Global Information Assurance Certification Paper

Toward Standardization of Information Security: BS 7799
Timothy Stacey
September 22, 2000

Abstract

This paper describes BS 7799, the "Code of Practice for Information Security Management" as an information security management system, identifies the industry movement toward BS 7799 certification, reports the current effort involving the transformation of BS 7799 into ISO 17799 and suggests a need for the information security professional to familiar with BS 7799.

Introduction

The information age has ushered in a whole new set of vocations in order to manage the associated software and systems processes. We matured from "seat-of-the-pants" programming to Software Engineering. We grew and adapted existing engineering/management specialties to develop the fields of Software Project Management, Software Quality Assurance, Software Configuration Management, Software Test Engineering and even Software Safety Engineering. We've progressed such a long way in a relatively short period in history. We progressed from the mainframe era through "down-sizing" to "right-sizing", from the large central data processing installations to distributed information systems, from punch card-fed monolithic isolated systems to global e-Commerce. But the one thing that has remained constant is the constantly increasing importance that the industry is placing on the science of Information Security. Enter e-Security!

Globalization of industries and the unification of continents and consumers (i.e., the European community) has emphasized the need for standardization in all endeavors. As standard management processes have developed and quality systems have progressed, the importance of standards has grown in the world of information technology as well. For example, witness: the influence of Military Standards on computer language development, the influence of the Carnegie Mellon Software Engineering Institute's Capability Maturity Model on software project management, or the influence ISO-9000's impact in shaping today's consumer quality expectations.

The emphasis on standardization in the information security arena has grown as well. In order to have confidence in companies, prospective clients are seeking assurances that information safeguards are in place. Additionally, they are seeking assurances that management will continually monitor the effectiveness of security protections for the information and associated systems. Thus, Information Security Management Systems ISMSs) have immerged. The leading ISMS has been developed by the British Standards Institute and is known as the *Code of Practice for Information Security Management* (BS-7799).

What is BS 7799

The British Standards Institute (BSI) was formed in 1901 and incorporated under Royal charter in 1929. As a British standards body, BSI is responsible for the coordination of all interested parties toward the development of British industry policies and standards. Currently BSI supports over 3,000 technical committees and working groups covering 16,000 standards projects. BSI, as a member of the European standards organizations and the International Organization for Standardization (ISO), is responsible to make sure that British views are represented in the international arena.

In the early 1990's, the need was recognized for a practical guide for information security management. In response, a group of leading companies including: BOC, BT, Marks and Spencer, Midland Bank, Nationwide Building Society, Shell and Unilever combined to develop the Code of Practice for Information Security Management, now known as BS 7799 Part 1 *Code of Practice*. BS 7799 Part 2 *the Specification for Information Security Management Systems* was published in February 1998.

BS7799 is based on assuring integrity, availability, and confidentiality of information assets. Assurance is attained through controls that management creates and maintains within the organization. The ten key controls identified by BS 7799 for the implementation of a successful information security program are:

- A documented information security policy
- Allocation of information security responsibilities within the organization

- Information security education and training
- Security incident reporting and response
- Virus detection and prevention controls
- Business continuity planning
- Control of proprietary software copying
- Critical record management processes
- Protection of personal data (privacy)
- Periodic compliance reviews

BS 7799 Certification

Once standard practices are defined it becomes advantageous that these standards become incorporated consistently both regionally and globally. In terms of ISO 9000, the associated ISO-9000 certification offers assurance that products produced by different organizations in different geographical areas will live up to some consistent level of quality expectation. In the field of information security, certification offers an expectation that the security of information systems of different organizations will be managed in a consistent manner. While all companies depend on information to operate their business processes, now business partners, clients and suppliers, exchange much of their information over computer networks. Clearly, the inter-networking of organizations, e-Commerce and the Web has driven the need for information security certification.

The UK Government's Department of Trade and Industry commissioned the BS 7799 certification scheme, in 1998. The scheme, managed by BSI, requires participating certification bodies to be accredited by recognized national accreditation bodies. The United Kingdom Accreditation Service has accredited six bodies under ISO Guide 62 (EN 45012) to perform certification to BS 7799:

- BSI Quality Assurance
- Bureau Veritas Quality International Ltd.
- Det Norske Veritas Quality Assurance Ltd.
- Lloyd's Register Quality Assurance Ltd.
- National Quality Assurance Ltd.
- SGS Yarsley International Certification Service Ltd.

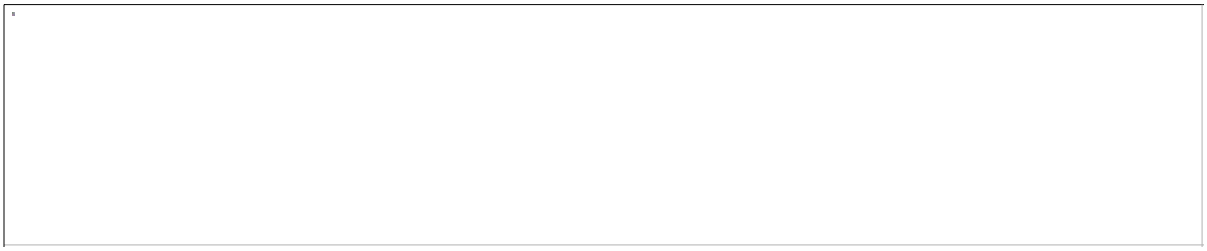
ISO 17799

Following the establishment of the UK BS 7799 certification effort, BSI has lead a drive to have BS 7799 be accepted world-wide. The primary thrust has been through the Joint Information Technology Committee of the International Standards Organization (ISO) and the International Electro-technical Commission (IEC). These organizations have agreed to "fast track" the transition of BS 7799, The *Code of Practice for Information Security Management*, into an international standard known as ISO 17799. It appears that ISO 17799 will become accepted/issued by ISO in the October, 2000 time frame. Following its acceptance, it is anticipated that the BS 7799 certification authorities listed above will offer ISO 17799 certification as well.

Conclusion

So, who needs BS 7799 certification? Table 1, Requirement for BS-7799 Certification (below), illustrates the results of a survey conducted recently by Gamma Secure Systems. Of 673 respondents, It appears that 581 respondents do. The survey results indicate that they need it now and the results indicate that their scope should encompass all three aspects of information security: confidentiality, integrity and availability. Additionally, out of the 581 respondents who have indicated an immediate need for BS 7799 certification, only 270 respondents claimed to have an information security management system in place.

Table 1. Requirement for BS-7799 Certification



Therefore, with the BS 7799 certification scheme stable and with ISO 17799 promised for the near future, we as security professionals had better become proficient in these standards

References

1) The British Standards Institute. 22 September, 2000.
URL: http://www.bsi.org.uk/index.xhtml

2) The United Kingdom Accreditation Service. "Accredited certification for BS 7799 & c:cure" 22 September, 2000.
URL: http://www.ukas.com/docs/technical-bs7799.htm

3) The National Computing Centre Limited. "BSI news - Elevation of BS7799 to ISO17799" 22 September, 2000.
URL: http://www.ncc.co.uk/standards/standardsnews.html

4) Det Norske Veritas. "Information Security Management Systems Certification BS 7799: BS7799: Frequently Asked Questions" 22 September, 2000
URL: http://www.dnv.com/certification/Services/BS7799_FAQ.htm

5) National Quality Assurance. "Factsheet: Information Security Management Systems" 22 September, 2000.
URL: http://www.nqa.com

6) Security Risk Associates. "ISO 17799 Security Standard: ISO17799 Compliance & Positioning" 22 September, 2000.
URL: http://www.securityauditor.net/iso17799/

7) Gamma Secure Systems. "BS 7799 Survey" 5 September, 2000
URL: http://www.gammassl.co.uk/bs7799/survey.html