DPG

Deer Park Group, Inc.

Security Assessment, Risk Analysis and ISO 17999

Larry Runge

Information security is the practice of shielding information assets from accidental or intentional misuse by persons inside or outside of a company, whether these be employees, consultants, competitors or malicious individuals seeking to conduct hi-tech vandalism.

The ISO 17799 Security Standard is a comprehensive set of policies and guidelines for computer security. Implementing it is a major effort—on a level with Six Sigma—which requires thousands of man-hours over a period of a year or more, and is sometimes quite costly. It is more popular in Europe than in the United States, although approximately 100 companies in the U.S. are involved with some level of implementation of its measures.

As a standard that is primarily conceptual, ISO 17799 is not a set of specific *How To* procedures, rather it is a checklist of recommendations to follow which are broken down into ten categories. It has large numbers of proponents and detractors, the prior extolling its virtues and the latter decrying its faults.

It is technology neutral, providing security requirements without relying on specific technologies and their implementation procedures. It is deliberately comprehensive in scope so it can be applied to businesses of any size and to any industry. Because of this, few companies would employ every section of the standard, rather it is more "mix and match" than other ISO standards. Flexibility is its watchword.

Again, ISO 17799 is divided into ten sections. To summarize, these and their purpose are:

1. Business Continuity Planning

To continue business activity in spite of major failures or disasters, enabling the business to conduct its operations from a remote, less than optimum site if necessary.

2. System Access Control

To control access to information while preventing or enabling the detection of unauthorized access. In essence, to prevent external intruders from accessing the system and to prevent internal users from maliciously damaging it.

3. System Development and Maintenance

To ensure that security is built into applications and that these are developed in a secure area. Furthermore, to prevent loss, misuse or modification of data while protecting the authenticity of the information.

4. Physical and Environmental Security

To prevent unauthorized access, interference or damage to business premises and information processing facilities. Also to prevent loss, compromise, theft or damage to information assets. This includes such efforts as controlling facility access and having backup uninterruptible power supplies and generators.

5. Compliance

To avoid breach of any criminal or civil laws, regulatory or contractual obligations, and to ensure compliance with security policies and standards. This is an area steering many companies into ISO 17799 compliance.

6. Personnel Security

To reduce the risks of human error, theft, fraud or misuse of information assets, and to minimize damage from security incidents. As part of this, established security procedures are instilled in all employees, while new employees are screened for past abuses. Confidentiality agreements are employed where necessary.

7. Security Organization

Defines the roles of the security organization within the company. Proscribes how to manage and maintain security of information assets accessed by third parties, whether customers or outsourcing partners. Responsibilities are defined and a process for recognizing and responding to security incidents is put into place.

8. Computer & Operations Management

To ensure secure operations of computing facilities while maintaining the integrity of such processes. To minimize risk from system failures and prevent damage to information assets. To avoid business interruptions, while ensuring adequate backup procedures are in place.

9. Asset Classification and Control

Maintain appropriate level of protection to information assets. These are inventoried and levels of protection are established commensurate with the value of the asset.

10. Security Policy

To provide management direction and support for the security policy. Define expectations and evaluate performance against these goals.

Obviously, there is a certain amount of overlap between these categories, but that is the nature of the standard—to be flexible and all encompassing.

Some critics say because the structure of ISO 17799 is intended to reach across all industries and environments, it is too imprecise to be of real use. Because ISO 17799 is at a very high level, and is broad in scope and conceptual in nature, it is sometimes accused of being two miles wide but only a foot deep.

Since it is generic to business categories and technologies, it is so large that few organizations would ever need to implement all of its recommendations. Companies may gain certification for a single service or department within their organization if they so wish.

However, this "one size fits all" approach leads critics to claim that in attempting serve every company, it serves none of them well. As with clothing, *one size fits all* really means that it fits no one properly. Another concern is that it does not provide a mechanism to test controls, measures, and procedures from the perspective of someone on the outside who is trying to get in. Others point out the challenges related to certification and its expected excessive cost are daunting.

Still other reservations is that it mandates a company must protect its information assets but does not describe methods of doing so, and that it rarely takes in to account those security measures which already exist, thus providing no means of evaluating these. Neither does it provide commonsense advice such as only enabling necessary services.

One weakness of the standard is that it compels adopters to inventory their portfolio of systems and then assign values to information assets, yet it doesn't explain how this is to be accomplished. Furthermore, it focuses on tangible assets, ignoring the intangible—but often highly valuable—assets.

As self-assessments are often blind to existing problems and leave room for error in interpretation, the British Standards Institute advocates having a professional

risk assessment performed before starting an ISO 17799 compliance effort.

Thus if a company wishes to implement a comprehensive security plan, typically they begin by performing a *Security Assessment*, which is then followed by a *Security Risk Analysis*. This is then used to plug security holes and to help the company decide if it wishes to embark upon a full ISO 17799 effort. If so, the Security Risk Analysis serves as the basis for deciding which portions of the ISO 17799 Security Standard to implement and in what order.

In summary, ISO 17799 is a comprehensive set of guidelines and recommendations for implementing security measures which are technology and industry neutral. It is broad based to accommodate any variation or contingency and few companies would need to implement every one of its recommendations. It has both advocate and detractors, and is a large undertaking whose cost of implementation may well be substantial. Yet is it highly regarded in Europe and is seeing more and more adoption in the United States.

The Deer Park Group

(847) 382-5171
www.DeerParkInc.com