

## ISO/IEC SECURITY ASSESSMENT

### Matching Risk to Reward

The pace of technology has outpaced the IT manager's ability to keep up with the security of the enterprise. Often, marketing and sales implement their own web sites and on-line applications without the guidance and expertise of the information technology team. Product development becomes the production environment, without the benefit of a careful review to ensure security holes are closed and affected systems are secure. Above all, customer privacy is at stake. Names, addresses, and even personal financial information are all stored on electronic media, often within reach of the Internet hacker.

Controlling these risks becomes more difficult in light of the very competitive nature of business today. "First-to-market" is on every analyst's lips and every organization must make it to the web. Customer delight hinges on instant and accurate access to information, and the ability to do commerce on the Internet at any time. Success depends upon meeting these objectives while avoiding the pitfalls posed by faulty security.

### Striking the Balance

Doing business well is about setting priorities and executing to them. Planning, including a good security policy, design, and the procedures to implement them must address the most credible and likely threats. Operations must realize the design and faithfully carry out the procedures to ensure that no vulnerabilities are created. Constant re-evaluation is the only way to gauge the accomplishment of this continually shifting equilibrium.

### The Assessment Process

Network & Security Technologies consultants apply expert knowledge to the challenges of your business. The electronic marketplace is a networked marketplace. Only Network & Security Technologies can deliver the right combination of veteran network expertise with a firm grasp of the security principles to keep online commerce safe.

The security assessment is a three-phase process:

- I. Gather information about technology and processes through interviews, document review, hands-on evaluation, and testing.
- II: Analyze and quantify the risk posed by the vulnerabilities identified in terms of both likelihood and impact.
- III: Produce a plan for reducing the risk to an acceptable residual through actionable recommendations.

The output of the assessment is a report that permits the IT manager and business executive to understand the probable impact of the vulnerabilities in their technology and processes, as well as the likelihood that the vulnerability will be exploited by an attack. While every organization's needs are different, Network & Security Technologies security and network consultants review the full spectrum of security controls. secure configuration of network elements.

These include:

- **Personnel:** Staff background and capabilities
- **Physical:** Facility and equipment protection, as well as handling of media or printed matter
- **Network:** Firewalls, virtual private networks, intrusion detection systems, packet filters, and secure configuration of network elements
- **System:** Configuration and management of workstation, server, and mainframe operating systems
- **Application:** Configuration of off-the-shelf and custom developed software
- **Database:** Management and configuration of data storage and processing

Each of these areas includes evaluation of both technology and procedures necessary to ensure security and privacy policies are maintained. Network & Security Technologies security and network experts possess the experience and expertise to evaluate a wide range of vendors and products. Where a novel solution is in use, Network & Security Technologies consultants have the hands-on knowledge in secure product development to analyze software and configuration to identify weaknesses and pitfalls.

### Knowledge is Power, Power is Money

Network & Security Technologies security and network experts understand that no organization is well served by costly and drawn-out evaluation processes. Resources are best used to build plans and implement changes, not to analyze. Thus, Network & Security Technologies experts focus their attention on the highest network and security risks facing your organization. The assessment is a starting point; a roadmap to get on track while spending the least money. It is the modest investment that any good manager must make to guarantee a well-run business will not face a crisis of confidence by its customers or stockholders.

#### THE SECURITY EQUATION

- $\text{THREAT} = \text{VULNERABILITY} + \text{ADVERSARY}$
- $\text{RISK} = \text{LIKELIHOOD} \times \text{IMPACT}$