available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Holistic security management framework applied in electronic commerce

Albin Zuccato[†]

Karlstad University, Universitetsgatan 1, 65 188 Karlstad, Sweden

ARTICLE INFO

Article history:
Received 10 January 2006
Revised 25 October 2006
Accepted 1 November 2006

Keywords:
Holistic security management
Security management process
Security engineering
Security requirements
Electronic commerce security

ABSTRACT

With the advance of electronic commerce more and more companies have become dependent on their information systems for their daily business operations. This dependency requires the security of these systems to be managed. This paper presents a holistic security management framework that should allow for easy and affordable security management. This process framework is described by hierarchically organized processes which allow for a business, technology and social driven security management. It presents the activities involved in the five core and two support processes which are conducted iteratively. To support this framework three cases of successful applications and an informal evaluation against SSE-CMM are presented.

1. Introduction

With the diffusion of the Internet our lives have changed. This technology has enabled globalization and commercialization in a way the society has not seen before. Modern organizations have adopted the Internet for their daily operations and have become dependent on it. Many organizations have started to conduct electronic commerce which means that their business processes incorporate activities (e.g. buying, selling, etc.) which rely solely on information processing systems. This trend implies the need for protecting the information systems by means of information security in an orderly (i.e. managed) way. To do this a number of different security management approaches have been developed over the years. It seems, however, that those approaches are not applied because they are perceived as complex and expensive to implement by practitioners (DTI and Coopers, 2004). In addition many of those approaches do not take the changed environmental circumstances of electronic commerce fully into account.

Based on these findings, we have developed a holistic security management framework that should allow companies to conduct security management more easily, at lower costs and tailored to the needs of an e-commerce system. We, therefore, propose a hierarchically organized process framework that can be applied "off the shelf" in the first hand and tailored later on to fit the organizational needs more accurately. This article presents the full Holistic Security Management Framework (HSMF) but due to space restrictions only to the first sub-level. A full description of the process and a motivation for the activities are available in Zuccato (2005b).

This paper is divided into five sections. Section 2 presents security management approaches and suggests shortcomings that should be overcome by a new process. In Section 3 the

E-mail address: albin.zuccato@teliasonera.com
[†] Present address: TeliaSonera, R&D Information Security, Vitsandsgatan 9, 12386 Farsta, Sweden.
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.11.003

special environmental circumstances implied by electronic commerce are presented. These circumstances motivate some of the process characteristics introduced in Section 4. This section also describes the holistic security management framework by its activities and iterations. In addition the special role of privacy in HSMF is further discussed. Section 5 evaluates the framework and also presents some cases where it was successfully applied. Lastly, conclusions are offered in Section 6.

2. Security management processes today

Today's security management approaches can be divided into three groups. The first group includes the approaches that are based on security management standards. The second group is based on best practices and the third is based on more formal approaches. To give a complete overview of all security management approaches is out of the scope of this work and only a selection (based primarily on public availability) for each group is presented.

Most commonly when security management is discussed today the standard ISO 17799 (ISO 17799, 2000) is referred to. This standard describes what to consider in information security management. A frequently mentioned problem with ISO 17799 (2000) is that it does not provide a process of how to conduct security management but it is merely a checklist (see e.g. Björck (2001)). This is a problem that ISO also acknowledges and it has provided ISO 27001 (2005) which provide requirements what a security management process should incorporate. A second problem is that it is tailored for a ''conventional'' organization and not entirely suitable for e-commerce. The third problem is that risk analysis alone is not sufficient to derive the security requirements in e-commerce.[1] Therefore, a more holistic approach is needed (Zuccato, 2004).

An important member of the second group, the best practices, is the special publications on security by the US National Institute of Standards and Technology (NIST). These NIST publications are very useful as they provide an overview and suggest some activities for most information security areas. The greatest objection to them is the focus on US Federal Agencies which have different needs than private organizations (e.g. private organizations have to consider security as a business enabler and not only as an asset protection mechanism). A second problem is the threshold implied by the great amount of pages to read before one can start.

In respect to the formal approaches we can further identify three sub-groups that are of interest. The first relies on engineering practices, the second combines engineering with either business or social theories and the third applies system engineering approaches.

The engineering based approaches are the oldest group of security management approaches. Two representatives are Automated Secure System Development (ASSDM) (Booysen and Eloff, 1995) and UMLsec (Jürjens, 2002). ASSDM is an approach that propose a security engineering processes based on the spiral model. The greatest objection to these approaches is their strong technical focus. In addition these approaches usually only cover parts of the system lifecycle (i.e they start to late and end to early). A great benefit of these approaches is that they normally aim to harmonize software and security design.

The second sub group contains for example Virtual Methodology (VM) by (Hitchings, 1995) or Business Process Models for Security Design (Holbein et al., 1996). The greatest objection to these approaches is that they commonly focus on only one or two activities of the system lifecycle. In addition every approach usually suffers from very high emphasis of the non-technical dimension which leads to problems in the application – for further discussion see Zuccato (2005b).

One approach from the system theoretic group is the Integral Framework for Information Security Management (Trcek, 2003). This framework integrates practices proposed in different standards and relies on risk analysis. Like ISO 17799 the sole reliance on risk analysis implies the lack of holism. A minor problem is that although maintenance is mentioned the activities are not described.

We can summarize the following problems that need to be solved when designing a new security management framework.

Research claims (von Solms, 2001) and practice have shown that a lot of dimensions have to be considered in security management. To take these dimensions into account a holistic approach that simultaneously considers them is therefore necessary. However, most state-of-the-art security management approaches are *not holistic*.

Modern system (and software) engineering approaches assume a lifecycle that starts with an idea for the system and ends with the disposal of the system. However, most approaches only *cover parts of the system lifecycle*.

E-commerce implications on security management (see next section) are often *not supported sufficiently*.

3. Electronic commerce

With the widespread availability and use of the Internet it has also become an interesting channel to advertise, sell and buy products. Different business models have developed over the years. Some of them were not successful (which led to a bad reputation for e-commerce in general) but others have succeeded and are a part of the daily business of organizations.

The two important business models are e-commerce and e-business (Chaffe, 2002; Österle and Winter, 2000). In e-commerce the business process is supported electronically and is interconnected. The acquisition, selling, and support are done over the Internet. However, the e-commerce system communicates with the existing systems of the organization. Mostly e-commerce is conducted in parallel to ''conventional''

[1] A practical example can be provided from the experience of the author. In one of the cases the risk analysis suggested that an additional authorization system for transactions would not be required because the asset value, the threats and the probabilities would not justify such an investment. However, market forces demanded such an investment into security as the consumers considered it a necessary precondition to use the service. Obviously the conventional security risk analysis is not sufficient here. Similar evidence is reflected in requirement engineering process of a large Swedish telecommunication provider.