UNIT V

INFORMATION SECURITY PROJECT MANAGEMENT

Once the organization's vision and objectives are documented and understood, the processes for translating the blueprint into a project plan can be defined. Organizational change is not easily accomplished.

The major steps in executing the project plan:

- Planning the project.
- Supervising tasks and action steps within the project plan.
- Wrapping up the project plan.

The project plan can be developed in any number of ways. Each organization has to determine its own project management methodology for IT and information security projects. Whenever possible, information security projects should follow the organizational practices of project management. If your organization does not have clearly defined project management practices, the following general guidelines on project management practices can be applied.

Developing the Project Plan

Planning for the implementation phase involves the creation of a detailed project plan. The creation of the project plan can be accomplished using a simple planning tool, such as the work breakdown structure (WBS). Common task attributes are:

- Work to be accomplished (activities and deliverables)
- Individuals (or skills set) assigned to perform the task
- Start and end dates for the task (when known)
- Amount of effort required to complete the task in hours or work days
- Estimated capital expenses for the task
- Estimated noncapital expenses for the task
- Other tasks on which the task depends

Each major task is then further divided into either smaller tasks or specific action steps. Key components of the project plan include the following:

- Identify work to be accomplished.
- Describe the skill set or individual person needed to accomplish the task.
- Focus on determining only completion dates for major milestones.
- Estimate the expected capital expenses for the completion of this task, subtask, or action item.
- Estimate the expected noncapital expenses for the completion of the task, subtask, or action item.
- Note wherever possible the dependencies of other tasks or action steps on the task or action step at hand.

Project Planning Considerations

The project plan is developed, adding detail to the plan is not always straightforward. The following special considerations:

- Financial
- Priority
- Time
- Staff
- Scope
- Procurement
- Organizational feasibility
- Training and indoctrination
- Change control and technology governance

The following financial considerations:

- No matter what information security needs exist in the organization, the amount of effort that can be expended depends on the funds available.
- A cost-benefit analysis prepared earlier in the lifecycle must be verified prior to developing the project plan.

- In many organizations, the information security budget is a subsection of the overall IT budget.
- In others, information security is a separate budget category that may have parity with the IT budget.
- Both public and private organizations have budgetary constraints, albeit 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.

The following considerations regarding priority:

- In general, the most important information security controls should be scheduled first.
- The implementation of controls is guided by the prioritization of threats and the value of the information assets that are threatened.
- A control that is not considered as important as other choices may be moved ahead of more important options if it addresses a group of specific vulnerabilities and will cumulatively improve the security posture of the organization to a greater degree than other individual controls, even if they have a higher individual priority.

The time and scheduling considerations:

- Time is another constraint that has a broad impact on the development of the project plan.
- Time can impact dozens of points in the development of a project plan, including the following:

    - Time to order and receive a security control due to backlogs of the vendor or manufacturer
    - Time to install and configure the control
    - Time to train the users
    - Time to realize the return on investment of the control

Staffing considerations:

- The lack of enough qualified, trained, and available personnel also constrains the project plan.
- Experienced staff is often needed to implement available technologies and to develop and implement policies and training programs.
- If no staff members are trained to configure a firewall that is being purchased, someone must be trained, or someone must be hired who is experienced with that particular technology.

Procurement considerations:

- All IT and information security planners must consider the acquisition of goods and services.
- There are a number of constraints on the selection process for equipment and services in most organizations, specifically in the selection of certain service vendors or products from manufacturers and suppliers.
- These constraints may change the specifics of a particular technology or even eliminate it from the realm of possibilities.

Some considerations surrounding organizational feasibility:

- Policies require time to develop, and new technologies require time to be installed, configured, and tested.
- Employees need to understand how a new information security program impacts their working lives.
- The goal of the project plan is to prevent new security components from directly impacting daily operations.
- This means that changes should be transparent to systems users unless the new technology causes changes to procedures, such as requiring additional authentication or verification.

Some considerations surrounding training and indoctrination:

- The size of the organization and the normal conduct of business may preclude a single large training program on security procedures or technologies.

- As a result, the organization should conduct a phased-in or pilot approach to implementation, such as roll-out training for one department at a time.
- In the case of policies, it may be sufficient to brief all supervisors on new policy and then have the supervisors update end users in normal meetings.
- Ensure that compliance documents are also distributed that require all employees to read, understand, and agree to the new policies.

Scope Considerations

Project scope describes the amount of time and effort-hours needed to deliver the planned features and quality level of the project deliverables. The scope of any given project plan should be carefully reviewed and kept as small as possible given the project's objectives. Organizations should implement large information security projects in stages, in order to control scope. There are several reasons why the scope of information security projects must be evaluated and adjusted with care.

The need for project management

- Project management requires a unique set of skills and a thorough understanding of a broad body of specialized knowledge.
- Realistically, most information security projects require a trained project manager—a CISO or skilled IT manager who is versed in project management techniques and can oversee the project.
- In addition, even experienced project managers are advised to seek expert assistance when engaging in a formal bidding process to select advanced or integrated technologies or outsourced services.

Concept of supervised implementation

- Some organizations may designate a champion from general management to supervise the implementation of the project plan for security information.
- An alternative is to designate a senior IT manager or the CIO of the organization to lead the implementation.

- The optimal solution is to designate a suitable person from the information security community of interest, since the inherent focus is on the information security needs of the organization.
- In the final analysis, it is up to each organization to find the leadership for a successful project implementation that best suits its specific needs and the personalities and politics of the organizational culture.

The process of executing the plan

- Once a project is underway, it is managed to completion using a process known as a negative feedback loop or cybernetic loop, which ensures that progress, is measured periodically. The measured results are compared against expected results.
- When significant deviation occurs, corrective action is taken to bring the task that is deviating from plan back into compliance with the projection, or else the estimate is revised in light of new information. Corrective action is required because of two basic situations: either the estimate was flawed or performance has lagged.
- When an estimate is flawed, as when the number of effort-hours required is underestimated, the plan should be corrected and downstream tasks updated to reflect the change.
- When performance has lagged due, for example, to high turnover of skilled employees, correction is required by adding resources, lengthening the schedule, or reducing the quality or quantity of the deliverable.
- The decisions are usually expressed in terms of trade-offs. A project manager can often adjust one of the three following planning parameters for the task being corrected:

    - Effort and money allocated
    - Elapsed time or scheduling impact
    - Quality or quantity of the deliverable

The process of project wrap-up

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

TECHNICAL ASPECTS OF IMPLEMENTATION

Some parts of the implementation process are technical in nature and deal with the application of technology, while others are not and deal instead with the human interface to technical systems.

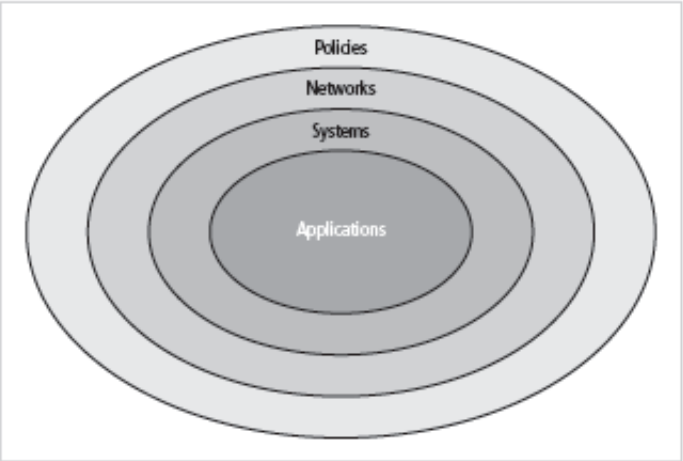
Conversion strategies

As the components of the new security system are planned, provisions must be made for the changeover from the previous method of performing a task to the new method. The four basic approaches used for changing from an old system or process to a new one are:

- Direct changeover: Also known as going "cold turkey," a direct changeover involves stopping the old method and beginning the new.
- Phase implementation: The most common approach, phase implementation involves rolling out a piece of the system across the entire organization.
- Pilot implementation: Pilot implementation involves implementing all security improvements in a single office, department, or division, and resolving issues within that group before expanding to the rest of the organization.
- Parallel operations: Parallel operations involve running the new methods alongside the old methods.

The Bull's-Eye Model

By reviewing the information security blueprint and the current state of the organization's information security efforts in terms of the four layers of the bulls-eye model, project planners can determine where to lobby for expanded information security capabilities.



This approach relies on a process of evaluating project plans in a progression through four layers:

- Policies

  The foundation of all effective information security programs is sound information security and information technology policy. Since policy establishes the ground rules for the use of all systems and describes what is appropriate and what is inappropriate, it enables all other information security components to function correctly.
- Networks

  This layer includes designing and implementing the secure zone for the organization thereby providing authentication and authorizations to users for connecting to networks.
- Systems

  This layer includes computers used as servers, desktop computers, and systems used for process control and manufacturing systems.
- Applications

  The layer that receives attention last is the one that deals with the application software systems used by the organization to accomplish its work.

The bull's-eye model can be used to evaluate the sequence of steps taken to integrate parts of the information security blueprint into a project plan.

This means the following:

- Until sound and useable IT and information security policy is developed, communicated, and enforced, no additional resources should be spent on other controls.
- Until effective network controls are designed and deployed, all resources should be spent to achieve that goal.
- After policy and network controls are implemented, implementation should focus on the information, process, and manufacturing systems of the organization.
- Once there is assurance that policy is in place, networks are secure, and systems are safe, attention should move to the assessment and remediation of the security of the organization's applications.

To Outsource or Not

Just as some organizations outsource IT operations, so too can organizations outsource part of or all of their information security programs. When an organization has outsourced IT services, information security should be part of the contract arrangement with the outsourcer. Because of the complex nature of outsourcing, it is best to hire the finest outsourcing specialists possible and then retain the best attorneys possible to negotiate and verify the legal and technical intricacies of the outsourcing contract.

Technology Governance and Change Control

There are other factors that determine the success of an organization's IT and information security are technology governance and change control processes. Technology governance is a complex process that an organization uses to manage the impacts and costs caused by technology implementation, innovation, and obsolescence. Technology governance also facilitates the communication about technical advances and issues across the organization. Medium or large organizations deal with the impact of technical change on the operation of the organization through a change control process.

By managing the process of change, the organization can:

- Improve communication about change
- Enhance coordination between organizational groups as change is scheduled and completed

- Reduce unintended consequences by having a process to resolve potential conflict and disruption
- Improve quality of service as potential failures are eliminated and groups work together
- Assure management that all groups are complying with the organization's policies regarding technology governance, procurement, accounting, and information security

NONTECHNICAL ASPECTS OF IMPLEMENTATION

Other parts of the implementation process are not technical in nature and deal with the human interface to technical systems. These topics include creating a culture of change management as well as considerations for organizations facing change.

The Culture of Change Management

In any major project, the prospect of change, the familiar shifting to the unfamiliar, can cause employees to unconsciously or consciously resist. Even when employees embrace change, the stress of making changes and adjusting to the new procedures can increase the probability of mistakes or create vulnerabilities in the system. By understanding and applying some of the basic tenets of change management, project managers can lower the resistance to change, and they can even build resilience for changes, thereby making ongoing change more palatable to the entire organization.

One of the oldest models of change, the Lewin change model, which consists of:

- Unfreezing: "Thawing out" hard and fast habits and established procedures
- Moving: The transition between the old way and the new way
- Refreezing: The integration of the new methods into the organizational culture by creating an atmosphere in which the changes are accepted as the preferred way of accomplishing the requisite tasks

Considerations for Organizational Change

Steps can be taken to make an organization more amenable to change. These steps reduce resistance to change from the beginning of the planning process and encourage members of the organization to be more flexible as changes occur during project implementation.

Reduce resistance to change from the outset

- The level of resistance to change affects the ease with which an organization is able to implement the changes it needs.
- The more ingrained the previous methods and behaviors are within the organization, the more difficult making the change is likely to be.
- The primary mechanism used to overcome this resistance to change is to improve the interaction between the affected members of the organization and the project planners in the earlier phases of the SecSDLC.
- The guideline to improve this interaction is a three-step process: communicate, educate, and involve.

Develop a culture that supports change

- An ideal organization fosters resilience to change.
- This resilience means the organization has come to expect that change is a necessary part of organizational culture, and embracing change is more productive than fighting it.
- To develop such a culture, the organization must successfully accomplish many projects that require change.

INFORMATION SYSTEMS SECURITY CERTIFICATION AND ACCREDITATION

It may seem that only systems handling secret government data require security certification or accreditation. Organizations are increasingly finding that in order to comply with the myriad of new federal regulations protecting personal privacy, their systems need to have some formal mechanism for verification and validation.

Certification versus Accreditation

In security management, accreditation authorizes an IT system to process, store, or transmit information. Certification, which is defined as "the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.". Organizations pursue accreditation or certification to gain a competitive advantage, or to provide assurance or confidence to their customers.

NIST SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

NIST SP 800-37 states that "The security certification and accreditation process consists of four distinct phases:

- Initiation Phase
- Security Certification Phase
- Security Accreditation Phase
- Continuous Monitoring Phase

NSTISS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP)

Nnational security interest systems have their own security certification and accreditation standards. The National Information Assurance Certification and Accreditation Process (NIACAP) establish the minimum national standards for certifying and accrediting national security systems. The NIACAP is designed to certify that the IS meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle.

ISO 27001/27002 Systems Certification and Accreditation

Entities outside the United States apply the standards provided under the International Standards Organization standard ISO 27001 and 27002. Organizations wishing to

demonstrate their systems have met this international standard must follow the certification process.

POSITIONING AND STAFFING THE SECURITY FUNCTION

Charles Cresson Wood indicates that the security function can be placed within the following organizational functions:

- IT function, as a peer of other functions (networks, applications development, and help desk)
- Physical security function, as a peer of physical security or protective services
- Administrative services function, as a peer of human resources or purchasing
- Insurance and risk management function
- Legal department

The challenge is to design a reporting structure for the information security function that balances the competing needs of each community of interest. Organizations find compromise by placing the information security function where it can best balance its duty to enforce organizational policy with its ability to provide the education, training, awareness, and customer service needed to make information security an integral part of the organizational culture.

Staffing the Information Security Function

The criteria on which selecting information security personnel is based, includes the principles of supply and demand. Many future IS professionals seek to enter the security market by gaining the skills, experience, and credentials they need to qualify as a new supply. Until the new supply reaches the demand level, organizations may pay the higher costs associated with limited supply. Once the supply meets or exceeds the demand, the organizations that are hiring these individuals become selective, and the amount they are willing to pay drops. At the present time, the information security industry is experiencing a period of high demand, with few qualified individuals available for organizations seeking their services.

Qualifications and requirements

There are a number of factors that influence an organization's hiring decisions. In many organizations, information security teams lack established roles and responsibilities. For the information security discipline to move forward, these factors must be addressed:

- Management should learn more about position requirements and qualifications for both information security positions and IT positions that impact infosec.
- Upper management should also learn more about the budgetary needs of the infosec function.
- IT and management need to learn more about the level of influence and prestige the information security function should be given in order to be effective.

In most cases, organizations look for a technically qualified information security generalist who has a solid understanding of how an organization operates. In many other career fields, the more specialized professionals become, the more marketable they are. However, in the information security discipline, overspecialization is often a risk. It is important to balance one's technical skills with general information security knowledge.

When hiring information security professionals, organizations frequently look for individuals who understand:

- How an organization operates at all levels
- That information security is usually a management problem and is seldom an exclusively technical problem
- How to work with people and have strong communications and writing skills
- The roles of policy, education, and training
- The threats and attacks facing an organization
- How to protect the organization from attacks
- How business solutions can be applied to solve specific information security problems
- Most mainstream IT technologies (not necessary as experts, but as generalists)
- The terminology of IT and information security

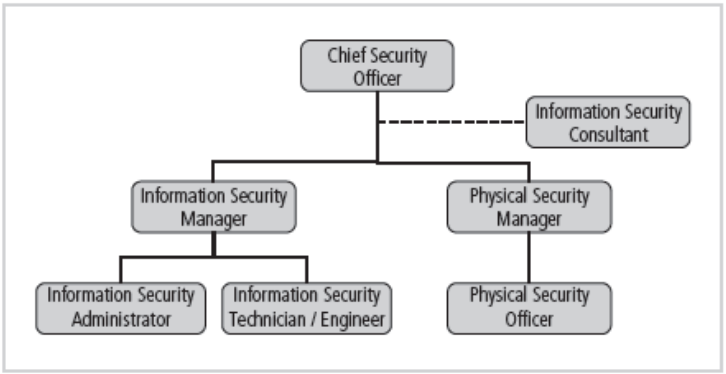
Entry into the information security profession

Many information security professionals enter the field through one of two career paths:

- First, ex-law enforcement and military personnel are often involved in national security and cyber-security tasks and move from those environments into the more business-oriented world of information security.
- Second, technical professionals find themselves working on security applications and processes more often than on traditional IS tasks.

Today, college graduates and upper-division students are selecting and tailoring degree programs to prepare to work in the field of information security. The current perception of information security is that a security professional must first be a proven professional in another field of IT. IT professionals who move into information security, however, tend to focus on the technology—sometimes in place of general information security issues. Organizations can foster greater professionalism in the information security discipline by establishing clearly defined expectations and position descriptions**.**

Information security positions



The use of standard job descriptions can increase the degree of professionalism in the information security field as well as improve the consistency of roles and responsibilities among organizations. Organizations that are revising the roles and responsibilities of information security staff can consult Wood's book, *Information Security Roles and Responsibilities Made Easy*, or Schwartz, Erwin, Weafer, and Briney's report, "Information Security Staffing Help Wanted." The following is an excerpt from this report:

“Definers 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…Then you have the builders. They're the real techies, who create and install security solutions…You have the operators who run and administrate the security tools, the security monitoring function, and the people who continuously improve the processes. This is where all the day-to-day, hard work is done. What I find is we often try to use the same people for all of these roles.”

Position of the chief information security officer

This position is typically considered the top information security officer in the organization. The CISO is usually not an executive-level position and frequently reports to the Chief Information Officer. Though CISOs are business managers first and technologists second, they must also be conversant in all areas of security, including the technical, planning, and policy areas.

The CISO performs the following functions:

- Manages the overall information security program
- Drafts or approves information security policies
- Works with the CIO on strategic plans, develops tactical plans, and works with security managers on operational plans
- Develops information security budgets based on available funding
- Sets priorities for the purchase and implementation of information security projects and technology
- Makes decisions or recommendations on the recruiting, hiring, and firing of security staff
- Acts as the spokesperson for the security team

The most common qualification expected for this type of position is the Certified Information Systems Security Professional. A graduate degree in one of the following areas is also often required: criminal justice, business, or technology. To qualify for this level position, the candidate must demonstrate experience as a security manager and present experience with planning, policy, and budgets.

Position of security manager

- Security managers are accountable for the day-to-day operation of the information security program. They accomplish the objectives that are identified by the CISO and resolve issues that are identified by technicians.
- Within the information security community, there are a number of positions with titles that contain the word manager or other language that suggests management responsibilities, but only those people who are responsible for management functions, such as scheduling, setting relative priorities, or administering budgetary control, should be considered true managers.
- Candidates for this position often have a CISSP. Traditionally, managers earn the CISSP, and technical professionals earn the Global Information Assurance Certification.
- Security managers must have the ability to draft middle- and lower-level policies as well as standards and guidelines. They must have experience in traditional business matters, including budgeting, project management, and hiring and firing. They must also be able to manage technicians, both in the assignment of tasks and in the monitoring of activities.

Position of security technician

- Security technicians are the technically qualified individuals who configure security hardware and software and coordinate with administrators to ensure that security is properly implemented.
- A security technician is often offered as an entry-level position; however, some technical skills are usually required to be hired in this position.
- Just as in the networking field, security technicians tend to be specialized, focusing on one major security technology group and further specializing in one software or hardware package within the group.
- If a security technician wants to move up the corporate hierarchy, he or she must gain an understanding of the general organizational issues related to information security.

- The technical qualifications and position requirements for a security technician are varied. Organizations prefer the expert, certified, proficient technician. Regardless of the area, the particular job description includes some level of experience with a particular hardware and software package. Sometimes familiarity with a technology secures an applicant an interview; however, experience in using the technology is usually required.

EMPLOYMENT POLICIES AND PRACTICES

The general management community of interest should integrate solid information security concepts into the organization's employment policies and practices. If the organization can include security as a documented part of every employee's job description, then information security may be taken more seriously. From an information security perspective, the hiring of employees is a responsibility laden with potential security pitfalls. The CISO and information security manager should establish a dialogue with the human resources department to provide information security input to the guidelines used for hiring personnel.

Job Descriptions

To incorporate information security perspectives into the hiring process, it begins with reviewing and updating all job descriptions. To prevent people from applying for positions based solely on access to sensitive information by having the organization avoid revealing access privileges to prospective employees when it advertises open positions.

Interviews

The next point of contact with a potential employee is the job interview. An opening within the information security department presents a unique opportunity for the security manager to educate HR on the certifications, experience, and qualifications of a good candidate. For other areas, information security should advise HR to limit the information provided to the candidate about the responsibilities and access rights the new hire would have. For those organizations that include on-site visits as part of the interviews, it is important to exercise caution when showing a candidate around the facility.

Background Checks

A background check, which is an investigation into the candidate's past that specifically, looks for criminal behavior that could indicate the potential for future misconduct. A number of regulations govern what the organization can investigate and how much of the information uncovered can be allowed to influence the hiring decision. The security and HR managers should discuss these matters with legal counsel.

Background checks differ in the level of detail and depth with which they examine a candidate. The following are various types of background checks:

- Identity checks
- Education and credential checks
- Previous employment verification
- References checks
- Worker's compensation history
- Motor vehicle records
- Drug history
- Credit history
- Civil court history
- Criminal court history

There are federal regulations regarding the use of personal information in employment practices. One such regulation is the Fair Credit Reporting Act (FCRA), which governs consumer credit reporting agencies and the uses of the information procured from these agencies. These reports contain information on a job candidate's credit history, employment history, and other personal data. Among other things, the FCRA prohibits employers from obtaining these reports unless the candidate is informed in writing that such a report will be requested as part of the employment process. The FCRA also restricts the periods of time these reports can address.

Employment Contracts

Once a candidate has accepted the job offer, the employment contract becomes an important security instrument. Many policies require an employee to agree in writing to

monitoring and nondisclosure agreements. If an existing employee refuses to sign these contracts, the security personnel are placed in a difficult situation. With new employees, security personnel can institute policies classified as "employment contingent upon agreement." This classification means the employee is not actually employed until he or she agrees in writing to conform to the binding organizational policies.

New Hire Orientation

As new employees are introduced into the organization's culture and workflow, they should receive an extensive information security briefing. This briefing should cover all the major policies, procedures, and requirements related to information security within the new position. The levels of authorized access should be outlined, and training should be provided on the secure use of information systems. By the time employees are ready to report to their positions, they should be thoroughly briefed and ready to perform their duties securely.

On-the-Job Security Training

As part of the new hire's ongoing job orientation, and as part of every employee's security responsibilities, the organization should conduct periodic security awareness and training. Keeping security at the forefront of employees' minds minimizes employee mistakes and is an important part of the information security mission. Formal and informal seminars should also be used to increase the security awareness level of all employees, especially that of security employees.

Evaluating Performance

Information security awareness and change workplace behavior, organizations should incorporate information security components into employee performance evaluations. Employees pay close attention to job performance evaluations, and if the evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level.

Termination

When an employee leaves an organization, there are a number of security-related issues. Key among these is the continuity of protection of all information to which the employee had access.

The tasks that must be performed when an employee prepares to leave:

- Access to the organization's systems must be disabled.
- Removable media must be returned.
- Hard drives must be secured.
- File cabinet locks must be changed.
- Office door locks must be changed.
- Keycard access must be revoked.
- Personal effects must be removed from the organization's premises.

Once the employee has delivered keys, keycards, and other business property, he or she should be escorted from the premises. In addition to the tasks listed above, many organizations use an exit interview to remind the employee of contractual obligations, such as nondisclosure agreements, and to obtain feedback on the employee's tenure in the organization. At this time, the employee should be reminded that should he or she fail to comply with contractual obligations, civil or criminal action may be initiated. Security cannot risk the exposure of organizational information. The simplest and best method to handle the out-processing of an employee is to select, based on the employee's reasons for leaving, one of the following scenarios:

Hostile Departure:

- Hostile departures (non-voluntary) include termination for cause, downsizing, lay-off, or some instances of quitting.
- Before the employee knows that he or she is leaving, security terminates all logical and keycard access. As soon as the employee reports for work, he or she is escorted into the supervisor's office for the news.
- Upon receiving notice, the employee is escorted to his or her area, and allowed to collect personal effects. No organizational property is taken from the premises.
- The employee is asked to surrender all keys, keycards, and other company property. The employee is then escorted out of the building.

Friendly Departure:

- Friendly departures (voluntary) include retirement, promotion, or relocation. In this case, the employee may have tendered notice well in advance of the actual departure date. This actually makes it more difficult for security to maintain positive control over the employee's access and information usage.

    - Employee accounts are usually allowed to continue with a new expiration date.
    - Employees come and go at will and collect their own belongings and leave on their own.
    - They are asked to drop off all organizational property "on their way out the door."

In either circumstance, the offices and information used by the employee must be inventoried, their files must be stored or destroyed, and all property must be returned to organizational stores. In either situation, employees might foresee their departures well in advance and might begin collecting organizational information or anything that could be valuable in their future employment. Only by scrutinizing systems logs after the employee has departed and sorting out authorized actions from systems misuse or information theft can the organization determine if there has been a breach of policy or a loss of information. In the event that information is illegally copied or stolen, the action should be declared an incident and the appropriate policy should be followed.

INTERNAL CONTROL STRATEGIES

Separation of duties is a cornerstone in the protection of information assets and in preventing loss. The completion of a significant task that involves sensitive information should involve two people. If one person has the authorization to access a particular set of information, there may be nothing to prevent this individual from copying it and removing it from the premises. The checks and balances method requires two or more people to work together to complete a task and is designed to reduce the risk of collusion—that is, of unscrupulous workers conspiring to commit an unauthorized task. The odds of two people being willing and able to misuse or abuse the system are much lower than that of one.

Related to the concept of separation of duties is that of two-man control, the requirement that two individuals review and approve each other's work before the task is categorized as finished. This is different from separation of duties, in which the two people work in sequence. In two-man control, each person completely finishes the necessary work and then submits it to the other coworker. Each coworker examines the work performed, double-checks the actions performed, and makes sure no errors or inconsistencies exist.

Another control used to prevent personnel from misusing information assets is job rotation or task rotation, the requirement that every employee be able to perform the work of another employee. Ensuring that all critical tasks can be performed by multiple individuals greatly increases the chance that one employee will be able to detect when another employee misuses or abuses information or the system. A mandatory vacation of at least one week provides the ability to audit the work of an individual. Individuals who are stealing or misusing information or systems are reluctant to take vacations because they are afraid that their actions will be detected while they are away. Employees should be provided access to the minimal amount of information for the minimal amount of time necessary for them to perform their duties.

Similar to the concept of need-to-know, least privilege ensures that no unnecessary access to data exists, and that only those individuals who must access the data do so. The whole purpose of information security is to allow those people with a need to use information to do so without being concerned about the system's ability to maintain the confidentiality, integrity, and availability of the information. Everyone who can access data probably will, and such a situation could have devastating consequences on the organization's information security.

SECURITY MANAGEMENT MODELS

Only by creating an aggressive external and internal monitoring program can the information security team hope to stay abreast of changes in the environment. To assist the information security community in managing and operating 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.

NIST SP 800-100 Information Security Handbook: A Guide for Managers

The NIST SP 800-100, which is a guide to information security governance, covering thirteen areas of information security management. The guidance describes specific monitoring activities for the information security management team to ensure continuous compliance and adaptability.

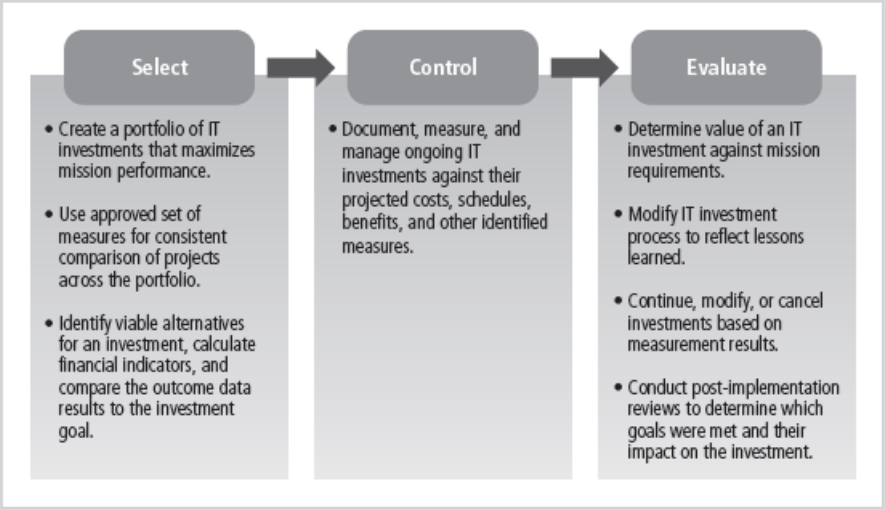


Figure: Select-Control-Evaluate Investment Life Cycle

1. Information security governance, which mandates that agencies should monitor the status of their programs to ensure that:
    a. Ongoing information security activities are providing appropriate support to the agency mission.
    b. Policies and procedures are current and aligned with evolving technologies, if appropriate.
    c. Controls are accomplishing their intended purpose.
2. The system development life cycle as a multistep process, incorporating information security related minima to assure and incorporate information security into implemented systems.
3. Awareness and training as the backbone of an information security program, ensuring that all users are both aware and trained on a minimum level of information security.
4. Capital planning and investment control, which implements a three-step process for the investment life cycle, select-control-evaluate, resulting in a seven-step process for prioritizing security investments.

5. System interconnection: NIST SP 800-47 approach includes a four phase (plan, establish, maintain, and disconnect) plan for all interconnected systems.
6. Performance measures: With this type program, organizations develop information security metrics that measure the effectiveness of their security program, and provide data to be analyzed and used by program managers and system owners to isolate problems, justify investment requests, and target funds to the areas in need of improvement.
7. Security planning, in which strategic, tactical and operational plans must be developed in alignment with and support organizational and IT plans, goals, and objectives.
8. Information technology contingency planning as a seven-step methodology explained in SP 800-34, *Contingency Planning for Information Technology Systems*.

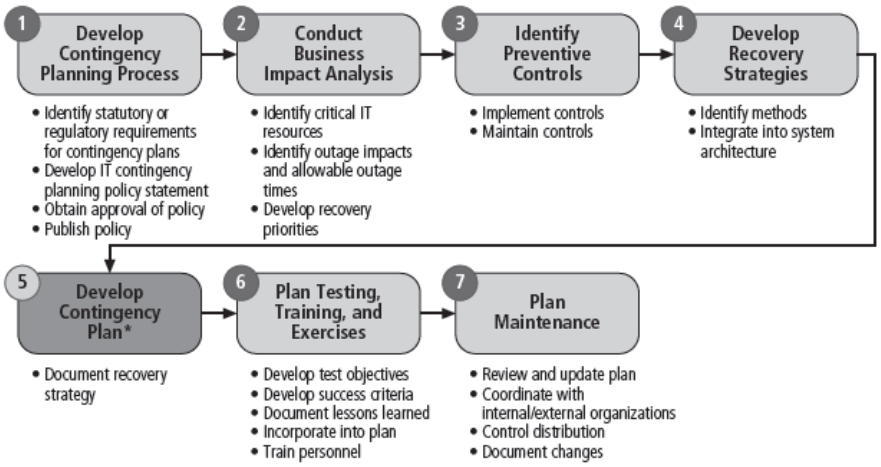


Figure: The NIST Seven-Step Contingency Planning Process

9. Risk management as a cycle that is fundamental to the information security program and its continuous improvement.
10. Certification, accreditation, and security assessments as a monitoring program that implements the following, as a minimum:
    a. Configuration management and configuration control processes for the information system
    b. Security impact analyses on changes to the information system
    c. Assessment of selected security controls in the information system and reporting of information system security status to appropriate agency officials

11. Security services and products acquisition, which states that when acquiring information security products, organizations are encouraged to conduct a cost benefit analysis—one that also includes the costs associated with risk mitigation. This cost benefit analysis should include a life cycle cost estimate for the status quo and one for each identified alternative while highlighting the benefits associated with each alternative.
12. Incident response, which prescribes the four-phase incident response procedure from NIST SP 800-61, and includes preparation, detection and analysis, containment, eradication, and recovery, and post-incident recovery.

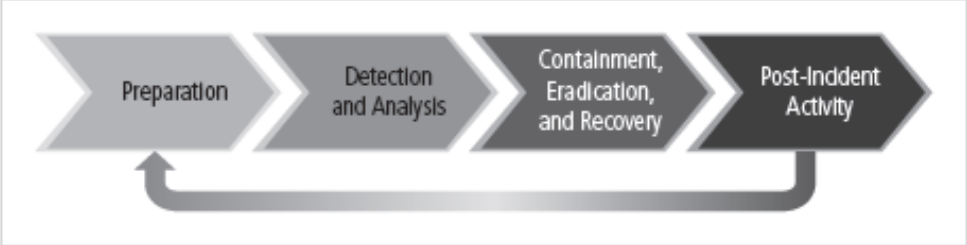


Figure: The Incident Response Life Cycle

13. The configuration (or change) management process as one that involves the continuous monitoring and management of changes to information systems or networks

The Security Maintenance Model

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

Figure illustrates a full maintenance program and serves as a framework for the discussion of maintenance that follows. The model is based on five subject areas or domains:

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

Monitoring the External Environment:

The objective of the external monitoring domain in 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.

Data sources

- Acquiring data about threats, threat agents, vulnerabilities, and attacks is not difficult. There are many sources of raw intelligence and few costs associated with gathering it. What is challenging and can be expensive is turning this flood of good and timely data into information that decision makers can use.
- External intelligence can come from three classes of sources:
    - Vendors
    - CERT organizations
    - Public network sources
- Regardless of how the organization collects external monitoring data, the CISO evaluates the actions and personnel needed to act on the information. The responsibility for establishing a viable external monitoring program includes the following tasks:
    - Creating documented and repeatable procedures

- Providing proper training to primary and backup staff members who are assigned to perform the monitoring tasks
- Equipping assigned staff members with proper access and tools to perform the monitoring function
- Designing criteria and cultivating expertise among the monitoring analysts so that they can perform analytic steps to cull meaningful summaries and actionable alerts from the vast flow of raw intelligence
- Developing suitable communications methods for moving processed intelligence to designated internal decision makers in all three communities of interest
- Integrating the incident response plan with the results of the external monitoring process for appropriate, timely responses

Monitoring, escalation, and incident response processes

- The basic function of the external monitoring process is to monitor activity, report results, and escalate warnings.
- The optimum approach for escalation is based on a thorough integration of the monitoring process into 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.

Monitoring the Internal Environment

It is just as important to monitor the internal computing environment, as it is to monitor the external environment. The primary goal of the internal monitoring domain is to maintain an informed awareness of the state of all of the organization's networks, information systems, and information security defenses. Internal monitoring is accomplished by:

- Building and maintaining an inventory of network devices and channels, IT infrastructure and applications, and information security infrastructure elements
- Active participation in, or leadership of, the IT governance process within the organization to integrate the inevitable changes found in all network, IT, and information security programs
- Real-time monitoring of IT activity using intrusion detection systems to detect and initiate responses to specific actions or trends of events that introduce risk to the organization's assets
- Periodic monitoring of the internal state of the organization's networks and systems. This recursive review of the network and system devices that are online at any given moment and of any changes to the services offered on the network is needed to maintain awareness of new and emerging threats. This can be accomplished through automated difference-detection methods that identify variances introduced to the network or system hardware and software

Network characterization and inventory process

- 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 is called characterization, as it is the systematic collection of the characteristics of the network and computer devices that are present in the environment. Once the characteristics have been identified, they must be carefully organized and stored using a manual or automated mechanism that allows timely retrieval and rapid integration of disparate facts.

Intrusion detection and prevention 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 that it can be used to prevent risk in the future.
- Whether the organization outsources IDS monitoring, staffs IDS monitoring 24/7, staffs IDS monitoring during business hours, or merely ignores the real-time alerts from IDS, the log files from the IDS engines can be mined for information that can be added to the internal monitoring knowledge base.
- Analyzing attack signatures for unsuccessful system attacks can identify weaknesses in various security efforts.

Detect differences

- One approach that has achieved good results is to perform various combinations of manual and automated difference analysis to identify changes to the internal environment.
- Difference analysis is a procedure that compares the current state of a network segment (the systems and services it offers) against a known previous state of that same network segment (the baseline of systems and services).

Planning and Risk Assessment

The primary objective of the planning and risk assessment domain is to keep a lookout over the entire information security program. This is done in part by identifying and planning ongoing information security activities that further reduce risk. The risk assessment group also identifies and documents risks introduced by both IT projects and information security projects. The group also identifies and documents risks that may be latent in the present environment.

Primary objectives of this domain as follows:

- Establish a formal information security program review process that complements and supports both the IT planning process and strategic planning processes.

- Institute formal project identification, selection, planning, and management processes for information security follow-up activities that augment the current program.
- Coordinate with IT project teams to introduce risk assessment and review for all IT projects, so that risks introduced from the launching of IT projects are identified, documented, and factored into projects decisions.
- Integrate a mindset of risk assessment across the organization to encourage the performance of risk assessment activities when any technology system is implemented or modified.

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 future IT needs of the organization and the impact those needs will 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 a part of that process.
- Projects that organizations might fund to maintain, extend, or enhance the information security program will arise in almost every planning cycle. Larger information security projects should be broken into smaller, incremental projects. Doing this is important for several reasons:

    - Smaller projects tend to have more manageable impacts on the networks and users.
    - Larger projects tend to complicate the change control process in the implementation phase.
    - Short planning, development, and implementation schedules reduce any uncertainty for IT planners and financial sponsors.
    - Most large projects can easily be assembled from smaller projects, providing 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 of identifying and documenting the risk that a project, process, or action introduces to the organization and may also 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 RA
    - Dialed modem RA
    - Business partner RA
    - Application RA
    - Vulnerability RA
    - Privacy RA
    - Acquisition or divesture RA
    - Other RAs

Vulnerability Assessment and Remediation

The primary goal of the vulnerability assessment and remediation domain is to identify specific, documented vulnerabilities and remediate them in a timely fashion. This is accomplished by:

- Using vulnerability assessment procedures that are documented to safely collect intelligence about networks, 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

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

Penetration testing

Penetration testing uses the systematic use of tools to attempt to undermine the security of a system to demonstrate potential weaknesses of a system for the purpose of strengthening the security posture of the organization.

The Internet vulnerability assessment process

- 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.
- Because 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 to be 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 in 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: The organization records 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 process

- 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 below.

    - Planning, scheduling, and notification of the penetration testing: There will be substantially more systems to assess. Intranet administrators often prefer that 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 correspond with 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 it is 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 as Internet analysis: classify, validate, and document.
- Record keeping: Identical to the one followed in an Internet vulnerability analysis.

Platform security validation process

- 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 process.

- 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.

- Because 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 process.

- The modem vulnerability assessment process is designed to find and document any vulnerability that is present on dial-up modems that are 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 is called war dialing, which involves using scripted dialing attacks against a pool of phone numbers.

Document vulnerabilities

- The vulnerability database, like the risk, threat, and attack database, both store and tracks information. It should provide details about the vulnerability being reported as well as linkage to the information assets that are characterized in the risk, threat, and attack database.
- While this can be done through manual data storage, the low cost and ease of use associated with 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 to manage the reporting and tracking processes in the remediation phase

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

Remediating vulnerabilities

- The objective of remediation is to repair the flaw that is causing a vulnerability instance or remove the risk associated with 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.
- Remediation of vulnerabilities can be accomplished by accepting or transferring the risk, removing the threat, or repairing the vulnerability.

Acceptance or transference of risk involves the following issues:

    - In some instances, risk must simply be acknowledged as part of the organization's business process.
    - The information security professional must assure the general management community that the decision to accept the risk was made by properly informed decision makers. These decision makers must have the proper level of authority to accept the risk.
    - In the final analysis, the information security group must make sure the right people make risk assumption decisions and that these people are aware of both the potential impact of their decision and the cost of the possible security controls.

Threat removal involves the following issues:

- 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 controls that require an expensive repair but allow the risk associated with the vulnerability to be successfully removed from the situation.

Vulnerability repair involves the following issues:

- 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, the most common repair is 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 to keep it 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. Policy needs to be reviewed periodically. As policy needs shift, a thorough and independent review of the entire information security program should be undertaken. While an exact timetable for review is not proposed here,

many organizations find that the CISO should conduct a formal review annually. Major planning elements should be rehearsed whenever possible. Rehearsal adds value by exercising procedures, identifying shortcomings, and providing security personnel the opportunity to improve the security plan before it is needed. In addition, rehearsals make people more effective when an actual event occurs. Rehearsals that closely match reality are called war games.

DIGITAL FORENSICS

When the asset attacked is in the purview of the CISO, the executive is expected to understand how policies and laws require the matter to be managed. In order to protect the organization and to possibly assist law enforcement in the conduct of an investigation, they must act to document what happened and how. The investigation of what happened and how is called digital forensics. Digital forensics is based on the field of traditional forensics. Forensics is the coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting. Digital forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis. Like traditional forensics, it follows clear, well-defined methodologies, but still tends to be as much art as science.

Evidentiary material (EM), also known as an item of potential evidentiary value, is any information that could potentially support the organization's legal or policy-based case against a suspect.

Digital forensics can be used for two key purposes.

1. To investigate allegations of digital malfeasance: A crime against or using digital media, computer technology, or related components (computer as source or object of crime), is referred to as digital malfeasance.
2. To perform root cause analysis: If the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, as well as to determine how pervasive and successful the attack was.

Some investigations are undertaken by organizational personnel, while others require immediate involvement of law enforcement. The organization must choose one of two approaches when employing digital forensics.

1. Protect and forget: This approach, also known as patch and proceed, focuses on the defense of the data and the systems that house, use, and transmit it.
2. Apprehend and prosecute: This approach, also known as pursue and prosecute, focuses on the identification and apprehension of responsible individuals, with additional attention on the collection and preservation of potential EM that might support administrative or criminal prosecution.

The Digital Forensics Team

Most organizations cannot sustain a permanent digital forensics team. Even so, there should be people in the information security group trained to understand and manage the forensics process. This expertise can be obtained by sending staff members to a regional or national information security conference with a digital forensics track, or to dedicated digital forensics training.

Affidavits and Search Warrants

An affidavit is sworn testimony that certain facts are in the possession of the investigating officer that they feel warrant the examination of specific items located at a specific place. When an approving authority signs the affidavit or creates a synopsis form based on this document, it becomes a search warrant—or permission to search for EM at the specified location and/or to seize items to return to the investigator's lab for examination. In corporate environments, the names of these documents may change and in many cases may be verbal in nature, but that the process should be the same. Formal permission is obtained before an investigation occurs.

Digital Forensics Methodology

In digital forensics, all investigations follow the same basic methodology:

1. Identify relevant items of evidentiary value (EM).
2. Acquire (seize) the evidence without alteration or damage.

3. Take steps to assure that the evidence is at every step verifiably authentic and is unchanged from the time it was seized.
4. Analyze the data without risking modification or unauthorized access.
5. Report the findings to the proper authority.

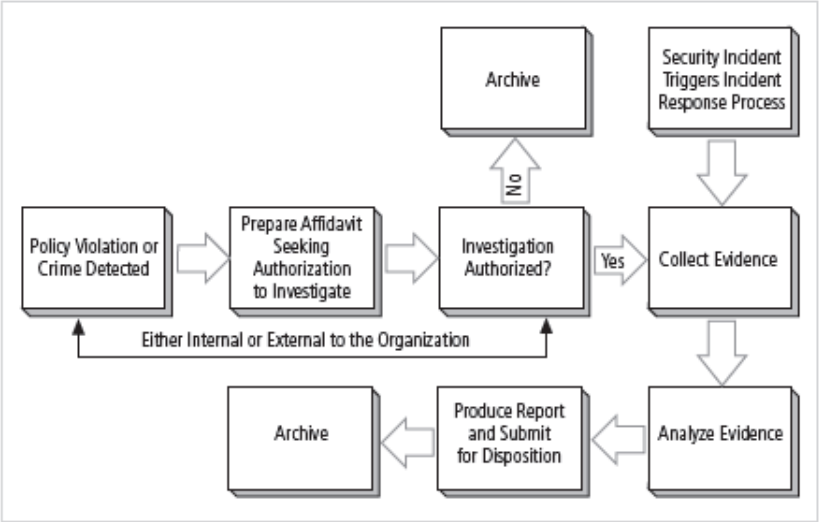


Figure: The Digital Forensics Process

In order to support the selection and implementation of a methodology, the organization may wish to seek legal advice or consult with local or state law enforcement. The affidavit or warrant authorizing a search action must specifically identify what items of evidence can be seized. The principal responsibility of the response team is to acquire the information without altering it. One of the most heated ongoing debates in digital forensics is the "to pull or not to pull" argument—that is, balancing the investigator's need to acquire the EM without modifying it against the possible loss of information in volatile memory. To "pull" means to pull the power cord on whatever computer technology is suspected of housing the EM.

There are generally two methods of acquiring evidence from a system. The first is the offline model, in which the investigator removes the power source and then uses a utility or special device to make a bit-stream sector-by-sector copy of the hard drives contained in the system. In online or "live" data acquisition, investigators use network-based tools to acquire a protected copy of the information. The only real difference between the two methods is that the source system cannot be taken offline, and the tools must be sophisticated enough to avoid altering the system during the data acquisition. The creation of a copy or image can

take a substantial amount of time. Not all EM is on a suspect's computer hard drive. A technically savvy attacker is more likely to store incriminating evidence on other digital media, such as removable drives, CDs, DVDs, flash drives, memory chips or sticks, or on other computers accessed across the organization's networks, or via the Internet. Once the evidence is acquired, both the copy image and the original drive should be handled so as to avoid legal challenges based on authenticity and preservation of integrity. Chain of evidence or chain of custody is defined as the detailed documentation of the collection, storage, transfer, and ownership of collected evidence from crime scene through its presentation in court. The copy or image is typically transferred to the laboratory for the next stage of authentication. The team must be able to demonstrate that any analyzed copy or image is a true and accurate replica of the source EM. This is accomplished by the use of cryptographic hash tools.

The most complex part of an investigation is the analysis of the copy or image for potential EM. While the process can be performed manually using simple utilities, two industry leading applications dominate the market for digital forensics:

1. Guidance Software's EnCase (www.guidancesoftware.com)
2. AccessData Forensics Tool Kit (FTK) (www.accessdata.com)

Each of these tools is designed to support a law enforcement investigation and assist in the management of the entire case.

Evidentiary Procedures

In information security, most operations focus on policies—those documents that provide managerial guidance for ongoing implementation and operations. In digital forensics, however, the focus is on procedures. Strong procedures for the handling of potential evidentiary material can minimize the probability of an organization losing a legal challenge. Organizations should develop specific procedures, along with guidance on the use of these procedures. The policy document should specify the following:

- Who may conduct an investigation
- Who may authorize an investigation
- What affidavit-related documents are required

- What search warrant-related documents are required
- What digital media may be seized or taken offline
- What methodology should be followed
- What methods are required for chain of custody or chain of evidence
- What format the final report should take, and to whom it should it be given

The policy document should be supported by a procedures manual, developed based on the documents discussed earlier, along with guidance from law enforcement or consultants.