ITL BULLETIN FOR JUNE 2010

HOW TO IDENTIFY PERSONNEL WITH SIGNIFICANT RESPONSIBILITIES FOR INFORMATION SECURITY

Mark Wilson
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Effective management and proper use of information technology (IT) systems are key factors in protecting the security of an organization's information and its systems. Federal organizations have specific responsibilities to conduct awareness and training programs and to assure that staff members understand their information security responsibilities and the organization's policies.

Under the Federal Information Security Management Act (FISMA) of 2002, the head of each federal agency is directed to delegate to the Chief Information Officer (CIO) the authority to designate a senior agency information security officer – known in many agencies as the Chief Information Security Officer (CISO). The CISO is responsible for, among other duties, "training and overseeing personnel with significant responsibilities for information security," also known as significant information security responsibilities (SISRs).

To help agencies identify those individuals with SISRs, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) is planning to update NIST Special Publication (SP) 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003). This bulletin provides interim assistance to federal organizations until the revision of NIST SP 800-50 has been completed.

The Computer Security Act of 1987 first codified the requirement to train people who have information security responsibilities. Some departments and agencies had been identifying and training personnel with information security responsibilities for years and even decades before a federal law specified that task.

Ensuring that personnel receive the information security training that they need to perform their jobs is challenging and can easily be the topic of spirited discussions within information security program offices and with internal and/or external auditors. Users, for example, could cause significant harm by misusing an application. Training for users is generally known as awareness training under FISMA, and awareness training initiatives for users are managed by the Office of Management and Budget and the Department of Homeland Security.

While it can be a daunting task to identify all personnel in an organization who have *some* responsibility for information security, it seems to be even more challenging to identify those personnel with *significant* responsibilities. In identifying personnel with SISRs, it is important that the correct personnel be identified. Identifying all personnel with security responsibilities "above the rank of user" would include everyone in the organization who has any information security responsibility beyond the user population. This could result in a significant resource drain for the organization. However, the resource drain could be manageable if the training is scaled to role, such as the following examples:

- develop and teach just that amount of information security-related material needed in a course or module;
- develop the material at the proper level of complexity for the intended audience; and
- develop training for each role that has information security responsibilities.

Key to this effective use of limited resources is ensuring that training is provided first to those who need it most. As discussed in NIST SP 800-50, a needs assessment can identify the groups of individuals and those people in specific roles who need security training.

Train All With Information Security Responsibilities

Stating that personnel above the rank of user who have *any* information security responsibilities *are* those with SISRs *may* be the correct solution for an organization, depending on its mission, the robustness of its information security program, and how it manages risk across the organization. On the other side of the coin, if an organization pays lip service to the requirement and identifies too few personnel in a "check the box" solution to the FISMA requirement, personnel who *actually do have* significant security responsibilities will not have the information security training that they need to protect the organization's information and information system resources. If this issue is left unresolved, personnel who have *some*, but not organization-determined *significant*, information security responsibilities will not have the finely honed skill sets that they need to meet their information security responsibilities. Therefore, CISOs, supervisors, managers, information owners, and system owners should insist that *all* personnel with responsibilities for information security – beyond the organization's information system user population – are trained to the degree necessary for them to perform their security tasks in a satisfactory manner, whether they have *some* or *significant* information security responsibilities.

> CISOs, supervisors, managers, information owners, and system owners should insist that *all* personnel with responsibilities for information security are trained to the degree necessary for them to perform their security tasks in a satisfactory manner, whether they have *some* or *significant* information security responsibilities.

If Not All, How To Identify Some For Training?

In many departments and agencies, resources available for training, including information security training, are rarely sufficient to adequately train all personnel. If an organization cannot implement this "train all who have information security responsibilities (beyond what is expected of users)" approach, then selecting and evaluating criteria from appropriate sources (e.g., regulations, security-related standards and guideline documents, personnel or human resource documents) could be helpful in identifying just those personnel with organization-determined SISRs.

The challenge associated with identifying personnel with organization-determined SISRs seems to be a matter of selecting some but not all personnel who have some additional nonuser information security responsibilities. Naturally, when asked to select these personnel, the question arises: What criteria should we use to make these selections and where can we find evidence of security responsibilities?

At the end of the day, however, it is the responsibility of each organization using this approach to determine what is *significant* with regard to information security responsibilities, in light of the need to protect the information resources that support mission-critical functions. Involvement, support, and commitment by executive or senior management-level personnel, including those responsible for enterprise-wide risk management, must be sought and secured for the organization-determined SISRs process. Determining who has SISRs is the crucial first step that will allow the organization to better use its scarce information security training resources where they are most needed.

The following two sections offer some criteria and sources of criteria that organizations can use to determine who has organization-determined SISRs.

Criteria to Consider

The following seven criteria may help an organization determine who has SISRs. Reviewing and analyzing these criteria may result in the selection and blending of several criteria to form an organization-specific approach. This blended criteria approach may serve the organization better than determining SISRs on the basis of just one factor. Organizations may discover that they have additional criteria that can be reviewed and analyzed in this determination process.

Position Sensitivity – Position sensitivity is identified in each position description and can be used to help identify whether the incumbent has SISRs. The position designation (Special-Sensitive, Critical-Sensitive, Noncritical-Sensitive, High Risk, Moderate Risk, Low Risk), access level, and type of investigation required for a position are indicators that can be used in the decision-making process. Tied to position sensitivity are issues related to IT responsibilities and public trust positions. These two "sub-criteria" should also be reviewed.

Role – The prevailing tendency in some of the federally focused information security training and workforce development initiatives is to suggest that people in specific information security roles have SISRs by virtue of role alone. For example, it may be easy to justify that personnel serving in roles such as Agency Head, Chief Information Officer (CIO), and CISO (or Senior Agency Information Security Office [SAISO]) have SISRs since FISMA clearly states that these individuals are directly responsible for the organization's information security program. It may also be relatively easy to state that there are other "usual suspects" whose role titles place them in the SISRs camp. These usually include System Administrator, Network Administrator, Information Owner, System Owner, Auditor, Assessor, Incident Response Coordinator or Analyst, Information System Security Officer, Risk Executive, Security Administrator, Security Engineer, and Security Architect.

However, a potential pitfall in selecting personnel for SISRs designation by role lies in unintentionally grouping high- and low-impact roles. For example, a System Administrator for a low-impact system will be consolidated with a System Administrator for a high-impact system if the sole factor for determination of SISRs is role. This could lead to an imbalance of the training provided, if all System Administrators attend the same training course or module. This may also result in spending scarce training dollars on individuals who have limited impact on overall security.

Continuing with the example of a System Administrator, understanding the tasks within a role is critical to determining SISRs. While some System Administrators may only add and remove accounts or perform other relatively minor tasks, other System Administrators might be responsible for configuration management, installing patches, performing backups, reviewing audit records, etc. The tasks performed within a role might be a better indicator for SISRs than role alone.

Another significant issue with using role as the sole determinant of SISRs comes to light in the list of roles contained in an Office of Personnel Management (OPM) Regulation (5 CFR Part 930, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*). Organizations need to understand the impact on their training resources if and when personnel in the roles contained in the OPM regulation are determined to have SISRs. This is not to say that the OPM regulation should be ignored. Role may be analyzed with other criteria listed in 5 CFR Part 930 and a hybrid approach developed that meets the intent of the OPM regulation while effectively managing and maximizing the organization's training resources. The OPM regulation is discussed in greater detail in the next section on sources of criteria.

Impact Level – Instead of using role as the sole determinant of SISRs, the impact level assigned to information and information systems should also be considered. Organizations may opt to state that personnel with information security responsibilities for information and information systems declared to be "moderate" and "high" (or just "high") impact have SISRs. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), NIST SP 800-60 Volume I, Revision 1, *Guide for Mapping Types of*

Information and Information Systems to Security Categories (August 2008), and NIST SP 800-60, Volume II, Revision 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories* (August 2008), provide detailed information about impact levels and categorization. Analysis and blending of role and impact level criteria can provide organizations with a better method to determine SISR than viewing each separately.

Greatest Vulnerabilities – This criterion allows an organization executive, Risk Executive, CISO, or other senior managers to ask: Where are our vulnerabilities or weaknesses? Who has the ability or responsibility to fix them? Are the problems being fixed or not? Once these questions have been answered, and if a lack of progress is due to a lack of training of people critical to the reduction of the vulnerabilities or weaknesses, the organization can designate them as having SISRs and prioritize the necessary training. Vulnerabilities or weaknesses can be found in audit reports, information security plans, plans of action and milestones (POA&Ms), and in the results of continuous monitoring efforts. This factor is not the same as the impact-level criteria because the impact level is based upon the FIPS 199 and SP 800-60 categorization. The greatest vulnerability factor is more in line with a risk-based approach.

Security Controls – Those personnel with the responsibility to select, implement, and assess system security controls may be deemed to have SISRs. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009), and SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (July 2008), contain titles or roles of personnel who are directly involved in these tasks. Security controls, analyzed in conjunction with roles and impact levels, can help organizations identify the correct set of personnel.

Risk Management – Those personnel with the responsibility for risk management of systems may be deemed to have SISRs. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), contains a significant number of titles or roles of personnel who are directly involved with risk management and the Risk Management Framework (i.e., categorize information systems, select security controls, implement security controls, assess security controls, authorize information systems, monitor security controls). Risk management, analyzed in conjunction with roles, impact levels, and greatest vulnerabilities, can help organizations identify personnel with SISRs.

Security Program Management – Those personnel with the responsibility to implement, manage, maintain, and audit information security programs may be considered to have SISRs – from executive-level "thirty-thousand foot" perspectives to system-, application-, and network-level management. NIST SP 800-100, *Information Security Handbook: A Guide for Managers* (October 2006), contains a significant number of titles or roles of personnel who are directly involved with managing the many aspects of an organization's information security program. These personnel, or many of them, may be identified as having SISRs.

Sources of Criteria

The following seven sources of criteria may help an organization determine who has SISRs. Organizations may discover that they have additional sources of criteria that can be included in this determination process. It is a coincidence that seven criteria and seven sources of criteria are listed. There is no presumed one-to-one correlation between them. However, position sensitivity and IT-specific responsibilities can be found in position descriptions, for example, and roles can be found in a number of sources, including the NIST standards and guidelines cited in sources below.

OPM Regulation (5 CFR Part 930) – This OPM requirement, part of the U.S. Code, issued in June 2004, requires agencies to train the following personnel:

- Executives;
- Program and functional managers;
- CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers); and
- IT function management and operations personnel.

OPM Regulation (5 CFR Part 930) builds on the information security awareness training and the (role-based) training requirements, which are contained in FISMA. It can be said that this OPM regulation answers the often-asked question: Who has SISRs? However, if an organization identifies personnel using only the criteria provided, it will result in role being the only factor by which personnel with SISRs are determined. As stated in the Criteria to Consider section above, determining who has SISRs by role alone seems to be a straightforward approach, but this method has potential pitfalls, especially if an organization does not have the resources to train all their personnel in those roles identified in the OPM regulation.

Position Descriptions – When determining who has SISRs, reviewing existing position descriptions (PDs) may bring to light language that suggests that the incumbent's job involves information security work that can be categorized as significant. Similarly, when creating a new PD, organizations can take the opportunity to state in the PD that the incumbent does (or does not) have SISRs, and can document those tasks or groups of tasks that makes this so. Organizations can also establish a policy that position descriptions will contain a phrase that states whether the incumbent does or does not have SISRs.

Performance Plans – These plans may contain detailed information related to management's expectations of the individual's performance of information security responsibilities which can help in the determination of SISRs. A person, such as the individual's supervisor or CISO (or designee), should be able to determine if the performance plan indicates that the incumbent has SISRs. Similarly, when performance plans are generated and/or updated, management can take that opportunity to add language to make it clear if the individual does or does not have SISRs. Organizations

can also establish a policy that performance plans will contain a phrase that states whether the incumbent does or does not have SISRs.

Individual Development Plans – While the focus of an individual development plan (IDP) is to document management's expectations of an individual relative to the training (and/or education) required to carry out their job, a review of an existing IDP may help to determine whether the incumbent has SISRs.

Security Plans – Security plans should clearly identify personnel with information security responsibility for general-support systems and major applications. The titles of some of these personnel or roles are included in NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems* (February 2006). Security plans, combined with other criteria, can help organizations identify the correct set of personnel.

Contingency Plans – Contingency plans, like security plans, should clearly identify personnel with responsibility for planning for, responding to, and recovering from disruptions of information and information system-related resources. Draft NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems* (October 2009), contains titles or roles of those personnel who are directly involved in these tasks. Contingency plans, combined with other criteria, can also help organizations identify the correct set of personnel.

Inspectors' Reviews – Departments and agencies can use input from audit reports conducted by internal and/or external auditors to fine-tune their process for determining who has SISRs, or to modify the number of personnel designated to have SISRs, based on auditor recommendations with regard to criteria selection. However, a more proactive approach would be to engage auditors during an audit to discuss the organization's current approach to determine which personnel have SISRs, and better yet, to involve the internal audit function in the initial and ongoing determination process. While audit findings may provide an authoritative "answer" to any lingering SISR determination issue, waiting until an audit report recommends changes to the organization's current and perceived appropriate approach may not provide the organization much leeway. Instead, an organization might feel compelled to make an unpopular change to its process, rather than to keep open a finding or several findings. Organizations should consider including internal auditors in the initial SISR determination process as well as in ongoing efforts, and/or working with internal and external auditors during an audit to discuss potential conflicting viewpoints and reasonable solutions, rather than waiting for post-inspection reports.

Workforce Planning – One Approach to Determine SISRs

Workforce planning is an effort undertaken by an organization in an attempt to identify the human resource needs to accomplish the mission; to determine what knowledge, skills, and experience are required to get the job done; and to determine how large and what type of workforce is required to provide that mix of knowledge, skills, and

experience. Key aspects of workforce planning include: 1) identifying competencies needed in the workforce, both at present and in the future; 2) selecting and developing the workforce; 3) anticipating change rather than being surprised by events; and 4) addressing present and anticipated workforce issues.

A workforce planning effort, with a focus on the information security workforce, might include analysis of:

1) core functions (i.e., manage, acquire, design and develop, implement and operate, review and evaluate); and

2) core positions (e.g., those personnel who perform some or any information security work, beyond the organization's user population).

A study that identifies the following information for each person in each core position or role can yield valuable data that can be expressed in a matrix (with core positions or roles listed along the y-axis, and core functions or responsibilities listed along the x-axis).

1) time requirements to perform information security tasks (e.g., 0-30% = low, 30%-70% = medium, 70%-100% = high); and

2) responsibility requirements (e.g., low, medium, high).

Each intersection of a core position (role) with a core function (responsibility) is a cell. Each cell, after data gathering (via surveys and/or interviews), will contain the time requirement expressed by "low," "medium," or "high," and the responsibility requirement, also expressed by "low," "medium," or "high." Each value should be separated by "/" so the contents of each cell appears to be (time requirement value) / (responsibility requirement value) or (time requirement value) "over" (responsibility requirement value).

Analysis of the results of this data-gathering effort, by studying the "time over responsibility" values relative to the select number of core functions that make up the information security-related workload of each core position, can show whether that position or individual has SISRs.

The following graphic captures this workforce planning effort relative to the information security workforce, and focused on determining who has SISRs. Organizations may use this approach, modify it to meet their needs, or develop their own approach.

	Manage	**Acquire**	**Design & Develop**	**Implement & Operate**	**Review & Evaluate**	**SISRs ?**
	Time/ Resp	Time/ Resp	Time/ Resp	Time/ Resp	Time/ Resp	
Executives						
Director						Y/N
Deputy Director						Y/N
Program/ Functional Managers						
Division Chief						Y/N
Branch Chief						Y/N

Key:

- "Time" = Time requirements expressed as low, medium, or high
- "Resp" = Responsibility requirements expressed as low, medium, or high
- "SISRs" = Significant information security responsibilities

Players in the SISR Decision-Making Process

Some organizations have left the determination of who has SISRs up to the CISO's office. In some cases, a single individual – even the one person responsible for developing information security training – is tasked with making this determination. While the CISO's office should be involved in helping an organization determine who has SISRs, other personnel in the organization could be invited and encouraged to be stakeholders in the process. A team could be assembled, including representatives from human resources, labor unions, the CIO's office, physical security, Office of General Counsel, internal audit, and functions that perform critical missions of the organization. System owners and information owners related to these critical missions could be invited. Organization size, culture, homogeneity, and other factors will determine if a team approach is appropriate to determine who has SISRs.

These stakeholders should: 1) decide what criteria will be used to determine who has SISRs, and 2) lead the effort to identify individuals, groups of individuals, or roles who match the chosen criteria. The training needs of these individuals or groups of individuals should then be identified using the guidance contained in NIST SP 800-50.

Conclusion

An ineffective SISR determination process will likely result in some personnel receiving unneeded training, while those who truly need additional training may not receive it. This approach will likely not allow an organization to adequately protect the information and information systems that support its mission(s). Nor will this approach help remedy the ongoing "people problem," in that the gap will not be closed that exists between current insufficient knowledge, skills, and abilities and the level of knowledge, skills, and abilities that are needed among the information security workforce.

With senior management involvement, support, and commitment, the determination of who has SISRs will not become a "check the box" exercise, done simply because a requirement exists that must be satisfied, but will be completed in the spirit of the requirement and for the benefit of the organization. Determining who has SISRs is the crucial first step that allows the organization to focus its information security training resources where they are most needed.

For More Information

For information about NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

Office of Personnel Management Regulation, 5 CFR Part 930, *Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*, is available at http://www.opm.gov/fedregis/2004/69-061404-32835-a.htm.

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.