

[ISO 9000](#)
[ISO 14000](#)
[Automotive](#)
[Telecommunications](#)
[Aerospace](#)
[Information Security](#)
[Quality Management](#)
[International](#)
[Health & Medical](#)
[Other Standards](#)
[FRONT PAGE](#)

Features

BSI's Information Security Standard - BS 7799 - Becomes Global Standard Information security - a must for success in the digital economy

by Ned Hamson

The critical need to sort out who is just "talking" information security (infosec) and who can actually deliver a complete infosec system has driven the fast track adoption of BSI's standard this past December as the new global standard ISO 17799. (please see comments by BSI's Chris Ferrant, Chris.Ferrant@bsi-global.com, in accompanying boxed story on Fast Tracking Global Infosec Standard.)

The ISO 17799 information security standard (based on BSI's BS 7799 standard) was designed to help organizations satisfy internal security needs and those same needs by partners, clients, retail customers, as well as suppliers in a systematic and reliable manner. It is not well known in North America as yet, but it soon will be. And it will likely provide the kind of reliable security needed to give retail, as well as B2B (business to business) consumers and clients the confidence needed to grow the digital economy in depth and breadth.

Supporters of the standard in the US were drawn to it by on-the-ground experience with infosec issues, as well as their basic business sense for achieving desired, not "hoped for" results. When Mary Geers, Director of Sales at Intelispan, an Atlanta, GA and New York-based provider of virtual private networks (VPN) first began looking at the information management security issue, she did so with ten years of working with law firms and their needs to assure clients that information entrusted to the law firms remained secure at all times.

Geers an enthusiastic supporter of this infosec standard bases her judgement on her years of experience working with law firms involved in facilitating complex negotiations of partnerships, alliances and mergers that are dependent upon ultra-secure virtual private networks. She notes that such negotiations, as well as the ensuing relationships require that all involved have both free and easy access via VPNs to necessary confidential or proprietary information and the assurance that the information will be remain confidential or proprietary regardless of the negotiation's outcome. As such negotiations increase and become even more complex, Geers notes that law firms need a management system based on BSI's BS 7799's (now ISO 17799) standards to protect their own liability and the security needs of their clients.

Geers also notes that the information privacy and security, as well as liability concerns in the healthcare and finance sectors require the highest levels of management system sophistication. She believes BS 7799, now ISO 17799, provides managers with a recognized framework for building just such a system.

As she talks with both technical and non-technical executives in the legal, healthcare and finance sectors, she is finding that they "get it." The most pressing corporate need, she reports, to move forward with designing and implementing management systems that will pass BS 7799 and ISO 17799 muster is appointing and training good project managers.

Dan Woolley, President and COO of Global Integrity a Reston, VA (acquired by Predictive Systems in December 2000) and a well-known infosec expert expressed why he was a supporter of using BS 7799 in this straight forward manner: "The old expression holds true: Would you sleep at night if your most sensitive corporate information was located on your partner's systems? In B2B relationships, there is a lot of sensitive information that companies require their partners to secure. The complexity of these relationships are often cumbersome and onerous." (September 2000: Information Security)

Robert E. Johnston, CISSP, a senior information systems security solution architect with Hewlett-Packard Co. stated in a June issue of Information Security, his reason for supporting fast adoption of BS 7799 as a global standard was his experienced-based understanding that "...well-founded policies and standards [BS 7799] enable business processes by ensuring that well thought-out, management-supported decisions provide staff with the guidelines necessary to ensure the success of the enterprise."

Using the standard

BSI, Inc 2001

Internet banking how safe?

A UK-based internet bank "smile" (www.smile.co.uk) was the first in the world to be registered to the information security standard, BS 7799 (Smile is backed by another UK financial institution, the Co-operative Bank). Keith Girling, director of technology at the Co-operative Bank said: "...It is very satisfying to know we have met all the rigorous requirements [BS 7799] laid down by BSI."

Adero - a Boston-based, internet start up: Self-described "security guy," Joe Judge said (in a recent article in Information Security) that when drawing up and implementing a security management system for Adero, rather than "reinvent the wheel," he drew upon the "numerous models of tried and true infosec principles and policies." Step one, for Judge was to use "BS 7799 as a model" to devise an infosec policy for Adero. Why use BS 7799? Judge notes, that BS 7799 "is becoming the de facto standard for information security organizations and the "ISO 9000" of our [infosec] field."

Judge also notes that devising and implementing a management policy based on BS 7799 is not a one-person job. He, Judge, soon realized that to the level of detail needed for full implementation would require the "assistance and input of outside experts."

Keys to success or learnings by Judge at Adero?

1. Roll up your sleeves and get involved with the people doing the day-to-day information creation, processing and transmission work.
2. Stay on target that is cooperate and get involved but maintain your focus on establishing and maintaining an information securing management system.

Nutshell history BS 7799

BS 7799, first published BSI in February 1995 was designed to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce, and to be used by large, medium and small organizations. It was significantly revised and improved in May 1999. BSI has offered assessment and registration to BS 7799 since 1997.

What Makes Up ISO 17799?

ISO 17799, is a detailed security standard. It consists of ten major sections, each covering a different topic or area:

1. Business Continuity Planning
2. System Access Control
3. System Development and Maintenance
4. Physical and Environmental Security
5. Compliance
6. Personnel Security
7. Security Organization
8. Computer & Network Management
9. Asset Classification and Control
10. Security Policy

Fast Tracking BSI's BS 7799 into a Global Infosec Standard

by Chris Ferrant - BSI Global

The need for a global standard on information security was so compelling ISO fast tracked the adoption of BS 7799. Some of the reasons for this fast track approach were demands from industry and the public to control information. Recent years, the growth in information security breaches has been phenomenal.

Personal medical files being found on rubbish bins, confidential memos finding their way to the press, account details being posted for all to see on websites. The list is endless, with every day bringing more reports of breaches in security. We are all, both personal and commercially, data subjects and all types of organizations hold information about us. We have a right to expect that the organizations collecting, holding and processing data about us keep it secure and correct.

Resistance or objections easily overcome

Some countries were initially reluctant to take on the standard as an ISO. The main objection would seem to be the "not invented here syndrome", often seen at standards submissions meetings. After some debate and almost no change to BS 7799, other than referencing words, the committee was formally balloted in September. The committee members voted and BS 7799 achieved the required majority to take it to the final resolution stage.

In October at the ballot resolution meeting the i's were dotted and the t's were crossed and the final draft went to the ISO/IEC JT1 meeting in November for formal adoption as a full ISO standard. On the 1st of December 2000 the standard ISO/IEC 17799 (2000) was published. BS 7799 had become an ISO standard in record breaking time such is it's strength. The project of ongoing management has been assigned to ISO/IEC JTC1/SC27 at ISO with SC27/WG1 working group responsible for future maintenance and revisions.

Implementation of the specifications in the code of practice can take up to six months or more for larger companies. So this standard does represent a considerable commitment from any organization. The return on that commitment however is incalculable as the loss of one piece of information can bring down governments, bankrupt a business or destroy a reputation. Information is the key to all organization, information is one of the most valuable assets of an organization, it need to be protected and managed ISO 17799 does this.