Chapter 13
An Information Security Model for Implementing the New ISO 27001

Margareth Stoll
Independent Researcher, Italy

ABSTRACT

The importance of data privacy, information availability, and integrity is increasingly recognized. Sharpened legal requirements and increasing data leakages have further promoted data privacy. In order to implement the different requirements in an effective, efficient, and sustainable way, the authors integrate different governance frameworks to their holistic information security and data privacy model. More than 1.5 million organizations worldwide are implementing a standard-based management system. In order to promote the integration of different standards, the International Standard Organization (ISO) released a common structure. ISO/IEC 27001 for information security management was changed accordingly in October 2013. The holistic model fulfills all requirements of the new version. Its implementation in several organizations and the study's results are described. In that way data privacy and security are part of all strategic, tactical, and operational business processes, promote corporate governance and living security, as well as the fulfillment of all standard requirements.

INTRODUCTION

Due to globalization and increasing competition, information and supporting technology have become key asset and differentiators for modern organizations. Organizations and their information and information systems are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. 92% of large enterprises had a security incident in the last year with an average cost of 280.000-690.000 £ for the worst incident (PricewaterhouseCoopers, 2010). Threat agents have increased in the last years sophistication of their attacks and their tools (ENISA, 2013). The security incident have increased 25% over the previous year, while the average financial cost of incidents are up 18% (PricewaterhouseCoopers, 2013). Mobile and cloud computing, off-shoring, social networks and the increasingly interconnected, flexible and virtualized business complexity and dependencies are still great challenges for data privacy and information security.

DOI: 10.4018/978-1-5225-7113-1.ch013

In the last years, the legal and regulatory requirements in this area have been sharpened. Most modern corporate governance guidelines, and always more laws, make the board and specifically the CEO responsible for the well-being of the organization. Data breaches and lack of security compliance may result in loss of confidence of customers, partners and shareholders, as well as severe civil and criminal penalties for board members (Saint-Germain, 2005; Clinch, 2009). More and more organizations are reducing their business risks by seeking assurance that their supplier and partners are properly protecting information assets and ensuring business continuity (Saint-Germain, 2005). In this respect the availability of all essential assets, confidentiality, data privacy, data integrity and legal and regulatory compliance are central for organizations' success (Bélanger & Crossler, 2011; Da Veiga & Eloff, 2007; Solms & Solms, 2009; Sowa, Tsinas & Gabriel, 2009). This poses great challenges for small and medium sized organizations. They need a very efficient and functional approach, which can be smoothly integrated in their daily business.

More than 1.5 million organizations worldwide are implementing a standard based management system based on international standards (e.g. quality ISO 9001, or environment ISO 14001, IT service management ISO 22000 and others) (ISO, 2013a). In order to promote an efficient integration of different standards, the International Standard Organization [ISO] released a common structure for all management systems' standards, the Annex SL of the ISO/IEC Directives (ISO, 2013d). In accordance to this new structure, ISO published in October 2013 the new version of the ISO/IEC 27001 (ISO, 2013b) and ISO/IEC 27002:2013 (ISO, 2013c) information security management standards. More than 19.500 organizations worldwide have just implemented an information security management system in accordance to the old version of ISO/IEC 27001 (ISO, 2013a). In order to maintain their certificate they have to adjust their system to the new requirements. The international standard provides requirements for establishing, implementing, maintaining and continually improving an information security management system to meet the specific security and business needs/objectives of the organization. It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls (ISO, 2013b; 2013c).

Despite the huge amount of research on privacy and information security (see Bélanger &Crossler; 2011; Pavlou, 2011; Smith, Dinev & Xu, 2011), the calls for more interdisciplinary information security research (Dhillon & Backhouse, 2000; Dinev, 2014; Pavlou, 2011; Warkentin &Willison 2009) and for studies at the group and organizational level (Bélanger &Crossler; 2011; Pavlou, 2011;), the current understanding of information security and data privacy (Dinev, Xu, Smith, & Hart; 2013) is largely fragmented. We found no integrated information security and data privacy framework. Several international best practices for information security management have been developed to provide guidance and ensure comprehensiveness. Some of the most commonly used include Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL) and national guidelines, such as NIST SP 800 series in the US or IT Security Guidelines from the Federal Office for Information Security in Germany.

To meet optimally all data privacy and information security requirements we have developed an efficient, effective and sustainable information security and data privacy model. This model integrates the different information security governance frameworks with different best-practice methods (COBIT, ITIL) (IT Governance Institute, 2007; Office of Government Commerce [OGC], 2007). The holistic approach integrates data privacy and information security into all strategic, tactical and operational business processes and promotes thereby living data privacy and information security as part of corporate