Information & Management 46 (2009) 267–270

Contents lists available at ScienceDirect

Information & Management

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

Information security management standards: Problems and solutions

Mikko Siponen [a,*], Robert Willison [b]

[a] University of Oulu, IS Security Research Center and Department of Information Processing Science, Linnanmaa, P.O. Box 3000, FIN-90014, Finland
[b] Copenhagen Business School, Howitzvej 60, DK-2000 Frederiksberg, Denmark

ARTICLE INFO

Article history:
Received 28 July 2003
Received in revised form 10 April 2007
Accepted 7 December 2008
Available online 20 May 2009

Keywords:
Information systems security
Information security management standards
Information security management
Information security management guidelines
Information security certification

ABSTRACT

International information security management guidelines play a key role in managing and certifying organizational IS. We analyzed BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP, and the SSE-CMM to determine and compare how these guidelines are validated, and how widely they can be applied. First, we found that BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP and the SSE-CMM were generic or universal in scope; consequently they do not pay enough attention to the differences between organizations and the fact that their security requirements are different. Second, we noted that these guidelines were validated by appeal to common practice and authority and that this was not a sound basis for important international information security guidelines. To address these shortcomings, we believe that information security management guidelines should be seen as a library of material on information security management for practitioners.

1. Introduction

Information security management (ISM) guidelines, which attempt to provide the best ISM practices, are used by organizations. By adopting an authoritative guideline, organizations can demonstrate their commitment to secure business practices; organizations may then apply for certification, accreditation, or a security-maturity classification attesting to their compliance to a set of rules and practices.

Complying with security management guidelines is essential. However, current guidelines have two problems. First, the well known ones are generic in scope, while organizations need methods tailored to their environment and operations. Second, they have not been validated but are fostered by an appeal to common practice, which is an unsound basis for a true standard.

2. Research framework

2.1. Information security management guidelines

Different international ISM guidelines have been proposed, including the TCSEC/Orange Book, GMITS, CobiT, IT Baseline Protection Manual, Generally Accepted Information Security Principles (GAISP), the System Security Engineering CMM (SSE-CMM) [22], and BS7799 and its derivatives (BS7799, BS ISO/IEC17799: 2000).

These, not surprisingly, have common features. First, they were offered either to help secure organizations' IS or for certification purposes, to prove that organizations' IS complied with the guideline; in theory, all standards can be used for both purposes. Second, they were externally developed by committees. Third, they provided an authoritative voice on infosec management.

Of the "*standards*", we selected BS7799, BS ISO/IEC17799: 2000, GASSP/GAISP and the SSE-CMM for analysis on the basis of three factors. First, they are all relatively new. Second, they are widely advocated by scholars and practitioners; these four standards or guidelines have received positive recognition. Third, their advocates are geographically dispersed. BS7799 has advocates in Australia, New Zealand, South-Africa and the UK [1] and the SSE-CMM is well-known in Canada and the U.S.

The Common Criteria [9] and ITSEC [16] focused on technical security features [18]. The Common Criteria has been used primarily for evaluating security properties of IT products. Here, we are focusing on ISM aspects and guidelines, which emphasize organizational, social and behavioural aspects of ISM in organizations. Such issues include development of organizational strategies that ensure that employees are educated to comply with the security policies [11]. In addition, BS, GASSP and the SSE-CMM were selected over GMITS, the OECD guideline, ISF and the IT Baseline Protection Manual [17]. Furthermore the GASSP's "pervasive principles" were based on the OECD principles [10]. Hence, GAISP can be viewed as an later version.

* Corresponding author. Fax: +358 553 1890.
E-mail address: msiponen@tols16.oulu.fi (M. Siponen).

0378-7206/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.im.2008.12.007

2.1.1. Generally accepted systems security principles (GASSP)

The development of GASSP started in 1992, with support from the U.S. government, the International Information Security Foundation, and other world-wide organizations. GASSP version 2.0 was published in 1999, and with the release of version 3.0 the name was changed to Generally Accepted Information Security Principles. The aim in the development of GAISP was to document common practice. The preface stated: "*We believe it is time for the Information Security profession to create our own set of accepted principles and practices.*" [11].

GAISP proposed three levels of information security principles: pervasive (few, rarely changing) such as those of ethics and awareness; broad functional (more detailed); and most detailed. Pervasive principles lay down the basis for the others. In total, there are nine pervasive principles. GAISP version 3.0 included the "Detailed Principles Cookbook" for guiding GAISP developers in detailing the principles from authorities such as OECD and ISF.

2.1.2. BS7799 and derivatives

BS7799 was developed in 1995 by the UK Department of Trade and Industry, with international companies joining in the effort. An international version (BS ISO/IEC17799:2000 [7]) was later published. The 1995 version [5] is well-known and respected. Later versions were published in 1999 [6] and 2000 [7] but for clarity, we refer to these as BS Version 1, BS Version 2 and BS Version 3, respectively. A standard known as BS 7799-2: 2002 [8] will be referred to as BS Version 4. BS Version 1 included ten *key controls* that are essential for all organizations, however the term key controls was changed in versions 2 and 3 to "information security starting point" with eight "critical success factors."

BS Version 4 described a process for use of the guideline, known as the "Plan–Do–Check–Act" process:

- Plan → establish a security policy and relevant procedures and controls; then prepare a statement of the scope of its application, justifying why the controls were selected and why others were not;
- Do → implement the security policy and relevant procedures;
- Check → assess and measure the process performance, and report the results to management;
- Act → take appropriate corrective actions.

These methods were intended for use both in securing IS and in their certification.

2.1.3. The system security engineering capability maturity model (SSE-CMM)

The development of the SSE-CMM started in 1993 as an NSA-sponsored endeavor to extend the capability maturity model [14]. The purpose of the effort was to use the model to address security issues in systems development. To aid in development of the SSE-CMM, the International Systems Security Engineering Association (ISSEA) was founded.

Versions 2.0 and 3.0 of the SSE-CMM both included base practices that were grouped into 22 key process areas (11 security-related and 11 general project-oriented), and six maturity levels. Version 3.0 included 129 base practices, such as: "Identify system security vulnerabilities." The 11 security-related process areas were: (1) administer security controls; (2) assess impact; (3) assess security risk; (4) assess threat; (5) assess vulnerability; (6) build assurance argument; (7) coordinate security; (8) monitor security posture; (9) provide security input; (10) specify security needs; and (11) verify and validate security.

The SSE-CMM was intended to be used in certificating the maturity level of an organization's IS security and thus its security processes. Version 3.0 of the SSE-CMM also included a 10-point set of *rules of thumb*, which could be seen as a process guiding the use of the guideline. The maturity levels are similar to those of SEI's CMM/CMMI: (0) not performed; (1) performed initially, based on individual effort; (2) planned and tracked, when there is a security process in place; (3) well-defined, where the security process is standardized, tailorable and integrated into the organization-wide process; (4) quantitatively controlled, where the security process is quantitatively measured; and (5) continuously improving, where metrics are used to collect feedback that is then used to improve the process.

2.2. Criteria for assessing infosec management guidelines

The guidelines were analyzed from the perspectives shown in Table 1.

2.3. Scope of application

It is important to know how broadly ISM guidelines can be applied, and also to assess the extent to which a guideline is suited to the needs of small to large organizations. The scope of a guideline may be *generic* (applying throughout organizations, with rare exceptions where the it does not), *universal* (applicable, to all organizations, from small to multinational, without exception) or *company-specific* (where every company may have a unique set of requirements). Thus a *company-specific* international ISM guideline would start by listing and modeling the organization's unique security goals and requirements. We argue that guidelines should be company-specific, to a certain degree. General and generic security practices may overlook specific requirements, which may result in expenditure in the wrong places, resulting in waste and potentially insecure systems [4].

2.4. Type of evidence

Two types of evidence, validation and argumentation, are important in research and development efforts.

Given the importance of information security guidelines, it is necessary to examine how, and on what evidence they are validated. Claims may be based on arguments that have empirical support. However, one criterion is accepted: that the research processes and types of evidence should be made public and visible. In argumentation theory, several fallacies are discussed, including appeals to popularity (*Ad Populum*), to common practice and authority (*Ad Verecundiam*). We argue that ISM guidelines should not be based on fallacious arguments.

3. Analysis of BS7799, GAISP/GASSP, and the SSE-CMM

3.1. Scope of application

BS Version 1 (and derivatives), the SSE-CMM, and GASSP/GAISP appear to be generic or universal in scope. The following citations illustrate how these principles were embodied.

BS Version 1 states that "*some controls are not applicable to every IT environment and should be used selectively. However, most of the controls documented are widely accepted*" ... and ... "*recommended good practices for all organizations.*" [5]. Thus, the controls are applicable to all organizations, while leaving room for exceptional

Table 1
Criteria for evaluating ISM guidelines and guidelines.

Viewpoints	Examples
Scope of application	Generic, universal, company-specific
Type of evidence	Is the research process visible? Is the evidence sound?