Securing Your Organization's Information Assets

Dr. Bill Brykczynski and Bob Small
Software Productivity Consortium

Tuesday, 29 April 2003
Track 7: 1:00 - 1:40
Room 251 A - C

Leading companies are recognizing the criticality of their information assets and are implementing information security management systems (ISMSs) to systematically identify and protect these assets. ISO 17799 "Code of Practice for Information Security Management" is an international standard that provides a best practices framework for implementing security controls. British Standard (BS) 7799-2 "Information Security Management Systems – Specification with Guidance for Use" provides a life-cycle framework for implementing ISMSs. Accredited certification bodies have certified that more than 200 organizations worldwide meet the requirements of BS 7799-2.

All employees, whether in the public or private sector, are inextricably dependent on information in the workplace. Therefore, an organization's information assets, whether tangible or intangible, are essential. They are necessary for day-to-day productivity and for the ongoing viability of missions. Information assets are pervasive in contemporary organizations.

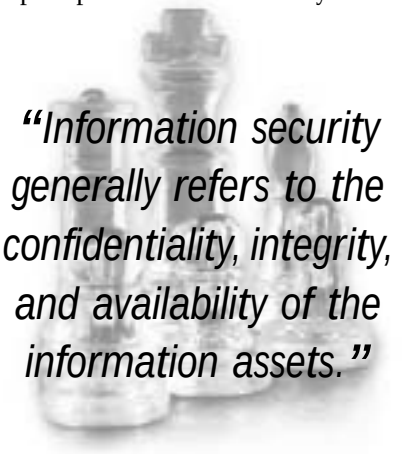
Information exists in many forms, and different types of information have different values to an organization. The impact of threats to confidentiality, integrity, and availability of information also depends on the information and an organization's mission. As information systems become increasingly interconnected, the opportunities for compromise increase.

Consider the following questions:

- Do all of your employees understand their responsibilities to protect the organization's information assets? How safe are your information assets from competitors or inadvertent exposure by your partners or customers?
- If an employee lost a laptop computer, how confident are you that you could recover from the loss with minimal disruption and compromise? What is your *risk tolerance* for such a loss?
- Are you protecting your intangible information assets, e.g., intellectual property (IP) and proprietary information, as well as your tangible information assets, e.g., computers and routers? Do your security investments complement each other to form a system of protection? Are your information assets protected in proportion to their value to the organization?
- Can your chief executive officer (CEO) tell your board of directors that your company has made a concerted effort to protect all tangible and intangible information assets?

Imagine if your company were to be sued by a customer for disclosure of sensitive financial information. The existence of an information security management system (ISMS) that was certified as meeting the requirements of a recognized standard (e.g., British Standard [(BS)] 7799-2 "Information Security Management Systems – Specification with Guidance for Use") would provide a strong defense against negligence.

Recent developments have created new tools and techniques to help organizations gain and maintain control of the complex problem of effectively securing their information assets. Before getting into the details, the following will clarify some terms:



- **Information** is what an organization has compiled or its employees know. It can be stored and communicated, and it might include customer information, proprietary information, and/or protected (e.g., by copyright, trademark, or patent) and unprotected (e.g., business intelligence) IP.
- **Information assets** are intangible information and any tangible form of its representation, including printed copies, computer files, and databases.
- **Information security** generally refers to the confidentiality, integrity, and availability of the information assets.
- **Information security management** includes the controls used to achieve information security and is accomplished by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures, and software functions.
- **ISMS** is the life-cycle approach to implementing, maintaining, and improving the interrelated set of policies, controls, and procedures that ensure the security of an organization's information assets in a manner appropriate for its strategic objectives.

ISO 17799 and BS 7799-2

In 2000, the ISO adopted the British Standard (BS) 7799-1 (Part 1) as ISO 17799, "Code of Practice for Information Security Management" [1]. ISO 17799 is a best practices framework for information security management. The standard is structured in the following 10 sections (i.e., control areas):

1. Security policy.
2. Organizational security.
3. Asset classification.
4. Personnel security.
5. Physical and environmental security.
6. Communications and operations management.
7. Access control.
8. Systems development and maintenance.
9. Business continuity planning.
10. Compliance.

Within these control areas are 36 control objectives and 127 controls. The control objectives provide guidance to the ISMS implementers on the standard's intention in a particular section. The controls are enablers; they are succinct specifications of best practices that might be incorporated into the ISMS. The controls

do not explain how they should be implemented – simply that they might be required. The standard is explicit that these controls might not be sufficient for all situations. Organizations that implement an ISMS in accordance with the standard are encouraged to create their own controls to provide additional guidance as necessary.

The following illustrates a *control objective* (from Section 3.1, Information Security Policy Document):

> Objective: To provide management direction and support for information security. Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization. [1]

The following is an example of an *enabling control* for the previous control objective (from Section 3.1.1, Information Security Policy Document): A policy document should be approved by management, published, and communicated, as appropriate, to all employees [1].

Section 3.1.1 also provides guidance on what should be included in the policy document, and how it should be communicated to the users.

Whereas ISO 17799 provides *guidance* for information security controls, BS 7799-2 states the following:

> …specifies the *requirements* for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS within the context of the organization's overall business risks [emphasis added]. [2]

The succinct requirements found in BS 7799-2 provide the basis for independent, third-party certification. BS 7799-2 also requires a life-cycle support system for the ISMS and recommends using the Plan-Do-Check-Act (PDCA) model. Figure 1 shows the PDCA model and illustrates the activities that occur in each phase.

To summarize, ISO 17799 is a framework (not a specification) that provides best practices for information security management. To actualize the appropriate set of controls requires the implementation of an ISMS. The BS 7799-2 specifies how an ISMS is developed and maintained in order to make operational the controls in ISO 17799.

Figure 1: *Principal Activities in the Plan-Do-Check-Act Cycle*

Accreditation, Certification, and Compliance

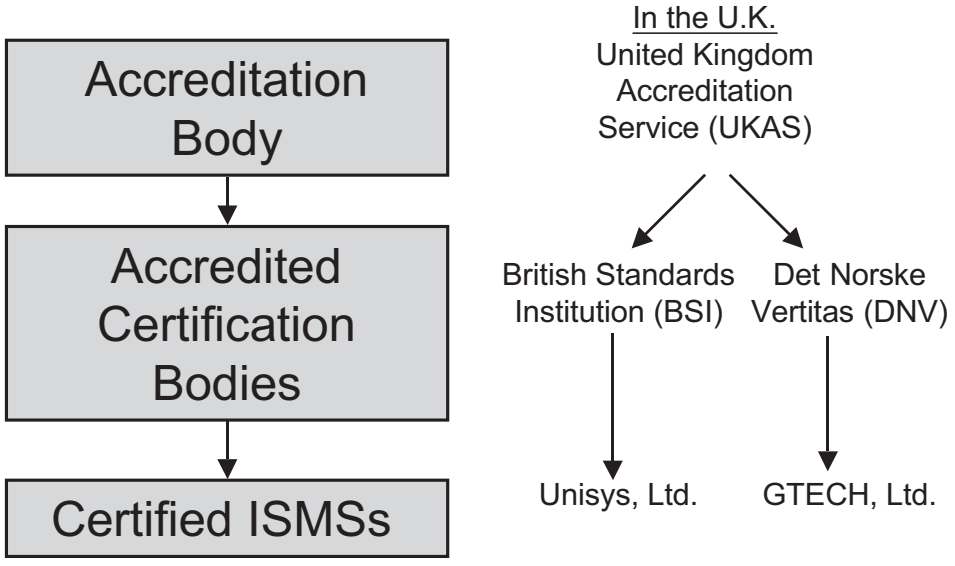
The terms accreditation, certification, and compliance are used in a variety of contexts, even within the broad area of information security. Therefore, it is important to briefly present what these terms mean in the context of ISMS:

- *Accreditation* is the means by which an authorized organization (i.e., the accreditation body) formally recognizes the competence of a certification body to assess and certify/register the ISMS of an organization with respect to published ISMS standards (e.g., BS 7799-2).
- *Certification* (or registration) is conferred by an accredited certification body on an organization upon the successful completion of an independent audit, attesting that the management system meets the requirements of a particular standard (e.g., BS 7799-2).
- *Compliance* is a self-assessment performed by an organization to validate that it has implemented a system in accordance with a standard.

Figure 2 illustrates the hierarchy of these types of organizations and credentials.

In the United States, the Registrar Accreditation Board (RAB) is the predominant accreditation body for quality management systems (ISO 9001) and environmental management systems (ISO 14000) [3]. The RAB accredits certification bodies to issue certificates to organizations fol-

Figure 2: *The Hierarchy of Credentials Leading to Certification*



lowing successful audits within these two broad areas.

In the United States today, there are no domestic accreditation or certification bodies for BS 7799-2. In the United Kingdom, the United Kingdom Accreditation Service offers accreditation to certification bodies for BS 7799-2 and other management systems standards.

For an organization considering the implementation of an ISMS, compliance is obviously a weaker claim than certification, although it is a necessary first step. For organizations that wish to implement the information security best practices in ISO 17799 today, BS 7799-2 is the companion specification for deploying and managing an ISMS. ISO has begun the formal study period on ISMSs (e.g., BS 7799-2) that will presumably lead to an ISO standard.

To date, more than 200 organizations worldwide have been certified using BS 7799-2 [4]. The Software Productivity Consortium sees increasing interest among its members in pursuing certification or at least compliance. The following three subsidiaries or divisions of consortium members have publicly acknowledged BS 7799-2 certificates:

- Fuji-Xerox in Japan.
- GTECH in Ireland and the United Kingdom.
- Unisys, Ltd. in the United Kingdom.

Unlike certification, achieving compliance is based on a self-assessment and is not a rigorously controlled credential. An organization might declare itself ISO 17799 compliant if it has implemented the information security best practices in this standard via some process. ISO 17799 is not concerned with how it is implemented and does not use the term ISMS.

Achieving BS 7799-2 certification requires achieving compliance as a first step. The PDCA model must complete at least one cycle to produce the records from the ISMS and give management the opportunity to monitor, review, and improve the system. Typically an ISMS must be in operation for at least three months before it has produced the artifacts required for audit.

An organization wishing to achieve certification for its ISMS must contract with a certification body that will assign a lead auditor to the job. As in other management systems, the size of the audit team will depend on the size and complexity of the system being audited, as well as any special domain knowledge requirements.

The audit consists of a documentation review in which the auditors review the objectives of the ISMS, and an implementation audit in which the auditors sample the artifacts of the system throughout the PDCA life cycle. The audit includes interviewing stakeholders to validate that they understand their roles and responsibilities within the ISMS.

The lead auditor will debrief the organization at the conclusion of the implementation audit and share the audit team's recommendation for certification. The certification body, in almost all cases, acts in accordance with the lead auditor's recommendation.

Critical Success Factors for Implementation

A successful ISMS, like most systems, depends on the careful balance and interaction between people, process, and technology. The principal result is to reduce risk to the organization from the potential compromise of any information asset.

Three critical success factors must be taken into account to achieve a successful ISMS implementation: effective information security, responsive management system, and organizational change management.

"In the final analysis, if the ISMS implementation does not change people's behaviors within the organization, it becomes shelfware."

In theory, risk is equal to the product of the probability of a compromising event and the impact of the compromise. Note that if either the probability is high or the impact is high, then the risk might be high. In practice, however, it is difficult to know the likelihood of most compromises, and most intangible assets do not have a monetary value. Therefore, risk analysis is not a rote exercise.

The point of implementing the ISMS is to reduce risk to the organization by improving the security of its information assets. The requisite risk analysis and mitigation planning require sound judgment to provide a solution that effectively protects the information assets from compromise to their confidentiality, integrity, and availability. In addition, confidentiality and availability may not be equally critical from organization to organization, but integrity is generally considered to be essential – without integrity, what value are the information assets?

Like other management systems, the ISMS must be designed to meet certain functional requirements, have clearly defined stakeholders with roles and responsibilities clearly defined, and include appropriate mechanisms for collecting feedback and using it to improve the system. Management systems require a commitment of time and resources.

In the final analysis, if the ISMS implementation does not change people's behaviors within the organization, it becomes shelfware. In every organization, people are already busy and do not need another set of things to do in addition to their full-time jobs. The ISMS must be intrinsic to each person's job and not merely be something else to do. Each must understand what is expected.

Peter Senge wrote the following about organizational change:

> If I stand back a distance and ask, "What's the score?" how much learning has actually been accomplished? I have to conclude that organizational inertia is winning by a large margin … Of course, there have been enough exceptions to indicate that learning is possible. However, there are many more organizations that haven't gotten to first base when it comes to real learning, and many others that have given up trying. [5]

Business Case for Implementing an ISMS

So why would an organization choose to make the investment in an ISMS and have it certified? Several questions were posed at the beginning of this article to illustrate merely a few important information security questions that might be difficult to answer. Most organizations do, in fact, have many information security controls in place. In the absence of a formal ISMS, however, these tend to be independent point-solutions rather than a unified approach to a pervasive organizational problem.

The problem is complex due to the following factors:

- The enormous quantity of information assets in most organizations.
- Assets' inherent vulnerabilities and the potential threats to their confidentiality, integrity, and availability.

- The many requirements for information security, including legal and regulatory, marketplace requirements from customers and partners, and corporate governance.

There are several reasons why an organization should make the investment in obtaining certification of an ISMS; these are outlined in the following sections.

Comprehending the Problem

In today's environment, effectively managing risk is a significant undertaking. The old adage about a chain being as strong as its weakest link certainly applies here. There are too many information assets and interfaces to be managed effectively without an ISMS. Defense in depth is an essential strategy; ultimately, however, there is no such thing as absolute security. First, understand which information assets are most important, how they might be compromised, and what the impact of a loss might be. Then, determine risk tolerance and put appropriate controls in place to ensure their security.

Earning and maintaining customer trust and protecting your organization's IP and the IP that it licenses are essential objectives in information security management. A company's reputation can easily be tarnished if management fails to take due-diligent steps to prevent compromise.

A Concrete Example

Identity theft is the fastest growing crime in the United States [6]. The largest identity-theft ring to date was broken in November 2002. It was reported that the principal suspect in the crime was a former employee of a New York company that provided software to banks and other financial institutions. The employee left the firm in March 2000 after less than a year of employment but continued to have access to private data through his own computer. This was how he was able to steal private information for criminal use [7].

What would the CEO of this company say about the need for a systematic ISMS? What would it be worth to this company to have been spared any association with this crime?

Had this company implemented an ISO 17799-compliant or BS 7799-certified ISMS, it is very likely that they would have identified many (or all) of the *links* in the chain of events that led to this disastrous outcome. They would have established controls and procedures to create a *defense in depth* that would have served them very well.

No one likes bad news, but information security risks are a part of life, and an ISMS is not a guarantee that bad things will not happen. An effective ISMS can go a long way toward reducing risk by identifying the most important assets, building appropriate risk-management solutions, and changing the culture of the organization so that information security management is intrinsic to everyone's job. In the worst outcomes, the organization is best prepared to deal with bad news, should it arise.

Organizations that have achieved certification that their ISMS meets the requirements of BS 7799-2 have objective, third-party evidence that they have taken due-diligent actions to protect the security of their information assets. At the end of the day, that is the best that can be done.

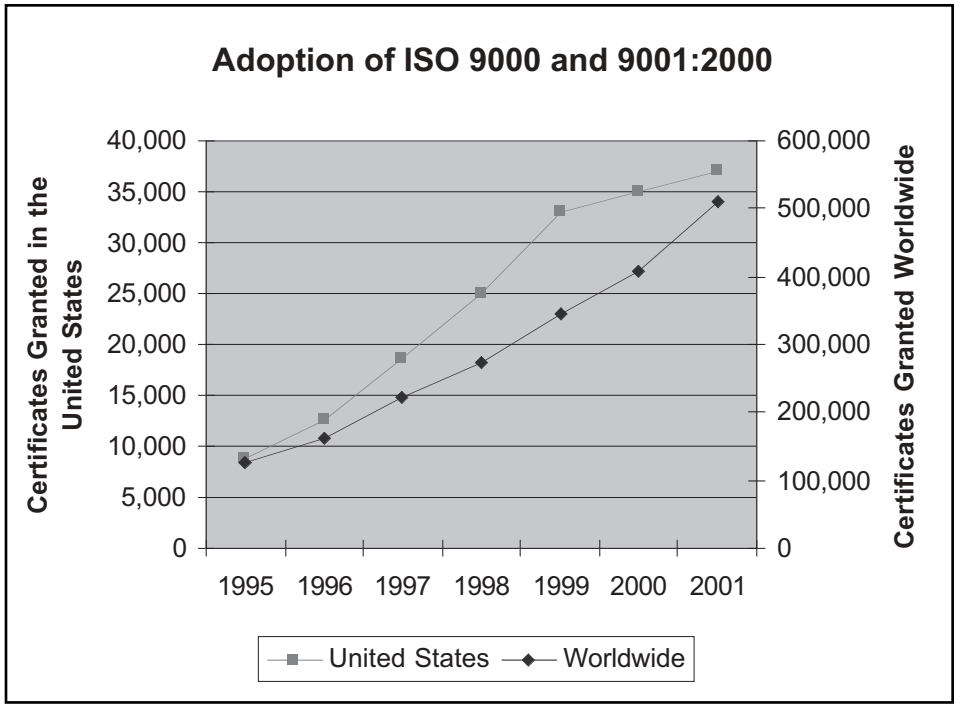


Figure 3: *Adoption of ISO 9000 as a Bellwether for ISO 17799*

Outlook for ISO 17799

This technology is still in the early adopter phase. If ISO adopts an auditing specification for 17799, the authors believe that will significantly increase demand for certification in the United States.

ISO 9000/9001 began life as a British standard. In 1995, there were almost 9,000 certificates in the United States. This grew to more than 37,000 by the end of 2001. The U.S. marketplace has hovered at around 7 percent of the global market [8]. Figure 3 illustrates the growth in the United States and worldwide markets. This might be a bellwether for ISO 17799.

Even before ISO might adopt an auditing specification for 17799, the consortium sees interest by several of its member companies to achieve BS 7799-2 certification as a discriminator in the marketplace. Others are working toward ISO compliance now as a first step toward certification in the future.

Acknowledgements

This article is based in part upon work sponsored by the Defense Advanced Research Projects Agency under Grant MDA972-01-1-0006. This article also benefited from technical review by Doron Becker, Justus Riek, Geetha Elengical, and Bernard Eydt.◆

References

1. ISO. Information Technology – Code of Practice for Information Security Management. ISO/IEC 17799:2000. Geneva, 2000.
2. British Standards Institution. Information Security Management Systems – Specification With Guidance for Use. BS 7799-2:2002. London, 2002.
3. Registrar Accreditation Board. About RAB. 2002 <www.rabnet.com/ab_main.shtml>.
4. One 7799 World, Ltd. International Register of BS 7799 Accredited Certificates <www.xisec.com>.
5. Senge, Peter, Art Kleiner, Charlotte Roberts, Rick Ross, George Roth, and Bryan Smith. The 5th Discipline: Dance of Change. New York: Doubleday/Currency, 1999.
6. Identity Theft Resource Center. Facts and Statistics: Find Out More About the Nation's Fastest Growing Crime. May 2002 <www.idtheftcenter.org/html/facts_and_statistics.htm>.
7. Weiser, Benjamin. "Identity Ring Said

to Victimize 30,000." New York Times 26 Nov. 2002.
8. ISO. Adoption of ISO 9000 and 9001:2000. <www.iso.ch/iso/en/prods-services/otherpubs/pdf/survey11thcycle.pdf>.

Additional Reading

1. For an overview of how accreditation bodies achieve their credentials, see ISO/IEC 17011, One Standard for Accreditation of All Conformity Assessment: Challenges for ISO/CASCO Working Group 18 <www.iso.ch/iso/en/commcentre/pdf/Casco0102.pdf>.
2. The ISO 17799 and BS 7799-2 standards may be obtained from <www.ceem.com/infosecurity_standards.asp>, which also contains some case studies and Web seminars.

Bob Small will also be speaking at STC 2003 on "Reducing Internet-Based Intrusions" on Wednesday, 30 April, Track 7, Room 251 A-C, from 1:50-2:30 p.m.

About the Authors

Bill Brykczynski, Ph.D., leads the security program at the Software Productivity Consortium. His professional and research interests include applied security research and software inspection processes. He has a Bachelor of Science in systems science from the University of West Florida, a Master of Science in information management from George Washington University, and a doctorate in information technology from George Mason University.

Software Productivity Consortium
2214 Rock Hill Road
Herndon, VA 20170-4227
Phone: (703) 742-7134
Fax: (703) 742-7350
E-mail: bryk@software.org

Bob Small is a principal member of the technical staff at the Software Productivity Consortium. His areas of interest include applied security research and building communities of practice. He has a Bachelor of Science in economics from Ursinus College and a Master of Science in computer science from the University of New Haven.

Software Productivity Consortium
2214 Rock Hill Road
Herndon, VA 20170-4227
Phone: (973) 984-8213
Fax: (703) 742-7350
E-mail: small@software.org

WEB SITES

Software Metrics Sites

http://user.cs.tu-berlin.de/~fetcke/measurement

The Software Metrics Sites is a guide to Internet resources on software measurement, process improvement, and related areas. Topics include electronic papers, bibliographies, and conferences on software measurement, object-oriented metrics, functional size measurement, and software process improvement. Several mailing lists that are used for discussions and the exchange of ideas can be found as well as software measurement tools that are available for downloading.

USC Center for Software Engineering

http://sunset.usc.edu/index.html

The University of Southern California's Center for Software Engineering was founded in June of 1993 by Dr. Barry W. Boehm to provide an environment for research and teaching in the areas of large-scale software design and development processes, generic and domain specific software architectures, software engineering tools and environments, cooperative system design, and the economics of software engineering. A main goal of the center is to perform research and development of practical software technologies that can reduce cost, customize designs, and improve design quality by doing concurrent software and systems engineering.

Software Technology Conference

www.stc-online.org

In its 15th year, the Software Technology Conference (STC) is the premier software technology conference in the Department of Defense and is co-sponsored by the United States Army, United States Marine Corps, United States Navy, United States Air Force, Defense Information Systems Agency, and Utah State University Extension. The STC planners anticipate more than 2,500 participants this year April 28 – May 1 in Salt Lake City from the military services, government agencies, defense contractors, industry, and academia.

MITRE

www.mitre.org

MITRE is a not-for-profit national resource that provides systems engineering, research and development, and information technology support to the government. It operates federally funded research and development centers for the DoD, the FAA, and the IRS, with principal locations in Bedford, Mass., and northern Virginia. MITRE publishes numerous periodicals and newsletters, maintains a news center, hosts numerous technology information centers, and more.

Institute for Software Research

www.isr.uci.edu

The Institute for Software Research's (ISR) mission is to advance software and information technology through research partnerships. The ISR supports research projects, develops technology, and sponsors technical and professional meetings. It works with established companies, start-ups, government agencies, and standards bodies to develop and transition the technologies to widespread and practical application. ISR was established July 1, 1999 from the Irvine Research Unit in Software.