August 2003

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

IT SECURITY METRICS

Elizabeth B. Lennon, Editor
Information Technology Laboratory
National Institute of Standards and Technology

Introduction

IT security metrics provide a practical approach to measuring information security. Evaluating security at the system level, IT security metrics are tools that facilitate decision making and accountability through collection, analysis, and reporting of relevant performance data. Based on IT security performance goals and objectives, IT security metrics are quantifiable, feasible to measure, and repeatable. They provide relevant trends over time and are useful in tracking performance and directing resources to initiate performance improvement actions.

This *ITL Bulletin* summarizes the recently published NIST Special Publication (SP) 800-55, *Security Metrics Guide for Information Technology Systems*, by Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo. NIST SP 800-55 provides guidance for IT managers and security professionals at all levels, inside and outside of government. The document describes the development and implementation of an IT security metrics program and provides examples of metrics based on the critical elements and security controls and techniques contained in NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Both documents are available at http://csrc.nist.gov/publications/nistpubs/index.html.

Why Measure IT Security?

Regulatory, financial, and organizational reasons drive the requirement to measure IT security performance. For federal agencies, a number of existing laws, rules, and regulations cite IT performance measurement in general, and IT security performance measurement in particular, as a requirement. These laws include the Clinger-Cohen Act, Government Performance and Results Act (GPRA), Government Paperwork Elimination Act (GPEA), and Federal Information Security Management Act (FISMA). In the financial arena, organizations that measure successes and failures of past and current security investments can use metrics to justify and direct future security investments. From an organizational point of view, metrics improve accountability to stakeholders, ensure an appropriate level of mission support, determine IT security program effectiveness, and improve customer confidence.

The Metrics Development Process

The IT security metrics development process consists of two major activities:

- ☐ Identification and definition of the current IT security program; and
- ☐ Development and selection of specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls.

The process steps need not be sequential. Rather, the process provides a framework for thinking about metrics and facilitates the identification of metrics to be developed for each system. The type of metric depends on where the system is within its life cycle and the maturity of the IT system security program. The framework facilitates tailoring metrics to a specific organization and to the different stakeholder groups in each organization.

Identify Stakeholders and Interests. Anyone within an organization is an IT security stakeholder, though some functions have a greater stake than others: CIO, program manager/system owner, security program manager, resource manager, and training/

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since April 2002

- ☐ *Techniques for System and Data Recovery*, April 2002
- ☐ *Contingency Planning Guide for Information Technology Systems*, June 2002
- ☐ *Overview: The Government Smart Card Interoperability Specification*, July 2002
- ☐ *Cryptographic Standards and Guidelines: A Status Report*, September 2002
- ☐ *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 2002
- ☐ *Security for Telecommuting and Broadband Communications*, November 2002
- ☐ *Security of Public Web Servers*, December 2002
- ☐ *Security of Electronic Mail*, January 2003
- ☐ *Secure Interconnections for Information Technology Systems*, February 2003
- ☐ *Security for Wireless Networks and Devices*, March 2003
- ☐ *ASSET: Security Assessment Tool for Federal Agencies*, June 2003
- ☐ *Testing Intrusion Detection Systems, July 2003*

human resources personnel. Metrics-related roles and responsibilities are dispersed throughout an organization. Each stakeholder needs a set of metrics that provides a view of the organization's IT security performance within their needs, for a total of no more than 5-10 metrics per stakeholder. Many IT security metrics can be created to measure each aspect of the organization's IT security. Selecting the most critical elements of the organization's IT security program during metrics prioritization will make the program manageable and successful.

Define Goals and Objectives. IT security performance goals and objectives are expressed in the form of high-level policies and requirements in many laws, regulations, policies, and guidance that describe the dimensions of an effective IT security program. These include the Clinger-Cohen Act, Presidential Decision Directives, Federal Information Security Management Act (FISMA), OMB Circular A-130, Appendix III, and NIST Federal Information Processing Standards (FIPS) and Special Publications. IT security performance goals identify the desired results of system security program implementation, while IT security performance objectives enable the accomplishment of goals. IT security metrics monitor the accomplishment of goals and objectives.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

Review Current IT Security Policies, Guidance, and Procedures. Organizations must describe control objectives and techniques that lead to accomplishing performance goals and objectives. Resources include the organization's policies and procedures, the Federal Agency Security Practices Website (http://csrc.nist.gov/fasp), and NIST SP 800-26, *Self-Assessment Guide for IT Systems* (http://csrc.nist.gov/publications), which provides many control objectives and techniques for IT systems.

Review the System Security Program Implementation. Organizations must ensure that processes and procedures are in place, existing capabilities are documented, areas for improvement are noted, existing metrics are identified, and existing data sources are available that can be used to derive metrics data. These may be documented in the following sources (and others): system security plans, OMB Plan of Actions and Milestones reports, the latest GAO and IG findings, tracking of security-related activities, and risk assessments and penetration testing results.

Establish Level of Implementation. The focus of the metrics program depends on the IT security program maturity within an organization. Most organizations are new to measuring IT security with performance metrics. They will begin by measuring the implementation level of established security standards, policies, and procedures.

Quantify Program Results. As an organization's security program implementation increases and performance data becomes readily available, metrics will focus on program efficiency and effectiveness. Examples include the timeliness of security service delivery and operational results experienced by security program implementation.

Assess Business/Mission Impact. Business impact can be measured through correlation analysis once an organization's processes are self-regenerating and measurement data gathering is transparent. Examples include business value gained or lost, or an acceptable loss estimate.

Metrics Development and Selection

The selection of metrics is critical to the success of the program. Selected metrics must use data that can realistically be obtained from existing processes and data repositories, and must measure processes that already exist and are relatively stable. Use output from standard security activities to quantify IT security performance. Potential sources include, but are not limited to, incident handling reports, testing results, network management logs and records, audit logs, network and system billing records, configuration management, contingency planning, training records, and certification and accreditation. (NIST SP 800-55, Appendix A, provides sample security metrics.) When selecting data sources, keep in mind that IT security metrics data collection must be as automated and non-intrusive as possible.

The universe of possible metrics, based on existing policies and procedures, will be quite large. Metrics must be prioritized to ensure that the final set selected for initial implementation facilitates improvement of high-priority security control implementation (as defined by an audit or risk assessment). Based on current priorities, use no more than 10-20 metrics at a time. This ensures that an IT security metrics program will be manageable.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Selected metrics should be useful and relevant. Not all data are useful, and collecting irrelevant data could cause stakeholders to lose confidence in the IT security metrics approach. To ensure the acceptable quality of data, standardize data collection methods and data repositories. Define standard data-reporting formats for events throughout the organization, and store reports in a data repository.

Once metrics are selected, obtain organizational acceptance. Validate metrics with the organization's stakeholders at headquarters and in the field. Metrics should also be vetted through appropriate approval channels. Lastly, phase out old metrics and phase in new metrics when performance targets are reached or requirements change.

Metrics Program Implementation

The iterative process of implementation consists of six phases, which, when fully executed, will ensure continuous use of IT security metrics for security control performance monitoring and improvement.

Prepare for Data Collection. Key activities of this first phase include identifying, defining, developing, and selecting the IT security metrics. After the metrics have been identified, specific implementation steps should be defined on how to collect, analyze, and report the metrics. These steps should be documented in the Metrics Program Implementation Plan.

Collect Data and Analyze Results. Phase 2 of the process involves collecting metrics data, consolidating collected data in the prescribed format conducive to data analysis and reporting (e.g., a database or spreadsheet), analyze data and identify gaps between actual and desired performance, and discover areas needing improvement.

Identify Corrective Actions. Phase 3 involves the development of a plan to close the performance gaps identified in Phase 2. Organizations must determine a range of corrective actions, select the most appropriate corrective actions, and prioritize corrective actions based on overall risk mitigation goals.

Develop Business Case. Phase 4 addresses the budgeting cycle required for obtaining resources required for implementing remediation actions identified in Phase 3. The steps involved in developing a business case are based on industry practices and mandated guidance. Steps include developing a cost model, performing a sensitivity analysis, developing the business case, and preparing a budget submission. The results of the prior three phases will be included in the business case as supporting evidence.

Obtain Resources. Phase 5 includes allocating the budget, prioritizing available resources, and assigning resources.

Apply Corrective Actions. Phase 6 of the process involves implementing corrective actions in technical, management, and operational areas of security controls. After corrective actions are applied, the cycle completes itself and restarts with a subsequent data collection and analysis. Iterative data collection, analysis, and reporting will track progress of corrective actions, measure improvement, and identify areas for further improvement. The iterative nature of the cycle ensures that the progress is monitored and the corrective actions are affecting system security control implementation in an intended way.

Conclusion

In summary, IT security metrics provide a practical approach to measuring the effectiveness of an IT security program within organizations, large and small. The results of a robust IT metrics program provide useful data for organizations to allocate information security resources and prepare performance-related reports. NIST SP 800-55 and related documents are available at our website http://csrc.nist.gov/publications.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900