Measuring and Evaluating an Effective Security Culture

Today's network-connected businesses and organizations face ever-increasing security threats. In response, they need a focus on security that goes beyond ad-hoc or reactive measures. Today's businesses require a culture of security that is pervasive throughout the organization, aligning people and practices with security goals. And they need to continually measure and assess the effectiveness of their security efforts. Network security technologies make it possible to measure attempts and incidents of online intrusion and disruption. But defining metrics for measuring the effectiveness of a security culture requires a closer look at the dynamics of the organization.

This paper focuses on the behavioral dimension of security and how to measure the effectiveness of a security culture.

Summary

Maintaining enterprise security today is as much about mitigating internal threats and negligence as it is about handling attacks from outside of the organization. In a 2006 survey of members of the Computer Security Institute (CSI), conducted jointly by CSI and the U.S. Federal Bureau of Investigation, 30 percent of the large companies responding to the survey said that threats from inside their organizations were the cause of at least half their losses from security breaches in 2005. Similarly, in a *CSO Magazine*/Cisco poll of chief security officers (CSOs), approximately 59 percent reported employee error as the number one threat, while 37 percent reported employee or partner sabotage as the number one threat.

The concept of fostering a security culture within every organization—where employees feel a sense of ownership in a core set of security principles, receive ongoing training in security best practices, and hold themselves accountable for their actions—is gaining publicity and adherents. The evolving role of the CSO, whose mission is to embed security in the company culture from the most senior executive down to the individual contributor, is also gaining prominence in many organizations.

Creating security awareness programs and establishing best practices to bolster security are logical action items, but they must be accompanied by the creation of metrics to gauge the effectiveness of such a companywide effort. Developing composite security metrics that are simple to understand and clearly linked to the business was ranked as the primary imperative among security leaders at Fortune 500 firms, according to a 2006 report published by the Center for Digital Strategies at the Tuck School of Business at Dartmouth and the Institute for Information Infrastructure Protection.

Awareness of and compliance with security best practices throughout an organization can be measured with metrics, just as security technology metrics measure uptime and downtime, intrusion attempts, malware, and vulnerabilities. A study in Norway found that measuring this awareness can elevate security best practices within organizations, leading to fewer security incidents due to carelessness or neglect. Employees took more responsibility for the security of physical and data assets in such an environment and they assumed a more active role in discovering and reporting incidents.

Challenge

The 2006 *InformationWeek* and Accenture Global Security Survey of 2193 global business technology and security professionals found that rates of reported attacks on customer records and identity theft had doubled from 2005. China is experiencing the highest level of such attacks, with 23 percent of companies reporting that customer data has been compromised and 27 percent saying they had faced identity theft. In July 2006, the international Anti-Phishing Working Group reported that 154 brands (including financial institutions, Internet service providers, and government agencies) were hijacked by e-mail phishing campaigns. This is more than twice the number of brands reported victimized in 2005.

There were also many well-publicized incidents involving the theft of physical and data assets during 2006. In the U.S., a Veteran's Affairs Department laptop and removable hard drive with 26.5 million personnel records was stolen during a home burglary. Similar thefts or negligence occurred at insurance and financial services companies, banks, a major healthcare provider, and even at a European security agency during 2006, all resulting in exposure of corporate or personal data.

Continual training to maintain a high degree of awareness and best practices within a security culture can help mitigate such vulnerabilities. Creating metrics to manage the effectiveness of these activities can help managers better understand and improve their companies' security posture.

Solution

Metrics to measure the effectiveness of a security culture are not as tangible as determining how many viruses or worms have been detected trying to invade a network. The frequency of security awareness training can be measured. So too can the number of unique hits to a Webpage offering security best practices or video training. These metrics alone, however, will not necessarily demonstrate or predict improvements in security. Security experts say that it is the sum total of metrics from security technologies, processes, and behavior that can give a clearer picture of an enterprise's security posture.

Measuring Perceptions of Security

In 2006, the Massachusetts Institute of Technology (MIT) launched the first phase of a study of 1259 individuals from six companies in six industries, with questions related to each person's assessment of the organization's readiness to combat a specific type of security risk and the perceived importance of that risk. The study applied a Total Quality Management methodology used in manufacturing to improve processes for quality and efficiency. Respondents included business executives, IT managers, and several categories of employees, plus partners, customers, and suppliers. Each respondent was asked to answer questions both for the organization and for partners and suppliers, as shown in Table 1.

Table 1. MIT "Toward Total Security Quality Management" Study Sample Questions

Questions		Your Organization		Partner Organization	
		Assessment	Importance	Assessment	Importance
1	The organization's data and networks are rarely tampered with by unauthorized access.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
2	In the organization, security is adequately funded.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
3	Customers trust the organization not to disclose data about them.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
4	The organization's security strategy sets direction for its security practices.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
5	Business managers in the organization are involved with IT security policies.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7

The MIT study sought to identify how perceptions shape decisions related to the type of security solutions organizations purchased and how individuals within and outside of an organization perceive security readiness. It was also designed to uncover any perceptual differences among different roles (for example, mid-level managers compared to senior management) within each company. The assessment scale ranged from 1 (security statement is true to a very small extent in my or my partner's organization) to 7 (security statement is true to a very large extent in my or my partner's organization). The importance scale ranged from 1 (not important to me that my or my partner organization address this security statement) to 7 (very important that they address this statement).

The study's results showed significant gaps between respondents' answers related to the importance of eight security constructs and their assessment of the organization's current security readiness in those areas. The eight security constructs included security culture, accessibility, vulnerability, confidentiality, financial resources, IT resources, business strategy, and security policy. Awareness of good security practices fell far short of what respondents perceived was needed.

The largest gap was between the perceived importance of a security culture and its presence in the companies surveyed. Other lessons from the study included the realization that organizations focus on their own security to the exclusion of the security of partners, suppliers, and customers; that people at different levels within an organization are not equally knowledgeable about security tools and best practices; and that executives have the greatest awareness of the need to improve the current security posture.

The MIT study suggests that such gaps are widespread. Organizations must understand what is perceived and what is real within their own environments when it comes to security, and implement measures to enforce security cultures.

Communication and Training Metrics

Metrics to assess how effectively security policies and procedures have been communicated and understood may include:

Questionnaires

- Employee satisfaction surveys can ask “How aware are you of security policies and procedures?” and the answers can be further scrutinized with supplementary questions that seek details to validate this awareness.
- Customer, supplier, and partner surveys can solicit and measure feedback related to the company’s security controls.

Existing Data

- Metrics may also be derived from existing measures, such as help desk cases. Flagging and analyzing security-related incidents reported to the help desk as part of other technical support issues could uncover hidden vulnerabilities and gaps.
- Data on security incidents can be analyzed to determine how many were employee-related.
- Managers and security “champions” can submit ongoing reports with behavioral metrics that may include the frequency of passwords left exposed in work areas, failure to activate a secure screensaver when an employee has left their desk, and other instances of lack of compliance with security policies.
- Security personnel can measure and report on the quantity and content of interactions with employees to see where vulnerabilities may exist.

Training

- The percentage of employees who attended regular security training, either in class or online, can be measured.
- Audience feedback from awareness training can be turned into metrics.
- Security-related training should stress what is expected of all employees from the beginning of employment. These should be reinforced throughout an employee’s career. Ongoing confidentiality expectations for safeguarding intellectual property should be reinforced during the employee exit interview. All of these sessions should be measured so that any gaps in the training of individual employees can be corrected.

Process Metrics

The network is one of the most fertile areas of security vulnerability, offering the potential for both useful collaboration and harmful intrusion. Organizations must put processes in place to review all existing and new applications for anything that could leave networks vulnerable to intrusion.

With the increased trend toward outsourcing and channel marketing, large organizations must make sure that individuals in each area of the company competently oversee each external relationship with partners, suppliers, developers, and customers. Security risks must be well-understood and considered in decision making. These processes must be systematized (for example, made part of the Request for Proposal [RFP] process) and not left undefined. For example, in application service provider relationships, where a company’s application and data are outsourced, part of the evaluation process should be a stringent architectural review to maintain adequate safeguards for the transmission and storage of data and access to the application. All of these procedures should be tracked with metrics so that managers can make sure that risks are adequately addressed.

There is an element of risk inherent in today’s business. However, processes and metrics that seek to define, mitigate, and measure risk provide insight into those risks from the front line to the highest levels of a company.

Top-Down Views of Metrics

The CSO or equivalent within a company can enhance companywide vigilance by engaging executives and line managers in regular review of security metrics. They can do so through dashboards or balanced scorecards, which are usually Web-based collections of metrics that may span the financial, operational, manufacturing, sales, and security functions of a company. These customized portals bring together key measures of business performance. Adding security metrics to these management views elevates the importance of security and underscores the connection of security policies and procedures to the achievement of company goals.

Each dashboard or balanced scorecard can be tailored to deliver views of security metrics from different divisions, geographic areas, or other meaningful subsets. The goal is to alert managers at different levels of the organization to any anomalies so they can take action before vulnerabilities become liabilities.

Feedback on metrics should be solicited on an ongoing basis to help refine the metrics and ensure their relevance. As organizations evolve, some metrics may become outdated and newer ones may become necessary.

Conclusion

Research has shown that many employees overestimate how secure their organizations and assets are. There are fewer controls in place than imagined. A good security culture includes people, processes, and technology. It involves employees and partners at all levels in positive steps to ensure the security of data and physical assets. Metrics should measure the qualitative aspects of the culture, including awareness of security policies and procedures, along with quantitative measures from security technologies, such as the number of online intrusion attempts, virus outbreaks, and phishing attempts.

Creating metrics to measure a security culture is not as simple as choosing from “one-size-fits-all” options. Each organization is unique, and metrics to measure behavior must be carefully adapted to capture the relevant behavior and processes. Just as maintaining security preparedness is an ongoing job, so is measuring that preparedness. The very awareness among employees and managers that security culture metrics are being gathered on a regular basis and are seen by upper management can go a long way toward strengthening compliance with security policies. The ultimate success of a security culture comes not from measurement of awareness and compliance, but from data that shows fewer serious security incidents; lower rates of neglect or carelessness among employees, partners, and suppliers; tighter controls on data and physical assets resulting in lower rates of theft and loss; higher rates of incident discovery, reporting, and mitigation; better incident handling; and more active participation by stakeholders to improve security throughout the company.

For More Information

Enterprise Security Perception and the “House of Security”—Massachusetts Institute of Technology Study
http://web.mit.edu/smadnick/www/Presentations/2006-09-06%20TSQM.ppt.

Establishing an Organization’s Security Culture, White Paper, Cisco Systems
http://www.cisco.com/web/about/security/intelligence/05_07_security-culture.html.

10 Tips for Building a Business of Pervasive Security Culture
http://www2.csoonline.com/whitepapers/index.html.

“To Each Nation, It's Own Security Culture”—*CSO Magazine* article, May 2005
http://www.csoonline.com/read/050105/briefing_brief_nation.html.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-380432-00 03/07

