

# ISO 17799: Is This the New Universal Security Standard?

By **Bruce Gorman**  
*bruce@wtchmc.com*

## Introduction

The breakneck pace of technology continues to change all our lives in dramatic ways. This is particularly true of information security. The reality is business now relies on timely, accurate information to make critical decisions. Information is an asset which, like other important business assets, has value to an organization and needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Indeed, the widespread and well documented problems business now faces from information security breaches is a clear indicator that we are continuing to play catch up. On June 17, 2005, MasterCard International Inc. said up to 40 million cardholders of multiple brands across North America could be vulnerable to fraud due to a security breach that began in 2004<sup>1</sup>. Breaches like that underscore the need for businesses to pay close attention to security concerns at all levels and be ready to thoroughly account for their decision-making processes.

This has led to the necessity of a common framework for information security management. Such standards have many benefits including building trust between business partners and consumers as well as providing a common benchmark for assessing an organization's Information Security Management System (ISMS). In addition, more organizations are looking towards certification of their systems. Currently this can be accomplished using a variety of standards.

ISO 17799 is one such standard gaining international popularity.

## Background

ISO 17799 is a descendant of the British Standard Institute (BSI) Information Security Management standard BS 7799. The BSI Group<sup>2</sup> is a leading business services provider to organizations worldwide. They have focused on information security standards for over 10 years. In 1991, a working group devoted to information security was first established. Two years later a "Code of Practice for Information Security Management" was formed. This evolved into the first version of the BS 7799 standard released in 1995.

BSI then formed a program to accredit auditing firms to audit BS 7799. Currently the BS 7799 standard now consists of Part 1: Code of Practice, and Part 2: Specification of Information Security Management Systems.

BS7799 Part 1 is essentially a best practices standard. Anyone can buy the standards document and implement the security best practices. BS7799 Part 2 is for organizations seeking certification.

It is important to understand the distinctions between the two parts. Part 1 is an implementation guide. It is used as a means to evaluate and

build comprehensive information security infrastructure. Part 2 is an auditing guide based on requirements. To be certified as BS 7799 compliant, organizations are audited against Part 2.

## Emergence of ISO 17799

While many organizations utilize the BS 7799 standard, demand grew for an internationally recognized information security standard under the directions of an internationally recognized body, such as the ISO. This demand led to BSI fast tracking BS 7799 Part 1, resulting in the initial release of ISO 17799 by the ISO. Currently only BS 7799 Part 1 has been accepted for ISO standardization. ISO standardization for part two is not currently being pursued.

ISO 17799 is high level, broad, and conceptual in nature. This approach allows it to be applied across multiple types of enterprises and applications. ISO 17799 is the only standard focused on Information Security Management in a field generally governed by guidelines and best practices.

ISO 17799 is organized into 10 major sections:

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 and Network Management
9. Asset Classification and Control
10. Security Policy

## Survey of Other Standards

Many other security standards have emerged including:

1. Control Objectives for Information and related Technology (COBIT), published by the IT Governance Institute, represents a collection of documents that can be classified as generally accepted framework and standards for IT governance, security, control and assurance.
2. The IT Infrastructure Library's (ITIL's) Security Management is a methodology describing how IT security management processes link into other IT infrastructure management processes.
3. Generally Accepted Information Security Principles (GAISP) is a collection of security principles that has been defined and produced as a collective effort. GAISP is a work in progress under the direction of the

Information Systems Security Association (ISSA) with support from groups such as the International Information Systems Security Certification Consortium (ISC)<sup>2</sup>.

4. Systems Security Engineering—Capability Maturity Model (SSE-CMM) Model is a guide to the concepts and application of a model to improve and assess security engineering capability.
5. ISO/IEC 13335 Information Technology—Guidelines for the Management of IT Security, released by the International Organization for Standardization and the International Electrotechnical Commission, is technical guidance subdivided into five parts which provide guidance on aspects of information security management.
6. ISO/IEC 15408:1999 Security Techniques—Evaluation Criteria for IT Security is based on the Common Criteria for Information Technology Security Evaluation 2.0 (CC). ISO/IEC 15408:1999 is used as a reference to evaluate and certify the security of IT products and systems.
7. NIST 800-12 An Introduction to Computer Security—The NIST Handbook, released by the US National Institute of Standards and Technology (NIST), describes the common requirements for managing and implementing a computer security program and some guidance on the types of controls that are required.
8. Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>R</sup>) is a set of principles, attributes and outputs for risk assessment.
9. Organization for Economic Cooperation and Development (OECD) Guidelines for the Security of Information Systems and Networks provides a set of nine information security principles aimed at fostering a “culture of security.”

While duplication occurs among the frameworks, some are more complementary than overlapping and companies often employ more than one. Particularly complementary frameworks to ISO 17799 include ITIL and COBIT.

ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organizations’ growing dependency on IT and embodies best practices for IT Service Management.<sup>3</sup>

The ethos behind the development of ITIL is the recognition that organizations are becoming increasingly dependent on IT in order to satisfy

their corporate goals and meet their business needs. This leads to an increased requirement for high quality IT services.

CobiT provides a reference framework for IT, security, auditing managers and users. Now in its third edition, CobiT is growing in acceptance as a good practice for control over data, systems and related risks. It helps companies deploy effective governance over systems and networks.<sup>4</sup>

CobiT’s management guidelines component consists of tools to measure a company’s capabilities in 34 IT processes. These include performance measurement elements, a list of critical success factors that provides best practices for each IT process, and maturity models to help in benchmarking.

In terms of ISO 17799, ITIL is strong in IT processes, but limited in security and system development. CobiT is strong in IT controls and IT metrics, but does not say how (i.e. process flows) and is not strong in security.

## Value Proposition

It is unfortunate that we often see trade-offs in terms of balancing the requirements of business against the need for confidentiality, integrity, and availability of information. Traditionally, information security management has been based on loosely established best practices and guidelines with the primary goal of preventing, detecting, and containing security breaches. ISO 17799 provides companies with an established framework from which to build an effective ISMS. The value proposition for properly implemented ISO 17799 is compelling. As a comprehensive information security process, the ISO 17799 standard provides business with a host of benefits including:

1. Achieving competitive advantage
2. Greater likelihood of achieving business objectives
3. Improved enterprise security
4. More effective security planning and management
5. More secure partnerships and e-commerce
6. Enhanced customer confidence
7. More accurate and reliable security audits
8. Reduced liability

ISO 17799 will become more recognizable and respected over time just as other ISO standards like ISO 9000 and ISO 14000 have. Just being associated with ISO is an important distinction for the standard.

## Limitations

Although the benefits of ISO 17799 are compelling, there are certain limitations that must be understood.

ISO 17799 is a compilation of recommendations for best security practices that can be applied by any business and was written with flexibility in mind. Its recommendations are technology neutral, in that they do not provide help in evaluating or understanding existing security measures. It discusses the need for intrusion prevention systems but does not speak to how they should be used. Detractors have suggested that ISO 17799 is too vague.

Others suggest that ISO 17799 is short on methodologies for measuring the standard’s effectiveness. Each section contains language on the need for periodic reviews and regular compliance checks, but the standard has no mechanisms for these checks. Without such matrices, critics say the standard has no way of proving its value.

Several nations have indicated that portions of ISO 17799 are in conflict with their national laws, particularly those concerning privacy. In Canada there has been significant discussion surrounding ISO 17799 and the Personal Information Privacy and Electronics Document Act (PIPEDA). These discussions have focused on what the privacy framework should allow you to do and that impact on ISO 17799.<sup>5</sup>

Despite the detractors, others suggest that the standard will address these concerns as it matures. The ISO’s latest revision was recently published on June 10, 2005.<sup>6</sup> ISO/IEC 17799:2005 revises ISO/IEC 17799:2002. It provides organizations with many state-of-the-art additions and improvements.

## Market Adoption

The continuing adoption of ISO 17799 has caught the attention of the information security community at all levels. More promising is its newfound global acceptance after transitioning from BS 7799. Indeed for security management, ISO 17799 is the most widely accepted standard. This is not a particularly profound statement right now, but in time as adoption rates continue, ISO 17799 will be an important part of the information security landscape. For now the best measure of its current success may be that other standards bodies are trying to compete with this ISO specification.

It is not surprising that this standard has been widely adopted in the United Kingdom and Pacific Rim, where it originated. In North

America ISO 17799 continues to gain acceptance. According to the latest edition of the ISO 17799 Newsletter,<sup>7</sup> recent purchases show the UK has 379 and the US has 588. A listing of formally registered companies, including scope information, is available at the ISMS International user group Web site.<sup>8</sup>

North American companies like BMO Financial Group (BMO)<sup>9</sup> are leading the way and have shown the value of the standard. With a clear information security mandate, and senior-level support, BMO is poised to take advantage of much of what ISO 17799 has to offer. BMO provided a compelling case for ISO 17799, including consistency of security functions throughout the organization and compliance with related mandates and laws.

Sun Life Financial<sup>10</sup> is another ISO 17799 success story. As part of their security governance strategy, ISO 17799 has helped them deal with regulators and international business partners, it has helped them justify their security policies and standards, and it has afforded them flexibility as a security management standard and not a technical standard.

The adoption of ISO 17799 has also been influenced by the ISO 17799 toolkit. This toolkit is widely recognized as the de facto set of blueprints for implementation. In essence it is a collection of the basic building blocks for the standard and includes:

1. The ISO17799 Standard
2. ISO17799 Aligned Security Policies
3. A Roadmap for Certification
4. An Audit Kit
5. A Disaster Recovery Kit
6. A Management Presentation
7. Business Impact Analysis

Organizations around the world are continuing to adopt ISO 17799. In many cases market conditions and private-sector initiatives have helped drive this adoption. Increasing concerns surrounding personal privacy and information warfare are key contributors.

## Legislative Considerations

In recent years, legal and regulatory concerns have been driving organizations to adopt frameworks to manage compliance and accompanying controls. Privacy and security breaches have fueled an explosion of government legislation and regulations around the world.

U.S. companies have been impacted by a variety of federal and state government mandates related to information security. These include:

- ▼ Sarbanes-Oxley Act of 2002
- ▼ Homeland Security Act of 2002
- ▼ USA Patriot Act of 2001
- ▼ Gramm-Leach-Bliley Act of 1999 (GLBA)
- ▼ Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Other countries have enacted security-related legislation as well. The European Union has implemented numerous privacy directives, including the 1998 EU Data Protection Directive, which requires member states to enact comprehensive legislation protecting the privacy of personal data. Similarly in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) does the same.

The recent emergence of international legislation highlights the need for an effective global security standard. The growing adoption and continuing maturity of ISO 17799 clearly set it apart from the crowd. ISO 17799 con-

tinues to establish itself and is well equipped to support existing and future legislation. All this at a time when many other standards lack direction, are not well organized, and do not have global appeal.

## The Future

The future of ISO 17799 is bright, as the bandwagon of support continues to gain momentum. Key indicators include:

1. ISO 17799 is quickly becoming the de facto standard in Europe and the Pacific Rim.
2. The number of certified organizations in North America continues to increase as does the purchase of the standard.
3. The erosion of personal privacy and the growing concern of information warfare has placed and kept information security in the limelight; the time is right for ISO 17799.
4. The National Cyber Security Partnership (NCSP) recently issued its report, which recommends the use of ISO 17799.<sup>11</sup>
5. The fact that it is an ISO Standard.

Indicators such as these make a strong case for future success, however it is important that the road to success be carefully traveled. Success factors include:

1. Security policy properly reflecting business objectives
2. The approach to implementation must be consistent with the organization's culture
3. Management must provide clear commitment and support
4. A sound understanding of security risk analysis, risk management and security requirements is critical
5. Marketing of security to employees
6. Education and training
7. A measurement system to evaluate performance.

With success factors such as these clearly understood, agile organizations around the world including Citibank and KPMG in the US, and BMO and Sun Life in Canada are showing us a glimpse of the future right now.


## Conclusions

ISO 17799 is rapidly becoming the de facto security standard in Europe and the Pacific Rim. Several Asian governments including Taiwan, Singapore and Hong Kong are requiring companies to receive certification to do electronic transactions with the government. Large multinationals such as Citibank, KPMG, Sony Electronics, and Unisys have certified their security programs.

Security standards are indeed commonplace, but there's little uniformity in determining which set of best practices must be and should be applied to the wide variety of environments. Establishing a universally recognized standard of security policies and practices is tremendously appealing. ISO 17799's chief attribute is its flexibility. Written in an open framework, the standard's compilation of best practices can be applied by any organization regardless of size or industry.

Despite some growing pains, the good news story of ISO 17799 will continue. Establishing all-encompassing best practices will have its challenges, but is doable. The latest revision of ISO 17799 published in June of 2005 confirms the commitment and global interest.

The information security community around the world is watching ISO 17799 carefully. With the current level of acceptance, and the compelling

benefits of ISO 17799, this standard has the clear potential to rival the success of any other information security standards and be the new universal security standard. It could become as recognizable as other widely known ISO standards such as ISO 9000 and ISO 14000. 

---

*Bruce A. Gorman, B.S., M.S., C.I.S.M., I.S.P., is Manager of Information Technology at Trade Centre Limited in Halifax, Nova Scotia, Canada. Trade Centre Limited is a crown corporation of the Province of Nova Scotia government.*

<sup>1</sup> MasterCard International Identifies Security Breach at CardSystems Solutions, A Third Party Processor of Payment Card Data. In Mastercard International. Retrieved from <http://www.mastercardinternational.com/cgi-bin/newsroom.cgi?id=1038>

<sup>2</sup> BSI Global. Retrieved from <http://www.bsi-global.com/index.xalter>

<sup>3</sup> About ITIL. In UK Office of Government Commerce. Retrieved from <http://www.ogc.gov.uk/index.asp?id=1000367>

<sup>4</sup> COBIT Framework 3rd Edition, Information Systems Audit and Control Association, Rolling Meadows, Illinois, 2000

<sup>5</sup> Burke, C. Privacy Compliance and ISO 17799, Integrity Incorporated, 2004, pg 10. In ISO 17799 User Group Canada. Retrieved from

<http://www.scienton.com/7799ug/images/Privacy%20and%20ISO17799%20in%20Canada%20-%20Conference%20Presentation%20-%20Carolyn%20L%20Burke%20-%20Jan2004.pdf>

<sup>6</sup> ISO/IEC FDIS. In International Organization for Standardization. Retrieved from <http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&scopelist=PRO-GRAMME&showrevision=y>.

<sup>7</sup> ISO 17799 Security Newsletter Issue 10. In ISO 17799 Security Newsletter. Retrieved from <http://www.iso17799-web.com/issue10.htm>

<sup>8</sup> ISMS International User Group. Retrieved from <http://www.xisec.com>.

<sup>9</sup> BMO Financial Group. Retrieved from <http://www.bmo.com>.

<sup>10</sup> Sun Life Financial. Retrieved from <http://www.sunlife.com>.

<sup>11</sup> Security Governance, A Call to Action. (April 2004) In National Cyber Security Partnership. Retrieved from [http://www.cyberpartnership.org/InfoSecGov4\\_04.pdf](http://www.cyberpartnership.org/InfoSecGov4_04.pdf).

