, 2006; B. von Solms & von Solms, 2004). Every situation requires different solutions while standards are more of a general baseline for information security. In each specific situation the special context of the IT environment have to be taken into account when the standards are applied, in order to establish unique information security requirements of an organisation (Gerber & von Solms, 2005; Hsu, 2009).

Furthermore, the literature emphasizes the importance of dialogue between information security professionals and business managers when deciding information security goals for an organization (McFadzean, Ezingeard, & Birchall, 2006; B von Solms, 2001). Information security professionals typically have technical backgrounds and focus on technical aspects of information security, while business managers are mainly concerned with managerial and organizational aspects of information security. These two different views are important to consider in establishing information security goals for a specific organisation (Rainer, Marshall, Knapp, & Montgomery, 2007). Unfortunately, many organisations apply the standards without addressing the actual security needs of the organisation (Hsu, 2009; Thomson, von Solms, & Louw, 2006).

A consequence of applying security standards without considering the organisational context is the focus on Confidentiality, Integrity and Availability (the CIA-triad) as the only objectives for information security management. This means running the risk of missing specific information security goals that an organization needs. The CIA-triad has been criticized in the literature for its technical focus and ignorance of the socio-organizational context of information security management (e.g. Anderson, 2002; Dhillon & Backhouse, 2000; Trompeter & Eloff, 2001). Moreover it has been pointed out that the CIA-triad are general objectives for information security management, while information security objectives should be related to the organisational context (B. von Solms & von Solms, 2004). Therefore researchers agree that the CIA-triad should be complemented and/or re-defined; including ethical, social, and organizational aspects of information handling (Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006; Trompeter & Eloff, 2001).

For health care organisations, secure information is central to effective and good health care and to ensure patient security (Leitheiser, 2001). However, although information security and protecting patient information have always been of high priority in the health care sector, the level of information security in this sector is still insufficient (Nanji, 2010; Prince, 2008). Various reports of information security breaches (PWC, 2008) and unintended information disclosures of confidential patient information (Prince, 2008) have raised the awareness about security issues of health information systems (HIS) (Luethi & Knolmayer, 2009). We need to develop better knowledge about what constitutes secure information and good information management in hospital settings. With this in mind, is the purpose of the study presented in this paper to analyse information security goals in a Swedish hospital. This will bring us a little bit further in our quest to develop a secure information environment in hospitals.

The introduction of HIS and patient electronic health records (EHR) are seen as possibilities for improved health care quality, lower costs and also as an important part of meeting the new challenges arising in the health care sector in today’s society (Miettinen & Korhonen, 2008). However, without adequate information security, there will be no trust for the health care services and the hope for improved patient care and reduced health care costs will be in tatters (Nanji, 2010). Therefore information security is important in health care sector.

Management of information security in health care organizations is not easy. An important aspect of health care work, which influences information security, is the complexity in delivering health