USING PERFORMANCE MEASUREMENTS TO EVALUATE AND STRENGTHEN INFORMATION SYSTEM SECURITY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Performance measurements are valuable tools that produce useful, timely information about the security of information systems for the decision makers of organizations. When organizations can measure and evaluate the performance of their information security practices, they can take steps to strengthen the overall security of their information and their information systems.

Organizations that collect, analyze, and report performance-related data can use that data in many internal operations and processes. Performance measurements enable an organization to improve its accountability for information security and to bolster the effectiveness of its information security activities. In addition, the organization can use the performance data to demonstrate compliance with laws, rules, and regulations, and to provide quantifiable inputs for decisions on resource allocations. Ultimately, the organization can assess the impact that information system and program security activities have on its ability to carry out its mission, and to demonstrate that its information security practices contribute to successful operations of the organization.

To help organizations measure and evaluate the performance of their security controls, policies, and procedures, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently updated its guide to the effective use of performance measurements to improve information security.

Federal Requirements for Measuring Information System Performance

Performance measures are especially useful for federal managers who must meet regulatory, financial, and organizational requirements for their information security practices. Federal government organizations are required to measure their performance in general, and their information security performance in particular, under the provisions of legislation, including the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA). NIST has developed standards and guidelines for conducting information system security programs to help federal agencies meet these legislative reporting requirements, as well as the requirements of the Office of Management and Budget (OMB) to report annually on the status of agency information security.

Performance measurement programs help federal agencies operate more securely and more efficiently. Using performance measurement tools, agencies can link the implementation of their information security programs to the agency's strategic planning efforts, and can tie the effectiveness of their security controls to the agency's success in its mission-critical activities.

Information security measurements can provide quantifiable data for assessing individual information systems, as well as enterprise-wide information security programs. Performance measurements help agencies apply the risk management approach to information security, the process for identifying the risks to information and information systems, assessing the risks, and taking steps to reduce risks to an acceptable level. Performance measurements also support the security certification and accreditation process.

Measurements can be used throughout the system development life cycle (SDLC) to monitor the implementation of appropriate security controls. Different measures may be needed for the different activities of the SDLC, from system acquisition and development through implementation and assessment. By collecting, analyzing, and reporting appropriate security information, agencies can improve the cost-effective integration of information security into the system development effort, rather than adding costly controls later on.

NIST Special Publication (SP) 800-55, Revision 1, *Performance Measurement Guide for Information Security*

Issued in July 2008, NIST SP 800-55, Revision 1, *Performance Measurement Guide for Information Security*, was written by Elizabeth Chew, Marianne Swanson, and Kevin Stine of NIST and by Nadya Bartol, Anthony Brown, and Will Robinson of Booz Allen Hamilton. SP 800-55, Rev. 1, expands upon NIST's previous work on the measurement of information security, and supersedes NIST SP 55, *Security Metrics Guide for Information Technology Systems*, which had been issued in July 2003. The new guide also supersedes NIST Draft SP 800-80, *Guide to Developing Performance Metrics for Information Security*. NIST SP 800-55, Revision 1, is available from the NIST website http://csrc.nist.gov/publications/PubsSPs.html.

The revised guide provides specific advice on developing, selecting, and implementing information system-level and program-level performance measures, and then using the performance measures to evaluate the adequacy of existing security controls, policies, and procedures. The information helps managers decide what security controls are nonproductive and where to invest in additional information security resources. The performance measures also help managers select and prioritize security controls for continuous monitoring. The guide explains the measurement development and implementation processes and how measures can be used to adequately justify information security investments and support risk-based decisions.

One section of the guide describes the roles and responsibilities of the agency staff members who develop, implement, and manage the information security measures. While information security is the responsibility of all members of the organization, staff members such as the agency head, chief information officer, and other security officials have a direct interest in the success of the information security program, and in the establishment of an information security measurement program. Another section of the publication provides guidelines on the background and definition of information security measures, the benefits of implementation, various types of information security measures, and the factors that directly affect the success of an information security measurement program. Other topics covered in the guide include the links between information security and strategic planning, the approach and process recommended for the development of information security measures, and the factors that can affect the implementation of an information security measurement program.

The appendices to the guide provide practical examples of information security measures that can be used or modified to meet specific organizational requirements. Also included in the appendices are an extensive reference list and examples of minimum security requirements that are specified for federal agencies.

Performance Measurements and Security Controls

NIST SP 800-55, Rev. 1, advises organizations to design their performance measurement programs to support the selection and implementation of security controls. Security controls are

the management, operational, and technical safeguards or countermeasures that protect the confidentiality, integrity, and availability of an information system and its information. Decisions on security controls for information systems and information support the organization's day-to-day operations, and protect its assets and individuals.

For federal agencies, the process for selecting security controls is specified in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. Under FIPS 199 and 200, federal agencies must categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability, and then select an appropriate set of security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, to satisfy their minimum security requirements.

NIST SP 800-55, Rev. 1, uses the security controls identified in NIST SP 800-53 as a basis for developing measures that support the evaluation of information security programs. The performance measurement guide also lists other potential measures that agencies can tailor, expand, or use as models for developing other measures.

Foundation for a Successful Performance Measurement Program

Some of the factors that help shape a successful performance measurement program include the following:

· **Strong upper management support** is critical to the implementation and the success of the information security program. A strong commitment to information security within the highest levels of the management of an organization helps to protect the security program from organizational pressures and budget limitations.

· **Information security policies and procedures** that are enforced and backed by management are essential for an effective information security measurement program. Information security policies delineate the information security management structure, assign information security responsibilities, and lay the foundation needed to reliably measure progress and compliance. These policies and procedures help to assure that data is available and can be used for measurement processes.

· **Quantifiable performance measures** are necessary in order to capture and provide meaningful performance data. Quantifiable information security measures must be based on information security performance goals and objectives, and must be easily obtainable, feasible to measure, and repeatable. The information provided should demonstrate performance trends and facilitate decisions for future resource investments.

· **Periodic results-oriented analysis of the measures data** must be a consistent part of the information security measurement program. The analyses are used to apply lessons learned, improve the effectiveness of existing security controls, and plan for the implementation of future security controls to meet emerging information security requirements. All stakeholders and users must be committed to the accurate collection of data that is meaningful and useful in improving the overall information security program.

The success of the information security measurement program can be judged by the results that are produced, and by their use in supporting the decisions affecting the organization's information

security posture, its budget and personnel requests, its allocation of available resources, and the preparation of required reports on information security performance.

Developing a Performance Measures Program

Investing time early in the development of a performance measures program is more effective than retrofitting requirements once the effort is under way. Important considerations for setting up an information security performance measures program include:

- Selecting the measures most appropriate for the organization's strategy and business environment, including mission and information security priorities, environment, and requirements;
- Taking time to collect input and get buy-in from, and provide education to, all relevant stakeholders; and
- Ensuring that appropriate technical and process infrastructure is in place, including creation/modification of data collection, analysis, and reporting tools.

Two processes—measures development and measures implementation—guide the establishment and operation of an information security measurement program.

Measures Development Process

As the first step in developing performance measures, an organization should **select the measures** that are most appropriate for the organization's strategy and business environment, considering mission and information security priorities, environment, and requirements. All involved stakeholders should take part in the development of the information security measures to ensure management and organizational support for the information security performance measurement program.

The measures that are selected must yield quantifiable information, such as percentages, averages, and numbers, and the data that supports the measures should be readily obtainable. Only repeatable information security implementation processes should be considered for measurement, and the measures must be useful for tracking performance and directing resources.

The performance measures that are developed should enable the organization to identify the causes of poor performance and to adopt appropriate corrective actions. Three types of measures can be applied:

- **implementation measures** can be used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures;
- **effectiveness/efficiency measures** can be used to assess the results of the implementation of security controls; and
- **impact measures** can be used to assess the impact of information security on an organization's mission. These measures are organization-specific since each organization has a unique mission.

Information system security performance goals and objectives should be identified and documented to guide the implementation of security controls for an information system. Federal organizations may choose to represent their goals and objectives in terms of the high-level policies and requirements, laws, regulations, guidelines, and guidance which they are required to implement.

The types of measures that can realistically be obtained, and that can also be useful for performance improvement, depend on the maturity of the agency's information security program and the implementation of security controls in information systems. Different types of measures can be used simultaneously, and the primary focus of information security measures may change as security controls are implemented.

Organizations should **refer to their information security practices when developing their performance measurement programs**, including the details of how security controls should be implemented to achieve information security performance goals and objectives.

The development of performance measures should focus on gauging the security performance of a specific security control, a group of security controls, or a security program. This approach will result in measures that help the organization determine how well it is supporting its strategic objectives.

Because there are so many possible measures that are based on existing policies and procedures, the measures should be prioritized to ensure that those measures selected for initial implementation reflect the organization's existing information security program priorities. See Appendix A of NIST SP 800-55, Rev. 1, for examples of program-level and system-level measures. Organizations can tailor and adapt these measures for their information security programs.

Performance targets should be established as a component of defining information security measures. Performance targets establish a benchmark by which success is measured. Success should be based on the proximity of the measure result to the stated performance target. The mechanics of establishing performance targets differ for implementation measures and for measures of effectiveness/efficiency and impact. Setting performance targets for effectiveness/efficiency and impact measures is more complex because these aspects of security operation do not assume a specific level of performance. Organizations should determine appropriate levels of security effectiveness and efficiency, and use these levels as targets of performance for applicable measures. It may not be possible to establish performance targets until some data is collected to establish a performance baseline.

Organizations should **document their performance measures** in a standard format to ensure repeatability of measures development, tailoring, collection, and reporting activities. A standard format will provide the detail required to guide the measurement collection, analysis, and reporting activities.

Measures that are ultimately selected for implementation will be useful for measuring performance, identifying causes of unsatisfactory performance, and pinpointing improvement areas. The measures also will help the organization facilitate continuous policy implementation, effect information security policy changes, redefine its goals and objectives, and support continuous improvement.

Implementing Performance Measures for Information Security and Management Improvement

To implement an information security measurement program, organizations should apply measures for monitoring information security control performance and use the results to initiate performance improvement actions. To make continuous use of performance measures, organizations should:

· **Prepare for data collection** by identifying, defining, developing, and selecting information security measures. An implementation plan is essential to the success of the information security measurement program. The plan should contain provisions for continuous monitoring of the information security program through activities such as configuration management, information security impact analyses of changes to the information system, assessment of a subset of security controls, and status reporting.

· **Collect data and analyze results** by aggregating and consolidating the collected data, conducting gap analyses, identifying causes of poor performance, and identifying areas that require improvement.

· **Identify the potential corrective actions** for each performance issue and prioritize the actions, based on the overall risk mitigation goals. The most appropriate corrective actions should be selected for use in a full cost-benefit analysis.

· **Develop a business case**, based on industry practices and on federal guidelines, including OMB Circular A-11, the Clinger-Cohen Act, and GPRA. The business case should reflect the results of the above three steps. Agencies frequently have guidelines for building business cases and the life-cycle spending thresholds to determine which investments and budget requests require the development of a formal business case. In general, the level of effort to develop the business case should correspond to the size and scope of the funding request.

· **Evaluate budget requests** following the development of the business case, prioritize resources, and assign resources to budget requests as needed to implement corrective actions.

· **Apply corrective actions** in the security program, or in the technical, management, and operational areas of security controls. This process is used to document and monitor the status of corrective actions.

More Information

Publications developed by NIST help information management and information security personnel in planning and implementing a comprehensive approach to information security. Organizations that use performance measures to quantify the performance of their information security programs can draw upon the results of many information security activities and sources of information, including:

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires that agencies determine minimum security requirements after they have categorized their systems, and select an appropriate set of security controls to satisfy the minimum requirements. Security controls are specified in NIST SP 800-53.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance to organizations in identifying the risks to their missions brought about by the use of information systems, assessing the risks, and taking steps to reduce the risks to an acceptable level.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, recommends procedures for the security certification and accreditation of information systems. Performance measures help to support this process.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidance in selecting, specifying, and tailoring security controls that will provide an appropriate level of security, based on the organization's assessment of mission risk.

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, recommends assessment methods and procedures that can be used to determine if the security controls selected by the organization are implemented correctly, operating as intended, and meeting the security requirements of the organization. The assessment data produced can be used as data for information security measurement.

NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Controls Process*, presents common criteria that organizations can use to prioritize security activities and ensure that identified corrective actions are incorporated into the capital planning process for cost-effective information security.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, reviews the components essential to establishing and implementing effective information security programs to help managers select and implement appropriate security controls.

For information about NIST standards and guidelines that are listed above, as well as other security-related publications that support performance measurement programs, see NIST's web page http://csrc.nist.gov/publications/index.html.

OMB directives and guidelines are available at http://www.whitehouse.gov/omb/.

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.