TEL2813/IS2820
Security Management

Developing the Security Program

Jan 29, 2008
Introduction

- Security programs
  - describe the entire set of personnel, plans, policies, and initiatives related to information security

- Information security program
  - describe the structure and organization of the effort that contains risks to the information assets of organization
Organizing for Security

- Some variables that determine how to structure an information security program are:
  - Organizational culture
  - Size
  - Security personnel budget
  - Security capital budget
Security in Large Organizations

- InfoSec departments in large organizations
  - tend to form and re-form internal groups to meet long-term challenges
  - Functions are likely to be split into groups

- InfoSec departments in small organizations
  - typically create fewer groups, perhaps only having one general group of specialists
Very Large Organizations
More than 10,000 Computers

- Security budgets often grow faster than IT budgets
- Even with large budgets, average amount spent on security per user is still smaller than any other type of organization

Where small orgs spend more than $5,000 per user on security, very large organizations spend about 1/18th of that, roughly $300 per user

- Does a better job in the policy and resource mgmt areas, although only 1/3 of organizations handled incidents according to an IR plan
Large Organizations
With 1,000 to 10,000 computers

- At this size,
  - approach to security is often matured,
  - Integration of planning and policy into organization’s culture

- Unfortunately, large organization does not always put
  - large amounts of resources into security considering vast numbers of computers and users often involved
  - Tend to spend proportionally less on security
<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>Evaluates risk present in IT initiatives and/or systems</td>
<td>Identifies the sources of risk and may offer advice on controls that can reduce risk</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Implements or oversees use of controls to reduce risk</td>
<td>Often paired with risk assessment</td>
</tr>
<tr>
<td>Systems Testing</td>
<td>Evaluates patches used to close software vulnerabilities and acceptance testing of new systems to assure compliance with policy and effectiveness</td>
<td>Usually part of the incident response and/or risk management functions</td>
</tr>
<tr>
<td>Policy</td>
<td>Maintains and promotes information security policy across the organization</td>
<td>Must be coordinated with organization-wide policy processes</td>
</tr>
<tr>
<td>Legal Assessment</td>
<td>Maintains awareness of planned and actual laws and their impact, and coordinates with outside legal counsel and law enforcement agencies</td>
<td>Almost always external to the information security and IT departments</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Handles the initial response to potential incidents, manages escalation of actual incidents, and coordinates the earliest responses to incidents and disasters</td>
<td>Often cross-functional and drawn from multiple departments should include middle management to manage escalation processes</td>
</tr>
<tr>
<td>Planning</td>
<td>Researches, creates, maintains, and promotes information security plans; often takes a project management approach to planning as contrasted with strategic planning for the whole organization</td>
<td>Must coordinate with organization-wide policy processes</td>
</tr>
<tr>
<td>Measurement</td>
<td>Uses existing control systems (and perhaps specialized data collection systems) to measure all aspects of the information security environment</td>
<td>Management relies on timely and accurate statistics to make informed decisions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Verifies that system and network administrators repair identified vulnerabilities promptly and correctly</td>
<td>Poses problems for good customer service because it is difficult to be customer-focused and to enforce compliance at the same time</td>
</tr>
<tr>
<td>Centralized Authentication</td>
<td>Manages the granting and revocation of network and system credentials for all members of the organization</td>
<td>Often delegated to the help desk or staffed in conjunction and co-located with the help desk function</td>
</tr>
<tr>
<td>Systems Security Administration</td>
<td>Administers the configuration of computer systems, which are often organized into groups by the operating system they run</td>
<td>Many organizations may have originally assigned all security functions to these groups outside of the information security function; this can be a source of conflict when organizations update their information security program</td>
</tr>
<tr>
<td>Training</td>
<td>Trains general staff in information security topics, IT staff in specialized technical controls, and internal information security staff in specialized areas of information security, including both technical and managerial topics</td>
<td>Some or all of this function may be carried out in conjunction with the corporate training department</td>
</tr>
<tr>
<td>Network Security Administration</td>
<td>Administers configuration of computer networks, often organized into groups by logical network area (i.e., WAN, LAN, DMZ) or geographic location</td>
<td>Many organizations may have originally assigned some security functions to these groups outside of the information security function, which may require close coordination or reassignment</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Locates exposure within information assets so these vulnerabilities can be repaired before weaknesses are exploited</td>
<td>Sometimes called the penetration testing team or the ethical hacking unit; often outsourced to consultant “tiger teams”</td>
</tr>
</tbody>
</table>

Suggested Functions Needed to Implement InfoSec Program
Security in Large Organizations

- Recommended approach: separate into 4 areas:
  - Functions performed by non-technology business units outside of IT
    - Legal; Training
  - Functions performed by IT groups outside of information security area of management control
    - Network/systems security administrator
    - Centralized authentication
  - Functions performed within information security department as customer service
    - Risk assessment; systems testing; incident response; planning; measurement; vulnerability assessment
  - Functions performed within the information security department as compliance enforcement obligation
    - Policy; compliance; risk management
Responsibilities in Large Organizations

- CISO’s responsibility - see that
  - information security functions are adequately performed somewhere within the organization
- Deployment of full-time security personnel depends on a number of factors,
  - sensitivity of information to be protected,
  - industry regulations and
  - general profitability
Typical Information Security Staffing in a Large Organization

**CISO**
- **Technical Security**
  - Firewall/IDS
  - Malware and Servers
- **Risk Management and Policy**

1–2 Full-time security managers
3–4 Full-time security administrators/technicians
3–4 Part-time security managers
10–12 Part-time security administrators/technicians

**FIGURE 5-1** Information Security Staffing in a Large Organization
Typical InfoSec Staffing in a Very Large Organization

**Figure 5-2** Information Security Staffing in a Very Large Organization

4–5 Full-time security managers
10–15 Full-time security administrators/technicians
5–10 Part-time security managers
30–35 Full-time security administrators/technicians
Security in Medium-Sized Organizations (100-1,000 PCs)

- Have smaller total budget
- May have same sized security staff as small org, but larger need
- Typically relies on help from IT staff for plans and practices
- May be large enough
  - to implement multi-tiered approach to security
  - with fewer dedicated groups and more functions assigned to each group
- Medium-sized organizations tend to ignore some security functions.
Typical InfoSec Staffing in a Medium Organization

Security Manager

- Security Administrator
- Security Technician

1 full-time manager and partial support staff members

FIGURE 5-3 Information Security Staffing in a Medium-Sized Organization
Security in Small Organizations
10-100 Computers

- Have simple, centralized IT organizational model
- Spend disproportionately more on security
- Information security in small org is often responsibility of a single security administrator
- Such organizations frequently have little in the way of formal policy, planning, or security measures
  - Commonly outsource their Web presence or electronic commerce operations
  - Security training and awareness is commonly conducted on a 1-on-1 basis
  - Policies are often issue-specific
  - Formal planning is often part of IT planning
- Threats from insiders are less likely in such an environment
InfoSec Staffing in a Smaller Organization

1 full-time/part-time manager and part-time support staff members

**Figure 5-4** Information Security Staffing in a Smaller Organization
In large organizations,

- InfoSec is often located within IT department,
  - headed by CISO who reports directly to top computing executive, or CIO

By its very nature, an InfoSec program is sometimes at odds with the goals and objectives of the IT department as a whole
Placing Information Security Within An Organization (Continued)

- Possible conflicts between CIO/CISO goals
  - Current movement to separate information security from IT division

- The challenge is
  - to design a reporting structure for the InfoSec program that balances the needs of each of the communities of interest
IT Department

Departments not related to Information Security have been omitted from diagram for clarity.

From Information Security Roles and Responsibilities Made Easy, used with permission.

**FIGURE 5-5** Wood’s Option 1: Information Security Reports to Information Technology Department
Broadly Defined Security Department

From Information Security Roles and Responsibilities Made Easy, used with permission.

**FIGURE 5-6** Wood’s Option 2: Information Security Reports to Broadly Defined Security Department
Administrative Services
Department

Departments not related to Information Security have been omitted from diagram for clarity.

Audit Committee → Board → Information Security Management Committee

Internal Audit
- EDP Audit
- Quality Assurance

Strategic Planning
- Business Contingency Planning
- Risk & Insurance

Legal
- Physical Security
- Public Relations

Marketing & Sales
- Systems Development Consulting on Security
- Systems Contingency Planning
- Computer Emergency Response

Administration Services
- Information Security
- Human Resources
- Personnel Security & Safety

Information Technology
- Systems & Network Administration
- Database Administration & Data Warehousing
- Help Desk
- Systems Development
- Records Management
- Internet Commerce
- Telecommunications
- Computer & Network Operations

---

From *Information Security Roles and Responsibilities Made Easy*, used with permission.
Insurance & Risk Mgmt Department

Departments not related to Information Security have been omitted from diagram for clarity.

From *Information Security Roles and Responsibilities Made Easy*, used with permission.

**FIGURE 5-8** Wood’s Option 4: Information Security Reports to Insurance and Risk Management Department
From Information Security Roles and Responsibilities Made Easy, used with permission.

**FIGURE 5-9** Wood’s Option 5: Information Security Reports to Strategy and Planning Department

From Information Security Roles and Responsibilities Made Easy, used with permission.
Wood’s Option 6: Information Security Reports to Legal Department

From Information Security Roles and Responsibilities Made Easy, used with permission.
Other Options

- Option 7: Internal Audit
- Option 8: Help Desk
- Option 9: Accounting and Finance Through IT
- Option 10: Human Resources
- Option 11: Facilities Management
- Option 12: Operations
Components of the Security Program

- Determining what level the information security program operates on depends on the organization’s strategic plan
  - In particular, on the plan’s vision and mission statements
- The CIO and CISO should use these two documents to formulate the mission statement for the information security program
  - NIST SP 800-14 Generally Accepted Principles for Securing Information Technology Systems
  - SP 800-12 An Introduction to Computer Security: The NIST Handbook
### TABLE 5-2 Elements of a Security Program

<table>
<thead>
<tr>
<th>Primary Element</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Program Policy, Issue-Specific Policy, System-Specific Policy</td>
</tr>
<tr>
<td>Program Management</td>
<td>Central Security Program, System-Level Program</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Risk Assessment, Risk Mitigation, Uncertainty Analysis</td>
</tr>
<tr>
<td>Life-Cycle Planning</td>
<td>Security Plan, Initiation Phase, Development/Acquisition Phase, Implementation Phase, Operation/Maintenance Phase</td>
</tr>
<tr>
<td>Personnel/User Issues</td>
<td>Staffing, User Administration</td>
</tr>
<tr>
<td>Preparing for Contingencies and Disasters</td>
<td>Business Plan, Identify Resources, Develop Scenarios, Develop Strategies, Test and Revise Plan</td>
</tr>
<tr>
<td>Computer Security Incident Handling</td>
<td>Incident Detection, Reaction, Recovery, and Followup</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>SETA plans, Awareness Projects, and Policy and Procedure Training</td>
</tr>
<tr>
<td>Security Considerations in Computer Support and Operations</td>
<td>Help Desk Integration, Defending Against Social Engineering, and Improving System Administration</td>
</tr>
<tr>
<td>Physical and Environmental Security</td>
<td>Guards, Gates, Locks and Keys, and Alarms</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Identification, Authentication, Passwords, Advanced Authentication</td>
</tr>
<tr>
<td>Logical Access Control</td>
<td>Access Criteria, Access Control Mechanisms</td>
</tr>
<tr>
<td>Audit Trails</td>
<td>System Logs, Log Review Processes, and Log Consolidation and Management</td>
</tr>
<tr>
<td>Cryptography</td>
<td>TKI, VPN, Key Management, and Key Recovery</td>
</tr>
</tbody>
</table>
Information Security Roles

- Information security positions can be classified into one of three types:
  - Those that define,
    - provide the policies, guidelines, and standards. They’re the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth.
  - Those that build
    - They’re the real techies, who create and install security solutions.
  - Those that administer
    - who operate and administrate the security tools, the security monitoring function, and the people who continuously improve the processes.
Information Security Titles

- Typical organization has a number of individuals with information security responsibilities
- While the titles used may be different, most of the job functions fit into one of the following:
  - Chief Information Security Officer (CISO)
  - Security managers
  - Security administrators and analysts
  - Security technicians
  - Security staff
Information Security Roles

FIGURE 5-11  Information Security Roles
Integrating Security and the Help Desk

- Help desk
  - an important part of the information security team,
  - enhances the ability to identify potential problems
- User’s complaint about his or her computer,
  - may turn out to be related to a bigger problem, such as a hacker, denial-of-service attack, or a virus
- Because help desk technicians perform a specialized role in information security,
  - they have a need for specialized training
Implementing Security Education, Training, and Awareness Programs

- SETA program:
  - designed to reduce accidental security breaches
  - consists of three elements:
    - security education,
    - security training, and
    - security awareness

- Awareness, training, and education programs offer two major benefits:
  - Improve employee behavior
  - Enable organization to hold employees accountable for their actions
Implementing SETA (Continued)

The purpose of SETA is to enhance security:

- By building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.
- By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely.
- By improving awareness of the need to protect system resources.
### Comparative SETA Framework

<table>
<thead>
<tr>
<th></th>
<th>AWARENESS</th>
<th>TRAINING</th>
<th>EDUCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute:</strong></td>
<td>&quot;What&quot;</td>
<td>&quot;How&quot;</td>
<td>&quot;Why&quot;</td>
</tr>
<tr>
<td><strong>Level:</strong></td>
<td>Information</td>
<td>Knowledge</td>
<td>Insight</td>
</tr>
<tr>
<td><strong>Objective:</strong></td>
<td>Recognition</td>
<td>Skill</td>
<td>Understanding</td>
</tr>
<tr>
<td><strong>Teaching Method:</strong></td>
<td>Media</td>
<td>Practical Instruction</td>
<td>Theoretical Instruction</td>
</tr>
<tr>
<td></td>
<td>- Videos</td>
<td>- Lecture</td>
<td>- Discussion Seminar</td>
</tr>
<tr>
<td></td>
<td>- Newsletters</td>
<td>- Case study workshop</td>
<td>- Background reading</td>
</tr>
<tr>
<td></td>
<td>- Posters, etc.</td>
<td>- Hands-on practice</td>
<td></td>
</tr>
<tr>
<td><strong>Test Measure:</strong></td>
<td>True/False</td>
<td>Problem Solving</td>
<td>Eassay</td>
</tr>
<tr>
<td></td>
<td>Multiple Choice (identify learning)</td>
<td>(apply learning)</td>
<td>(interpret learning)</td>
</tr>
<tr>
<td><strong>Impact Timeframe:</strong></td>
<td>Short-term</td>
<td>Intermediate</td>
<td>Long-term</td>
</tr>
</tbody>
</table>

NI ST 800-12
Security Training

- Security training involves
  - providing detailed information and
  - hands-on instruction to give skills to users to perform their duties securely

- Two methods for customizing training
  - Functional background:
    - General user
    - Managerial user
    - Technical user
  - Skill level:
    - Novice
    - Intermediate
    - Advanced
Training Techniques

- Using wrong method can:
  - Hinder transfer of knowledge
  - Lead to unnecessary expense and frustrated, poorly trained employees

- Good training programs:
  - Use latest learning technologies and best practices
  - Recently, less use of centralized public courses and more on-site training
  - Often for one or a few individuals, not necessarily for large group → waiting for large-enough group can cost companies productivity
  - Increased use of short, task-oriented modules and training sessions that are immediate and consistent, available during normal work week
Delivery Methods

- Selection of training delivery method:
  - Not always based on best outcome for the trainee
  - Other factors: budget, scheduling, and needs of the organization often come first
    - One-on-One
    - Formal Class
    - Computer-Based Training (CBT)
    - Distance Learning/Web Seminars
    - User Support Group
    - On-the-Job Training
    - Self-Study (Noncomputerized)
Selecting the Training Staff

- Employee training:
  - Local training program
  - Continuing education department
  - External training agency
  - Professional trainer, consultant, or someone from accredited institution to conduct on-site training
  - In-house training using organization’s own employees
Implementing Training

The following seven-step methodology generally applies:

- Step 1: Identify program scope, goals, and objectives
- Step 2: Identify training staff
- Step 3: Identify target audiences
- Step 4: Motivate management and employees
- Step 5: Administer the program
- Step 6: Maintain the program
- Step 7: Evaluate the program
Security Awareness

- Security awareness program:
  - one of least frequently implemented, but most effective security methods

- Security awareness programs:
  - Set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure
  - Remind users of the procedures to be followed
SETA Best Practices

- When developing an awareness program:
  - Focus on people
  - Refrain from using technical jargon
  - Use every available venue
  - Define learning objectives, state them clearly, and provide sufficient detail and coverage
  - Keep things light
  - Don’t overload the users
  - Help users understand their roles in InfoSec
  - Take advantage of in-house communications media
  - Make the awareness program formal; plan and document all actions
  - Provide good information early, rather than perfect information late
The Ten Commandments of InfoSec Awareness Training

- Information security is a people, rather than a technical, issue
- If you want them to understand, speak their language
- If they cannot see it, they will not learn it
- Make your point so that you can identify it and so can they
- Never lose your sense of humor
- Make your point, support it, and conclude it
- Always let the recipients know how the behavior that you request will affect them
- Ride the tame horses
- Formalize your training methodology
- Always be timely, even if it means slipping schedules to include urgent information
Employee Behavior and Awareness

- Security awareness and security training are designed to modify any employee behavior that endangers the security of the organization’s information.

- Security training and awareness activities can be undermined if management does not set a good example.
Awareness Techniques

- Awareness can take on different forms for particular audiences

- A security awareness program can use many methods to deliver its message

- Effective security awareness programs need to be designed with the recognition that people tend to practice a tuning out process (acclimation)
  - Awareness techniques should be creative and frequently changed
Developing Security Awareness Components

- Many security awareness components are available at little or no cost - others can be very expensive if purchased externally.
- Security awareness components include the following:
  - Videos
  - Posters and banners
  - Lectures and conferences
  - Computer-based training
  - Newsletters
  - Brochures and flyers
  - Trinkets (coffee cups, pens, pencils, T-shirts)
  - Bulletin boards
The Security Newsletter

- Security newsletter: cost-effective way to disseminate security information
  - In the form of hard copy, e-mail, or intranet
  - Topics can include threats to the organization’s information assets, schedules for upcoming security classes, and the addition of new security personnel

- Goal:
  - keep information security uppermost in users’ minds and stimulate them to care about security
The Security Newsletter (Continued)

Newsletters might include:

- Summaries of key policies
- Summaries of key news articles
- A calendar of security events, including training sessions, presentations, and other activities
- Announcements relevant to information security
- How-to’s
The Security Poster

- Security poster series can be a simple and inexpensive way to keep security on people’s minds.
- Professional posters can be quite expensive, so in-house development may be best solution.
- Keys to a good poster series:
  - Varying the content and keeping posters updated
  - Keeping them simple, but visually interesting
  - Making the message clear
  - Providing information on reporting violations
The Trinket Program

- Trinkets may not cost much on a per-unit basis, but they can be expensive to distribute throughout an organization.
- Several types of trinkets are commonly used:
  - Pens and pencils
  - Mouse pads
  - Coffee mugs
  - Plastic cups
  - Hats
  - T-shirts
Information Security Awareness Web Site

- Organizations can establish
  - Web pages or sites dedicated to promoting information security awareness
- As with other SETA awareness methods,
  - the challenge lies in updating the messages frequently enough to keep them fresh
Some tips on creating and maintaining an educational Web site are provided here:

- See what’s already out there
- Plan ahead
- Keep page loading time to a minimum
- Seek feedback
- Assume nothing and check everything
- Spend time promoting your site
Security Awareness Conference/Presentations

- Another means of renewing the information security message is to have a guest speaker or even a mini-conference dedicated to the topic.