12

Information Security Maintenance

> The only thing we can predict with certainty is change.
>
> JAYNE SPAIN, DEPARTMENT OF CHILDREN AND FAMILY LEARNING, STATE OF MINNESOTA

PRINCIPLES of INFORMATION SECURITY
Second Edition

Learning Objectives

Upon completion of this material, you should be able to:

- Understand why maintenance of the information security program is needed on an ongoing basis
- Recognize recommended security management models
- Define a model for a full maintenance program
- Identify the key factors involved in monitoring the external and internal environment

Learning Objectives (continued)

- Understand how planning and risk assessment tie into information security maintenance
- Understand how vulnerability assessment and remediation tie into information security maintenance
- Understand how to build readiness and review procedures into information security maintenance

Introduction

- Organization should avoid overconfidence after implementation of improved information security profile
- Organizational changes that may occur include: new assets acquired; new vulnerabilities emerge; business priorities shift; partnerships form or dissolve; organizational divestiture and acquisition; employee hire and turnover
- If program does not adjust, may be necessary to begin cycle again
- More expensive to reengineer information security profile again and again

Security Management Models

- Management model must be adopted to manage and operate ongoing security program

- Models are frameworks that structure tasks of managing particular set of activities or business functions

The ISO Network Management Model

- Five-layer approach that provides structure to administration and management of networks and systems

- Addresses management and operation thorough five areas: fault management; configuration and name management; accounting management; performance management; and security management

The ISO Network Management Model (continued)

- Five areas of ISO model transformed into five areas of security management:
  - Fault management
  - Configuration and change management
  - Accounting and auditing management
  - Performance management
  - Security program 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: administration of the configuration of security program components
- Change management: administration of changes in strategy, operation, or components
- Each involve non-technical as well as technical changes:
  - Non-technical 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

- Changes to information security may require implementing new policies and procedures
- Document manager should maintain master copy of each document; record and archive revisions made; and keep copies of revisions
- Policy revisions not implemented and enforceable until they have been disseminated, read, understood, and agreed to
- Software available to make creation, modification, dissemination, and agreement documentation processes more manageable

Technical Configuration and Change Management

- Terms associated with management of technical configuration and change: configuration item; version; build
- Four steps associated with configuration management
  - Configuration identification
  - Configuration control
  - Configuration status accounting
  - Configuration audit

Accounting and Auditing Management

- Chargeback accounting enables organizations to internally charge for system use
- Some resource usage is commonly tracked
- Accounting management involves monitoring use of particular component of a system
- Auditing is process of reviewing use of a system, not to check performance, but to determine misuse or malfeasance; automated tools can assist

Performance Management

- Important to monitor performance of security systems and underlying IT infrastructure to determine if they are working effectively
- Common metrics are applicable in security, especially when components being managed are associated with network traffic
- To evaluate ongoing performance of security system, performance baselines are established

Security Program Management

- ISO five-area-based framework supports a structured management model by ensuring various areas are addressed

- Two standards are designed to assist in this effort

- Part 2 of the British Standard (BS) 7799 introduces process model: plan; do; check; act

The Maintenance Model

- Designed to focus organizational effort on maintaining systems
- Recommended maintenance model based on five subject areas
  - External monitoring
  - Internal monitoring
  - Planning and risk assessment
  - Vulnerability assessment and remediation
  - Readiness and review

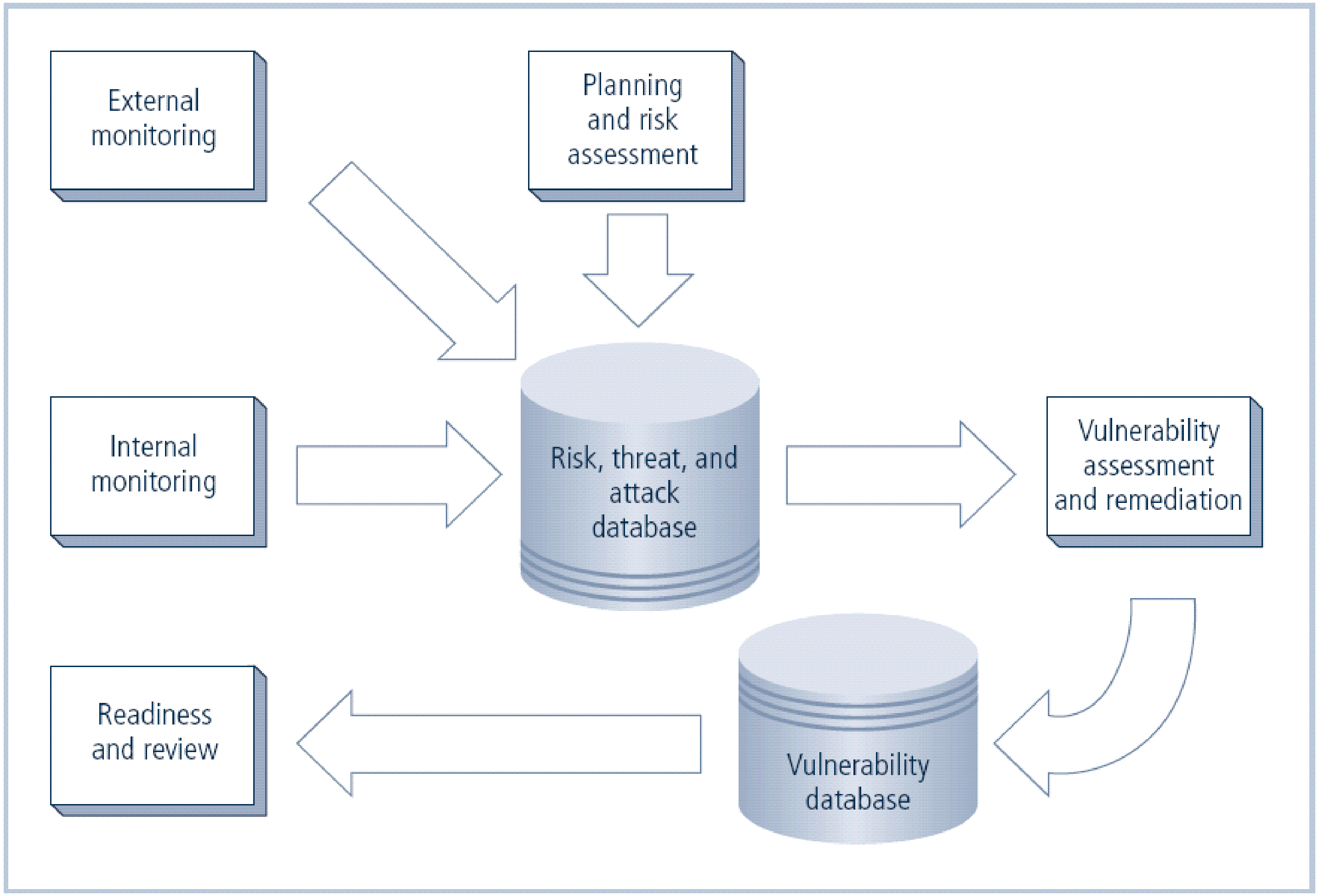
External monitoring
Planning and risk assessment
Internal monitoring
Risk, threat, and attack database
Vulnerability assessment and remediation
Readiness and review
Vulnerability database

FIGURE 12-1 The Maintenance Model

Monitoring the External Environment

- Objective to provide early awareness of new threats, threat agents, vulnerabilities, and attacks that is needed to mount an effective defense
- Entails collecting intelligence from data sources and giving that intelligence context and meaning for use by organizational decision makers

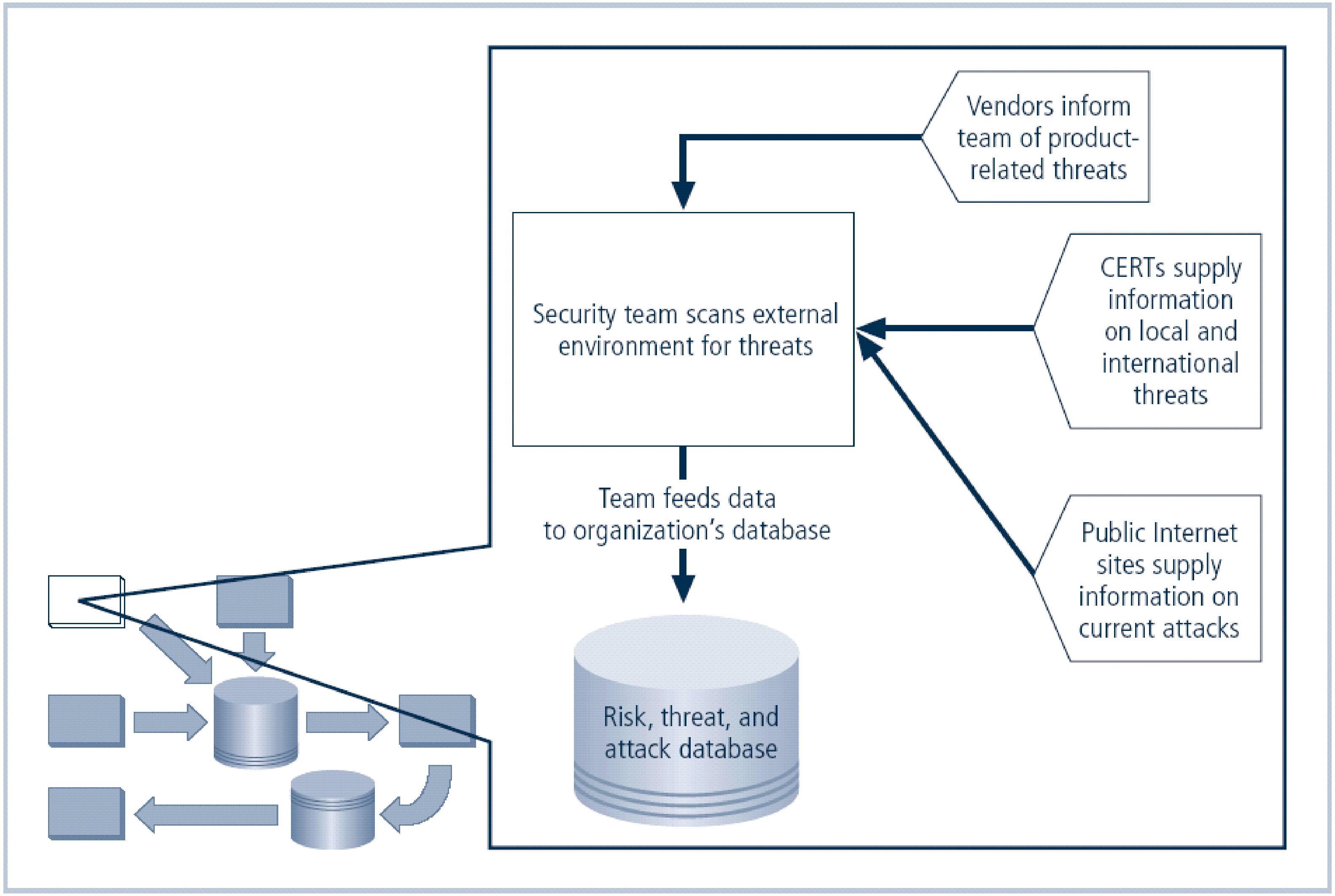
Vendors inform team of product-related threats
Security team scans external environment for threats
CERTs supply information on local and international threats
Public Internet sites supply information on current attacks
Team feeds data to organization's database
Risk, threat, and attack database

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

- Function of external monitoring process is to monitor activity, report results, and escalate warnings
- Monitoring process has three primary deliverables
  - Specific warning bulletins issued when developing threats and specific attacks pose measurable risk to organization
  - Periodic summaries of external information
  - Detailed intelligence on highest risk warnings

Data Collection and Management

- Over time, external monitoring processes should capture knowledge about external environment in appropriate formats

- External monitoring collects raw intelligence, filters for relevance, assigns a relative risk impact, and communicates to decision makers in time to make a difference

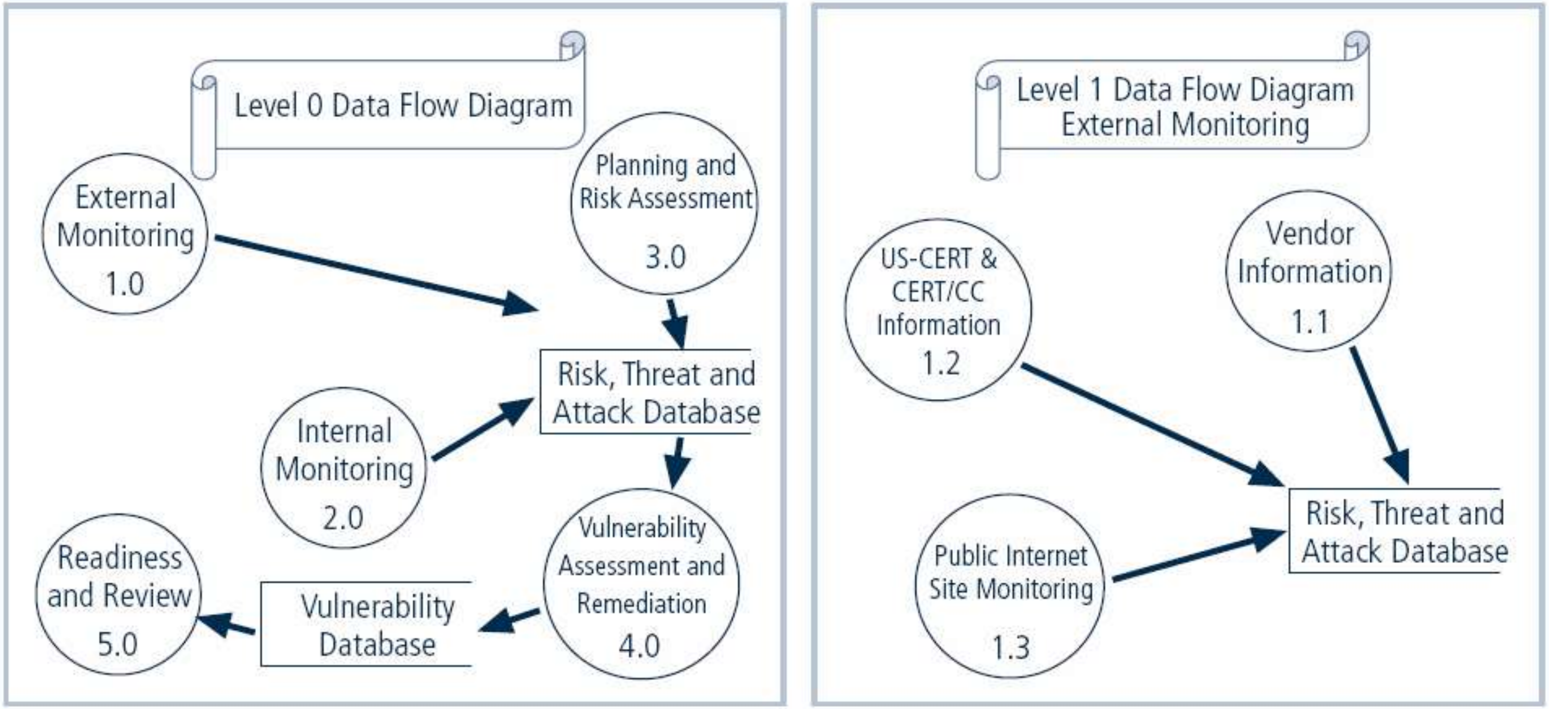
Level 0 Data Flow Diagram
External Monitoring 1.0
Planning and Risk Assessment 3.0
Risk, Threat and Attack Database
Internal Monitoring 2.0
Vulnerability Assessment and Remediation 4.0
Readiness and Review 5.0
Vulnerability Database
Level 1 Data Flow Diagram External Monitoring
US-CERT & CERT/CC Information 1.2
Vendor Information 1.1
Risk, Threat and Attack Database
Public Internet Site Monitoring 1.3

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

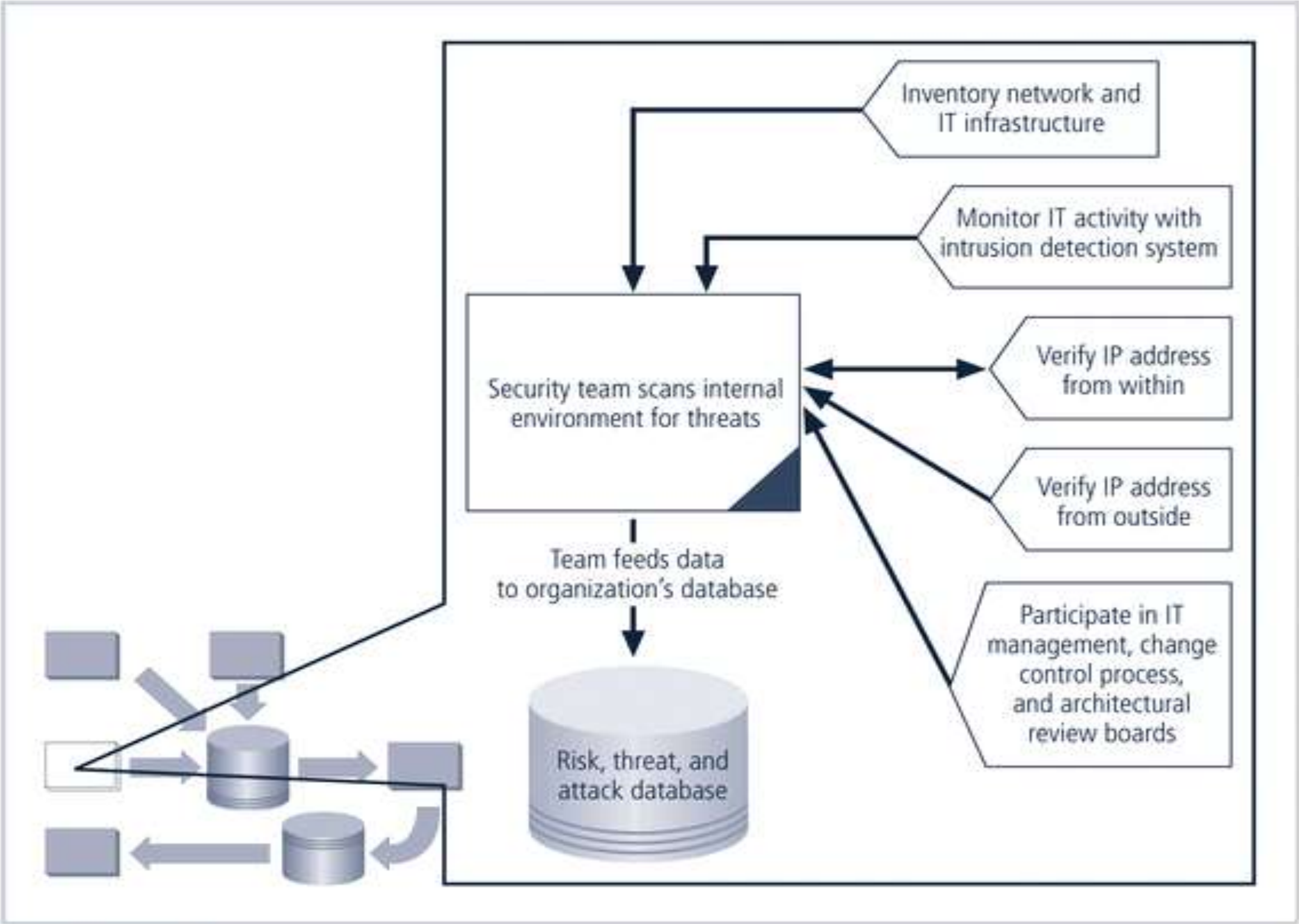
Inventory network and IT infrastructure
Monitor IT activity with intrusion detection system
Security team scans internal environment for threats
Verify IP address from within
Verify IP address from outside
Participate in IT management, change control process, and architectural review boards
Team feeds data to organization's database
Risk, threat, and attack database

FIGURE 12-4 Internal monitoring

Network Characterization and Inventory

- Organizations should have carefully planned and fully populated inventory for network devices, communication channels, and computing devices

- Once characteristics 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

- Primary value is increased awareness of the impact of change
- Awareness must be translated into description of risk that is caused by change through operational risk assessment
- Awareness of change based on two primary activities within IT governance process
    - Architecture review boards
    - IT change control process

Making Intrusion Detection Systems Work

- The most important value of raw intelligence provided by intrusion detection systems (IDS) is providing indicators of current or imminent vulnerabilities
- Log files from IDS engines can be mined for information
- Another IDS monitoring element is traffic analysis
- Analyzing attack signatures for unsuccessful system attacks can identify weaknesses in various security efforts

Detecting Differences

- Difference analysis: procedure that compares current state of network segment against known previous state of same segment

- Differences between the current state and the baseline state that are unexpected could be a sign of trouble and need investigation

Planning and Risk Assessment

- Primary objective to keep lookout over entire information security program
- Accomplished by identifying and planning ongoing information security activities that further reduce risk

Planning and Risk Assessment (continued)

- Primary objectives
  - Establishing a formal information security program review
  - Instituting formal project identification, selection, planning and management processes
  - Coordinating with IT project teams to introduce risk assessment and review for all IT projects
  - Integrating a mindset of risk assessment across organization

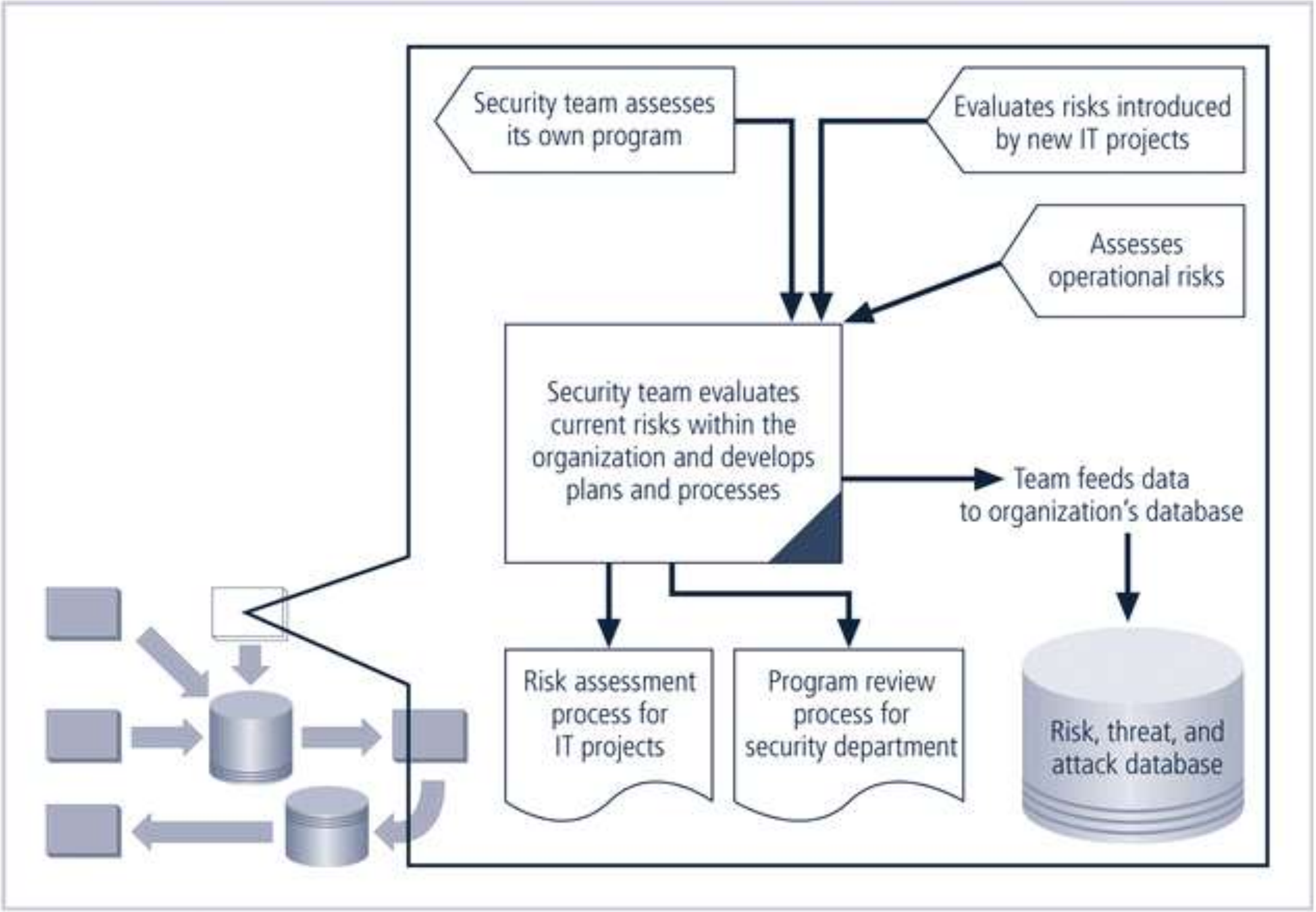
Security team assesses its own program
Evaluates risks introduced by new IT projects
Assesses operational risks
Security team evaluates current risks within the organization and develops plans and processes
Team feeds data to organization's database
Risk assessment process for IT projects
Program review process for security department
Risk, threat, and attack database

FIGURE 12-5 Planning and risk assessments

Information Security Program Planning and Review

- Periodic review of ongoing information security program coupled with planning for enhancements and extensions is recommended
- Should examine IT needs of future organization and impact those needs have on information security
- A recommended approach takes advantage of the fact most organizations have annual capital budget planning cycles and manage security projects as part of that process

Information Security Program Planning and Review (continued)

- Large projects should broken into smaller projects for several reasons
  - Smaller projects tend to have more manageable impacts on networks and users
  - Larger projects tend to complicate change control process in implementation phase
  - Shorter planning, development, and implementation schedules reduce uncertainty
  - Most large projects can easily be broken down into smaller projects, giving more opportunities to change direction and gain flexibility

Security Risk Assessments

- A key component for driving security program change is information security operational risk assessment (RA)
- RA identifies and documents risk that project, process, or action introduces to organization and offers suggestions for controls
- Information security group coordinates preparation of many types of RA documents

Vulnerability Assessment and Remediation

- Primary goal is identification of specific, documented vulnerabilities and their timely remediation
- Accomplished by:
  - Using vulnerability assessment procedures
  - Documenting background information and providing tested remediation procedures for reported vulnerabilities
  - Tracking vulnerabilities from when they are identified
  - Communicating vulnerability information to owners of vulnerable systems

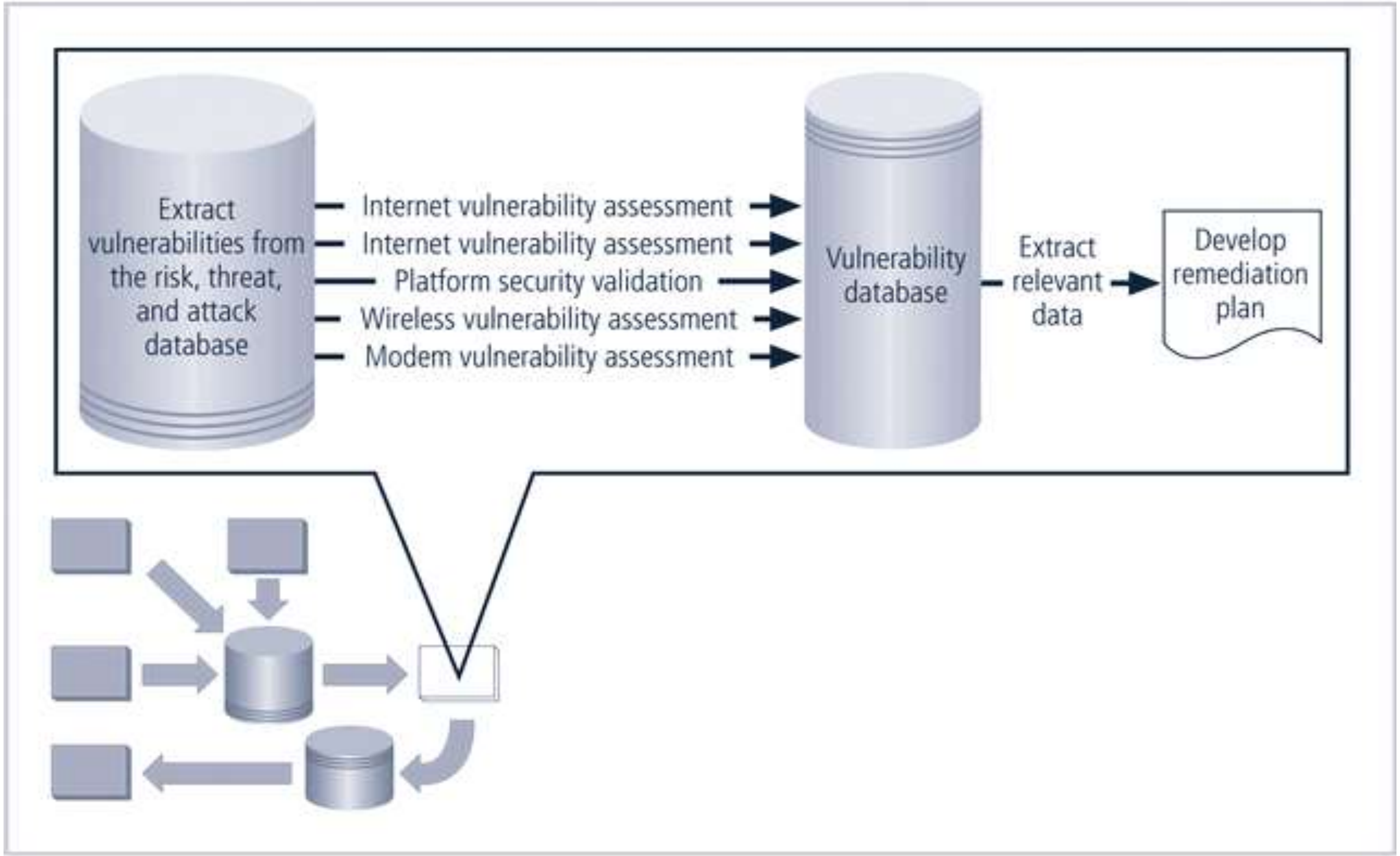
Extract vulnerabilities from the risk, threat, and attack database
Internet vulnerability assessment
Internet vulnerability assessment
Platform security validation
Wireless vulnerability assessment
Modem vulnerability assessment
Vulnerability database
Extract relevant data
Develop remediation plan

FIGURE 12-6 Vulnerability Assessment and Remediation

Vulnerability Assessment

- Process of identifying and documenting specific and provable flaws in organization’s information asset environment

- Five vulnerability assessment processes that follow can serve many organizations as they attempt to balance intrusiveness of vulnerability assessment with need for stable and productive production environment

Internet Vulnerability Assessment

- Designed to find and document vulnerabilities present in organization’s public-facing network
- Steps in the process include:
  - Planning, scheduling and notification
  - Target selection
  - Test selection
  - Scanning
  - Analysis
  - Record keeping

Intranet Vulnerability Assessment

- Designed to find and document selected vulnerabilities present on the internal network
- Attackers often internal members of 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
- Steps in process almost identical to steps in Internet vulnerability assessment

Platform Security Validation

- Designed to find and document vulnerabilities that may be present because of misconfigured systems in use within organization
- These misconfigured systems fail to comply with company policy or standards
- Fortunately, automated measurement systems are available to help with the intensive process of validating compliance of platform configuration with policy

Wireless Vulnerability Assessment

- Designed to find and document vulnerabilities that may be present in wireless local area networks of organization

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

Modem Vulnerability Assessment

- Designed to find and document any vulnerability present on dial-up modems connected to organization's networks
- Since attackers from this direction take advantage of any loophole or flaw, assessment usually performed against all telephone numbers owned by the organization
- One elements of this process, often called war dialing, uses scripted dialing attacks against pool of phone numbers

Documenting Vulnerabilities

- Vulnerability tracking database should provide details as well as a link to the information assets
- Low-cost and ease of use makes relational databases a realistic choice
- Vulnerability database is an essential part of effective remediation

Remediating Vulnerabilities

- Objective is to repair flaw causing a vulnerability instance or remove risk associated with vulnerability
- As last resort, informed decision makers with proper authority can accept risk
- Important to recognize that building relationships with those who control information assets is key to success
- Success depends on organization adopting team approach to remediation, in place of cross-organizational push and pull

Acceptance or Transference of Risk

- In some instances, risk must simply be acknowledged as part of organization’s business process

- Management must be assured that decisions made to assume risk the organization are made by properly informed decision makers

- Information security must make sure the right people make risk assumption decisions with complete knowledge of the impact of the decision

Threat Removal

- In some circumstances, threats can be removed without repairing vulnerability
- Vulnerability can no longer be exploited, and risk has been removed
- Other vulnerabilities may be amenable to other controls that do not allow an expensive repair and still remove risk from situation

Vulnerability Repair

- Optimum solution in most cases is to repair vulnerability
- Applying patch software or implementing a workaround often accomplishes this
- In some cases, simply disabling the service removes vulnerability; in other cases, simple remedies are possible
- Most common repair is application of a software patch

Readiness and Review

- Primary goal to keep information security program functioning as designed and continuously improving
- Accomplished by:
  - Policy review
  - Program review
  - Rehearsals

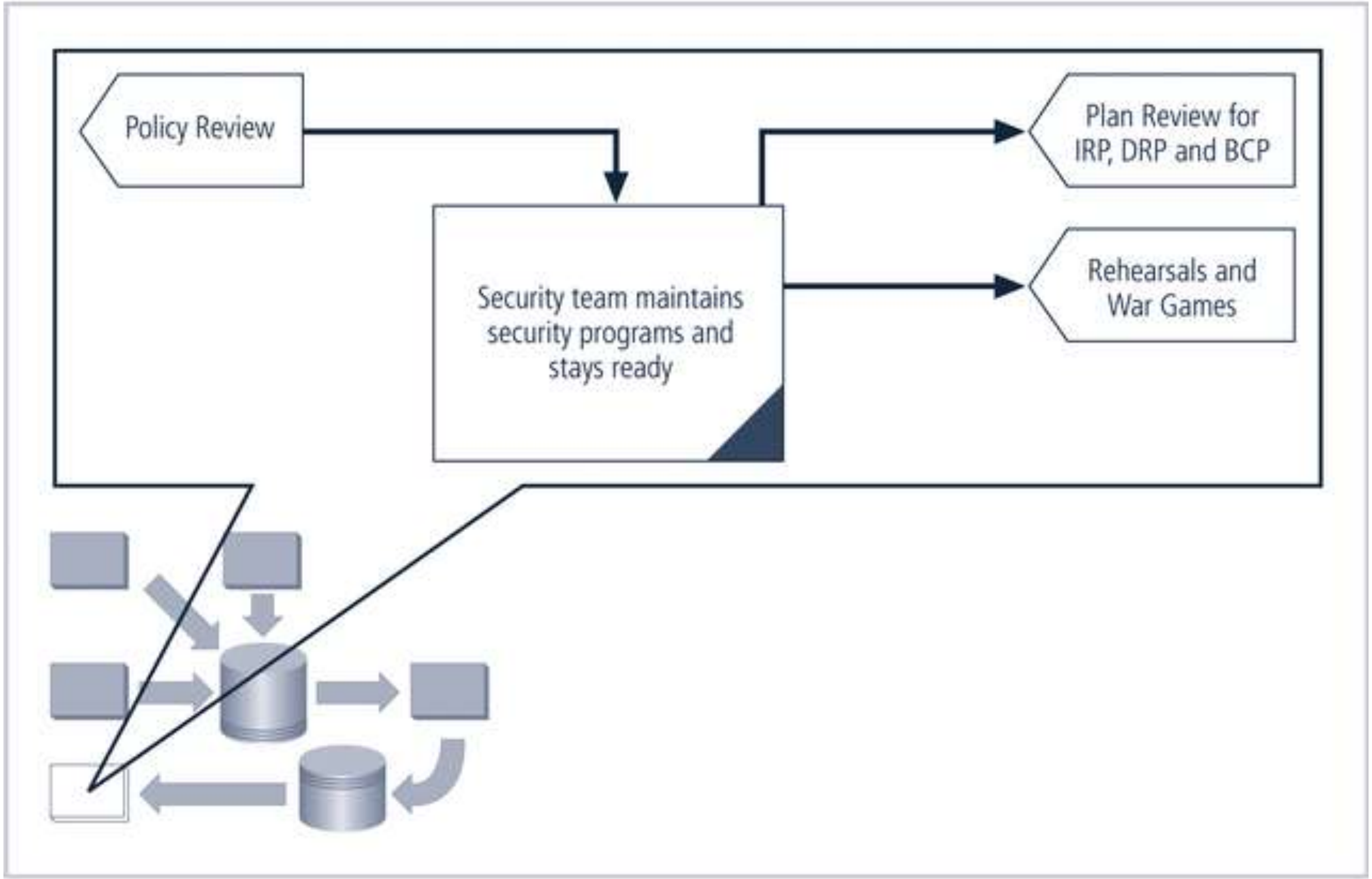
Policy Review
Plan Review for IRP, DRP and BCP
Security team maintains security programs and stays ready
Rehearsals and War Games

FIGURE 12-7 Readiness and review

Summary

- Maintenance of information security program is essential
- Security management models assist in planning for ongoing operations
- It is necessary to monitor external and internal environment

Summary

- Planning and risk assessment essential parts of information security maintenance
- Need to understand how vulnerability assessment and remediation tie into information security maintenance
- Need to understand how to build readiness and review procedures into information security maintenance