



Holistic Paths to Security

by Adam Lipson

Security tools are important for protecting company systems, but, says Adam Lipson, focusing on people can yield better results

How many senior executives find the more they spend on security technology, the less secure they feel? Investing in the latest hot product creates a lot of "buzz," yet somehow the real goal - protecting the revenue-producing components of the organization - falls further out of reach.

The standard provides a structure for addressing all aspects of the security problem
- Adam Lipson

The key reason is that security requires more than just technology. Sure, most of these tools play a vital role in IT protection. And, there's no doubt that the improvements and innovations we will see over the coming years will enhance the role that technology plays. Nevertheless, these controls will never amount to a complete program.

The standard that helps you sleep

Building a secure enterprise requires a holistic security program, not a collection of point technology solutions. The ISO 17799 standard embraces the idea that security is as much about processes and people as it is about technology.

It provides a roadmap for the CSO, CIO or other executive with a fiduciary responsibility for protecting valuable information and critical infrastructure. Through its successful implementation, we can find a way to get a good night's sleep.

Many organizations have already discovered the existence of 17799. Because it has the ISO (International Standards Organization) imprimatur, they have adopted it as their path to security. If a few important points are kept in mind, 17799 will provide excellent guidance.

ISO 17799 is a security framework. Many make the mistake of thinking the standard will spell out the equipment and configurations they need. In fact, it doesn't contain any technological or procedural specifics. Rather, it provides a structure that is both necessary and sufficient for addressing all aspects of the security problem.

Read the standard. ISO 17799 is aimed at the executive. Most of its requirements are relatively high level and the time invested to at least skim them will pay off down the line.

Creating foundations

The first security domain of the standard speaks to the need for security policy. (See list of domains). Policy is the most important security measure any enterprise can implement and is the foundation for the other nine ISO 17799 domains. Organizational security is the second most important.

Some organizations have in-depth expertise to interpret the requirements of the standard in a way that makes sense for them. Other companies, however, won't have the required in-house experience in building necessary security programs. Fortunately, there are a number of consulting organizations that can help.

Every organization that I have worked with to create an ISO-compliant security program has both dramatically improved overall security and saved money.

But it took time. No matter how committed you are, building a security program will take an enterprise years. It is a matter of building a security culture that cuts across the entire organization.

Don't be shy, internally market security. Develop awareness within management that security requires more than simple perimeter controls - it needs a far-reaching and over-arching security program. Use practical examples of incidents and their cost to the organization. For example, 'Blaster required us to shut down our email servers for four hours costing us \$318,000 of lost productivity.' Focus your communication about security on the end-users as well as management.

Only a holistic security program can truly reduce the overall risk facing any enterprise. Building such a program will take a commitment from every member of the executive team. But the means will justify the end.

ISO 17799 Security Domains

1. Security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

Adam Lipson is president and CEO at Network & Security Technologies (www.netsectech.com), a provider of digital security consulting solutions.

* The International Organization for Standardization (ISO) has published this standard to provide organizations a common basis for measuring the completeness of their security program.