Improved ISO/IEC 17799 heralds new series on information security management systems

by **Ted Humphreys**

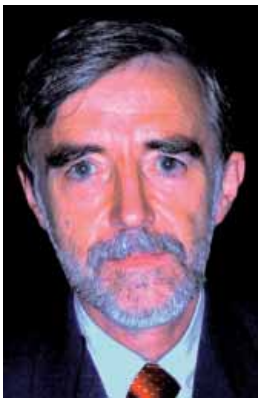
The newly published ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management, *is a revised, improved version of the standard that has become the international benchmark. It will be followed later this year by the new ISO/IEC 27001*, Information security management systems – Requirements, *intended for management system certification.*

All organizations have assets essential to their survival. Arguably, information in its various forms is one of the most important assets, be it printed, stored electronically, posted or e-mailed, shown on film or spoken.

For most businesses, information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image. But many businesses and most non-business organizations may hold information as their only asset. An absence of information security may threaten their integrity and, therefore, very existence.

The 2002 Computer Crime and Security Survey[1] of 503 computer security practitioners in the United States indicated that the threat from computer crime and other information security breaches continues unabated – and that the financial toll is mounting.

According to the survey's findings, 90 % of respondents detected computer security breaches within the 12 months covered by the survey, 80 % acknowledged financial losses due to computer breaches, and 46 % (223 respondents) reported their resulting financial losses as totalling USD 455 848 000[2] (excerpt from " Business standards : IT security – securing your business advantage ", *ISO Management Systems*, July-August 2003).



***Ted Humphreys** is Director of XiSEC, a company specializing in information security management systems. He serves as Convenor of the Joint Technical Committee, ISO/IEC JTC 1,* Information technology, *Subcommittee 27,* IT Security techniques, *Working Group 1,* Requirements, services and guidelines.

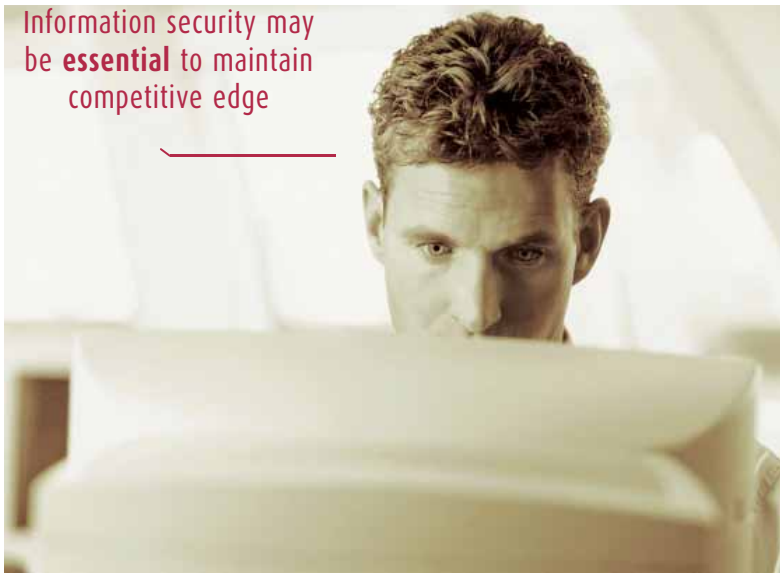
E-mail tedxisec@aol.com

Web www.xisec.com

Tel. + 44 1473 626615

Just published, the revised ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*[3], integrates the latest developments in the field to maintain it as the international standard code of practice.

Information security may be **essential** to maintain competitive edge



Improved protection guidelines

With exploitation of these computer vulnerabilities accelerating at an alarming rate, the work of Joint Technical Committee, ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*, Working Group 1, *Requirements, services and guidelines* has become timelier than ever.

In view of the critical need for the business world to protect the confidentiality and integrity of information, the ISO/IEC working group has developed an improved version of the joint ISO/IEC standard that has become the burgeoning e-commerce community's international benchmark for information security management. ISO/IEC 17799:2005 is a code of practice for information security management. It is not a certification standard and was neither designed, nor is it suitable for this purpose. It will be followed in the last

1) The survey is conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigations (FBI) Computer Intrusion Squad.

2) Refers to those respondents who were willing and/or able to quantify their financial losses.

3) ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*, costs 200 Swiss francs and is available from ISO national member institutes membership (these are listed with full contact details on ISO's Web site: **www.iso.org**) and from ISO Central Secretariat (**sales@iso.org**).

quarter of the year (publication currently expected in November 2005) by the specification standard ISO/IEC 27001, *Information security management system (ISMS) requirements*, which can be used for certification.

International language

The revised ISO/IEC 17799: 2005 is the most important standard for managing information security that has been developed – it establishes a truly international common language for information security for all organizations around the world to engage with each other to do business.

It provides organizations with many state-of-the-art additions and improvements in information security best practice. For example, better management of security arrangements with external businesses, outsourcing and service providers, enhanced indicant handling capability, dealing with problems of patch management, mobile devices, wireless technologies and harmful mobile code via the Internet, improvements in best practice managing human resources and several other new features.

The new version addresses the security of information in its widest sense, providing best business practice, guidelines and general principles for implementing, maintaining and managing information security in *any* organization, producing and using information in *any* form.

The new version provides best business practice for managing information security in ***any*** organization

ISO/IEC 17799:2005 identifies the controls that form the starting point for information security. It covers the critical success factors, the organization of information security, asset management, human resources, physical and environmental security, communications and operations management, information systems acquisition, development and maintenance, incident management, business continuity management and compliance. It is destined to become an essential tool for organizations of every type and size, whether public or private.

Here are some of the drivers for this revised edition of the Code of Practice, highlighting its new features that address the latest business requirements.

Business drivers and requirements

Several changes to business environments and new ways of doing business were important in driving the development of the revised ISO/IEC 17799:2005. We recognized:

- the growing dependence on the use of external services and the management of service delivery;
- changes to the risks and threats facing businesses;
- new and emerging technologies and greater connectivity, and the impact this has on protecting information; and
- growing security requirements for regulatory compliance.

External services

The revised edition introduces a number of improvements and updates and additional best practice provisions,

The business world is more dependent on external services for its outsourcing, off-shoring, networking and Internet hosting needs than ever before – and more business is being carried out with clients, business partners and supply chains using various on-line and networking arrangements.

While providing business efficiency and better information sharing in highly competitive markets, it also makes access to organizational systems easier and increases the vulnerability of sensitive and critical information.

ISO/IEC 17799:2005 extends best practice to external services to address today's business demands, and has also introduced new service management controls aimed at securing the availability and accessibility of external services.

Human resources

Another revision addresses the critical area of information security and employees. Irrespective of how good the security technology may be, people can be exploited and thus compromise security. ISO/IEC 17799:2005 improves best practice in three key areas:

1. Prior to employment

– the recruitment process;
– employee references and screening; and
– contracts, terms and conditions of employment

2. During employment

– allocating roles and responsibilities;
– giving access rights and establishing user accounts, and

What users think of ISO/IEC 17799

Has ISO/IEC 17799 been valuable to users? What do they expect from the revised version?

Here is some feedback from organizations around the world about benefits they have experienced from implementing the best practice given in this standard, to support the economic well-being of their businesses.

Microsoft: 'An invaluable toolset'

"The ISO/IEC 17799 standard, in particular, the newly revised version, is an invaluable toolset for information security professionals. This standard provides them with a universal approach of communicating information security management best practice, a way to ensure consistency of practice, and a means to establish and raise the baseline for managing information security risk in their environment."

Meng-Chow Kang,
CISSP, CISA and Chief Security & Privacy Advisor,
Asia Pacific Region, Microsoft.

Fujitsu: 'Much more user friendly'

"The 2000 version of ISO/IEC 17799 provided management with a tool to ensure that all important areas of information security were included in security control programmes including best practice advice to deal with the risks of third party access from suppliers, outsourcing arrangements and service delivery. The new 2005 version makes it much simpler to develop internal standards because the requirements are now clearly and consistently described for each control. We plan to start using it in our ISMS work as soon as possible because it is much more user friendly."

John Snare, *Fujitsu Australia.*

PCCW: 'has benefited extensively'

"By continuously enhancing its strategic and operational approach to the consistent management of information security, PCCW has benefited extensively from using the structured approach contained within ISO/IEC 17799. With the release of the new version, including the new multiple controls, the tightening of existing controls and the alignment of the new simplified structure, ISO/IEC 17799:2005 will allow PCCW to immediately enhance and further lead the industry in applying world best information security practices to the protection of its information assets."

Dale Johnstone,
Information Security Governance Risk Management,
PCCW Limited, Hong Kong.

– training and awareness, including applying procedures and reporting incidents

3. *At termination of employment*

– removing access rights and user accounts, thus preventing later access to the organization's systems and processes;

– removing physical access, e.g. cancellation of entry passes, and

– return of assets such as information, papers, storage media, software and laptops.

duced to counter the problem.

- *Potential problems of mobile code* – addressing the need for control of mobile software code to avoid breaches of information security, including unauthorised use or disruption of business systems, networks, or applications.
- *Pervasive use of mobile devices and wireless networks* – awareness that those sharing wireless networks can to gain access to mobile devices, lap-tops and business information.

Threats and vulnerabilities

ISO/IEC 17799:2005 also acknowledges a number of threats and vulnerabilities that have emerged recently, including:

- *Management of software patches* – in recognition of the increasing risk of new software being exploited before patches can be intro-

Helping organizations worldwide

ISO/IEC 17799:2005 is intended to provide organizations around the world with new best practice improvements and enhancements to help them:

- provide greater customer confidence and assurance that their systems and services are "fit for purpose";

- make more profitable use of their investment in information security as a business enabler;
- enhance management control of businesses information assets and information security risks;
- make improvements to internal security policies and procedures operations, and to security arrangements with suppliers and service providers;
- achieve compliance with applicable national and international security requirements.

ISO/IEC 27001 will serve information security as ISO 9001:2000 does quality

Complementary and supportive standard

While ISO/IEC 17799:2005 is a code of practice for information security management, it is not applicable to management system certification. However, the complementary and supportive standard ISO/IEC 27001, *Information security management systems – Requirements* is designed for this purpose.

Publication of the ISO/IEC 27001 ISMS is expected in November 2005. The specification standard is a revised version of BS 7799 Part 2:2002 (ISMS), which has been used for certification for the past seven years. Both use the Plan-Do-Check-Act process model as featured in ISO 9001:2000 and ISO 14001:2004, and are based on the same certification process as the QMS and EMS standards.

International certification activities

Already over 1300 organisations in over 50 countries have had their ISMS certified. The figure is rising by around 80-100 per month and it is expected that certification to ISO/IEC 27001:2005 will accelerate this growth via some 45 accredited certification bodies involved in the process.

A free access register, available on the ISMS International User Group Web site (**www.xisec.com**), provides details of the certificates to be registered and/or modified/deleted. This information is submitted regularly by all the accredited certification bodies involved.

The ISO/IEC 27000 series

ISO/IEC 17799:2005 and the future ISO/IEC 27001 are part of the ISO/IEC 27000 series of standards being developed by JTC 1/SC 27. There is a proposal to allocate the number ISO/IEC 27002 to ISO/IEC 17799 in 2007. Currently, SC 27 is developing ISO/IEC 27003 and ISO/IEC 27004, aimed at providing supporting guidance for ISO/IEC 27001.

The creation of a family of ISMS-related standards is intended to mirror the approach adopted by the ISO 9000:2000 series of QMS standards – and thus ISO/IEC 27001 will serve information security as ISO 9001:2000 does quality. •