# Security Program Management

* * * * * * * * * * * * * NOTE * * * * * * * * * * * * * * * * *

This file is a DRAFT chapter intended to be part of the NIST Computer Security Handbook. The chapters were prepared by different parties and, in some cases, have not been reviewed by NIST. The next iteration of a chapter could be SUBSTANTIALLY different than the current version. If you wish to provide comments on the chapters, please email them to roback@ecf.ncsl.gov or mail them to Ed Roback/Room B154, Bldg 225/NIST/Gaithersburg, MD 20899.

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *

DRAFT DRAFT DRAFT

## Purpose of Security Program Management

Organizations should view information resources security as a management issue, treated like any other item of strategic importance. Information and information processing assets (computers) are a critical component of most organizations' ability to perform their mission and business functions. The purpose of a security program is to protect these vital assets. Accordingly, ensuring security requires the development of a comprehensive management approach that integrates fundamental protection considerations.

In general, organizations divide the management of security into two major types of activities: 'Central' and 'System' activities. Central security activities are the tasks carried out on behalf of the organization such as policy development, compliance reviews, and oversight. System level security activities are those tasks performed by functional management, 'end-users,' and computer systems personnel to secure a particular computer system. These tasks include performing risk analyses, installing safeguards, and administering security.

The purpose of this chapter is to present security as a management function. An organization-wide approach to security program management is presented. Because organizations differ vastly in size, complexity, management styles, and culture, it is not possible to describe one ideal security program. However, this chapter does describe some of the features and issues common to most organizations.

Note: This chapter addresses security program management, not the various activities such as risk analysis or contingency planning, that make up an effective security program.

# Structure of a Security Program

Most organizations have security programs which are distributed throughout the organization with different elements performing different functions. While this is a desirable management structure, the distribution of the security function in many organizations is haphazard, based on chance. Instead, the distribution of the security function should be the result of a planned and integrated management philosophy.

Figure 5-1 shows a management structure based on that of an actual Federal agency. The agency in the example has five major units each of which has several large computer facilities. Each facility runs multiple applications. This type of organization needs to manage security at the agency level, the unit level, the computer facility level, and the application level.

figure 5-1 (see attachment)

There are many benefits to managing computer security at multiple levels. Each level contributes to the overall security program with different types of expertise, authority and resources. In general, the higher levels (such as the Headquarters or Unit Levels in the Agency described above) have more clout, better ability to set policy, to see the "big picture," and to enforce. On the other hand, the systems levels (such as the computer facility and applications levels) are more familiar with the technical and procedural requirements and problems of the systems and the users. The levels of security program management are complementary; each helps the other be more effective.

Recognizing that each organization will have its own structure, this chapter divides security program management into two levels: the central level and the system level. The central security program address the overall management of security within an organization or a major component of an organization. The system level security program addresses the management of security for a particular information processing system. Most organizations have at least these two levels and many organizations, such as the example above, have several more levels.

# Central Program

The purpose of a central security program, as stated above, is the overall management of security within an organization. In the federal government, the organization could consist of a department, agency, installation or other major operating unit.

A central security program provides two quite distinct types of benefits. The first type is increased efficiency and economy of security throughout the organization.

The second type is the ability to provide enforcement and oversight. Both of these benefits are in keeping with the purpose of the Paperwork Reduction Act, as implemented in OMB Circular A-130.

The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information management activities in an efficient, effective, and economical manner.... Agencies shall assure an adequate level of security for all agency automated information systems, whether maintained in-house or commercially. (Section 5; Appendix III, Section 3.)

OMB Circular A-130, therefore, requires that Federal agencies have computer security programs.

## Efficiency and Economy

A central security program can manage or coordinate the use of security-related resources across the entire organization. The most important of these resources are normally information and financial resources.

It is a truism to discuss both the overload of information available to modern managers and the utility of well-managed information. Most organizations, however, have trouble collecting information from myriad sources and effectively processing and distributing it within the organization. This section discusses some of the sources and uses of security information.

Within the Federal government, many organizations such as the Office of Management and Budget, the General Services Administration, and the National Institute of Standards and Technology provide information on computer, telecommunications, and information resources. This information includes security-related policy, regulations, standards, and guidance. A considerable portion of the information is channelled through the Senior Designated Official for each agency (see FIRMR Part 201-2). Agencies are expected to have mechanisms in place to distribute information received by the senior designated official.

Security-related information is also available from private and Federal professional societies and groups. These groups will often provide the information as a public service, although some private groups charge for it. However, even for information that is free or inexpensive, the costs associated with personnel gathering the information can be expensive. For instance, it is not cost effective for an organization to send everyone to every security conference.

Internal security-related information, such as procedures which worked, or did not work, virus infections, security problems and solutions also need to be shared within an organization. Often these issues are specific to the operating environment and culture of the organization.

A security program at the organization level should provide a way to collect the internal security-related information and distribute it as needed throughout the organization. Sometimes an organization can also share this information with external groups. Figure 5-2 shows a simplified version of this flow of information. For example, in most organizations, external interaction occurs at both the organization and system levels. However, the central security program should be aware of the interaction at the system level to aid in the sharing of information and to make sure that the organization has identified and tapped all important sources.

Another use of an organization-wide conduit of information is the increased ability to influence external and internal policy decisions. If the central security program office can speak for the entire organization, then it is more likely to be listened to by upper management and external organizations. However, to be effective, there must be excellent communication between the system level security programs and the organization level. For example, if an organization were considering consolidating its mainframes into one site (or considering distributing the processing currently done at one mainframe site), the central security program personnel could discuss the security implications and costs or cost savings. If the central security program knows the actual costs of providing for multiple contingency options and other security factors, then the central security program can speak authoritatively during policy discussions.

figure 2 (see attachment)

Beside being able to help an organization use information more cost effectively, a security program can also help an organization better spend its scarce security dollars. Organizations can develop expertise and then share it, reducing the need to contract out repeatedly for similar services. The following example is based on the Agency in Figure 1:

Each of the agency five operating units developed a separate specialized expertise, and the organization as a whole shares the increased knowledge base. Operating Unit #1, which uses primarily UNIX, developed skills in UNIX security. Operating Unit #2, which uses primarily MVS, but has one UNIX machine, concentrated on MVS security but relies on Unit #1's skills for their one UNIX machine.

The central security program can also develop its own areas of expertise. Many security programs develop skills in contingency planning and risk analysis in order to help the entire organization perform these vital security functions.

Besides allowing an organization to share expertise, and therefore save money, a central security program can also use its position to negotiate discounts based on volume purchasing of security hardware and software.

### Oversight

Besides helping an organization to improve the economy and efficiency of its security program, the central security program can also serve as an independent evaluation or enforcement function. The purpose of this oversight role is to ensure that organizational subunits are cost-effectively securing resources and following applicable policy. While the Office of Inspector General (OIG) and external organizations, such as the General Accounting Office (GAO), also perform a valuable evaluation role, they operate outside the regular management channels. See Chapter XXXX for a further discussion of the role of independent audit.

There are several reasons for having an oversight function within the regular management channel. First, since security is a part of the regular management of organization resources, it is a responsibility which cannot be abdicated to another organization. Second, it allows an organization to find and correct problems without the potential embarrassment of an IG or GAO audit or investigation. Third, the organization may find different problems than an outside organization. The organization better understands its assets, threats, systems and procedures than an external organization, and people involved in the audit may share information within the organization they would withhold from an outsider.

## Central Security Program Elements & Considerations

In order for a central security program to be effective, it must be an established part of organization management. If system managers and applications owners do not need to consistently interact with the security program, then it can become an empty token of upper management's "commitment to security." The following paragraphs describe some of the means of becoming an established program and some of the indicators that a program has achieved this goal.

Stable Program Management Function. A well-established program will have a program manager recognized within the organization as the IT security program manager. In addition, the program will be staffed with able personnel and links will be established between the program management function and IT security personnel in other parts of the organization. A security program is a complex function that needs a stable base from which to direct the management of security resources, such as information and financial resources. The benefits of an oversight function cannot be achieved if the security program is not recognized within an organization as having expertise and authority.

Stable Resource Base. A well-established program will have a stable resource base in terms of personnel, funds, and other support. Without a stable resource base, it is impossible to plan for and execute programs and projects effectively.

Published Mission and Function Statement. A published mission statement grounds the IT security program into the unique operating environment of the organization. The statement clearly establishes the function of the IT security program and defines responsibilities for both the IT security program and other related programs and entities. Without such a statement, it is impossible to develop evaluation criteria for the effectiveness of the IT security program.

Existence of Policy. Policy, as discussed in Chapter XX, provides the foundation for the IT security program and is the means for documenting and promulgating important decisions about IT security. In addition to policy, a central security program should also publish standards, regulations, and guidelines which implement and expand on policy. These are also discussed in Chapter XX.

Long-Term Security Strategy. A well-established program explores and develops long-term strategies to incorporate security into the next generation of information technology. Since the IT field moves rapidly, it is essential to plan for future operating environments.

Compliance Program. An IT security program must address whether the organization is in compliance with national policies and requirements as well as organization specific requirements. National requirements include those prescribed under the Computer Security Act of 1987, OMB Circular A-130, the FIRMR, and FIPS PUBs.

Liaison with Other Offices Within the Organization. There are many offices within an organization that potentially affect IT security. The IRM and traditional security offices (such as personnel, industrial, or physical security) are the two most obvious. However, IT security often overlaps with other offices such as Safety, Reliability, and Quality Assurance, Internal Control or the Inspector General. An effective program must have established relationships with these groups in order to integrate security into the management of an organization. The relationships must be more than just passing information; the offices must influence each other.

Example: Agency IRM Offices engage in strategic and tactical planning for both information and information technology, in accordance with the Paperwork Reduction Act and OMB Circular A-130. Security should be an important component of these plans. The security needs of the agency should affect information technology choices and the information needs of the agency should effect the security program.

Liaison with External Groups. As discussed in this chapter, there are many sources of security information, such as NIST's Computer Security Program Managers' Forum, computer security bulletin board, and the Forum of Incident Response and Security Teams (FIRST). An established program will be

knowledgeable of and take advantage of external sources of information. It will also be a provider of information.

## System Level Security Program

The purpose of the system level security program is to ensure appropriate and cost-effective security for each system. A central security program, as explained above, addresses the entire spectrum of information resources security for an organization. The system level security programs implement security for each information system. This includes influencing decisions about what controls to implement, purchasing and installing technical controls, day-to-day security administration, evaluating system vulnerabilities, responding to security problems, etc. It encompasses all the areas discussed in this Handbook.

The system level security program is the advocate for security. The system security officer is the person who must raise the issue of security and help work on solutions. For example, has the data owner made clear the security requirements of the system? Will bringing a new function online impact security? Is the system vulnerable to hackers and viruses? Has the contingency plan been tested? Raising these kinds of questions will force system managers and data owners to identify their security requirements and ensure that they are being met.

## System Level Security Program Elements and Considerations

Like the central security program, there are many factors which influence how successful a system level security program is. Many of these are similar to the organization level. This section addresses some additional considerations.

Integration with System Operations. The system level security program must consist of people who understand the system. For security management to be effective, it must be integrated into the management of the system. Effective integration will assure that system managers and data owners consider security in the planning and operation of the system. The system level security program manager must be able to participate in the selection and implementation of appropriate technical controls, security procedures, and must understand system vulnerabilities. The system level security program must be able to respond to system security problems in a timely manner.

For large systems, such as a mainframe data center, the security program will often include a manager and several staff positions in such areas as access control, user administration, and contingency and disaster planning. For small systems, such as an office-wide LAN, the security program may be an adjunct responsibility of the LAN administrator.

Separation From Operations. A natural tension exists between security and operational elements. In many instances, operational components, which tend to be far stronger entities, seek to resolve this tension by having the security program embedded in IT operations. The typical result of this organizational strategy is a security program that lacks independence, has minimal authority, receives little management attention, and has few resources. As early as 1978, the General Accounting Office (GAO) identified this organizational mode as one of the principal basic weaknesses in federal agency IT security programs. While it is possible for central security programs to face this problem, system level programs face this problem more often.

This conflict between the need to be a part of system management and independence has several solutions. The basis of many of the solutions is a link between the security program and upper management, often through the central security program. A key requirement of this setup is the existence of a reporting structure which does not include systems management. Another possibility is for the security program to be completely independent of system management and report directly to higher management. There are many hybrids and permutations such as co-location of security and systems management staff, but separate reporting (and supervisory) structures. Figure 5-3 presents an example of placement of the security program within a typical Federal agency.

Figure 5-3 (see attachment)

System Security Plans. The Computer Security Act mandated that agencies develop computer security and privacy plans for sensitivie systems. The purpose of this plan is to ensure that each Federal and Federal interest system has appropriate and cost-effective security. System level security personnel should be in a position to develop and implement security plans. Chapter XX, Life Cycle, discusses the plans in more detail.

## Interaction Between the Central and System Level Security Programs

The need for central and system level security programs to work together has been a major theme of this chapter. A system level program that is not integrated into the organizational program may have difficulty influencing significant areas affecting security.

The system level security program implements the policies, guidance, and regulations of the central security program. The system level office also learns from the information disseminated by the central program and uses the experience and expertise of the entire organization. The system level security program furthers distributes information to systems management as appropriate.

The communication, however, is not one way. The system level security program tells the central office about needs, problems, incidents, and solutions. The organization shares experience and expertise. The central security program can then represent the system to the organization's management and to external agencies and advocate programs and policies beneficial to the security of all the systems.

## Interdependencies

Policy. Policy is the basis for the IT security program. The central security program(s) normally produces policy concerning general and organizational security issues. However, the system level security program normally produced some issue-specific policies and policies affecting only one system. Chapter XX, Policy, provides additional guidance.

Life Cycle Management. The process of securing a system over its life cycle is the role of the system level security program. See Chapter XX Life Cycle Management.

Independent Audit. The independent audit function described in Chapter XXXX should be complementary to the compliance function performed by a central security program.

General. The general purpose of the IT security program, to improve security, causes it to overlap with every control. Most controls will be addressed at the policy, procedural, or operational level by the central or system security program.

## Cost Considerations

Section XXXX discussed how an organization-wide security program can manage security resources, including financial resources, more effectively. The cost considerations for a system level security program are more closely aligned with the overall cost savings in having security.

The most significant cost of a security program is personnel. In addition, many programs make frequent and effective use of consultants and contractors. A program also needs funds for training of personnel and travel to perform oversight, information collection and dissemination activities, and meet with personnel at other levels of security management.

## References

CSI Course: Managing an Organization Wide Security Program

OMB Circular A-130, especially Main Body and Appendix III

FIRMR 201-2 (Designated Senior Officials)

Information Resources Security: What Every Federal Manager Should Know. GSA IRMS

"Security Policy and Organization Structure" in Information

Security for Managers. Chapter 1.2

Computer Security Act of 1987

GAO Report LCD 78-123, "Automated Systems Security-Federal

Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data"