The permission form should specify the IP addresses and phone numbers (if war dialing or social engineering) to be included in the test. The tests should be restricted to a specified time window. If possible, the time window should not be selected such that the organization can be ready and waiting for the test. A window of at least seven days is typical. There also may be a need for some extended hours (over several days) to accommodate longer security scanning and test processes, especially if the testing window is restricted to several off hours for each of those days. Lastly, the type of testing should be described (e.g., vulnerability testing, penetration testing, social engineering, war dialing).

4.1.3.4 Accounts Required

The security risk assessment team must specify to the sponsor the number and types of accounts that will be required. The accounts required for any particular security risk assessment are dependent on the processes to be used by the security risk assessment team and the permissions that the customer will grant. An example of the accounts that should be requested is provided in Table 4.1.

4.2 Review Business Mission

Before attempting to assess and report on the risks to an organization and its assets, the security risk assessment team must first acquire a basic understanding of the organization, its mission, its objectives, and its critical systems. The security risk assessment team will never develop as complete an understanding of the organization as the organization's executives, but there must be a basic understanding of the corporate mission, structure, businesses, and culture. The security risk assessment team must understand the business mission of the organization to have a basic

Table 4.1 Example of Required Accounts

Account Required	*Privileges*	*Need*
Guest account	User privileges only	User security functions
Privileged account	Administrator privileges	Administrator security functions
Network component account	Read access	Read configuration files
Network access	Network media access	Vulnerability scanning, network sniffing

Note: The security risk assessment team will require multiple accounts with various privileges and access to properly gather information for the assessment.

understanding of the business assets, the potential risks, and the impact of risks on those assets.

4.2.1 What Is a Business Mission?

Every organization has a reason for existing outside of making money. Making money is a potential side effect of performing the mission well. Sometimes it can be difficult to determine the business mission. Other times, it is clearly stated and available. In either case, the security risk assessment team is looking for the answer to three simple questions:

1. Who Is the Customer?—The basic starting block for understanding a business is to understand the customers they serve. For example, consider the magazine publishing industry. A surface-level understanding of the business tells you that the readers and subscribers are the customers. However, the revenue generated from subscriptions and newsstand purchases typically covers only the cost of printing and distribution.

   The real customers of the magazine publishing industry are the advertisers and the customers of "nonadvertising marketing."[3] Understanding that these are the real customers of the magazine publishing industry will give the team members a better understanding of the assets, critical systems, and acceptable levels of risk for each of those assets.
2. What Does the Organization Offer the Customer?—Find out what they sell, how they make money, and what the product is. The business mission is not always clear, but if you want to find out how that mission is defined, follow the money. Business missions are defined by the various services or products offered by the organization. Ask about business units, organization charts, and sources of revenue for the organization.
3. What Makes the Organization Different from Its Competitors?—Even within an industry familiar to members of the assessment team, the assessed organization may have several unique characteristics that set it apart. Simply ask senior management how they differentiate themselves from competitors. For example, an organization may be the low-cost provider of e-commerce for certain items. In this case, you would expect them to accept more risk than most of their competitors. Although this organization would need to meet minimum standards set by regulations and customers, it is unlikely that they would want to expend a lot of resources to implement additional controls unless these controls had other clear benefits.

The business mission statement typically identifies the customers and how the organization plans to serve them. Beyond those simple elements, look for how this company sees itself as different from its competitors. There are only two ways to differentiate yourself:

- Offer a better product or service
- Offer a cheaper price

A better product or service can take on many forms. Better could mean higher quality (e.g., reliable, respected, fast) or more convenience (e.g., better integrated, easy ordering process). A cheaper price could mean less cost initially or less cost in the long run. In either case, the security risk assessment team is looking for the company to fall into one of three tiers of security need (see Table 4.2). In most cases, it becomes rather obvious into which tier a client falls, based on a cursory review of the business mission. Because of the need to differentiate one organization from its competitors, few companies are "on the fence" when it comes to these categories.[4]

4.2.2 Obtaining Business Mission Information

To the extent possible, the security risk assessment team should attempt to obtain the business mission prior to visiting with the organization. A review of public and provided information may produce the knowledge necessary to understand the

Table 4.2 Business Mission and Security Need

Security Level	*Business Mission Elements*	*Security Need*
Tier 1	• Cutting-edge organization • High-quality provider • Critical systems with critical data assets • Sensitive customers	Low risk acceptance • High availability • Defense in depth • Redundancy • High-security culture • Cutting-edge security mechanisms • First-rate security organization
Tier 2	Average Just do what is right	Average risk acceptance • Standard security practices
Tier 3	• Cost leader • Minimalist • Bare bones	High-risk acceptance • Minimal security practices

Note: A governing information security principle is that security needs are based on business objectives. This table provides a simplified illustration of how the business mission can affect the level of security required within an organization.

organization's business mission. Public information available to the security risk assessment team includes the organization's Web site, annual reports, and press releases. Other information that may contain statements relevant to the organization's mission includes introductory letters from the organization's chief executive officer, internal memoranda, or corporate training material. Any of these sources should yield a statement as to the customers served and the products or services offered.

The security risk assessment team leader should perform the basic research necessary to identify the organization's business mission. This proposed mission statement should be reviewed and approved by the customer organization and, if necessary, appropriately modified.

4.3 Identify Critical Systems

The customer organization is likely to have multiple information systems within the scope of the security risk assessment. All of these critical systems must be considered independently, as they will have unique critical assets, missions, data, procedures, controls, and data owners. Once these systems have been identified, the security risk assessment team may find some overlap between the systems in terms of some of these aspects. For example, there may be a single data owner for two or three systems supporting a business function. However, it is still important to identify these individual critical systems if there are any unique aspects.

Information systems are defined by their boundary of resources and characterized by their function, data, authorized users, and data owners. For example, a customer organization may have the information systems listed in Table 4.3 defined as part of the security risk assessment.[5]

4.3.1 Determining Criticality

The security risk assessment team should seek to obtain an understanding of the criticality of the various information systems to the success of the organization. This is part of understanding the organization's mission.

The criticality of information systems is determined by their support for business objectives. More specifically, critical systems are those that automate critical business functions. The assignment and prioritization of system criticality are difficult tasks, especially for a security risk assessment team that may not have adequate representation from all the business units of the organization. However, this should not be a problem. As described in this book, there are three approaches for determining the criticality of systems for a security risk assessment:[6]

References

NIST. DRAFT National Checklist Program for IT Products—Guidelines for Checklist Users and Developers, NIST Special Publication 800-70, Revision 2 December 22, 2010. http://csrc.nist.gov/publications/drafts/800-70-rev2/Draft-SP800-70r2.pdf. Accessed February 7, 2011

The Office of Management and the Budget. Management of Federal Information Resource Circular A-130, July 2, 1993.

Bibliography

ASIS International. *Protection of Assets Manual*, 2004. http://www.protectionofassets.com/

Dalkey, N. C. "The Delphi Method: An Experimental Study of Group Opinion," Rand Corporation, RM-5888-PR, 1969.

Department of Energy. "Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities." August 19, 2002. http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

Information System Security Association (ISSA). "Guideline for Information Valuation (GIV)." 1993.

Marshall, Alfred. *Principles of Economics*, 1920.

Milton, Thomas J., James G. Rabe, and Charles Wilhoite. *Economic Analysis of Intangible Assets and Intellectual Properties*, 1999.

NIST. "General Support Systems and Major Applications Inventory Guide." NIST Publications, July 2002. http://csrc.nist.gov/groups/SMA/fasp/documents/risk_mgmt/GSSMA-Inventory-Guide.doc (accessed 2/7/11).

NIST. "Guide for Developing Security Plans for Information Technology Systems." NIST Special Publication 800-18 Revision 1, February 2006. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1-final.pdf.

NIST. "Guide for Mapping Types of Information and Information Systems to Security Categories." NIST Special Publication 800-60 Revision 1, June 2004. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf (accessed 2/7/11).

NIST. "Guide for Selecting Automated Risk Analysis Tools." NIST Special Publication 500-174, October 1989. http://csrc.nist.gov/publications/nistpubs/500-174/sp174.txt.

NIST. "Recommended Security Controls for Federal Information Systems." NIST Special Publications 800–53 Revision 3. August 2009.

SECOND EDITION

THE SECURITY RISK ASSESSMENT HANDBOOK

A Complete Guide for Performing Security Risk Assessments

DOUGLAS J. LANDOLL

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK