



Executive Perspective

## Security Meets Total Quality Management

By Jeff Platon

**Total Quality Management is not a new concept. Organizations of all types and sizes have long used the principles of TQM to continuously improve everything from retail floor operations to R&D, from manufacturing to supply chain.**

It's only now that these same principles are being applied to an area of growing enterprise concern – network security.

In many organizations, security procedures are stretched across the enterprise, and they are further taxed by expanding interrelationships among customers, suppliers, and partners. The reality is that every organization is interconnected and must be prepared to deal with the vulnerabilities, threats, and noncompliance with policies that may exist in neighboring environments.

Two of the most difficult aspects of managing operational security are, first, determining the effectiveness of an organization's current efforts and, second, understanding how closely operational realities align with requirements and expectations. Unfortunately, most security analysis today is based either on traditional assessments performed by a small number of experts or on data gathered exclusively by security-assessment tools. Both types of evaluations tend to focus on the effectiveness of disparate and isolated elements of the security system, such as password policies and firewall technologies, or on measurements such as mean time between failures.

In their failure to take a holistic approach, these approaches often neglect the security policies themselves and, especially, the users' perceptions regarding those policies.

As a result, companies are struggling to evaluate the effectiveness of their security strategy and determine where security gaps exist. Incomplete or inaccurate information can lead to misspent appropriations, overconfidence, inadequate preparation, or worse: a security breach that shuts down business operations.

### A New Approach

At the MIT Sloan School of Management, Stuart E. Madnick and Michael Siegel have created a simple survey tool designed to help companies understand and measure the perceptions of their employees and managers regarding security. The survey borrows concepts of TQM in a comprehensive and scientific approach.

Total Quality Management is a combination of quality and management tools by which management and employees become involved in the continuous improvement of operations. The culture of TQM demands that organizations do it right first time and continuously improve from there.

Madnick and Siegel have identified about 300 security issues that define the three principal tenets of security: providing *accessibility*, minimizing *vulnerability*, and assuring *confidentiality*. These are equivalent to what the security professionals call "availability, integrity, and confidentiality."

These tenets are, in turn, anchored by five operational pillars:

- Technology resources for security
- Financial resources for security

- A business strategy for security
- Security policies and procedures
- A security culture

### **Perception vs. Reality**

The MIT survey is designed to identify variations in perceptions of security across all functional areas within an organization and its extended enterprise, from front-line employees to top-level managers.

The MIT survey is designed to identify variations in perceptions of security across all functional areas within an organization and its extended enterprise, from front-line employees to top-level managers.

The tool itself is a simple questionnaire that can be administered in as little as 15 minutes per respondent. Respondents are asked to rate a series of statements about their organization's security, specifically:

- What the current state of a particular security issue is within their organization (for example, whether people in the organization are aware of good security practices)
- How important that security issue is for their organization
- What the current state of that security issue is for a partner organization
- How important that security issue is for the same partner organization

A key part of this study involves performing gap analyses. An organization would look at, for example, the importance that managers assign to a certain security issue and what they think the current state of that security issue is. Differences in such perceptions can show an organization where improvements need to be made both in its security policies and in its efforts to improve the staff's understanding of those policies.

By analyzing the survey responses, organizations can develop a better understanding of their security needs, deploy better security technology and policies, and help ensure continuous improvement in the effectiveness of the organization's security efforts.

Suppliers and integrators can use the survey to develop more effective security strategies, products, and services.

The early results of the research are promising and were described in early September at the Security Standard conference in Boston.

For more information on the study:

<http://web.mit.edu/smadnick/www/Projects/TSQM/TSQM%20Security%20Exec%20Summary.pdf>.

### **About the Author**

Jeff Platon is Vice President of Security Marketing for Cisco Systems®



the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).