SECURITY PROGRAM MANAGEMENT

CSL BULLETIN
August 1993

This bulletin discusses the establishment and operation of a security program as a management function and describes some of the features and issues common to most organizations. OMB Circular A-130, “Management of Federal Information Resources,” June 25, 1993, requires that federal agencies establish computer security programs. Because organizations differ in size, complexity, management styles, and culture, it is not possible to describe one ideal security program.

Structure of a Security Program

Security programs are often distributed throughout the organization with different elements performing different functions. Sometimes the distribution of the security function may be haphazard, based on chance. Ideally, the structure of a security program should result from the implementation of a planned and integrated management philosophy.

Figure 1. shows a management structure based on that of an actual federal agency. The agency consists of five major units, each with 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.

Managing computer security at multiple levels brings many benefits. 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) better understand the organization as a whole, exercise more authority, set policy, and enforce compliance with applicable policies and procedures. On the other hand, the systems levels (such as the computer facility and applications levels) know the technical and procedural requirements and problems. The levels of security program management are complementary; each helps the other be more effective.

Most organizations have at least two levels of security management. The central security program addresses the overall management of security within the organization or a major component of the organization, including such activities as policy development and oversight. The system level security program focuses on the management of security for a particular information processing system. This function includes activities such as selecting and installing safeguards and may be performed by users, functional managers, or computer systems personnel.

Central Security Program

A central security program which manages or coordinates the use of security-related resources across the entire organization provides these benefits:

Efficiency and Economy

A central program can disseminate security-related information throughout the agency in an efficient and cost-effective manner. Information to be shared includes policies, regulations, standards, training opportunities, and security incident reports. Internal security-related information, such as procedures which worked or did not work, virus infections, security problems and solutions also should be shared within an organization. Often these issues are specific to the operating environment and culture of the organization.

Another use of an organization-wide conduit of information is the increased ability to influence external and internal policy decisions. A central security program office which speaks for the entire organization is more likely to be listened to by upper management and external organizations.

Also the central organization can share information with external groups as illustrated in Figure 2. Since external interaction occurs at both the organization and system levels, a central security organization should be aware of the interactions at the system level to exploit all important sources.

Sources of Security Information

NIST: Federal Information Processing Standards (FIPS), NIST
Publication List 91, Computer Security Publications,
and the NIST Computer Security BBS.
GSA: Federal Information Resources Management Regulation
(FIRMR) Parts 201-20 and 201-39.
OMB: OMB Circular A-130, Management of Federal Information
Resources, June 25, 1993
FIRST: Forum of Incident Response and Security Teams for
security incident-related information.

The central security program assists the organization in spending its scarce security dollars more efficiently. Such organizations can develop expertise and share it, reducing the need to contract out repeatedly for similar services, such as contingency planning or risk analysis. The expertise can be resident in the central security program or distributed throughout the system-level programs. Another advantage of a centralized program is its ability to negotiate discounts based on volume purchasing of security hardware and software.

Oversight

A central security program serves as an independent evaluation or enforcement function to ensure that organizational subunits secure resources cost-effectively and follow applicable policy. With a central oversight function, organizations can take responsibility for their own security programs, identify and correct problems before they become major concerns, and avoid external investigations and audits.

Elements of a Central Security Program

_A program manager should be selected as the information technology (IT) security program manager. The program should be staffed with able personnel and linked to the program management function and IT security personnel in other parts of the organization. The security program requires a stable base in terms of personnel, funding, and other support. Additionally, the benefits of an oversight function cannot be achieved if the security program is not recognized within an organization as having expertise and authority.

To be effective, a central security program must be an established part of organization management. If system managers and applications owners do not consistently interact with the security program, it becomes an empty token of upper management's "commitment to security."

_A security policy provides the foundation for the IT security program and is the means for documenting and promulgating important decisions about IT security. The central security program should also publish standards, regulations, and guidelines which implement and expand on policy.

_A published mission and function statement grounds the IT security program into the unique operating environment of the organization. The statement should clearly establish the function of the IT security program, define responsibilities for the IT security program and other related programs and entities, and provide the basis for evaluating the effectiveness of the IT security program.

_Long-term strategies should be developed to incorporate security into the next generation of information technology. Since the IT field moves rapidly, planning for future operating environments is essential.

_A compliance program enables the organization to assess conformance with national and organization-specific policies and requirements. National requirements include those prescribed under the Computer Security Act of 1987, OMB Circular A-130, Federal Information Resources Management Regulations (FIRMR), and Federal Information Processing Standards (FIPS).

_Liaisons should be established with internal groups including the information resources management (IRM) office and traditional security offices (such as personnel or physical security), other offices such as Safety, Reliability, and Quality Assurance, Internal Control, and the agency Inspector General. These relationships facilitate integrating security into the management of an organization. The relationships must be more than just sharing information; the offices must influence each other to assure that security is considered in agency plans for information technology.

_Liaisons should be established with external groups to take advantage of external information sources and to improve the dissemination of this information throughout the organization.

System Level Security Program

While a central security program addresses the entire spectrum of information resources security for an organization, the system level security programs implement security for each information system. Functions include influencing decisions about controls to implement, purchasing and installing technical controls, administering day-to-day security, evaluating system vulnerabilities, and responding to security problems.

The system security officer must raise security issues and help to develop 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 forces system managers and data owners to identify their security requirements and ensure that they are met.

Characteristics of a Viable System Level Security Program

_Security management should be integrated into the management of the system to assure that system managers and data owners consider security in the planning and operation of the system. The system level security program manager should participate in the selection and implementation of appropriate technical controls and security procedures, understand system vulnerabilities, and be able to respond quickly to system security problems.

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

_Security should be separated from operations. When the security program is embedded in IT operations, the security program often lacks independence, exercises minimal authority, receives little management attention, and lacks resources. The General Accounting Office (GAO) identified this organizational mode as a principal basic weakness in federal agency IT security programs (GAO Report LCD 78-123).

One approach to the conflict between needs for management and independence is a link between the security program and upper management through the central security program. Another arrangement is the complete independence of the security program from system management, with the security program reporting directly to higher management. Many hybrid alignments exist, such as co-location of the staff but separate reporting and supervisory structures.

_The development of system security plans by system level security personnel is a natural choice, as this staff knows the system thoroughly and can document weaknesses and solutions. Computer security and privacy plans for sensitive systems are mandated by the Computer Security Act of 1987.

Summary

Organizations, large and small, need to establish a computer security policy and program that integrates central office and system level security efforts, is supported by top management, and is publicized to all employees of the agency. Central and system level security programs must work together to achieve the common goal of protecting an organization’s vital information resources.