7799: The Code of Practice, the Specification, and TruSecure

by Marne E. Gordan
Director of Regulatory Affairs

November 2001

TruSecure

7799: The Code of Practice, the Specification, and TruSecure

Table of Contents

Complete copies of these standards are available for purchase in electronic format from http://www.bspsl.com/17799/ British Standards may also be obtained in hard copy from BSI Customer Services, 389 Chiswick High Road, London, W4 4AL. (Tel +44 (0) 20 8996 9001).

Service Comparison Charts

As a managed security service, TruSecure® Corporation's Enterprise 2001 is in complete alignment with both the BS ISO/IEC 17799 Code of Practice and the BS 7799:2 Specification. Organizations seeking to apply the code of practice to their corporate computing environment, or self-certify compliance with the specification, will find that TruSecure Enterprise 2001 supports the control objectives with Essential Practices that establish a baseline security posture for the organization across the enterprise. Those organizations seeking formal certification for BS 7799:2 will find that TruSecure Enterprise can streamline the preparation process, and provide documentation and third-party validation of controls in place to an accredited certification auditor.

Chart 1: The control categories of the Code of Practice and the Specification

Control Categories	BS ISO/IEC 17799	BS 7799:2	TruSecure Enterprise 2001
Security Policy	Best Practice Guidance	Best Practices	Policy and Procedure Review
Security Organization	Best Practice Guidance	Best Practices	Technical Reporting Management Level Reporting *Enterprise 2001 is a comprehensive security program. The Enterprise Risk Manager (ERM) and resulting documentation provide substantial information to be communicated to the client's working committees, management, and Board of Directors.*
Asset Classification and Control	Best Practice Guidance	Best Practices	Essential Practice Validation Electronic Assessment
Personnel Security	Best Practice Guidance	Best Practices	Essential Practice Review Policy and Procedure Review
Physical and Environmental Security	Best Practice Guidance	Best Practices	Essential Practice Review Physical Inspection
Communications and Operations Management	Best Practice Guidance	Best Practices	Essential Practice Validation Policy and Procedure Review
Access Control	Best Practice Guidance	Best Practices	Essential Practice Validation Electronic Assessment
Systems Development and Maintenance	Best Practice Guidance	Best Practices	Essential Practice Validation Policy and Procedure Review
Business Continuity Management	Best Practice Guidance	Best Practices	Essential Practice Review Policy and Procedure Review
Compliance	Best Practice Guidance	Best Practices	Policy and Procedure Review *Certain legal and compliance issues are considered by TruSecure to be core business issues for the client, and therefore outside the scope of information security.*

TruSecure Enterprise 2001 and TruSecure's Essential Practices are the products of private enterprise. As such, TruSecure derives its intelligence directly from the computer security industry. Its research division, the ICSA Labs, and its Risk Recon team of information security experts are responsible for the development and maintenance of the Essential Practices, which are the basis of the TruSecure Enterprise 2001 service. The Essential Practices are routinely reviewed and updated to accommodate changes in technology, as well as new and emerging threats and vulnerabilities. In addition, ICSA Labs sponsor a variety of industry consortia; volunteer participants include leading hardware and software manufacturers, as well as the major ISPs, which contribute to TruSecure Corporation's knowledge base.

Chart 2: Source information on the security practices

	BS ISO/IEC 17799	**BS 7799:2**	**TruSecure Enterprise 2001**
Sponsor	International Standards Organization	British Standards Institution	TruSecure Corporation
Source	International Electro-technical Commission	DISC Committee	ICSA Labs ICSA-sponsored industry consortia TruSecure Risk Recon team
Review Period	Committee review every five years; revisions published as necessary	Committee review every two years; revisions published as necessary	Committee review and revisions quarterly
Certification Period	N/A	Organizations certified under the specification remain so until the specification is revised	TruSecure certified clients are re-assessed quarterly, and remain certified as long as compliance with Essential Practices is maintained.
Certified Organizations	None	36 Worldwide*	130 Worldwide*

** as of November 1, 2001*

TruSecure Enterprise 2001 is a comprehensive information security program. Both the Code of Practice and the Specifications require that a risk assessment be performed to determine those criteria most appropriate to the organization, and that they are applied to the organization with sufficient security expertise. Even those organizations choosing to forgo formal certification often choose to outsource a security review against the code of practice or the specification. Unlike traditional security audits, those elements necessary to appropriately apply and support the 7799 standard, such as a risk assessment, are an integral part of TruSecure Enterprise delivery. TruSecure Enterprise also contains additional elements that allow client organizations to develop and maintain an effective security posture.

Chart 3: Delivery comparisons

Delivery	BS ISO/IEC 17799	BS 7799:2	TruSecure Enterprise 2001
Risk Assessment	Outside of the code of practice; determined by client/auditor	Outside of the certification criteria; determined by client/auditor	Standard
Evaluation Criteria	Best Practice Guidance	Best Practices	Essential Practices Risk-Weighted Metrics
Electronic Assessment	Not mandated by code of practice	Not mandated by certification criteria	Standard
Class C Scans	Auditor-dependent	Auditor-dependent	Standard
Firewall Configuration	Auditor-dependent	Auditor-dependent	Standard
Network Topology	Auditor-dependent	Auditor-dependent	Standard
Device Configuration	Auditor-dependent	Auditor-dependent	Standard (for critical devices)
Desktop Assessment	Auditor-dependent	Auditor-dependent	Standard (for current anti-virus software, active modems, screen saver/password)
War Dial	Auditor-dependent	Auditor-dependent	Standard
Technical Reporting	Auditor-dependent	Auditor-dependent	Standard Report measures client against Essential Practices Includes recommendations for corrective action
Management Reporting	Typically opinion-based	Typically opinion-based	Standard Report documents review of Essential Practices Report documents baseline security posture and corrective actions taken by client
Certification	None	Report	Seal Program
Periodic Review	Unknown	Unknown	Standard Quarterly electronic assessments Annual physical inspection
Customer Support Services	Auditor-dependent	Auditor-dependent	Unlimited telephone support
Alert Services	Auditor-dependent	Auditor-dependent	Standard TruSecure Monitor for routine alerts Emergency Alert push via pager, email, voice, and fax
Insurance Guarantee	None	None	Standard

Summary

As information security incidents and risk factors continue to escalate, many organizations seek to protect their corporate computing environments and electronic business relationships through compliance with generally accepted information security standards. Although there is no shortage of such voluntary standards in the marketplace, particularly in the United States, the BS 7799 security standard has gained significant attention in recent months. Since its debut several years ago, it has been increasingly well received by business and industry in the UK and commonwealth countries. Recent acceptance as an ISO standard has further extended its reception worldwide, leading to informal adoption by government and the financial services industry in Asia, as well as a movement toward informal adoption by the energy industry internationally.

As the standard continues to gain prominence, organizations are seeking expert guidance in order to understand correct usage, determine the criteria most appropriate to the proprietary environment, ensure proper application of those criteria, and measure the level of compliance with the standard. TruSecure Corporation has studied in detail the requirements of the BS 7799 security standard, in order to provide support and expertise to its client organizations that wish to apply the standard to their environments.

Introduction

The standard was developed in Great Britain; it was first published in 1995 as a national code of practice for information security, and rapidly gained recognition in Europe. It was followed by a specification for information security management systems, BS 7799 Part II, which was published as a certification standard in 1998. The standard was equally well received in the UK and Europe, and had gained acceptance in commonwealth nations such as Canada, Australia, New Zealand, and areas in the Asia-Pacific region where Britain has had great influence, such as Hong Kong. Although it had not yet become an international standard, many businesses in these regions began using it for due diligence purposes to support cross-border international commerce and trading. Both the code of practice and the standard are written as open frameworks, and can therefore be scaled to accommodate a wide variety of businesses and organizations.

Both parts of the BS 7799 are up for review every two years by DISC Committee BDD/2, Information Security Management, of the British Standards Institute. During the review period, this technical committee, which is made up of representatives from the computer industry, the financial services industry, the energy industry, government, and leading consulting firms, determines whether or not the code of practice and the certification standard should be updated. Both the code and the standard were reviewed and revised in 1999, to accommodate the changes in information technology, particularly the impact on networks and communication. An updated version of BS 7799 Parts I and II was published in 1999, at which time the original was withdrawn.

The International Electrotechnical Commission (IEC) of the International Standards Organization (ISO) had shown interest in the British Standard for some time, and in October 2000, adopted the code of practice (Part I) as an international standar — ISO/IEC 17799.

The Code of Practice

BS 7799 Part I, the Code of Practice for Information Security Management (hereafter referred to as "the code of practice"), is the larger and more detailed portion of the two-part British Standard. Unlike technical security standards, which typically govern configuration and deployment of hardware and software controls, the code of practice is a management standard that addresses many non-technical issues, such as physical security, personnel, and general management. It governs the secure operation of IT systems currently functioning within a given organization.

The code of practice was designed to provide a single, consolidated, national resource containing a broad spectrum of information security management concepts, and therefore constitutes a common source of best practice information that organizations use to develop information security policies and procedures. As such, it is a frame of reference for organizations of all types, and can therefore support security management within an individual organization, or between organizations that do business or share information electronically.

Within the document's introduction section, it identifies itself as "a starting point for developing organization-specific guidance[1]." The code of practice is divided into ten working sections, which address the following categories of control:

- Security Policy
- Asset Classification and Control
- Physical and Environmental Security
- Access Control
- Business Continuity Management
- Security Organization
- Personnel Security
- Communications and Operations Management
- Systems Development and Maintenance
- Compliance

Because the best practices are written at the high, conceptual level, they cannot be used by an organization as an implementation specification. Analysis and interpretation, supported by a certain level of expertise, are required prior to the application of the best practices to the user organization. The code of practice is intended to be used after the organization has completed a risk assessment, and determined areas of vulnerability. At that point, the organization should select appropriate criteria from within the code of practice, and use them to develop policies and procedures specific to its needs. Not all of the criteria within the code of practice are appropriate to every organization, and it is not intended to be used as a comprehensive program. By its own admission, additional controls and guidance may be required by user organizations[2].The best practices and their subordinate criteria may be appropriate to varying degrees, at varying times, under varying circumstances, to an organization based upon current business and information sharing practices.

The ISO Standard

The code of practice was adopted, in its entirety[3], by ISO as a standard in October 2000; the formal name for the combined standard is now the BS ISO/IEC 17799:2000 Information Technology — Code of Practice for Information Security Management. Support for adoption of the standard was by no means universal and it was opposed by several countries for technical and procedural reasons[4], including a lack of consensus on the merit of certain practices. Adoption was approved, however, by a narrow margin, which led to an almost immediate move by opposing committee members for revision; review of the code of practice is currently in progress.

[1] BS 7799-1:1999. Introduction, subhead 8.

[2] BS 7799-1:1999. Foreword.

[3] There are several minor differences between the BS 7799 Part I and the ISO/IEC 17799 standard. These amendments are primarily editorial in nature, and, aside from changes to the title and introduction sections of the standard, they affect only 22 individual criteria.

[4] Source: NIST ISO-IEC 17799:2000 Frequently Asked Questions. Canada, in particular, opposed adoption of the standard, and submitted a defect report shortly after its adoption. Other committee members objected to its adoption because they felt that the timeframe was insufficient to study the standard. Procedural objections were raised after a ballot submission controversy.

To date, there is no specification, and therefore no certification for the ISO standard. The code of practice does not contain the level of detail necessary to support a specification standard at this time, and BSI did not submit its specification standard to ISO for approval. Adoption of a certification standard will no doubt be discussed at the committee's technical review meeting in 2002, but at present it is not a work item for the committee, and there are no official plans for the publication of a 17799:2 specification[5].

The Specification

BS 7799 Part II, Specification for Information Security Management Systems (hereafter referred to as "the specification") is the actual certification standard. It follows the ten topics addressed by the code of practice[6], but these criteria are written as control objectives, which synthesize the best practice concepts into more precise requirements. As a result, the specification criteria are less detailed, but more absolute than those in the code of practice. These criteria are designed to be applied directly to an organization, in order to measure compliance with the standard. Organizations should be able to demonstrate specifically that these requirements have been met.

The specification may be used by an organization in two ways; some organizations seek formal certification from an auditor accredited by the British Standards Institute, while others self-certify, performing voluntary compliance audits against the standard either in-house, or through an independent outside auditor. Organizations seeking formal certification work with accredited auditors to prepare a Statement of Applicability. Just as in the code of practice, the specification standard contains a variety of criteria, not all of which will be applicable to every organization. There is no requirement within the specification that the organization meet each of the 165 criteria in order to become BS 7799 certified. The organization must determine which of the specification criteria are most appropriate to its environment. The Statement of Applicability defines the scope of the audit based upon the criteria selected and the control objectives defined within those criteria. There is no seal associated with BS 7799 certification; the organization receives a report from the auditor that states whether or not it has met the requirements of the specification standard.

Very few companies have pursued formal certification. As of September 30, 2001, less than 50 organizations worldwide were BS 7799:2 certified, and of those, only two are U.S. companies[7]. Several factors contribute to this low adoption rate, particularly in the United States, where there are cost issues associated with certification. Certification is obtained only through companies accredited by the British Standards Institute that perform formal specification audits. As there are only a handful of companies outside the UK that are licensed to perform such audits, it has become cost prohibitive.

Without a government mandate or a regulatory requirement for certification, there is little driving wide scale adoption. There is no real incentive for organizations to obtain formal certification when voluntary measurement against the specification remains a viable option for purposes of due diligence or security documentation. Without tangible incentives or legal requirements, it is difficult for most organizations to justify the effort and expense of formal certification.

[5] Ibid.

[6] Numeration of individual criteria differs between the code of practice and the specification standards. The specification is smaller, and does not map directly to the code of practice in detail.

[7] Source: British Standards Institute

Strengths of 7799

Perhaps more important than academic acceptance within the security industry and industry standards bodies is "real world" adoption of the standard by business and industry. The code of practice has become globally recognized as a resource for organizations developing security policies and procedures. The British Standard gained worldwide attention for quality security practices, and despite objections by some committee members, the code of practice was adopted as a management standard by the ISO. Both the code of practice and the specification have been in use throughout the UK and commonwealth countries since 1998, and they have become more widely recognized in Europe and Asia.

The specification standard has drawn the attention of industries such as banking and energy in Europe, Asia, and the U.S., and has the potential to lead to its adoption as a regulatory standard within those industries if it is adopted by ISO. The specification standard is already a model for information security for financial services in the Asia Pacific region, and the governments of Singapore, Taiwan, and Hong Kong require the use of the specification standard by organizations seeking to do business with them electronically.

Another elemental strength for both the code of practice and the specification standard is their scalability and technological neutrality. The code of practice is written at the conceptual level, and the specification standard is written objectively, so that both can accommodate a wide variety of organizations, technologies, and standard business practices. The code of practice and specification criteria do not vary according to hardware, software, systems, or services in operation. They can be applied to any organization's proprietary environment and work equally well on homogeneous or mixed-technology environment.

Finally, the scope of both the code of practice and the specification standard are written to include technical, physical, and administrative security measures that should be in place within the organization. This is a surprisingly new concept in information security standards, most of which focus almost entirely on technical security measures. The British Standard, and its ISO counterpart, recognize that effective security is more than a technical issue; in order for information security to be effective with the organization, there must be physical security controls in place, and policies, procedures, and practices that support the functions of both technical and physical security controls.

Implementation Issues

Despite the quality of the standards, many organizations experience problems using them appropriately. Oftentimes it is a question of proper interpretation, use, and implementation, rather than any definable weakness within the standards themselves. Although relatively few, the implementation issues experienced by most organizations using either the code of practice or the specification are significant.

The Code of Practice

The primary implementation issue experienced by most organizations is the drive towards applying best practices without appropriate assessment of the corporate computing and physical environments. Without a quantified assessment of risk to the enterprise, there can be no sound prioritization of security requirements and resources. In itself, the code of practice provides the organization little guidance in determining those requirements most necessary to protect the enterprise. Expert guidance, whether in-house or outsourced, is required in order to perform the appropriate risk assessment for any organization wishing to apply these practices[8].

[8] The necessity for expertise in application of the standard is specifically noted in the foreword of the BS ISO/IEC 17799:2000. It is not, of course, noted as a weakness.

These practices are written at the conceptual level, in order to accommodate a wide variety of organizations, technologies, and standard business practices, and are therefore too objective in nature to be applied without appropriate interpretation. After the initial risk assessment has been performed, expert guidance may be required in order to determine the appropriate level of risk to the organization, bearing in mind its business objectives. Then appropriate criteria must be selected from within the code of practice, as a base upon which to develop effective and reasonably enforceable policies and procedures, which will determine the organization's security posture. Significant security expertise is required to appropriately apply these practices to an individual organization.

Finally, the code of practice is reviewed by the standards body every few years, to determine whether or not updates are required. The original code of practice was issued by BSI in 1995, and revisions were not issued until 1999. Such a large gap in the review period cannot adequately address the rapid changes in information technology. ISO standards are typically reviewed for revision on a five-year cycle[9], which represents an enormous amount of time and dozens of "web cycles." There is great potential for obsolescence affecting significant portions of the standard between review periods, and organizations may find themselves vulnerable while waiting for revisions. Application of the code of practice must be supported by current industry intelligence in order to adequately protect the organization against current security risks.

The Specification

Similar to the code of practice, most of the implementation issues associated with the specification are not inherent in the standard itself, but lie in application of the standard to the organization. This is true whether the organization chooses to self-certify for compliance, or to seek formal certification from an accredited auditor.

The primary implementation issue in either case is one of subjectivity. Just as in the code of practice, the criteria in the specification are based upon control objectives, not the specific risks to an individual organization. Once again, it is up to the organization to determine which of these are appropriate to its target environment to be audited. The specification standard has no uniform requirement for application; the scope of the certification audit is determined by the client organization and the certification auditor. The organization must prepare a Statement of Applicability, selecting those certification criteria believed to be most appropriate to the target environment. The certification auditor then examines the client organization based solely on the self-selected criteria.

Because the target and scope of the audit are determined by the client, vulnerabilities may exist at points in the network, Internet perimeter, physical facility/data center, or in policies and procedures not identified by the client or examined by the auditor. An auditor will typically stay within the specified scope of the audit, and may not always suggest to the client that other controls might be more appropriate to the environment, or that additional controls are required. The client, therefore, can obtain BS 7799 certification based on a narrowly scoped application of the standard, while significant vulnerabilities remain within the target or across the enterprise.

The lack of uniform requirements for application of the specification places a burden on the auditor to determine the appropriate scope of the audit. The overall quality of the audit therefore may be determined by the experience and skillsets within the audit team. The specification is written broadly, in order to provide scalability to a variety of industries and businesses, but must be applied subjectively to the individual organization in order to provide effective information security protections. This requires information security expertise that is not always readily available in-house. Many third-party auditors are quite capable in terms of delivery, but without uniform requirements, even well-scoped and

[9] The five-year review period is mandatory for ISO standards; the national committees, however, may request a review of standards at any time after one year of publication or revision. ISO 17799 is currently under review at the request of Canada.

well-performed audits may vary significantly. Such variations erode the overall effectiveness of even the finest information security standards. If the audit team has great expertise, the client will no doubt get a complete and thorough audit; where the skillsets are lacking, however, the client runs the risk of getting a poor quality audit.

This leads to another implementation issue for many organizations, which is the lack of standardized validation methods. One auditor may rely heavily on electronic testing, while another relies primarily on client attestation. Those countries in which the standard is prevalent, such as the UK, Australia, and New Zealand, sponsor national accreditation schemes for organizations that are licensed to perform formal certification audits. But even those national standards may vary between the countries, and such schemes would not affect those organizations that choose to self-certify (either in-house or through outsourcing) for compliance. Such unevenness in the scope and delivery of the specification audit may ultimately serve to weaken the reliability of the BS 7799:2 certification.

Other common implementation issues experienced by organizations using the specification standard include:

Obsolescence

The specification audit is usually delivered on a static basis, resulting in a report that provides the client with a "snapshot" of its security posture at a given point in time. Typically, auditors will clearly document the timeframe in which the audit takes place, and routinely include disclaimers in audit reporting such as the following:

> The description of the controls at XYZ Company is as of October 31, 1999, and information about tests of the operating effectiveness covers the period from May 1, 1999 to October 31, 1999. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific controls at XYZ is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that
>
> 1. Changes made to the system or controls
> 2. Changes in processing requirements, or
> 3. Changes required because of the passage of time
>
> May alter the validity of such conclusions.[10]

Static or point-in-time audits, even those using the finest security standards, are not sufficient to keep pace with the rapid pace of technological development, or the dynamic nature of the common corporate computing environment. Even making simple, routine changes to a network, such as upgrading the operating system or replacing old/failing hardware, can introduce new vulnerabilities into the environment. As soon as the client makes such a change to the target, the audit report becomes obsolete.

Length of Certification Cycle

The BS 7799 certification process is somewhat notorious for being complicated and lengthy. Depending upon the scope of the audit, the certification process can take one year or more to complete. Once the client has completed the certification process, there are no provisions for the standard maintenance of the BS 7799:2 certification; organizations may choose to be reviewed annually, or every two or three years; in many cases, the certification remains valid until there is a

[10] The source of this quote was the introduction section of an audit report prepared for a TruSecure client by a "Big Five Firm." Name and dates were altered for purposes of confidentiality.

revision to the standard. While this may allow the organization to maintain its BS 7799 certification for an extended period of time, it does not provide a dynamic and continuous process for risk mitigation. In cases where substantial changes are made to the corporate computing environment after the audit has been completed, such as the addition of new applications, or upgrading key hardware, this may actually increase risk to the organization.

The TruSecure Approach

Clearly, the problems that most organizations experience when working with standards-based security reviews lie not in the standard itself, but in the way that it is applied to and reviewed by the organization.

Oftentimes, the use of an objective, high-level standard can lead to the development of a "fundamentalist" mentality, an approach to information security management that seeks to "finish" security with better technology, stronger controls, a more secure architecture. Meeting all of the requirements of a standard — completing a checklist — is the primary goal of such fundamentalism, with the overall objective of attaining perfect, complete information security within the organization. Unfortunately, this is no more possible in the eWorld than it is in the physical world. Just as there is no house, car, or store that cannot be physically robbed, neither is there a network that can be "fundamentally" secured from risk. Too many potential threats and non-quantifiable vulnerabilities exist to effectively address each one. Chasing such an impossible goal can lead an organization to invest too much time and resources in the wrong places, yielding a poor ROI without establishing a truly effective security posture.

The more common approach to information security is the audit, which seeks validation through regular annual inspection. As previously stated, whether an organization is using the code of practice or the actual specification as the basis of an audit, the burden rests with that organization and its auditor to determine the appropriate scope and select applicable criteria by which to examine the security controls in place. The auditor then typically reports back to the organization whether or not the controls in place are consistent with the standard. While this type of approach is perfect for measuring compliance with any given objective standard, it is unable to provide effective ongoing security for the organization, primarily because an audit focuses on a point in time, while in the real world, technology is changing rapidly and continuously. An audit performed in previous months provides no defense against current and emerging threats such as a new virus or hacking tool, and becomes immediately obsolete when the organization's computing environment changes. The point-in-time audit-based approach cannot possibly keep pace with the real world needs of the organization and provide effective security for the long term.

Secondly, most organizations use third party audits to evaluate information security because they lack adequate internal resources to determine and maintain a good baseline. Outsourcing managed security services can address this issue for an organization; an annual audit cannot. An audit against the 7799 standards will only evaluate the assignment and performance of current controls against objective metrics, but selecting and applying the appropriate metrics from either the code of practice or the specification is key to the quality of the audit. In cases when in-house security expertise is insufficient, the quality of the audit may be adversely affected, because it is the client that determines its scope. While many good auditors can appropriately tailor scope to the organization, weak in-house security resources may allow other factors, such as cost and impact on production, to unduly influence the scope of the audit. Finally, most audits are based on attestation from employees; neither the code of practice nor the specification contain specific requirements for testing techniques, nor proscribed methods for electronic assessments of systems, services, or devices, or demonstration of standard and/or emergency mode operating procedures.

Effective security management involves far more than simply implementing and evaluating performance against an objective standard. Even the finest of security standards must be implemented in a subjective manner, tailored to the specific environment of each organization, taking into account the idiosyncrasies associated with business model, business plans and objectives, technologies in use — including platforms, systems, and services — and, perhaps most importantly, personnel. The ultimate challenge in using a security standard is ensuring its effectiveness in the real world, using it as a basis upon which to develop policies and practices that reduce risk, and addressing a constantly changing technological environment. Unfortunately, traditional approaches to information security, such as annual audits based on objective standards, offer little assistance with these challenges.

A Risk-Based Security Methodology

The concept of risk assessment is mentioned briefly in the code of practice[11], but no detail as to how to perform such an assessment is included within the best practice documentation itself. In fact, it is suggested by the authors that risk assessment take place prior to the use of the code of practice by the organization, and very little guidance is given in terms of its practical application.

Rather than basing its managed security services on an objective standard, TruSecure Corporation's security program, TruSecure Enterprise 2001, is founded on a simple, practical, risk-based methodology. This approach is embodied in the equation:

*Risk = Threat * Vulnerability * Event Cost*

which provides the foundation for focusing resources on real risk reduction and mitigation.

Threat is defined as the rate at which a damaging event happens, i.e., the rate of viruses launched through the Internet.

Vulnerability is defined as the potential for a given target to be negatively effected by a given threat, i.e., the vulnerability of a web server to a hacker attack.

Event cost is defined by the total cost of the damages created by a successfully executed threat, i.e., the cost of downtime, lost data, damaged reputation and lost revenue from a successful hacking attack.

The total risk to the organization is the product of these three factors[12], which allow TruSecure Corporation to understand, quantify, and prioritize the many risks that its clients face in the real world. For example, because any number multiplied by zero equals zero, a risk that involves a threat, vulnerability or cost that is zero, or close to it, represents a fairly minimal risk. Using this approach, an organization can effectively focus time and resources on addressing the vulnerabilities that are associated with significant threats and costs. Therefore, the fundamentalist corporate missions to "fix everything", or comply with standards for the sake of compliance, can be abandoned in favor of a more pragmatic and effective focus on the issues that represent sources of immediate concern. Such a practical approach to risk often leads to addressing the many small and overlooked items that should be standard part of corporate cyber-hygiene, such as system maintenance and routine anti-virus updates, which provide far greater risk reduction than investment in stronger, more restrictive controls and technologies.

[11] BS 7799-1:1999 Introduction

[12] The purpose of this formula is not to attempt a gross simplification of a tremendously complex issue. Rather, it provides a better way for the organization to understand the components of risk and how they relate to each other.

The Keys to Effective Information Security

Using a simple formula like the risk equation allows TruSecure client organizations to quantify the most prevalent risks associated with business activities, corporate data, personnel, facilities, systems, services, and devices, and clearly identify those resources it considers critical. This is the basis upon which TruSecure Corporation has developed its security program, one that determines how best to mitigate those risks most prevalent to the client's critical resources. TruSecure Enterprise 2001 applies information security measures across the enterprise, taking into account the interdependencies between facilities, personnel, and technology. TruSecure Enterprise 2001 provides a seamless program for identifying and managing information security risks on a continuous basis. Underlying TruSecure Corporation's approach to information security is the belief that in order to be truly effective, an enterprise security solution must be pragmatic, holistic and dynamic.

Pragmatic Security. An effective information security program must focus on reducing the most important sources of risk, but at the same time, must not require compliance with extraordinarily rigid security practices. Overly stringent security controls can lead to significant loss of productivity among workers who struggle with time-consuming and awkward processes. Even worse, overly restrictive controls can undermine the efficacy of the entire program; for example, a policy that requires users to use 16+ character alpha-numero-symbolic passwords ultimately leads them to write those passwords on Post-It™ notes and paste them on their monitors.

The best way to reduce risk without excessive cost or loss of productivity is to layer together a series of synergistic controls. By combining several non-intrusive security measures that work together synergistically, an organization can achieve dramatic risk reduction without the undesirable consequences of more costly and infringing controls. A less demanding password requirement, supported by a well-communicated and enforced password management policy, based upon end-user access to critical resources defined by job function and assigned by the principle of least privilege, can together provide far greater total security than a single more powerful (and more costly and infringing) control. A single control, no matter how strong, is also a single point-of-failure.

As a second example, many organizations store data on their web servers. This is a high-risk practice, because it is far more profitable for hackers to look for large amounts of stored data than to try to capture single transactions as they speed across the Internet. A pragmatic approach to security in this example would involve:

- Identifying customer data as sensitive
- Keeping customer data available on the public facing web server only as long as needed (presumably the length of a single transaction)
- Routinely patching the operating system on the web server
- Passing customer data from the web server to a database server
- Locating the database server on an isolated network segment
- Limiting physical and logical (electronic) access to the database server
- Disallowing dynamic queries to the database
- Establishing and enforcing sensitive data handling policies within the organization designed to protect data from accidental or deliberate compromise

All of these elements, working together, significantly reduce the risk of a successful exploit of customer information.

Holistic Security. Experts recognize that information security is no longer confined to "the IT department." An effective information security program is one that can address technical, physical, and administrative security practices within the entire organization. Many organizations are vulnerable to attack or exploit due to insufficient security policies or those that are not properly enforced. Often, it is a low cost cyber-hygiene routine that can save an organization from a security breach. Melissa and the Love Bug successfully got past thousands of firewalls and outdated versions of anti-virus software, only to be opened at the desktop level by unsuspecting end-users. Such a breach can be easily avoided, at very low cost to the organization, by filtering email at the gateway, routine anti-virus updates at the network and desktop levels, routine staff security awareness training, and the correct communication and enforcement of corporate policy on personal email and opening email attachments. Policies and standard operating procedures are the backbone of the corporate cyber-hygiene routine. A holistic security program will address the interplay between personnel, devices, and technology. Hardware and software are only as good as the personnel that manage them; a firewall does nothing to protect the corporate network if improperly configured or easily breached. Intrusion detection systems are a good way to monitor for unauthorized access attacks, but do nothing to mitigate against an unhappy employee, with authorized access to critical systems, who decides to steal or destroy corporate data. In some cases, it is the non-technological solutions, such as enhanced security training for IT staff, and background checks on employees that have access to critical resources, that can prevent a breach or incident.

The holistic approach also recognizes that a sound security program extends beyond the organization's proprietary environment, and into its electronic relationships with business partners, vendors, and customers. In an inter-connected eWorld, effective information security depends upon all parties taking equal responsibility for security controls, and holding each other accountable.

A holistic approach to security must address these risks through a combination of assessment techniques, including electronic assessments, policy and procedure review (for establishment and enforcement at the end-user level), review of standard operating procedures and practices (for IT at the operational level), and routine vulnerability assessments. When such assessments are performed against an objective standard, these assessments must be scaleable to the organization, become a standard part of the organization's security program, and must be repeated on a regular basis, in order for the organization to maintain an effective security posture.

Dynamic Security. Information technology changes rapidly; as technology changes, so do the associated threats — new exploits, new attacks, new areas of weakness. As threats continue to change and grow, so does risk, and so, therefore, must the organization's information security program, if it is to remain effective. Good security must be a dynamic process that addresses the constantly changing environment. This requires a steady flow of information and analysis around emerging security issues, so that an organization can protect itself against new threats as they emerge. Just as hardware and software must be upgraded periodically and configurations maintained, policies and operating procedures must also be tested and updated regularly in order to remain relevant.

TruSecure Methodology

TruSecure Enterprise 2001 is TruSecure Corporation's security assurance program that is derived from these security principles. TruSecure Enterprise 2001 has roots that extend into established information security disciplines such as audit, penetration studies, and formal development methodologies; however, it both diverges from and augments these traditional methods in ways that yield effective security results at substantially less cost and effort. The program is built upon a four-phase risk reduction process.

Four Phases of Security Management

TruSecure Enterprise 2001 is unique in its ability to provide continuous and comprehensive security. Using a four-phased approach, it incorporates the risk-reduction program into a seamless and continuous process:

Identify — Discovering critical systems and assets

The process begins with TruSecure's unique method for identifying the critical assets of the organization: data, devices, networks, users, and physical locations. The process often identifies critical devices unknown to the IT staff.

Assess — Focusing appropriate resources on real risk

The next phase introduces the comprehensive risk assessment process, based on TruSecure's intelligence of the issues posing the most prevalent risks to client organizations. The risk assessment includes the Internet perimeter and the organization's internal network environment, addressing the six categories of risk: malicious code, hacking, privacy, human factors, physical security, and downtime.

Protect — Reducing risk with synergistic, layered controls

The program next implements risk reduction measures to protect critical systems and information. TruSecure's methodology employs layered security controls that cost-effectively reduce risk without excessive impact on resources. TruSecure's Security Analysts guide and support the organization's IT staff through this process, providing valuable knowledge transfer.

At this point, the implementation phase of TruSecure Enterprise 2001 is complete, and the client is ready for TruSecure certification, which means that the client has satisfactorily completed the process and met TruSecure's Essential Practices requirements. The TruSecure Security Analyst will present an overview of the work completed to the client's senior management, and formally award certification. Upon achieving certification, the maintenance phase of the TruSecure Enterprise 2001 program begins.

Assure — Maintaining systems at minimum risk levels; repeating the process as needed to guard against new risks

In order to remain effective, the security posture must be maintained over time. TruSecure's Risk Recon Team monitors and maintains current intelligence on the Internet and the Computer and Information Security industries for emerging threats, in order to remain current. Client's have access to the TruSecure Risk Monitor, which is an ongoing alert service that summarizes the findings of the Risk Recon Team, and will be notified by Emergency Alert Service in the event of a large-scale attack or widespread virus activity. TruSecure clients have unlimited access to Customer Support Services, and the Security Analysts conduct quarterly risk assessments for the client to ensure that no new vulnerabilities are created as the business and network environments change.

Successful compliance with the Essential Practices and maintenance of TruSecure certification status assures clients of the success of their security program.

Six Categories of Risk

TruSecure Corporation's risk model evaluates current and emerging threats across six categories of risk. TruSecure's Essential Practices are periodically reviewed and updated to remain current, and this classification system allows the characteristics of a threat to be readily communicated in a consistent fashion. TruSecure's six categories of risk are:

- ♦ Electronic Threat and Vulnerabilities — Issues that include sniffing, spoofing, hacking, and especially Distributed Denial of Service exploits
- ♦ Malicious Code — Issues pertaining to hostile agent's affects on systems
- ♦ Privacy — Issues that affect loss of confidentiality
- ♦ Human Factors — Issues relating to the actions of people, policies, and procedures
- ♦ Physical — Issues relating to security of environments
- ♦ Downtime — Issues that affect the availability of systems for use

Layered Security Model

TruSecure's LSM addresses security issues in logical layers. Each layer in the model has associated essential practices that address the security concerns of the enterprise within a particular context. The layers are:

Physical Environment — addresses physical characteristics that surround the facility and equipment. Examples of such variables that must be addressed from a security standpoint include: power source, water, doors, alarms, ventilation, etc.

Connectivity — addresses a collection of interfaces that enable computers and other devices at the physical site to provide Internet-based users with desired services, as well as the ability to contact and use other corporate resources to fulfill requests from Internet-based visitors. Examples of such devices are routers, firewalls, hubs, security domains, wiring /cabling, the interNIC, modems, DNS, etc.

Platform — addresses the computing devices that are generally the end-points of connectivity. Examples of these platforms are the physical computers and operating systems that are deployed as Internet servers, database servers, firewalls, routers, desktop computers, etc.

Services — addresses the utility and application programs and services that are vendor provided, user developed and/or purchased from third parties. Examples of these services are HTTP and FTP servers, CGI subsystems, databases, etc.

Policy/Human Factors — addresses those elements that affect the performance and awareness of human resources on the organization's security posture. Examples include corporate policies, standard operating procedures, and emergency mode operating procedures.

TruSecure Essential Practices are organized by control layers to encourage systematic evaluation of inter-related security issues.

TruSecure and 7799

Although this unique methodology and delivery model may seem generally contrary to the use and application of objective security standards to the organization, TruSecure Enterprise 2001 is actually quite well aligned with both the code of practice and the specification standard. In fact, for those organizations interested in using the code of practice (BS ISO/IEC17799) to develop an information security program, TruSecure's value lies in its ability to "interpret" the best practices, transforming policy and procedure concepts into practical steps and action items that the organization can implement as reasonable, effective security measures.

The Code of Practice

The following charts represent a random sampling of criteria selected from BS ISO/IEC 17799:2000* Code of Practice for Information Security Management, and demonstrates the corresponding TruSecure delivery that meets those requirements. This is similar to the type of criteria selection that might appear in a Request for Proposal from a prospective client organization.

4.2.1 Identification of Risks from Third Party Access

BS ISO/IEC 17799 Best Practices	TruSecure Essential Practices
4.2.1.1 Types of Access The type of access given to a third party is of special importance. For example, the risks of access across a network connection are different from risks resulting from physical access. Types of access that should be considered are: a) physical access, e.g., to offices, computer rooms, filing cabinets; b) logical access, e.g., to an organization's databases, information systems.	TruSecure mandates controlled secure access to the facility, data center, critical devices, systems, and data. TruSecure Essential Practices cover access at both the physical and logical (electronic) levels, including access controls, user rights and permissions, and authentication. In addition to the review of policies and procedures against TruSecure Essential Practices, the Security Analysts will perform electronic testing on the hardware, software, and controls associated with access authorization to critical systems and data. The analyst will also inspect the physical security of the facility and the data center. The analyst will interview appropriate staff on user rights and permissions, and may require demonstration of or attestation to certain procedures.
4.2.1.2 Reasons for Access Third parties may be granted access for a number of reasons. For example, there are third parties that provide services to an organization and are not located on-site but may be given physical and logical access, such as a) hardware and software support staff, who need access to system level or low level application functionality; b) trading partners or joint ventures, who may exchange information, access information systems or share databases.	TruSecure examines the controls that the client exercises over electronic access to systems and data, including the management of user rights and permissions. Essential practice review includes access control, user rights and permission review, and account management procedures review. In addition to the review of policies and procedures against TruSecure Essential Practices, the Security Analysts will perform electronic testing on the hardware, software, and controls associated with access authorization to critical systems and data. The analyst will also inspect the physical security of the facility and the data center.

**Extracts from BS ISO/IEC 17799: 2000 / BS 7799 Part 2: 1999 are reproduced with the permission of the British Standards Institution (BSI) under license number SK2001/0322. Copyright subsists in all BSI publications. Reproduction in any documentation other than as part of this report is not permitted without the permission of BSI. (Contact the BSI Copyright Manager on Tel +44 (0) 20 8996 7070).*

Complete copies of these standards are available for purchase in electronic format from http://www.bspsl.com/17799/ British Standards may also be obtained in hard copy from BSI Customer Services, 389 Chiswick High Road, London, W4 4AL. (Tel +44 (0) 20 8996 9001).

Information might be put at risk by access from third parties with inadequate security management. Where there is a business need to connect to a third party location a risk assessment should be carried out to identify any requirements for specific controls. It should take into account the type of access required, the value of the information, the controls employed by the third party and the implications of this access to the security of the organization’s information.

The analyst will interview appropriate staff on user rights and permissions, and may require demonstration of or attestation to certain procedures.

BS ISO/IEC 17799 Best Practices

6.3.1 Reporting Security Incidents

Security incidents should be reported through appropriate management channels as quickly as possible. A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. All employees and contractors should be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible. Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training (see 6.2) as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

TruSecure Essential Practices

TruSecure mandates reporting for standard operating procedures, security incidents, and exception reporting on all logged functions. Essential practice review includes documentation, responsibility, tracking, training, and active monitoring.

In addition to the review of policies and procedures related to incident response reporting and escalation, and exception reporting of fault logs, the Security Analyst will interview appropriate staff on network management and standard operating procedures. The analyst will review samples of log reports, and may ask for demonstration of or attestation to incident response escalation procedures.

BS ISO/IEC 17799 Best Practices

8.1.3 Incident Management Procedures

Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents (see also 6.3.1). The following controls should be considered

a) Procedures should be established to cover all potential types of security incident, including:

1) information system failures and loss of service;
2) denial of service;
3) errors resulting from incomplete or inaccurate business data;
4) breaches of confidentiality.

b) In addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures should also cover (see also 6.3.4):

1) analysis and identification of the cause of the incident;
2) planning and implementation of remedies to prevent recurrence, if necessary;
3) collection of audit trails and similar evidence;

TruSecure Essential Practices

The Security Analyst will review the specific elements of the incident response policies and escalation procedures, including:

a) Documented policies and procedures
b) Alert procedures
c) Escalation procedures
d) Identification of key personnel
e) Communication procedures
f) Recovery procedures
g) Routine review and update of policies and procedures
h) Routine testing of policies and procedures

The analyst will note deficiencies and suggest additions, corrections, or changes.

4) communication with those affected by or involved with recovery from the incident;
5) reporting the action to the appropriate authority.

c) Audit trails and similar evidence should be collected (see 12.1.7) and secured, as appropriate, for:
1) internal problem analysis;
2) use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
3) negotiating for compensation from software and service suppliers.

d) Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures should ensure that:
1) only clearly identified and authorized staff are allowed access to live systems and data (see also 4.2.2 for third party access);
2) all emergency actions taken are documented in detail;
3) emergency action is reported to management and reviewed in an orderly manner;
4) the integrity of business systems and controls is confirmed with minimal delay.

BS ISO/IEC 17799 Best Practices	TruSecure Essential Practices
8.3 Protection against malicious software *Objective: To protect the integrity of software and information.* Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses (see also 10.5.4) and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software, and managers should, where appropriate, introduce special controls to detect or prevent its introduction. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers.	Malicious code represents a huge and prevalent threat to computer security, and as such, represents a primary control layer of TruSecure.
8.3.1 Controls against malicious software Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Protection against malicious software should be based on security awareness, appropriate system access and change management controls.	TruSecure examines the client's preparedness for dealing with malicious code across several control layers. TruSecure's Essential Practices are in agreement with the practices stated in BS ISO/IEC 17799 8.3.1. The Security Analyst will examine the policies and procedures for network and desktop anti-virus software usage, as well as end-user computing policies related to acceptable use or corporate computing resources (i.e., receiving email

The following controls should be considered:

a) a formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software (see 12.1.2.2);
b) a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken (see also 10.5, especially 10.5.4 and 10.5.5);
c) installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis;
d) conducting regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated;
e) checking any files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, for viruses before use;
f) checking any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization;
g) management procedures and responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks (see 6.3and 8.1.3);
h) appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements (see clause 11);
i) procedures to verify all information relating to malicious software, and ensure that warning bulletins are accurate and informative. Managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or anti-virus software suppliers, are used to differentiate between hoaxes and real viruses. Staff should be made aware of the problem of hoaxes and what to do on receipt of them. These controls are especially important for network file servers supporting large numbers of workstations.

from unknown sources and proper handling of email attachments).

In addition, the analyst will perform electronic assessment of desktops connected to the network to determine the use of anti-virus software and compliance with corporate anti-virus procedures.

BS ISO/IEC 17799 Best Practices

9. Access control

9.1 Business requirement for access control

Objective: To control access to information.

Access to information, and business processes should be controlled on the basis of business and security requirements.

TruSecure Essential Practices

Controlling access to critical systems and information resources is another key element of the TruSecure program. TruSecure Enterprise 2001 examines access to information across a variety of control layers, and includes both physical and logical access.

9.1.1 Access control policy

9.1.1.1 Policy and business requirements

Business requirements for access control should be defined and documented. Access control rules and rights for each user or group of users should be clearly stated in an access policy statement. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:
a) security requirements of individual business applications;
b) identification of all information related to the business applications;
c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information;
d) consistency between the access control and information classification policies of different systems and networks;
e) relevant legislation and any contractual obligations regarding protection of access to data or services (see clause 12);
f) standard user access profiles for common categories of job;
g) management of access rights in a distributed and networked environment which recognizes all types of connections available.

TruSecure Essential Practices are in agreement with the practices specified in BS ISO/IEC 17799 9.1.1.1. The Security Analyst will review the client's access controls, including user rights and permissions, authentication, authorization, and user account management.

In addition to policy review, the analyst will perform electronic assessments on the critical devices and network segments housing sensitive data, in order to test the efficacy of access controls.

9.2 User access management

Objective: To prevent unauthorized access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

Using TruSecure Essential Practices, the Security Analyst will review policies, procedures and practices related to user account management. See above.

9.2.3 User password management

Passwords are a common means of validating a user's identity to access an information system or service. The allocation of passwords should be controlled through a formal management process, the approach of which should:
a) require users to sign a statement to keep personal passwords confidential and work group passwords solely within the members of the group (this could be included in the terms and conditions of employment, see 6.1.4);

TruSecure Essential Practices are in agreement with the practices specified in BS ISO/IEC 17799 9.2.3. The Security Analyst reviews policies, procedures and practices related to user password management, including protection, strength, and change management practices.

In addition, the Security Analyst will perform electronic assessment at the network and desktop level to assess compliance with password policies.

b) ensure, where users are required to maintain their own passwords, that they are provided initially with a secure temporary password which they are forced to change immediately. Temporary passwords provided when users forget their password should only be supplied following positive identification of the user; c) require temporary passwords to be given to users in a secure manner. The use of third parties or unprotected (clear text) electronic mail messages should be avoided. Users should acknowledge receipt of passwords. Passwords should never be stored on computer system in an unprotected form (see Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature verification and use of hardware tokens, e.g. chip-cards, are available, and should be considered if appropriate.	
9.2.4 Review of user access rights To maintain effective control over access to data and information services, management should conduct a formal process at regular intervals to review users' access rights so that: a) users' access rights are reviewed at regular intervals (a period of 6 months is recommended) and after any changes (see 9.2.1); b) authorizations for special privileged access rights (see 9.2.2) should be reviewed at more frequent intervals; a period of 3 months is recommended; c) privilege allocations are checked at regular intervals to ensure that unauthorized privileges have not been obtained.	TruSecure Essential Practices are in agreement with the practices specified in BS ISO/IEC 17799 9.2.4. The Security Analyst will review policies, procedures and practices related to the management of user rights and permissions; in particular, the assignment of access to resources based upon job function, and the routine review of permissions.
9.4 Network access control *Objective: Protection of networked services* Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring: a) appropriate interfaces between the organization's network and networks owned by other organizations, or public networks; b) appropriate authentication mechanisms for users and equipment; c) control of user access to information services.	Access to the corporate network is a key concern of TruSecure. Both physical and logical network access will be examined through physical inspection, electronic assessment, and policy review.
9.4.6 Segregation in networks Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might	TruSecure Essential Practices are in agreement with the practices specified in BS ISO/IEC 17799 9.4.3. In addition to policy and procedure review, the Security Analyst will perform network mapping to verify network segmentation, appropriate isolation of critical devices, and perform electronic assessment on isolated segments to test access controls.

increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, the introduction of controls within the network, to segregate groups of information services, users and information systems, should be considered. One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. Such a perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains (see 9.4.7 and 9.4.8) and to block unauthorized access in accordance with the organization's access control policy (see 9.1). An example of this type of gateway is what is commonly referred to as a firewall. The criteria for segregation of networks into domains should be based on the access control policy and access requirements (see 9.1), and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology (see 9.4.7 and 9.4.8).	
9.7 Monitoring system access and use *Objective: To detect unauthorized activities.* Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model (see 9.1) to be verified.	TruSecure Essential Practices are in agreement with the practices identified in BS ISO/IEC 17799 9.7. The Security Analyst will examine the client's system logs for tracking and monitoring use.
9.7.2.3 Logging and reviewing events A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of security incidents are given in 9.7.1. System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered. When allocating the responsibility for log review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.	TruSecure Essential Practices are in agreement with the practices identified in BS ISO/IEC 17799 9.7.2.3. The Security Analyst will review the client's event logs, and the policies and standard operating procedures associated with handling of event logs and exception reporting. In cases when procedures or policies are deficient, the Security Analyst will make recommendations for corrective action.

Particular attention should be given to the security of the logging facility because if tampered with it can provide a false sense of security. Controls should aim to protect against unauthorized changes and operational problems including: a) the logging facility being de-activated; b) alterations to the message types that are recorded; c) log files being edited or deleted; d) log file media becoming exhausted, and either failing to record events or over-writing itself.	
9.7.3 Clock synchronization The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Co-ordinated Time (UCT) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.	TruSecure Essential Practices are in agreement with the practices specified in BS ISO/IEC 7799 9.7.3.

It is important to note, of course, that TruSecure Essential Practices do not completely mirror the BS ISO/IEC 17799 code of practice. As previously stated, the TruSecure methodology is based upon the application of Essential Practices, appropriate to all organizations, across the enterprise; the 7799 code of practice is a collection of best practices upon which an organization can build its own security policies. Not all of these practices are suitable to every organization. Some of the best practices, in fact, border on "perfect" security. While TruSecure is in complete alignment with Sections 3 - 12 of the code of practice, and most of the subordinate criteria, TruSecure's Essential Practices differ, in some respects, at from certain criteria at the granular level.

For example:

BS ISO/IEC 17799 Best Practices	TruSecure Philosophy
6.3.2 Reporting security weaknesses Users of information services should be required to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their management or directly to their service provider as quickly as possible. Users should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.	While this is certainly a good concept, it does not practically mitigate against a strong risk to the organization, but does represent a burden to employees that, by its own admission, they may not be able to adequately address. In fact, this type of requirement may increase the workload on IT or security staff that would have to correct mistakes made by end-users. Using the TruSecure risk equation, this requirement does not represent a priority threat for the majority of TruSecure client organizations, and is therefore not included in TruSecure's Essential Practices.
7.1.5 Isolated delivery and loading areas Delivery and loading areas should be controlled and, if possible, isolated from information processing facilities	TruSecure's Essential Practices mandate that clients secure loading docks through the use of physical monitoring such as a security guard or observation

to avoid unauthorized access. Security requirements for such areas should be determined by a risk assessment.

The following controls should be considered.
a) Access to a holding area from outside of the building should be restricted to identified and authorized personnel.
b) The holding area should be designed so that supplies can be unloaded without delivery staff gaining access to other parts of the building.
c) The external door(s) of a holding area should be secured when the internal door is opened.
d) Incoming material should be inspected for potential hazards [see 7.2.1d)] before it is moved from the holding area to the point of use.
e) Incoming material should be registered, if appropriate (see 5.1), on entry to the site.

cameras. This practice mitigates against a vulnerability that is almost universal to client organizations.

The code of practice requirement goes beyond baseline security recommendations, however, and some of the requirements represent significant expense with a diminishing return on the investment. A specially constructed area or a series of redundant access doors can represent effort or expense that may not be necessary if the area is appropriately monitored.

While TruSecure is in alignment with the principles of this particular criterion, validation at the granular level, is somewhat different.

8.7.7 Other forms of information exchange
Procedures and controls should be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities. Information could be compromised due to lack of awareness, policy or procedures on the use of such facilities, e.g. being overheard on a mobile phone in a public place, answering machines being overheard, unauthorised access to dial-in voice-mail systems or accidentally sending facsimiles to the wrong person using facsimile equipment.

Business operations could be disrupted and information could be compromised if communications facilities fail, are overloaded or interrupted (see 7.2 and clause 11). Information could also be compromised if these are accessed by unauthorized users (see clause 9).

A clear policy statement of the procedures staff are expected to follow in using voice, facsimile and video communications should be established.
This should include:

a) reminding staff that they should take appropriate precautions, e.g. not to reveal sensitive information so as to avoid being overheard or intercepted when making a phone call by:

1) people in their immediate vicinity particularly when using mobile phones;
2) wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers when using analogue mobile phones;
3) people at the recipient's end;

b) reminding staff that they should not have confidential conversations in public places or open offices and meeting places with thin walls;

This requirement is somewhat impractical, because it seeks to eradicate human error through procedural control. The risks that an employee will misdial a fax number or leave a message on unsecured voicemail are present, but do not represent the most prevalent security risks to most organizations.

While it is important to make information security a part of the corporate culture, it is even more critical to make certain that policies and procedures are designed to mitigate against the most prevalent risks.

Most organizations face far more prevalent risk from employees using email for personal purposes, and opening *.exe attachments. TruSecure's Essential Practices in this regard are focused on those areas that represent the greatest points of weakness and potential for human error within the organization, such as the development of a corporate code of conduct, and appropriate use of policies for corporate computing resources. In addition, TruSecure mandates that all employees be trained on security policies and procedures, and that reminders are issued periodically. Regular communication and enforcement of these policies and procedures are the key to making information security a part of the corporate culture.

To another point, one of the elements of the criteria refers to the use of an analogue mobile phone. While a minor point, it does clearly illustrate the importance of current security practices. Analogue mobile phones have been almost completely replaced by digital phones, therefore the risks associated with this particular requirement have become relatively minimal.

c) not leaving messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a resultof misdialling; d) reminding staff about the problems of using facsimile machines, namely: 1) unauthorized access to built-in message stores to retrieve messages; 2) deliberate or accidental programming of machines to send messages to specific numbers; 3) sending documents and messages to the wrong number either by misdialling or using the wrong stored number.	
12.1.2.1 Copyright Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trademarks. Copyright infringement can lead to legal action which may involve criminal proceedings. Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization, or that is licensed or provided by the developer to the organization, can be used.	This requirement is valid. According to the TruSecure methodology, however, this type of requirement does not represent a risk related to information security. This is a business issue, and should be addressed by management.

While TruSecure does not correspond exactly these requirements, it is, with very few exceptions, consistent with the controls and each of their subordinate criteria. TruSecure Essential Practices meet approximately 85% of the BS ISO/IEC 17799 code of practice criteria.

The Specification

TruSecure Enterprise 2001 is even more closely aligned with BS 7799 Part II Specification* for Information Security Management Systems. Because these criteria make up the certification standard, the requirements are more practical and quantifiable. The following chart represents a random sampling of criteria selected from BS 7799:2 Specification for Information Security Management Systems, and demonstrates the corresponding TruSecure delivery that meets those requirements. This is similar to the type of criteria selection that might appear in a Statement of Applicability submitted by a client organization to an accredited BS 7799 certification auditor.

BS 7799:2 Specification Criteria	TruSecure Enterprise 2001 Delivery
4.3.1.1 Inventory of assets An inventory of all important assets shall be drawn up and maintained.	The Security Analyst will identify and inventory the client's critical systems and devices during the disclosure process (see 3.2) and perform network mapping for the client.

**Extracts from BS ISO/IEC 17799: 2000 / BS 7799 Part 2: 1999 are reproduced with the permission of the British Standards Institution (BSI) under license number SK2001/0322. Copyright subsists in all BSI publications. Reproduction in any documentation other than as part of this report is not permitted without the permission of BSI. (Contact the BSI Copyright Manager on Tel +44 (0) 20 8996 7070).*

Complete copies of these standards are available for purchase in electronic format from http://www.bspsl.com/17799/ British Standards may also be obtained in hard copy from BSI Customer Services, 389 Chiswick High Road, London, W4 4AL. (Tel +44 (0) 20 8996 9001).

	Control Objective: Critical Equipment Hardware Inventory The devices are identified on an inventory list that is active and current. **Control Objective: Ensuring Continuous Service** Spares Inventory A spares inventory is maintained on-site OR there is a maintenance contract for equipment and/or software applications within the target.
4.3.2 Information classification Objective: To ensure that information assets receive an appropriate level of protection.	**Control Objective: Data Handling and Disposal** Data Handling, Classification and Disposal Policy Policy or procedures for handling and classification of information assets should be established. Procedures must address all forms of media, including, but not limited to paper products, floppy disks, magnetic tape, and removable media.
4.4.3 Responding to security incidents and malfunctions Objective: To minimize the damage from incidents and malfunctions, and to monitor and learn from such incidents.	**Control Objective: Incident Response** Incident Response for Network Breaches A formal policy for the response to network breaches should be documented. The formal Incident Response Policy should clearly delineate responsible parties, escalation procedures, disciplinary procedures, as well as contact information.
4.5.1.1 Physical security perimeter Organizations shall use security perimeters to protect areas which contain information processing facilities.	**Control Objective: Perimeter Security** Physical Security Policy The site maintains a formal physical security policy that contains the following: 1) Facility design 2) Electrical requirements 3) HVAC requirements 4) Fire and water damage prevention 5) Physical access controls 6) Guards and surveillance
4.5.1.2 Physical entry controls Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	See 4.5.1.1 **Control Objective: Perimeter Security** a) Monitoring All points of user entry to the facility are monitored by people, cameras, or other methods of observation (i.e. Security Guard), that scan the immediate area. Tapes generated by security cameras are archived and stored off-site for 90 days. b) Locks/Access Control Locking mechanisms have been employed on doors and windows that control access to the physical business perimeter. c) Inbound Access/Data Center No inbound user access. Administrative access is locked and logged. Emergency egress access only.

4.6.1.3 Incident management procedures Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents.	**Control Objective: Incident Response** Incident Response for Network Breaches A formal policy for the response to network breaches should be documented. The formal Incident Response Policy should clearly delineate responsible parties, escalation procedures, disciplinary procedures, as well as contact information. **Control Objective: Perimeter Security** Physical Incident Response The site maintains a formal Incident Response Policy or procedure, which guides response to breaches of physical security. Elements of the policy include: 1) Key contacts and contact information 2) Notification 3) Escalation 4) Recovery 5) Disciplinary Procedures
4.6.1.5 Separation of development and operational facilities Development and testing facilities shall be separated from operational facilities.	**Control Objectives: Application Change Control** Application Change Control Policy Applications must be administered under a Change Control Policy that addresses: 1) Installing revisions and patches 2) Moving new code into production 3) Tracking and resolving problems 4) Isolation of development and testing function from the production environment.
4.6.2.1 Capacity planning Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.	**Control Objective: Performance and Capacity** a) System Acceptance All proposed additions to the IT infrastructure should be tested prior to acceptance for compatibility and capacity. b) Performance Monitoring Capacity and performance of the system should be monitored to avoid failures due to inadequate capacity. Capacity requirements should be periodically reviewed for alignment business requirements. c) Capacity Planning The baseline configuration of the system should be documented.
4.7.2.2 Privilege management The allocation and use of privileges shall be restricted and controlled.	**Control Objective: Access Control** Privilege Management Access to critical system's console functions is restricted to appropriate Systems Administrator(s) (e.g. root, admin.). No logins from anywhere other than the system console are permitted.

4.7.2.3 User password management The allocation of passwords shall be controlled through a formal management process.	**Control Objective: Access Control** Password Policy and Procedures The allocation of passwords to critical systems should be strongly controlled pursuant to a defined password policy. All users with passwords on critical systems are provided with guidelines on how to select and use passwords appropriately.
4.9.1.1 Business continuity management process There shall be a managed process in place for developing and maintaining business continuity throughout the organization.	**Control Objective: Ensuring Continuous Service** Disaster Recover Plan - Personnel Personnel identified as participants in the Business Continuity and Disaster Recovery Plan receive training on implementation details.

TruSecure Enterprise 2001 meets approximately 90% of the requirements of the BS 7799 Part II Specification for Information Security Management Systems. The program provides complete documentation to those organizations that choose to self-certify to the standard; those seeking formal certification will find that this documentation and third-party validation can significantly reduce time and effort spent preparing for the specification audit.

TruSecure Deliverables

In addition to the review of Essential Practices with the client, TruSecure Enterprise 2001 is performed through electronic assessment, interview and attestation, and inspection, and supported by technical and reporting, and customer service. Deliverables include:

Electronic Assessment — Scanning of the Internet perimeter, devices visible to the Internet, the corporate network, and end-user desktops.

Physical Inspection of the Facility — analyst verification of physical security controls within the facility that houses the target

Essential Practice Review — Review of security policies, procedures, and practices, measured against TruSecure's Essential Practices.

Technical Reporting — The outcome of the electronic assessment. Geared toward technical staff, these reports identify vulnerabilities on critical devices, and make recommendations for correction.

Management Reporting — The outcome of the initial phase of the TruSecure process. Geared toward management, this is appropriate to share with Board members or business partners for due diligence purposes.

TruSecure Monitor — an alert service available online to TruSecure clients. It is an essential resource for identifying new and emerging threats.

Emergency Alert Service — urgent notification to all TruSecure clients of high level threats, such as the Melissa virus or the DDoS attacks.

Unlimited Telephone Access to Analyst Support — Security Analysts provide unlimited customer support to TruSecure customers for the life of the contract.

On-going Assessment — during the life of the contract, routine electronic assessments and physical inspections are performed on a regular basis. In this way, TruSecure clients are assured that their security posture is maintained as they make changes to critical systems, and that those systems are protected against current and emerging threats.

TruSecure Certification — a seal program available to all clients that meet the essential practices and risk mitigation standards defined in the TruSecure Enterprise 2001 program.

Insurance Guarantee — TruSecure Corporation backs TruSecure Enterprise 2001 with an insurance guarantee in case of a breach of security. All TruSecure Enterprise 2001 clients that maintain certification standards are eligible[13].

Conclusion: TruSecure vs. BS 7799

The BS 7799 standards, and their ISO counterpart, are becoming the widely recognized and soon-to-be-adopted (albeit informally) security standards in the world. BS ISO/IEC 17799:2000 is a solid framework upon which to build the policies and procedures that support an organization's information security program, and BS 7799:2 is an outstanding means to measure subsequent security compliance. Despite their quality, however, these standards remain simply an objective framework for the development of information security practices within the organization. Like all objective standards, they need to be applied to the organization at the granular level, with substantial expertise, or else they may prove ineffectual against corporate security goals. Ideally, these standards must be supported by a security program in order to provide effective, real world protection to the organization's environment.

TruSecure Enterprise 2001 is a pragmatic, holistic, and dynamic security assurance program. Its risk-based methodology is applied across the enterprise to provide technical, physical, and administrative security measures to client organizations, and delivered on an ongoing basis in order to establish and maintain a current and effective security posture for the client. Because it is so closely aligned with the requirements of the 7799 codes of practice and specification standards, it can, for the most part, satisfy the best practice and/or compliance needs of organizations interested in those standards, and provide valuable documentation and third-party validation to those organizations seeking formal BS 7799:2 certification. TruSecure combines the best in current security intelligence with a unique methodology and delivery that provides its clients with risk-mitigating strategies and real world security protections.

About TruSecure Corporation

TruSecure Corporation is a worldwide leader in information security, providing managed security solutions for over 400 global web-enabled companies. ICSA Labs, a division of TruSecure Corporation, is the security industry's central authority for intelligence, research, and product testing, certifying more than 95% of the market's anti-virus software, network firewalls, cryptography and IPSec products. TruSecure's Media Group consists of *Information Security Magazine*, the leading industry publication with more than 45,000 readers; NTBugtraq, the premier online source of Microsoft-related security intelligence; and www.TruSecure.com, a public online information security forum.

A large segment of TruSecure Corporation's U.S. customer base comes from industries with global presence and international concerns. TruSecure Corporation's regulatory division monitors developing international security standards, as well as legislative and regulatory activity related to information security and privacy for heavily-regulated industries such as financial services and health care.

Acknowledgements

The author gratefully acknowledges the participation of Mark Ames of eGlobal Australia, David Capuano, Peter Horst, Garland B. Knott, Jeff Loos, and Barbara Thomas of TruSecure Corporation in the development of this paper.

[13] Certain restrictions apply.