Information Security Management and Security Reporting

I

Wolfgang Hommel
Leibniz Supercomputing Centre, Germany

INTRODUCTION

Unlike in public opinion twenty years ago, information security (IS) can no longer be considered a mere feature that is only relevant for military-grade systems. Several components of technical solutions, e.g., data encryption, and many terms, such as "demilitarized zones" for a specific communication network firewall architecture, still remind us of this past and origin. But today, IS is a must-have for almost any type of hardware and software, from applications running on mobile devices to network-based services in enterprises and inter-organizational data exchange workflows.

Because especially medium and large organizations have dozens of services running on hundreds or even thousands of devices, workstations, and servers, IS has scalability and prioritization challenges that cannot be met by only a small group of security specialists with technical measures at their disposal. Instead, similar to service and product quality, IS needs to be managed professionally and is a process in which everyone – staff and management alike – has to be involved adequately (Peltier, 2007). Consequently, organizational measures, such as sensitizing and training the users, are as important as technical measures and need to be continuously improved in today's ever-changing dynamic IT environment. However, many organizations still only spend a dauntingly low budget on IS. On the one hand, operating departments often rather invest in the improvement of an IT infrastructure's functionality or performance than in security measures, which often have a reputation for user-friendliness degradation. On the other hand, security measures are rarely attractive to decision-makers in executive boards because they cannot generate any direct return on invest, but only have a potential to prevent or limit financial damages or reputation losses that are caused by security incidents (Bazavan & Lim, 2006).

Information Security Management (ISM) is the discipline that gives us methodologies, defines processes, and provides tools to address these matters and constraints in a structured, well-proven manner. One of ISM's key building blocks is Security Reporting (SR), which often has been neglected in the past. SR's primary task is to aggregate measurements of the very specific, technical aspects of IS, process and refine them, and finally generate comprehensible and impartial bulletins for decision-makers, auditors, customers, and other target audiences. Because unlike its size, weight, or temperature, any given IT system's security cannot be measured in a physical unit, the design and application of meaningful security metrics poses many challenges on its own.

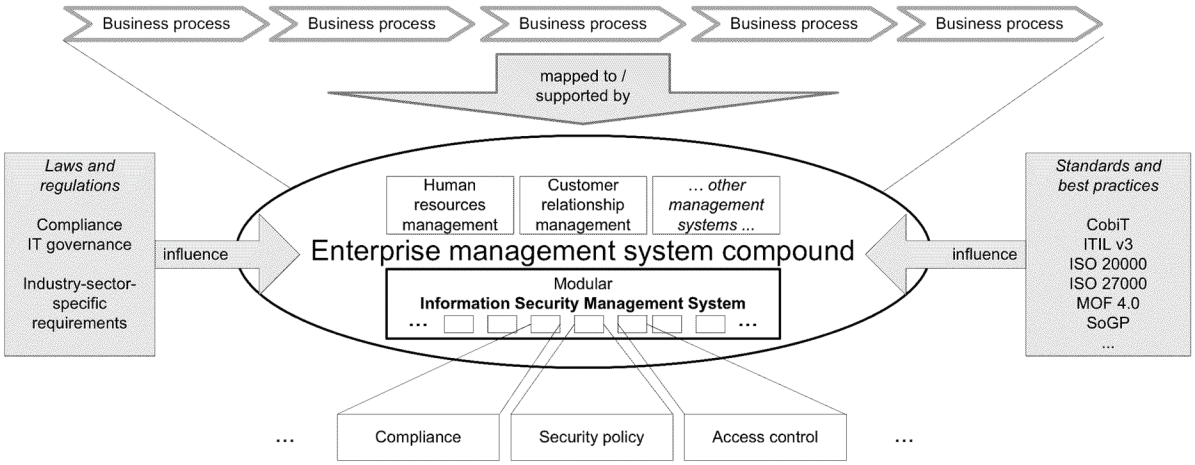
In this article, we first explain essential ISM basics and then describe the components and application of so-called Information Security Management Systems (ISMS), including risk management, continuous improvement, and security controls. Afterwards, we discuss the ingredients of successful security measurements, metrics, and reporting. Finally, we outline several future ISM research directions.

BACKGROUND

The basic goal of ISM is to ensure security properties – such as the confidentiality, integrity, and availability – for an organization's assets, i.e., any material or immaterial goods that are of value to the specific organization. IT assets typically include data, such as a customer database, software-based services like a web server, and hardware, e.g., the physical web server machine. Whereas any specific security measure, such as a network firewall, only has a limited scope – i.e., it protects only selected security properties of a subset of all assets – ISM takes a holistic approach and typically

DOI: 10.4018/978-1-4666-5888-2.ch426

Figure 1. The ISMS in the overall management system landscape



covers IS on an organization-wide scale (Whitman & Mattord, 2010).

Given the current state of the art in ISM, we basically need to consider three complementary building blocks:

1. ISM takes a risk-driven approach. In practice, perfect security can never be achieved. Due to the large number of assets, one needs to prioritize the measures that should be taken to ensure the best possible security level with the given personnel, time, and budget constraints (Roper, 1999).
2. ISM gives us a large pool of security measures to choose from. Security measures can be categorized as either technical or organizational, and considering their relationship to security incidents, they can be categorized as preventing, detecting, or reacting.
3. ISM applies the principle of continuous improvement. Only a limited number of deliberately chosen security measures can be implemented within a given period. These measures then must be analyzed for effectiveness, refined, and eventually complemented by additional measures (Cazemier, 2010).

The practical application of these theoretic ISM principles to a specific organization is the primary task of an ISMS. It is important to note that "ISM system" does not refer to a single piece of software or hardware in the same way the term "system" is often used in computer science. Instead, an ISMS includes "organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources," and is "based on a business risk approach, to establish, implement, operate, review, maintain and improve" IS according to the definition in the international standard ISO/IEC 27001 (ISO/IEC, 2005). Figure 1 shows how an ISMS is embedded into the overall management system landscape.

INFORMATION SECURITY MANAGEMENT SYSTEMS

ISO/IEC 27000 is a growing series of international standards; while several documents are still in preparation, ISO/IEC 27001 has been published in 2005 and has a very high international relevance and publicity because organizations can be certified by accredited registrars; similar to quality management certifications according to ISO 9001, an ISO/IEC 27001 certification helps organizations to demonstrate their commitment to IS. Almost any other literature explicitly points out its relationship to ISO/IEC 27000, and therefore, the following discussion of the essential ISMS components is aligned to it.

Risk Management

Risk management for IS is a process of its own, which means it is a series of coordinated activities that shall not be performed only once, but instead risks must be