UNIT-V

Implementing Information Security: information security project management, technical topics of implementation , Non- technical aspects of implementation, Security certification and accreditation

Security and Personnel: Positioning and staffing security function, Employment policies and practices, internal control strategies.

Information security Maintenance: Security management models. The maintenance model, Digital forensics

---

Introduction

- The SecSDLC implementation phase is accomplished through changing the configuration and operation of an organization's information systems
- Implementation includes changes to procedures, people, hardware, software, and data
- Organization translates the blueprint for information security into a concrete project plan

Information Security Project Management

- Once organization's vision and objectives for information security are understood, the process for creating project plan can be defined
- Major steps in executing project plan are:
    - Planning the project
    - Supervising tasks and action steps
    - Wrapping up
- Each organization must determine its own project management methodology for IT and information security projects

Developing the Project Plan

- Creation of project plan can be done using work breakdown structure (WBS)

- Major project tasks in WBS are
    - work to be accomplished;
    - individuals assigned;
    - start and end dates;
    - amount of effort required;
    - estimated capital and noncapital expenses;
    - and identification of dependencies between/among tasks

	Task or Subtask	Resources	Start and End Dates	Estimated Effort in Hours	Estimated Capital Expense	Estimated Noncapital Expense	Depen-dencies
1	Contact field office and confirm network assumptions	Network architect	S: 9/22 E:	2	0	200	
2	Purchase standard firewall hardware	Network architect and purchasing group	S: E:	4	4,500	250	1
3	Configure firewall	Network architect	S: E:	8	0	800	2
4	Package and ship to field office	Student intern	S: E: 10/15	2	0	85	3
5	Work with local technical resource to install and test firewall	Network architect	S: E:	6	0	600	4
6	Complete vulnerability assessment by penetration test team	Network architect and penetration test team	S: E:	12	0	1,200	5
7	Get remote office sign-off and update all network drawings and documentation	Network architect	S: E: 11/30	8	0	800	6

Financial Considerations

- No matter what information security needs exist, the amount of effort that can be expended depends on funds available
- Cost benefit analysis must be verified prior to development of project plan
- Both public and private organizations have budgetary constraints, though of a different nature
- To justify an amount budgeted for a security project at either public or for-profit organizations, it may be useful to benchmark expenses of similar organizations

Priority Considerations

- In general, the most important information security controls should be scheduled first
- Implementation of controls is guided by prioritization of threats and value of threatened information assets

Time and Scheduling Considerations

- Time impacts dozens of points in the development of a project plan, including:
    - Time to order, receive, install, and configure security control
    - Time to train the users
    - Time to realize return on investment of control

Staffing Considerations

- Lack of enough qualified, trained, and available personnel constrains project plan
- Experienced staff is often needed to implement available technologies and develop and implement policies and training programs

Procurement Considerations

- IT and information security planners must consider acquisition of goods and services
- There may be many constraints on the selection process for equipment and services in most organizations, specifically in the selection of service vendors or products from manufacturers/suppliers
- These constraints may eliminate a technology from realm of possibilities

Organizational Feasibility Considerations

- Policies require time to develop; new technologies require time to be installed, configured, and tested
- Employees need training on new policies and technology, and how new information security program affects their working lives
- Changes should be transparent to system users unless the new technology is intended to change procedures (e.g., requiring additional authentication or verification)

Training and Indoctrination Considerations

- Size of organization and normal conduct of business may preclude a single large training program on new security procedures/technologies
- Thus, organization should conduct phased-in or pilot approach to implementation

Scope Considerations

- Project scope: concerns boundaries of time and effort-hours needed to deliver planned features and quality level of project deliverables
- In the case of information security, project plans should not attempt to implement the entire security system at one time

The Need for Project Management

- Project management requires a unique set of skills and thorough understanding of a broad body of specialized knowledge
- Most information security projects require a trained project manager (a CISO) or skilled IT manager versed in project management techniques

Supervised Implementation

- Some organizations may designate a champion from the general management community of interest to supervise implementation of information security project plan
- An alternative is to designate a senior IT manager or CIO to lead implementation
- Optimal solution is to designate a suitable person from information security community of interest

- It is up to each organization to find the most suitable leadership for a successful project implementation

Executing the Plan

- Negative feedback ensures project progress is measured periodically
    - Measured results compared against expected results
    - When significant deviation occurs, corrective action taken
- Often, project manager can adjust one of three parameters for task being corrected: effort and money allocated; scheduling impact; quality or quantity of deliverable

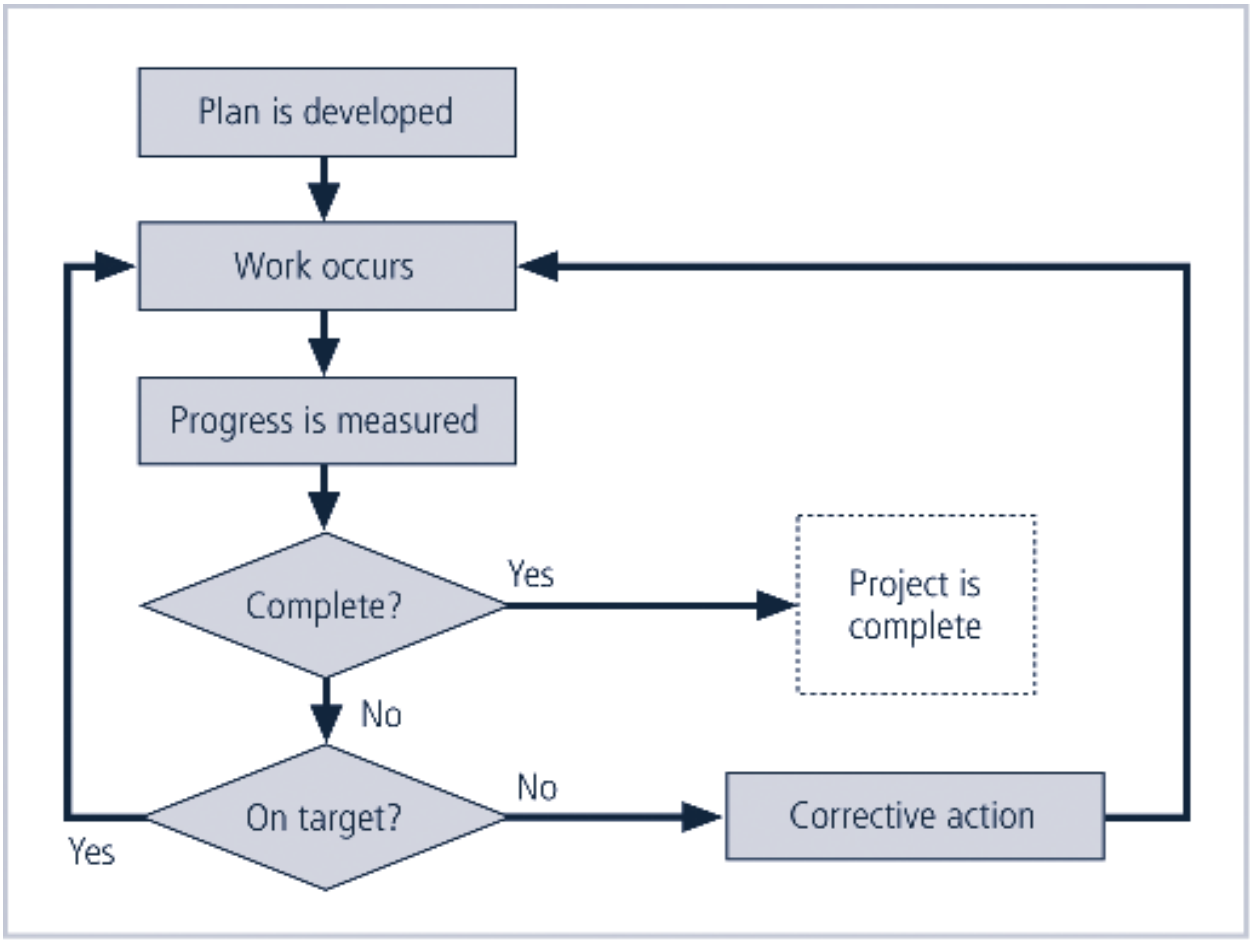


FIGURE 10-1 Negative Feedback Loop

Project Wrap-up

- Project wrap-up is usually handled as procedural task and assigned to mid-level IT or information security manager
- Collect documentation, finalize status reports, and deliver final report and presentation at wrap-up meeting
- Goal of wrap-up is to resolve any pending issues, critique overall project effort, and draw conclusions about how to improve the process for the future

Technical Topics of Implementation

- Some parts of implementation process are technical in nature, dealing with application of technology
    - Conversion strategies
    - Prioritization
    - Outsourcing
- Others are not, dealing instead with human interface to technical systems

Conversion Strategies

- As components of new security system are planned, provisions must be made for changeover from previous method of performing task to new method
- Four basic approaches:
    - Direct changeover
    - Phased implementation
    - Pilot implementation
    - Parallel operations

The Bull's-Eye Model

- Proven method for prioritizing program of complex change
- Issues addressed from general to specific
- Relies on process of evaluating project plans in progression through four layers: policies, networks, systems, applications

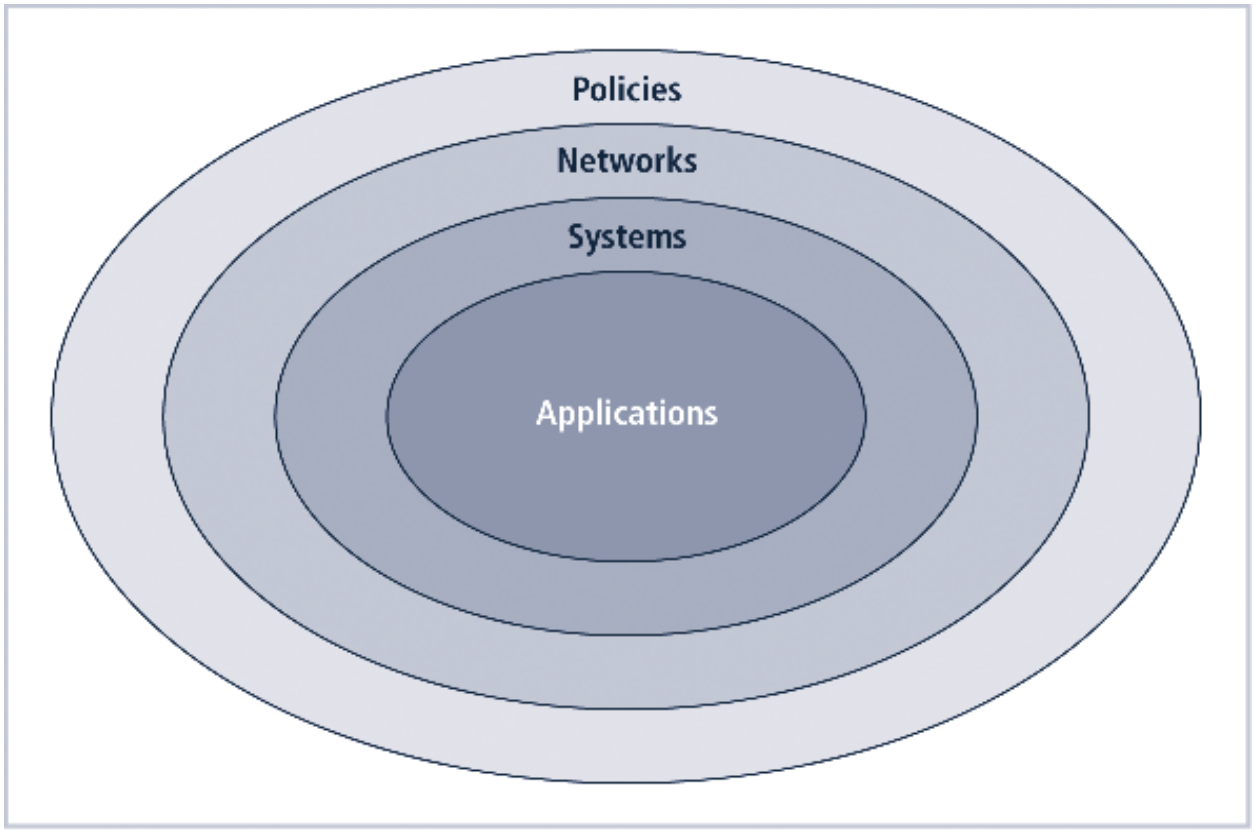


FIGURE 10-2 The Bull's-eye Model

To Outsource or Not

- Just as some organizations outsource IT operations, organizations can outsource part or all of information security programs

- Due to complex nature of outsourcing, it's advisable to hire best outsourcing specialists and retain best attorneys possible to negotiate and verify legal and technical intricacies

Non-technical Aspects of Implementation

- Other parts of implementation process are not technical in nature, dealing with the human interface to technical systems
- This includes creating a culture of change management as well as considerations for organizations facing change

The Culture of Change Management

- Prospect of change can cause employees to build up resistance to change
- The stress of change can increase the probability of mistakes or create vulnerabilities
- Resistance to change can be lowered by building resilience for change

Reducing Resistance to Change from the Start

- The more ingrained the previous methods and behaviors, the more difficult the change
- Best to improve interaction between affected members of organization and project planners in early project phases
- Three-step process for project managers: communicate, educate, and involve

Developing a Culture that Supports Change

- Ideal organization fosters resilience to change
- Resilience: organization has come to expect change as a necessary part of organizational culture, and embracing change is more productive than fighting it
- To develop such a culture, organization must successfully accomplish many projects that require change

Security and Personnel

Introduction

- When implementing information security, there are many human resource issues that must be addressed
    - Positioning and naming of the security function
    - Staffing for the security function
    - Evaluating the impact of information security across every IT function
    - Integrating solid information security concepts into personnel practices

Positioning and Staffing the Security Function

- The security function can be placed within:
    - IT function
    - Physical security function
    - Administrative services function
    - Insurance and risk management function
    - Legal department
- Organizations balance needs of enforcement with needs for education, training, awareness, and customer service

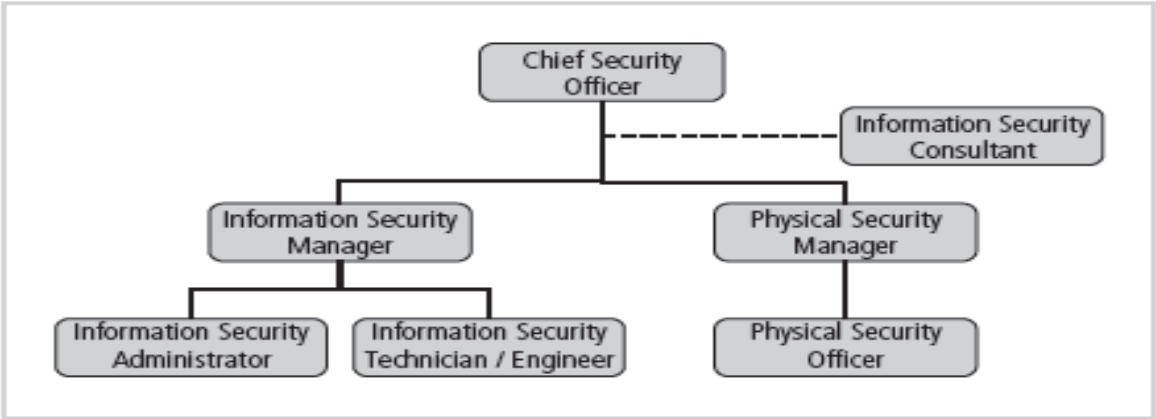
Staffing the Information Security Function

- Selecting personnel is based on many criteria, including supply and demand
- Many professionals enter security market by gaining skills, experience, and credentials
- At present, information security industry is in period of high demand

- Organizations typically look for technically qualified information security generalists
- Organizations look for information security professionals who understand:
  - How an organization operates at all levels
  - That information security is usually a management problem, not just a technical problem
  - Strong communications and writing skills
  - The role of policy in guiding security efforts
  - Most mainstream IT technologies
- Organizations look for information security professionals who understand (continued):
  - The terminology of IT and information security
  - Threats facing an organization and how they can become attacks
  - How to protect organization's assets from information security attacks
  - How business solutions can be applied to solve specific information security problems

Entry into the Information Security Profession

- Many information security professionals enter the field through one of two career paths:
  - Law enforcement and military
  - Technical, working on security applications and processes
- Today, students select and tailor degree programs to prepare for work in information security
- Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions



Information Security Positions

- Chief Information Security Officer (CISO or CSO)
  - Top information security position
  - Manages the overall information security program
  - Drafts or approves information security policies
  - Works with the CIO on strategic plans
  - Develops information security budgets
  - Sets priorities for security projects and technology
  - Makes recruiting, hiring, and firing decisions or recommendations
  - Acts as spokesperson for information security team
- Typical qualifications: accreditation, graduate degree, experience

- Security Manager
  - Accountable for day-to-day operation of information security program
  - Accomplish objectives identified by CISO and resolve issues identified by technicians.
- Typical qualifications: not uncommon to have accreditation; ability to draft middle- and lower-level policies; standards and guidelines; budgeting, project management, and hiring and firing; manage technicians

- Security Technician
- Technically qualified individuals tasked to configure security hardware and software
- Tend to be specialized
- Typical qualifications:
    - Varied; organizations prefer expert, certified, proficient technician
    - Some experience with a particular hardware and software package

Credentials of Information Security Professionals

- Many organizations seek recognizable certifications
- Most existing certifications are relatively new and not fully understood by hiring organizations
- Certifications include: CISSP and SSCP, CISA and CISM, GIAC, SCP, Security+, CCE, RSA security, CheckPoint, Cisco

Certification Costs

- Better certifications can be very expensive
- Even experienced professionals find it difficult to take an exam without some preparation
- Many candidates teach themselves through trade press books; others prefer structure of formal training
- Before attempting a certification exam, do all homework and review exam criteria, its purpose, and requirements in order to ensure that the time and energy spent pursuing certification are well spent

Job Descriptions

- Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions

- Organization should avoid revealing access privileges to prospective employees when advertising open positions

Interviews

- An opening within the information security department creates a unique opportunity for the security manager to educate HR on certifications, experience, and qualifications of a good candidate
- Information security should advise HR to limit information provided to the candidate on the responsibilities and access rights the new hire would have
- For organizations that include on-site visits as part of interviews, it's important to use caution when showing candidate around facility

Background Checks

- Investigation into a candidate's past
- Should be conducted before organization extends offer to candidate
- Background checks differ in level of detail and depth with which candidate is examined
- May include identity check, education and credential check, previous employment verification, references check, drug history, credit history, and more

Employment Contracts

- Once a candidate has accepted the job offer, employment contract becomes important security instrument
- Many security policies require an employee to agree in writing to monitoring and nondisclosure agreements
- New employees may find policies classified as "employment contingent upon agreement," whereby employee is not offered the position unless binding organizational policies are agreed to

New Hire Orientation

- New employees should receive extensive information security briefing on policies, procedures, and requirements for information security
- Levels of authorized access are outlined; training provided on secure use of information systems
- By the time employees start, they should be thoroughly briefed and ready to perform duties securely

On-the-Job Security Training

- Organization should conduct periodic security awareness training
- Keeping security at the forefront of employees' minds and minimizing employee mistakes is an important part of information security awareness mission
- External and internal seminars also increase level of security awareness for all employees, particularly security employees

Evaluating Performance

- Organizations should incorporate information security components into employee performance evaluations
- Employees pay close attention to job performance evaluations; if evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level

Termination

- When employee leaves organization, there are a number of security-related issues
- Key is protection of all information to which employee had access
- Once cleared, the former employee should be escorted from premises
- Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback

- Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting
    - Before employee is aware, all logical and keycard access is terminated
    - Employee collects all belongings and surrenders all keys, keycards, and other company property
    - Employee is then escorted out of the building
- Friendly departures include resignation, retirement, promotion, or relocation
    - Employee may be notified well in advance of departure date
    - More difficult for security to maintain positive control over employee's access and information usage
    - Employee access usually continues with new expiration date
    - Employees come and go at will, collect their own belongings, and leave on their own

Security Considerations for Nonemployees

- Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information
- Relationships with these individuals should be carefully managed to prevent possible information leak or theft

Temporary Employees

- Hired by organization to serve in temporary position or to supplement existing workforce
- Often not subject to contractual obligations or general policies; if temporary employees breach a policy or cause a problem, possible actions are limited

- Access to information for temporary employees should be limited to that necessary to perform duties
- Temporary employee's supervisor must restrict the information to which access is possible

Contract Employees

- Typically hired to perform specific services for organization
- Host company often makes contract with parent organization rather than with individual for a particular task
- In secure facility, all contract employees escorted from room to room, as well as into and out of facility
- There is need for restrictions or requirements to be negotiated into contract agreements when they are activated

Consultants

- Should be handled like contract employees, with special requirements for information or facility access integrated into contract
- Security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect organization
- Just because security consultant is paid doesn't make the protection of organization's information the consultant's number one priority

Business Partners

- Businesses find themselves in strategic alliances with other organizations, desiring to exchange information or integrate systems
- There must be meticulous, deliberate process of determining what information is to be exchanged, in what format, and to whom
- Nondisclosure agreements and the level of security of both systems must be examined before any physical integration takes place

Internal Control Strategies

- Cornerstone in protection of information assets and against financial loss
- Separation of duties: control used to reduce chance of individual violating information security; stipulates that completion of significant task requires at least two people
- Two-man control: two individuals review and approve each other's work before the task is categorized as finished
- Job rotation: employees know each others' job skills
- Mandatory vacations: company should require employees to take vacations.

Information security Maintenance

Introduction

Upon the successful implementation and testing of a new and improved security profile, an organization might feel more confident of the level of protection it is providing for its information assets.

It shouldn't.

By the time the organization has completed implementing the changes mandated by an upgraded security program, a good deal of time has passed.

In that time, everything that is dynamic in the organization's environment has changed.

Some of the factors that are likely to shift in the information security environment are:

- New assets are acquired.
- New vulnerabilities associated with the new or existing assets emerge.
- Business priorities shift.
- New partnerships are formed.
- Old partnerships dissolve.

- Organizational divestiture and acquisition occur.
- Employees who are trained, educated, and made aware of the new policies, procedures, and technologies leave.
- New personnel are hired possibly creating new vulnerabilities.

If the program is not adjusting adequately to change, it may be necessary to begin the cycle again.

That decision depends on how much change has occurred and how well the organization and its program for information security maintenance can accommodate change.

If an organization deals successfully with change and has created procedures and systems that can flex with the environment, the security program can probably continue to adapt successfully.

The CISO determines whether the information security group can adapt adequately and maintain the information security profile of the organization or whether the macroscopic process of the SecSDLC must start anew to redevelop a fundamentally new information security profile.

It is less expensive and more effective when an information security program is designed and implemented to deal with change.

It is more expensive to reengineer the information security profile again and again.

Security Management Models

To assist the information security community to manage and operate the ongoing security program, a management model must be adopted.

In general, management models are frameworks that structure the tasks of managing a particular set of activities or business functions.

The ISO Model

The ISO management model is a five-layer approach that provides structure to the administration and management of networks and systems.

The core ISO model addresses management and operation thorough five topics:

- Fault management
- Configuration and name management
- Accounting management
- Performance management
- Security management

Fault Management

- Identifying, tracking, diagnosing, and resolving faults in system
- Vulnerability assessment most often accomplished with penetration testing (simulated attacks exploiting documented vulnerabilities)
- Another aspect is monitoring and resolution of user complaints
- Help desk personnel must be trained to recognize security problem as distinct from other system problems

Configuration and Change Management

Configuration management is the administration of the configuration of the components of the security program.

Change management is the administration of changes in the strategy, operation, or components of the information security program.

Both configuration and change management administration involve nontechnical as well as technical changes.

Nontechnical changes impact procedures and people.

Technical changes impact the technology implemented to support security efforts in the hardware, software, and data components.

Nontechnical Change Management

When implementing changes to the information security program, the organization may need to implement a number of new policies and procedures.

The documents that result from these efforts should be changed when they are insufficient, outdated, or inaccurate.

As a result, the document manager should maintain a master copy of each document, record and archive revisions made, and keep copies of the revisions, along with editorial comments on what was added, removed, or modified.

As mentioned in earlier, policy revisions are not considered implemented and enforceable until they have been disseminated, read, understood, and agreed to.

Modern Web-based software is available to make the creation, modification, dissemination, and agreement documentation processes more manageable.

Technical Configuration and Change Management.

Just as documents have version numbers, revision dates, and requirements to monitor and administer change, so do technical components.

Configuration item: A hardware or software item that is to be modified and revised throughout its life cycle

Version: The recorded state of a particular revision of a software or hardware configuration item. These are often noted as the version number in the form M.N.b.

Major release: A significant revision of the version from its previous state – (M)

Minor release (update or patch): A minor revision of the version from its previous state – (N.b)

Build: A snapshot of a particular version of software assembled (or linked) from its various component modules

Build list: A list of the versions of components that comprise a build is called a build list

Configuration: A configuration is a collection of components that make up a configuration item

Revision date: The date associated with a particular version or build

Software library: A collection of configuration items that is usually controlled and that developers use to construct revisions and to issue new configuration items

Procedures associated with configuration management:

1.Configuration identification: The identification and documentation of the various components, implementation, and states of configuration items

2.Configuration control: The administration of changes to the configuration items and the issuance of versions

3.Configuration status accounting: The tracking and recording of the implementation of changes to configuration items

4.Configuration audit: Auditing and controlling the overall configuration management program

Configuration control is usually only performed by an entity that actually develops its own versions of configuration items.

Accounting and Auditing Management

Chargeback accounting enables organizations to internally charge their departments for system use.

While chargebacks for CPU cycle time are seldom used today, certain kinds of resource usage are commonly tracked, such as resources on a computing, or charges are made on a human effort-hour basis.

Accounting management involves the monitoring of the use of a particular component of a system.

With accounting management you begin to determine optimal points of systems use as indicators for upgrade and improvement.

In this context, auditing is the process of reviewing the use of a system, not to check performance, but to determine misuse or malfeasance.

Most computer-based systems used in security can create logs of their activity. The management of systems logs in large organizations is a complex process.

Fortunately, automated tools can consolidate various systems logs, perform comparative analysis, and detect common occurrences or behavior that is of interest.

Many vendors offer log consolidation and analysis features.

Performance Management

Because many information security technical controls are implemented on common IT processors, they are affected by the same factors as most computer-based technologies.

It is therefore important to monitor the performance of security systems and their underlying IT infrastructure to determine if they are working effectively.

Some common system and network metrics used in performance management are also applicable in security, especially when the components being managed are associated with the ebb and flow of network traffic.

To evaluate the performance of a security system, the administrators must establish performance baselines within the system.

In this context, a performance baseline is an expected level of performance against which all subsequent levels of performance are compared.

Organizations must establish baselines for a number of different criteria and for various periods of time.

To accomplish this effectively, the organization must monitor all possible variables, collecting and archiving performance baseline data, and then analyzing it.

Security Program Management

Once an information security program is functional, it must be operated and managed.

The ISO five-area framework that is currently being discussed is designed to support the structuring of a management model; however, it focuses on ensuring that various areas are addressed, rather than guiding the actual conduct of management.

The British Standard BS 7799 contains two standards that are designed to assist in this effort.

The second part is the BS 7799 (Part 2), which specifies requirements for establishing, implementing, and documenting an information security management system (ISMS).

Part 2 of the BS 7799 document introduces a process model with the steps of Plan-do-check-act.

Plan: by performing a risk analysis of the vulnerabilities faced by the organization

Do: by applying internal controls to manage risk

Check: by undertaking periodic and frequent review to verify effectiveness

Act: by using planned incident response plans as necessary

The Maintenance Model

A maintenance model is intended to complement the chosen management model and focus organizational effort on maintenance.

This figure diagrams a full maintenance program and forms a framework for the discussion of maintenance that follows.

- External monitoring
- Internal monitoring
- Planning and risk assessment
- Vulnerability assessment and remediation
- Readiness and review

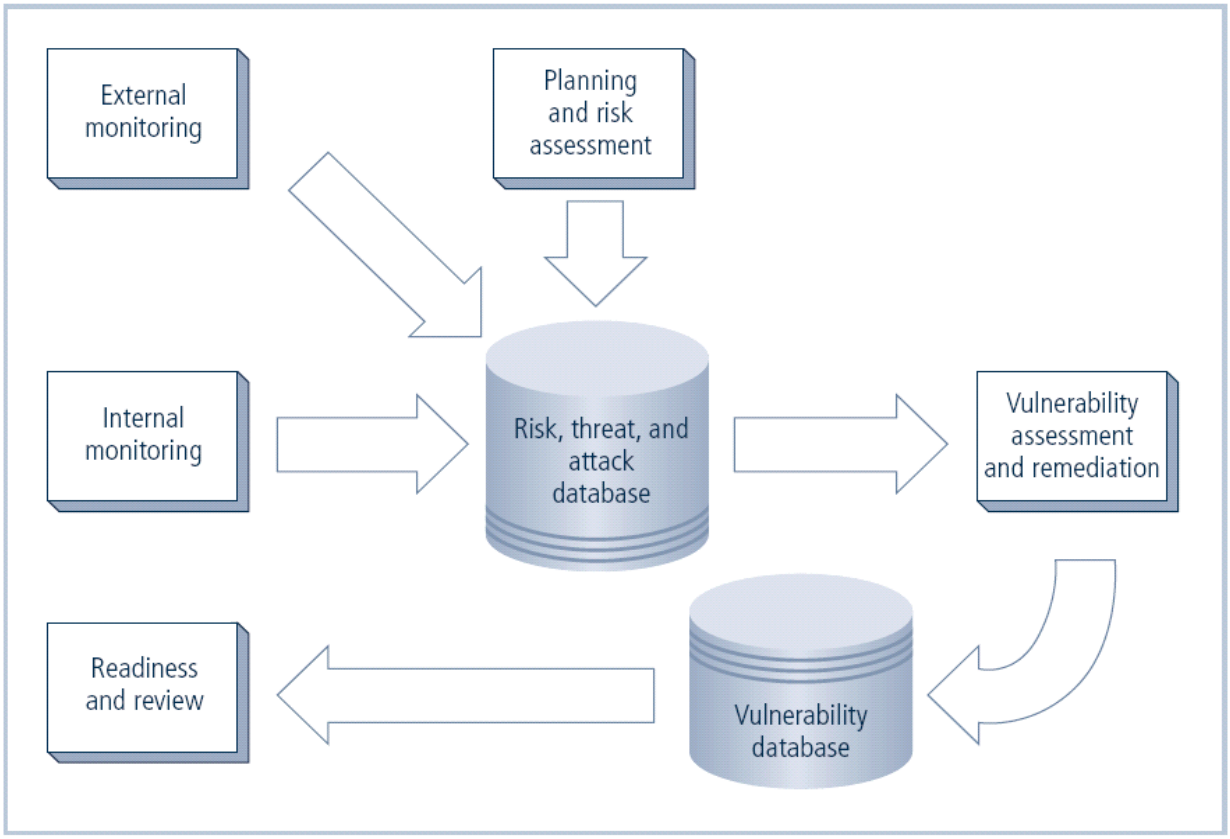


FIGURE 12-1 The Maintenance Model

Monitoring the External Environment

The objective of the external monitoring domain within the maintenance model is to provide the early awareness of new and emerging threats, threat agents, vulnerabilities, and attacks that is needed to mount an effective and timely defense.

External monitoring entails collecting intelligence from data sources and then giving that intelligence context and meaning for use by decision makers within the organization.

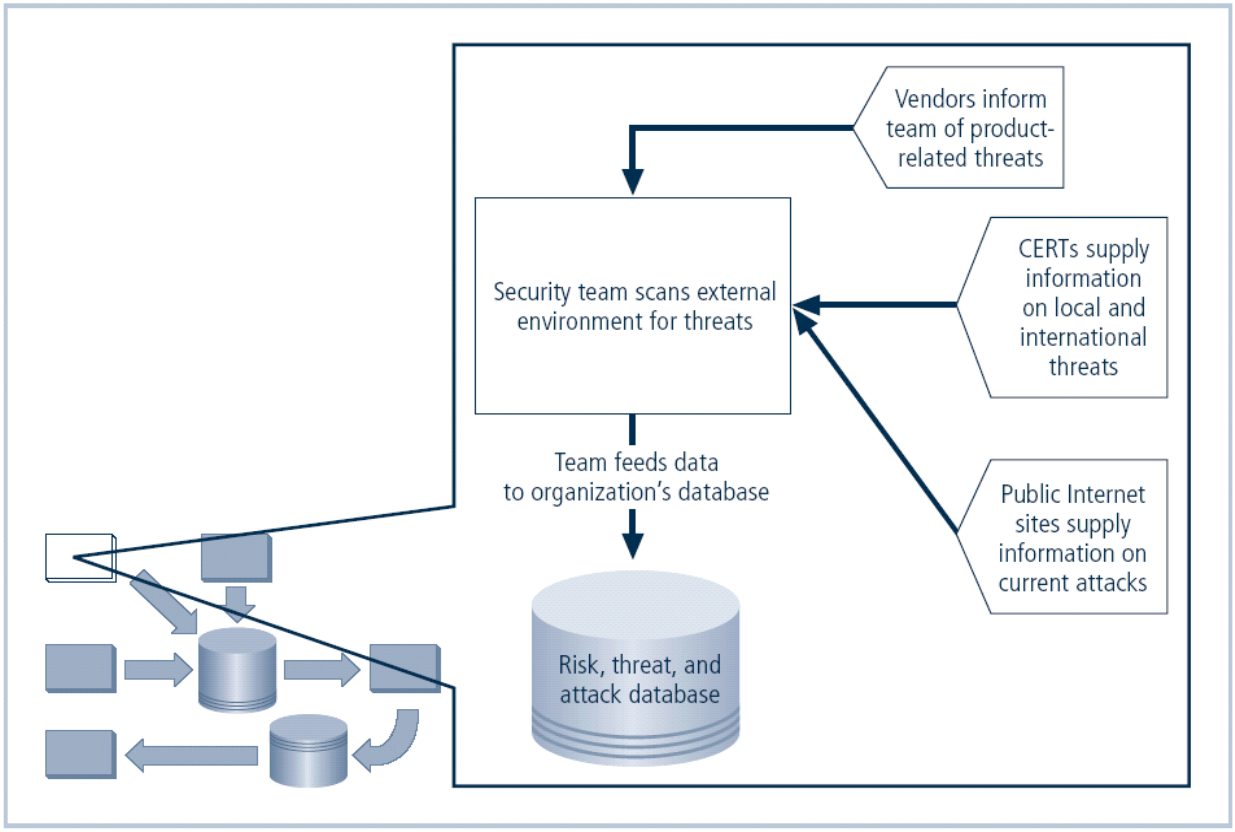


FIGURE 12-2 External Monitoring

Data Sources

- Acquiring threat and vulnerability data is not difficult
- Turning data into information decision makers can use is the challenge
- External intelligence comes from three classes of sources: vendors, computer emergency response teams (CERTs), public network sources
- Regardless of where or how external monitoring data is collected, must be analyzed in context of organization's security environment to be useful

Monitoring, Escalation, and Incident Response

The basic function of the external monitoring process is to monitor activity, report results, and escalate warnings.

The optimum approach for escalation is to rely on a thorough integration into the planning and process steps of the IRP .

The monitoring process has three primary deliverables:

- Specific warning bulletins issued when developing threats and specific attacks pose a measurable risk to the organization
- Periodic summaries of external information
- Detailed intelligence on the highest risk warnings

Data Collection and Management

Over time, the external monitoring processes should capture knowledge about the external environment in a format that can be referenced both across the organization as threats emerge and for historical use.

In the final analysis, external monitoring collects raw intelligence, filters it for relevance to the organizations, assigns it a relative risk impact, and

communicates these findings to the decision makers in time to make a difference.

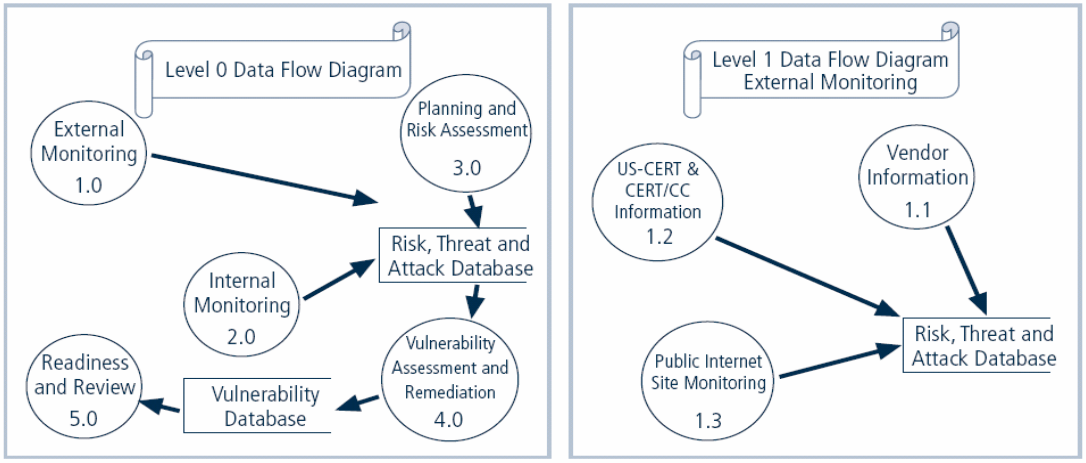


FIGURE 12-3 Data Flow Diagrams for External Data Collection

Monitoring the Internal Environment

- Maintain informed awareness of state of organization's networks, systems, and defenses by maintaining inventory of IT infrastructure and applications
- Internal monitoring accomplished by:
  - Active participation in, or leadership of, IT governance process
  - Real-time monitoring of IT activity using intrusion detection systems
  - Automated difference detection methods that identify variances introduced to network or system hardware and software

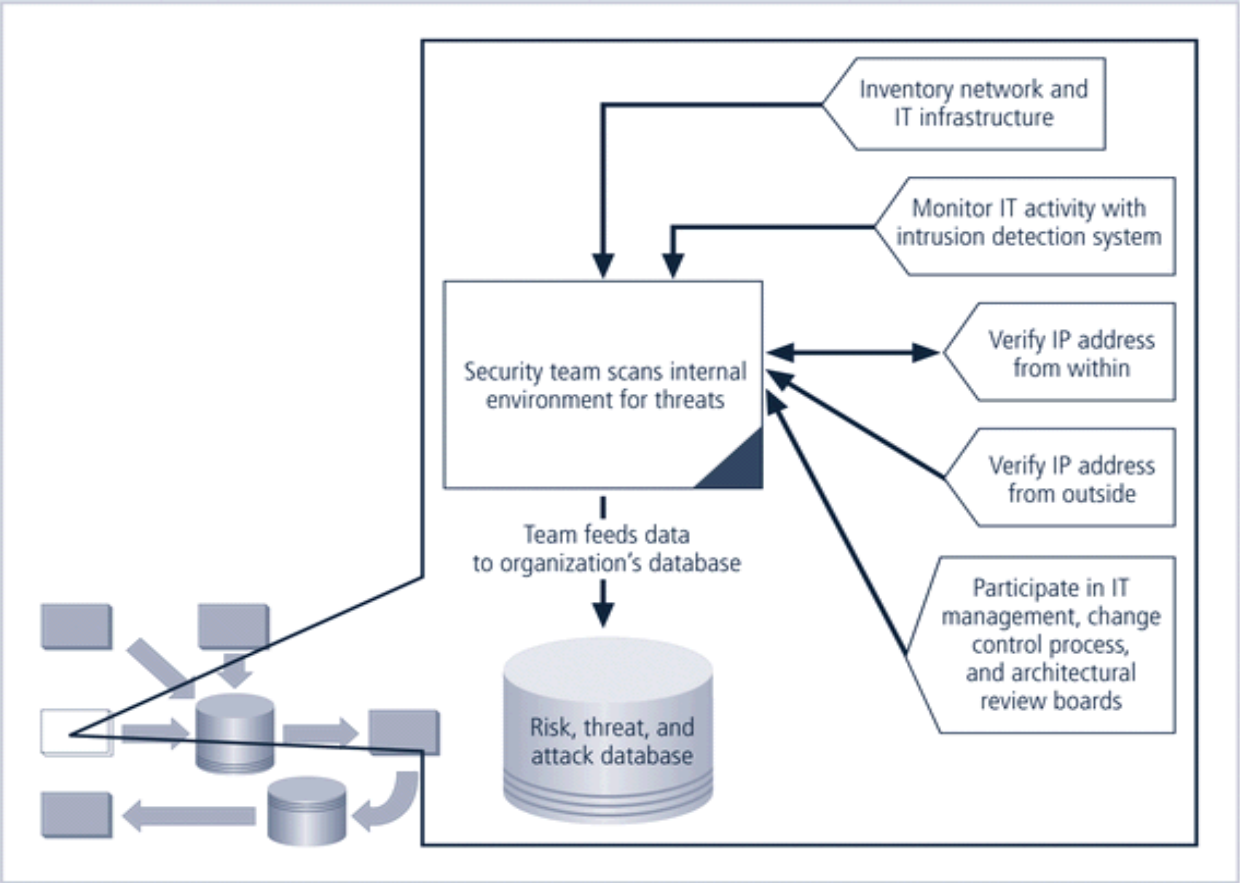


FIGURE 12-4 Internal monitoring

Network Characterization and Inventory

Each organization should have a carefully planned and fully populated inventory for all network devices, communication channels, and computing devices.

The process of collecting this information can be called characterization, which is the systematic collection of the characteristics of the network and computer devices present in the environment.

Once the characteristics have been identified, they must be carefully organized and stored using a mechanism, manual or automated, that allows timely retrieval and rapid integration of disparate facts.

The Role of IT Governance

The primary value of active engagement in an organization-wide IT governance process is the increased awareness of the impact of change.

This awareness must be translated into a description of the risk that is caused by the change.

Such a description is developed in the planning and risk assessment domain of operational risk assessment.

Awareness of change that flows from IT governance comes from two primary parts of the IT governance process:

- Architecture review boards: Many organizations have a group designated for the managed technology planning, review, and approval process that coordinates the acquisition and adoption of new technologies. The group directs the orderly introduction of change in information technology across the organization.
- IT change control process: Most organizations of appreciable size have implemented one or more mechanisms to control change in the network, IT infrastructure, and IT applications.

Making Intrusion Detection Systems Work

To be effective, IDS must be integrated into the maintenance process.

An endless flow of alert messages makes little difference to the effectiveness of the information security program.

After all, the IDS is reporting events that have already occurred.

The most important value of the raw intelligence provided by the IDS is to prevent risk in the future.

Whether the organization has outsourced IDS monitoring, staffs IDS monitoring 24 x 7, staffs IDS monitoring 8 x 5, or merely ignores the real-time alerts from IDS, the log files from the IDS engines can be mined to add information to the internal monitoring knowledge base.

Analyzing attack signatures for unsuccessful system attacks can identify weaknesses in various security efforts.

One approach that has achieved good results is to perform combinations of manual and automated difference analysis to identify changes to the internal environment.

Detecting Differences

A **difference analysis** is a procedure that compares the current state of a network segment against a known previous state of that same network segment.

Any differences between the current state and the baseline state that are unexpected could be a sign of trouble and will need to be investigated

Planning and Risk Assessment

The primary objective of the planning and risk assessment domain is to keep an eye on the entire information security program.

This is done in part by identifying and planning ongoing information security activities that further reduce risk.

Also, the risk assessment group identifies and documents risks introduced by both IT projects and information security projects.

Further, it identifies and documents risks that may be latent in the present environment.

The primary outcomes from this domain are:

- Establishing a formal information security program review process that complements and supports both the IT planning process and strategic planning processes
- Instituting formal project identification, selection, planning, and management processes for information security follow-on activities that augment the current program

- Coordinating with IT project teams to introduce risk assessment and review for all IT projects, so that risks introduced from the introduction of IT projects are identified, documented, and factored into projects decisions
- Integrating a mindset of risk assessment across the organization to encourage the performance of risk assessment activities when any technology system is implemented or modified

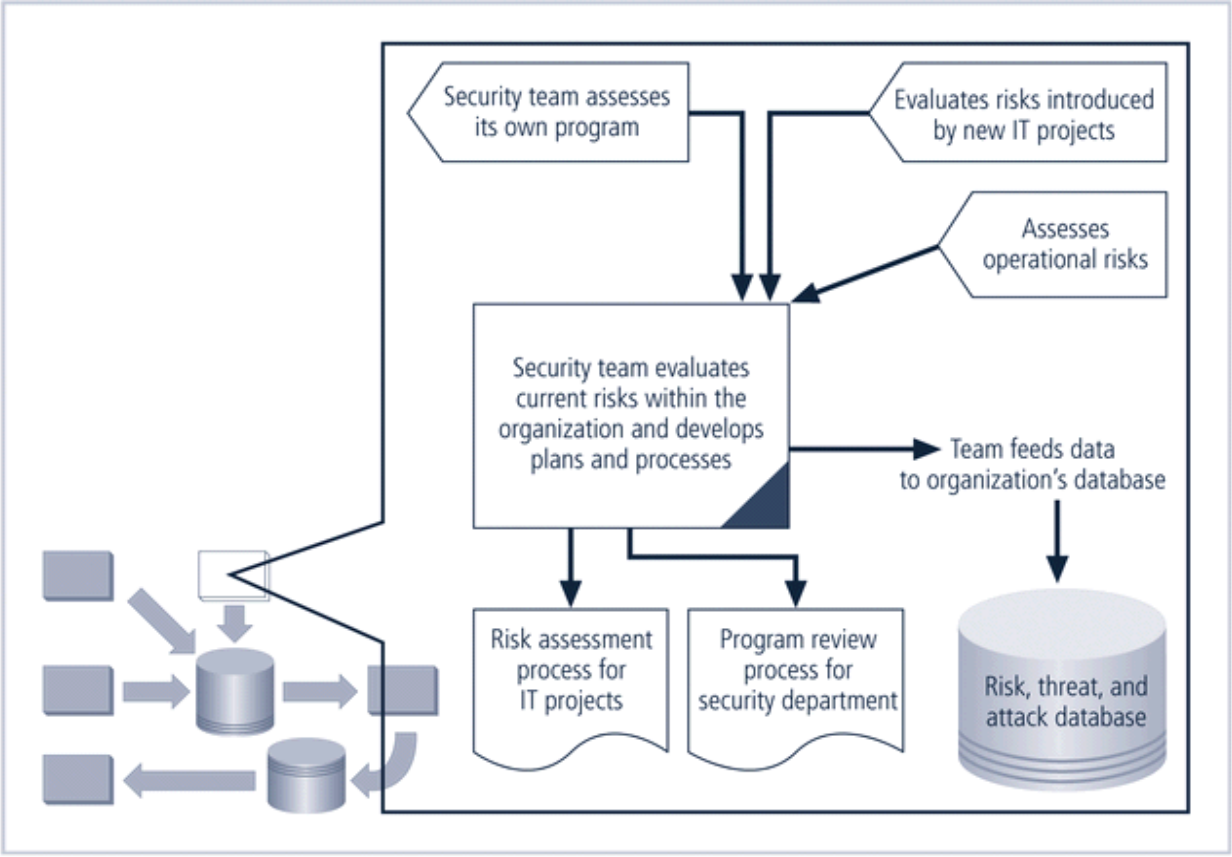


FIGURE 12-5 Planning and risk assessments

Information Security Program Planning and Review

Periodic review of an ongoing information security program coupled with planning for enhancements and extensions is a recommended practice for each organization.

The strategic planning process should examine the IT needs of the future organization and the impact those needs have on information security.

A recommended approach takes advantage of the fact that most organizations have annual capital budget planning cycles and manage security projects as part of that process.

InfoSec Improvement through Ongoing Projects

The projects follow the SecSDLC model for development and implementation, if the organization does not have a SDLC methodology that would supercede its use.

After the program is in place, large projects should be broken into smaller projects for several reasons:

- Smaller projects tend to have more manageable impacts to the networks and users.
- Larger projects tend to complicate the change control process in the implementation phase.
- Short planning, development, and implementation schedules reduce uncertainty for IT planners and financial sponsors.
- Most large projects can easily be assembled from smaller projects, giving more opportunities to change direction and gain flexibility as events occur and circumstances change.

Security Risk Assessments

A key component in the engine that drives change in the information security program is a relatively straightforward process called an information security operational risk assessment.

The RA is a method to identify and document the risk that a project, process, or action introduces to the organization and, perhaps offer suggestions for controls that can reduce that risk.

The information security group often finds itself in the business of coordinating the preparation of many different types of RA documents including:

- Network connectivity
- Dialed modem
- Business partner
- Application
- Vulnerability
- Privacy
- Acquisition or divesture
- Other RAs

Vulnerability Assessment and Remediation

The primary goal of the vulnerability assessment and remediation domain is the identification of specific, documented vulnerabilities and their timely remediation.

This is accomplished by:

- Using vulnerability assessment procedures that are documented to safely collect intelligence about network, platforms, dial-in modems, and wireless network systems
- Documenting background information and providing tested remediation procedures for the reported vulnerabilities
- Tracking, communicating, reporting, and escalating to management the itemized facts about the discovered vulnerabilities and the success or failure of the organization to remediate them

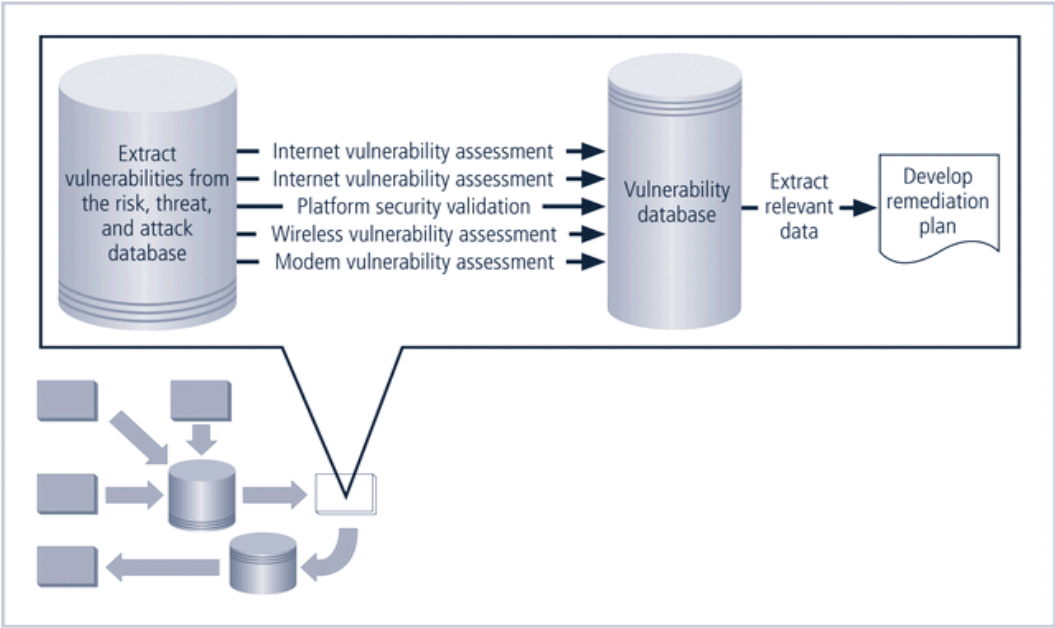


FIGURE 12-6 Vulnerability Assessment and Remediation

Vulnerability Assessment

The process of identifying and documenting specific and provable flaws in the organization's information asset environment is called vulnerability assessment.

While the exact procedures can vary, the following five vulnerability assessment processes can serve many organizations as they attempt to balance the intrusiveness of vulnerability assessment with the need for a stable and productive production environment.

Internet Vulnerability Assessment

The Internet vulnerability assessment process is designed to find and document the vulnerabilities that may be present in the public-facing network of the organization.

Since attackers from this direction take advantage of any loophole or flaw, this assessment is usually performed against all public-facing addresses, using every possible penetration testing approach.

The steps in the process are:

- Planning, scheduling, and notification of the penetration testing: Large organizations often take an entire month to perform the data collection phase, using nights and weekends and avoiding change control blackout windows. The various technical support communities are given the detailed plan so that they know when each device is scheduled for testing and what tests are used.
- Target selection: Working from the network characterization database elements that are stored in the risk, threat, and attack database, the penetration targets are selected.
- Test selection: Using the external monitoring intelligence generated previously, the test engine is configured for the tests to be performed.
- Scanning: The penetration test engine is unleashed at the scheduled time using the planned target list and test selection. The results of the entire test run are logged to text log files for analysis. This should be a monitored process so that if an invasive penetration test causes a disruption to a targeted system, the outage can be reported immediately for recovery.
- Analysis: A knowledgeable and experienced vulnerability analyst screens the test results for the vulnerabilities logged during scanning.
- Record keeping: Record the details of the documented vulnerability in the vulnerability database, identifying the logical and physical characteristics and assigning a response risk level to the vulnerability to differentiate the truly urgent from the merely critical.

Intranet Vulnerability Assessment

The intranet vulnerability assessment process is designed to find and document selected vulnerabilities that are likely to be present on the internal network of the organization.

Attackers from this direction are often internal members of the organization, affiliates of business partners, or automated attack vectors (such as viruses and worms).

This assessment is usually performed against selected critical internal devices with a known, high value by using selective penetration testing.

The steps in the process are almost identical to the steps in the Internet vulnerability assessment, except as noted.

- Planning, scheduling, and notification of the penetration testing: There will be substantially more systems to assess. Often intranet administrators prefer penetration testing be performed during working hours.
- Target selection: At first, the penetration test scanning and analysis should focus on testing only the highest value, most critical systems. As the configuration of these systems is improved, and fewer candidate vulnerabilities are found in the scanning step, the target list can be expanded.
- Test selection: The selection of the tests to be performed usually evolves over time to match the evolution of the threat environment. Most organizations focus their intranet scanning efforts on a few, very critical vulnerabilities at first, and then expand the test pool to include more scripts.
- Scanning: Just as in Internet scanning, the process should be monitored, so that if an invasive penetration test causes disruption, it can be reported for repair.

- Analysis: Follows the same three steps: classify, validate and document.
- Record keeping: Identical to the one followed in Internet vulnerability analysis.

Platform Security Validation

- The platform security validation (PSV) process is designed to find and document the vulnerabilities that may be present because of misconfigured systems in use within the organization.
- These misconfigured systems fail to comply with company policy or standards as adopted by the IT governance groups and communicated in the information security and awareness program.
- Fortunately automated measurement systems are available to help with the intensive process of validating the compliance of platform configuration with policy.

Wireless Vulnerability Assessment

The wireless vulnerability assessment process is designed to find and document the vulnerabilities that may be present in the wireless local area networks of the organization.

Since attackers from this direction are likely to take advantage of any loophole or flaw, this assessment is usually performed against all publicly accessible areas using every possible wireless penetration testing approach.

Modem Vulnerability Assessment

The modem vulnerability assessment process is designed to find and document any vulnerability that is present on dialup modems connected to the organization's networks.

Since attackers from this direction take advantage of any loophole or flaw, this assessment is usually performed against all telephone numbers owned by the organization, using every possible penetration testing approach.

One of the elements of this process, using scripted dialing attacks against a pool of phone numbers, is often called war dialing.

Documenting Vulnerabilities

The vulnerability database, like the risk, threat, and attack database, both stores and tracks information.

It should provide details about the vulnerability being reported as well as linkage to the information assets characterized in the risk, threat, and attack database.

While this can be manual data storage, the low cost and ease of use of relational databases makes them a more realistic choice.

The data stored in the vulnerability database should include:

- A unique vulnerability ID number for reporting and tracking remediation actions
- Linkage to the risk, threat, and attack database based on the physical information asset underlying the vulnerability
- Vulnerability details usually based on the test script used for the scanning step of the process
- Dates and times of notification and remediation activities
- Current status of the vulnerability instance
- Comments
- Other fields as needed

The vulnerability database is an essential part of effective remediation to avoid losing track of specific vulnerability instances as they are reported and remediated.

Remediating Vulnerabilities

The objective of remediation is to repair the flaw causing a vulnerability instance or remove the risk from the vulnerability.

As a last resort, informed decision makers with the proper authority can accept the risk.

When approaching the remediation process, it is important to recognize that building relationships with those who control the information assets is the key to success.

Success depends on the organization adopting a team approach to remediation, in place of cross-organizational push and pull.

Acceptance of Risk

In some instances risk must simply be acknowledged as part of organization's business process.

The information security professional must assure the general management community that the decisions made to assume risk for the organization are made by properly informed decision makers.

These decision makers must have the proper level of authority to assume the risk.

In the final analysis, the information security group must make sure the right people make risk assumption decisions with complete knowledge of the impact of the decision balanced against the cost of the possible security controls.

Threat Removal

In some circumstances, threats can be removed without repairing the vulnerability.

The vulnerability can no longer be exploited, and the risk has been removed.

Other vulnerabilities may be amenable to other controls that allow an inexpensive repair and still remove the risk from the situation.

Vulnerability Repair

The optimum solution in most cases is to repair the vulnerability.

Applying patch software or implementing a workaround to the vulnerability often accomplishes this.

In some cases, simply disabling the service removes the vulnerability. In other cases, simple remedies are possible.

Of course, a common remedy remains the application of a software patch to make the system function in the expected fashion and to remove the vulnerability.

Readiness and Review

The primary goal of the readiness and review domain is to keep the information security program functioning as designed and continuously improving over time.

This is accomplished by:

- Policy review: Sound policy needs to be reviewed and refreshed from time to time to provide a current foundation for the information security program.
- Readiness review: Major planning components should be reviewed on a periodic basis to ensure they are current, accurate, and appropriate.
- Rehearsals: When possible, major plan elements should be rehearsed.

- Policy review is the primary initiator of the readiness and review domain.

As policy is revised or current policy is confirmed, the various planning elements are reviewed for compliance, the information security program is reviewed, and rehearsals are held to make sure all participants are capable of responding as needed.

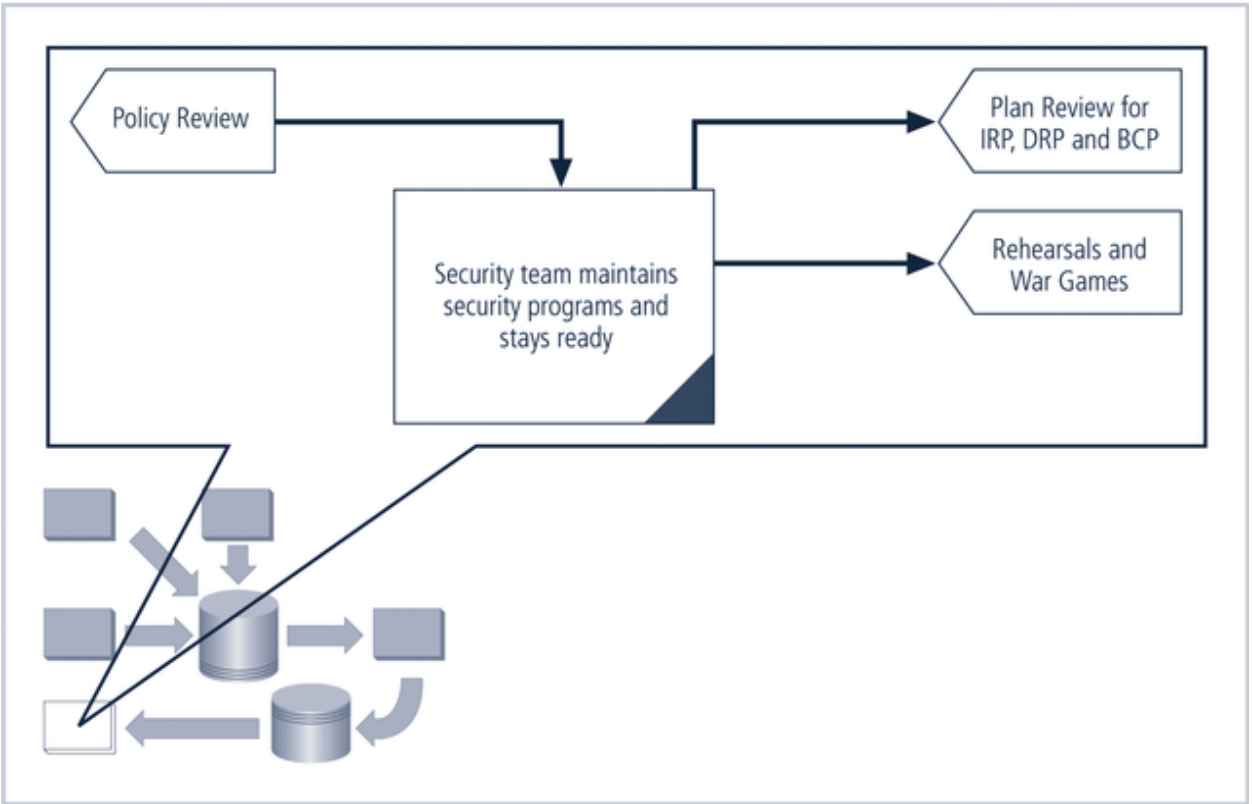


FIGURE 12-7 Readiness and review

Digital Forensics

- Digital forensics is used to investigate what happened during attack on assets and how attack occurred
- Based on the field of traditional forensics
- Involves preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
- Evidentiary material (EM) is any information that could potentially support organizations legal or policy-based case against suspect

- Digital forensics is used for two key purposes:
    - To investigate allegations of digital malfeasance
    - To perform root cause analysis
- Organization chooses one of two approaches:
    - Protect and forget (patch and proceed): focuses on defense of data and systems that house, use, and transmit it
    - Apprehend and prosecute (pursue and prosecute): focuses on identification and apprehension of responsible individuals, with

additional attention on collection and preservation of potential EM that might support administrative or criminal prosecution