UNIT 3

PLANNING FOR SECURITY

3.1 PLANNING FOR SECURITY

Introduction

An organization's information security effort succeeds only if it operates in conjunction with the organization's information security policy. An information security program begins with policy, standards, and practices, which are the foundation for the information security architecture and blueprint. The creation and maintenance of these elements require coordinated planning.

The role of planning in the modern organization is hard to overemphasize. All but the smallest organizations engage in some planning: strategic planning to manage the allocation of resources and contingency planning to prepare for the uncertainties of the business environment.

3.2 INFORMATION SECURITY POLICY, STANDARDS, AND PRACTICES

Management from all communities of interest, including general staff, information technology, and information security, must make policies the basis for all information security planning, design, and deployment. Policies direct how issues should be addressed and technologies should be used. Policies do not specify the proper operation of equipment or software this Information should be placed in the standards, procedures, and practices of users' manuals and systems documentation. In addition, policy should never contradict law, because this can create a significant liability for the organization.

Quality security programs begin and end with policy. Information security is primarily a management problem, not a technical one, and policy is a management tool that obliges personnel to function in a manner that preserves the security of information assets. Security policies are the least expensive control to execute, but the most difficult to implement properly.

They have the lowest cost in that their creation and dissemination requires only the time and effort of the management team. Even if the management team hires an outside consultant to help develop policy, the costs are minimal compared to those of technical

controls. However, shaping policy is difficult because policy must: Never conflict with laws Stand up in court, if challenged Be properly administered through dissemination and documented acceptance

Definitions

A **policy** is a plan or course of action that conveys instructions from an organization's senior. Management to those who make decisions, take actions, and perform other duties. Policies are organizational laws in that they dictate acceptable and unacceptable behaviour within the organization. Like laws, policies define what is right, what is wrong, what the penalties are for violating policy, and what the appeal process is. Standards, on the other hand, are more detailed statements of what must be done to comply with policy. They have the same requirements for compliance as policies. Standards may be informal or part of an organizational culture, as in de facto standards. Or standards may be published, scrutinized, and ratified by a group, as in formal or de jure standards. Finally, practices, procedures, and guidelines effectively explain how to comply with policy.

Figure shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines. Policies are put in place to support the mission, vision, and strategic planning of an organization.

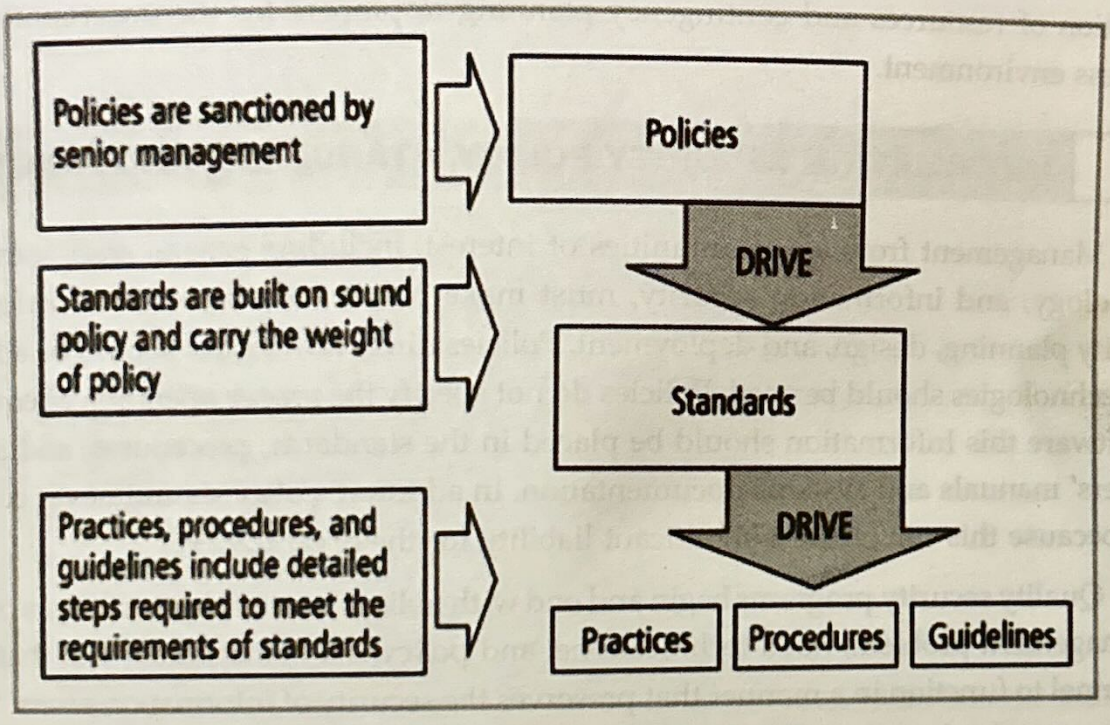

Figure : Policies, Standards, and Practices

Strategic planning is the process of moving the organization toward its vision. The meaning of the term security policy depends on the context in which it is used. Governmental agencies view security policy in terms of national security and national policies to deal with foreign states. A security policy can also communicate a credit card agency's method

for processing credit card numbers. In general, a security policy is a set of rules that protect an organization's assets. An information security policy provides rules for the protection of the information assets of the organization.

Criteria for Effective Security Policy

For a policy to be effective and thus legally enforceable, it must meet the following criteria:

1. **Dissemination (distribution):**The organization must be able to demonstrate that the policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.
2. **Review (reading):** The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recording the policy in English and other languages.
3. **Comprehension (understanding):** The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
4. **Compliance (agreement):** The organization must be able to demonstrate that the employee agrees to comply with the policy, through act or affirmation. Common techniques include logon banners which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.
5. **Uniform enforcement**: The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Types of Security Policy

Management must define three types of security policy, according to the National Institute of Standards and Technology's Special Publication 800-14.

1. Enterprise information security policies
2. Issue-specific security policies
3. Systems-specific security policies

1. Enterprise Information Security Policy (EISP)

An enterprise information security policy (EISP) is also known as a general security policy, organizational security policy, IT security policy, or information security policy. The EISP is based on and directly supports the mission, vision, and direction of the organization and sets the strategic direction, scope, and tone for all security efforts. The

EISP is an executivelevel document, usually drafted by or in cooperation with the chief information officer of the organization. This policy is usually two to ten pages long and shapes the philosophy of security in the IT environment. The EISP usually needs to be modified only when there is a change in the strategic direction of the organization.

The EISP guides the development, implementation, and management of the security program. It sets out the requirements that must be met by the information security blueprint or framework. It defines the purpose, scope, constraints, and applicability of the security program. It also assigns responsibilities for the various areas of security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users. Finally, it addresses legal compliance. According to the National Institute of Standards and Technology (NIST), the EISP typically addresses compliance in the following two areas:

1. General compliance to ensure meeting the requirements to establish a program and the Responsibilities assigned therein to various organizational components
2. The use of specified penalties and disciplinary action

When the EISP has been developed, the CISO begins forming the security team and initiating the necessary changes to the information security program.

2. Issue-Specific Security Policy (ISSP)

As an organization executes various technologies and processes to support routine operations, it must instruct employees on the proper use of these technologies and processes. In general, the **issue-specific security policy**, or **ISSP**, (1) addresses specific areas of technology as listed below, (2) requires frequent updates, and (3) contains a statement on the organization's position on a specific issue.

There are a number of approaches to creating and managing ISSPs within an organization.

Three of the most common are:

1. Independent ISSP documents, each tailored to a specific issue
2. A single comprehensive ISSP document covering all issues
3. A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements

3. Systems-Specific Policy (SysSP)

While issue-specific policies are formalized as written documents readily identifiable as policy, system-specific security policies (SysSPs) sometimes have a different look. SysSPs often function as standards or procedures to be used when configuring or maintaining systems. For example, a SysSP might describe the configuration and operation of a network

firewall. This document could include a statement of managerial intent; guidance to network engineerson the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSPs can be separated into two general groups, **managerial guidance** and **technical specifications**, or they can be combined into a single policy document.

Policy Management

Policies are living documents that must be managed. It is unacceptable to create such an important set of documents and then shelve it. These documents must be properly disseminated (distributed, read, understood, agreed to, and uniformly applied) and managed. How they are managed should be specified in the policy management section of the issue-specific policy described earlier. Good management practices for policy development and maintenance make for a more resilient organization. For example, all policies, including security policies, undergo tremendous stress when corporate mergers and divestitures occur; in such situations, employees are faced with uncertainty and many distractions.

System vulnerabilities can arise if, for instance, incongruent security policies are implemented in different parts of a new, merged organization. When two companies merge but retain separate policies, the difficulty of implementing security controls increases. Likewise, when one company with unified policies splits in two, each new company may require different policies. To remain viable, security policies must have a responsible individual, a schedule of reviews, a method for making recommendations for reviews, and a policy issuance and revision date.

3.3 SECURITY BLUE PRINT

The Information Security Blueprint

Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program. If one or more components of policies, standards, or practices have not been completed, management must determine whether or not to nonetheless proceed with the development of the blueprint.

After the information security team has inventoried the organization's information assets and assessed and prioritized the threats to those assets, it must conduct a series of risk assessments using quantitative or qualitative analyses, as well as feasibility studies and cost benefit analyses.

These assessments, which include determining each asset's current protection level, are used to decide whether or not to proceed with any given control. Armed with a general

idea of the vulnerabilities in the information technology systems of the organization, the security team develops a design blueprint for security, which is used to implement the security program.

This **security blueprint** is the basis for the design, selection, and implementation of all security program elements including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and maintenance of the security program. The security blueprint, built on top of the organization's information security policies, is a scalable, upgradeable, comprehensive plan to meet the organization's current and future information security needs. It is a detailed version of the **security framework**, which is an outline of the overall information security strategy for the organization and a roadmap for planned changes to the information security environment of the organization. The blueprint specifies the tasks and the order in which they are to be accomplished.

To select a methodology in which to develop an information security blueprint, you can adapt or adopt a published information security model or framework. This framework can outline steps to take to design and implement information security in the organization. There are a number of published information security frameworks, including ones from government sources. Because each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks. Experience teaches you that what works well for one organization may not precisely fit another.

The following steps in security blue print framework are as follows :

1. The ISO 27000 Series

One of the most widely referenced security models is the Information Technology–Code of Practice for Information Security Management, which was originally published as British Standard BS7799. In 2000, this code of practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799. The document was revised in 2005 (becoming ISO 17799:2005), and it was then renamed to ISO 27002 in 2007, to align it with the document ISO 27001, discussed later in this chapter. While the details of ISO/IEC 27002 are available to those who purchase the standard, its structure and general organization are well known.

2. NIST Security Models

Other approaches are described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (http://csrc.nist.gov). Because the NIST documents are publicly available at no charge and have

been available for some time, they have been broadly reviewed by government and industry professionals, and are among the references cited by the federal government when it decided not to select the ISO/IEC 17799 standards.

A. **NIST Special Publication 800-14** Generally Accepted Principles and Practices for Securing Information Technology Systems provides best practices and security principles that can direct the security team in the development of a security blueprint. In addition to detailing security best practices across the spectrum of security areas, it provides philosophical principles that the security team should integrate into the entire information security process.

B. **NIST Special Publication 800-18 Rev. 1** The Guide for Developing Security Plans for Federal Information Systems can be used as the foundation for a comprehensive security blueprint and framework. This publication provides detailed methods for assessing, designing, and implementing controls and plans for applications of varying size. SP 800-18 Rev. 1 can serve as a useful guide to the activities described in this chapter and as an aid in the planning process. It also includes templates for major application security plans. As with any publication of this scope and magnitude, SP 800-18 Rev. 1 must be customized to fit the particular needs of an organization.

3. IETF Security Architecture

The Security Area Working Group acts as an advisory board for the protocols and areas developed and promoted by the Internet Society and the Internet Engineering Task Force (IETF), and while the group endorses no specific information security architecture, one of its requests for comment (RFC), RFC 2196: Site Security Handbook, provides a good functional discussion of important security issues. RFC 2196: Site Security Handbook covers five basic areas of security with detailed discussions on development and implementation. There are also chapters on such important topics as security policies, security technical architecture, security services, and security incident handling.

The chapter within the RFC that deals with architecture begins with a discussion of the importance of security policies and continues with an examination of services, access controls, and other relevant areas.

4. Baselining and Best Business Practices

The baselining and best practices are reliable methods used by some organizations to assess security practices. Baselining and best practices don't provide a complete methodology for the design and implementation of all the practices needed by an organization; however, it is possible to piece together the desired outcome of the security process, and therefore to work backwards toward an effective design.

The Federal Agency Security Practices (FASP) site, http://csrc.nist.gov/groups/SMA/fasp, is a popular place to look up best practices.

FASP is designed to provide best practices for public agencies, but these practices can be adapted easily to private institutions. The documents found at this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.

5. Design of Security Architecture

To inform the discussion of information security program architecture and to illustrate industry best practices, the following sections outline a few key security architectural components. Many of these components are examined in detail in later chapters of this book, but this overview can help you assess whether a framework and/or blueprint are on target to meet an organization's needs.

3.4 SECURITY EDUCATION

Security Education, Training, and Awareness Program

Once your organization has defined the polices that will guide its security program and selected an overall security model by creating or adapting a security framework and a corresponding detailed implementation blueprint, it is time to implement a security education, training, and awareness (SETA) program. The SETA program is the responsibility of the CISO and is a control measure designed to reduce the incidences of accidental security breaches by employees.

Employee errors are among the top threats to information assets, so it is well worth expending the organization's resources to develop programs to combat this threat. SETA programs are designed to supplement the general education and training programs that many organizations use to educate staff on information security. For example, if an organization detects that many employees are opening questionable e-mail attachments, those employees must be retrained. As a matter of good practice, systems development life cycles must include user training during the implementation phase.

The SETA program consists of three elements: security education, security training, and security awareness. An organization may not be capable of or willing to undertake all three of these elements, and may outsource elements to local educational institutions. The purpose of SETA is to enhance security by doing the following:

1. Improving awareness of the need to protect system resources.
2. Developing skills and knowledge so computer users can perform their jobs more securely.

3. Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Table below compares the features of security education, training, and awareness within the organization.

Attribute	Education	Training	Awareness
Level	Why	How	What
Objective	Insight	Knowledge	Information
Teaching method	Understanding	Skill	Exposure
	Theoretical instruction	Practical instruction	Media
	• Discussion seminar • Background reading • Hands-on practice	• Lecture • Case study workshop • Posters	• Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

Table : Comparative Framework of SETA (from NIST SP800-1222)

Everyone in an organization needs to be trained and made aware of information security, but not every member of the organization needs a formal degree or certificate in information security. When management agrees that formal education is appropriate, an employee can investigate available courses from local institutions of higher learning or continuing education.

Security Training

Security training provides detailed information and hands-on instruction to employees to prepare them to perform their duties securely. Management of information security can develop customized in-house training or outsource the training program. Alternatives to formal training programs are industry training conferences and programs offered through professional agencies such as SANS (www.sans.org), (ISC)2 (www.isc2.org), ISSA (www.issa.org), and CSI (www.gocsi.com). Many of these programs are too technical for the average employee, but may be ideal for the continuing education requirements of information security professionals.

There are a number of available resources for conducting SETA programs that offer assistance in the form of sample topics and structures for security classes. For organizations, the Computer Security Resource Center at NIST provides several useful documents free of charge in their special publications area (http://csrc.nist.gov).

Security Awareness

One of the least frequently implemented, but most beneficial, programs is the security awareness program. A security awareness program is designed to keep information security at the forefront of users' minds. These programs don't have to be complicated or expensive. Good programs can include newsletters, security posters m, videos, bulletin boards, flyers, and trinkets. Trinkets can include security slogans printed on mouse pads, coffee cups, T-shirts, pens, or any object frequently used during the workday that reminds employees of security. In addition, a good security awareness program requires a dedicated individual willing to invest the time and effort into promoting the program, and a champion willing to provide the needed financial support.

The security newsletter is the most cost-effective method of disseminating security information and news to the employee. Newsletters can be distributed via hard copy, e-mail, or intranet.

Newsletter topics can include new threats to the organization's information assets, the schedule for upcoming security classes, and the addition of new security personnel. The goal is to keep the idea of information security in users' minds and to stimulate users to care about security. If a security awareness program is not actively implemented, employees may begin to neglect security matters and the risk of employee accidents and failures is likely to increase.

3.5 CONTINUITY STRATEGIES

A key role for all managers is contingency planning. Managers in the IT and information security communities are usually called on to provide strategic planning to assure the continuous availability of information systems. Unfortunately for managers, however, the probability that some form of attack will occur—from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic—is very high. Thus, managers from each community of interest must be ready to act when a successful attack occurs.

There are various types of contingency plans for events of this type: incident response plans, disaster recovery plans, and business continuity plans.

In some organizations, these might be handled as a single integrated plan. In large, complex organizations, each of these plans may cover separate but related planning functions that differ in scope, applicability, and design. In a small organization, the security administrator (or systems administrator) may have one simple plan that consists of a straightforward set of media backup and recovery strategies and service agreements from the company's service providers. But the sad reality is that many organizations have a

level of planning that is woefully deficient. Incident response, disaster recovery, and business continuity planning are components of contingency planning, as shown in Figure.

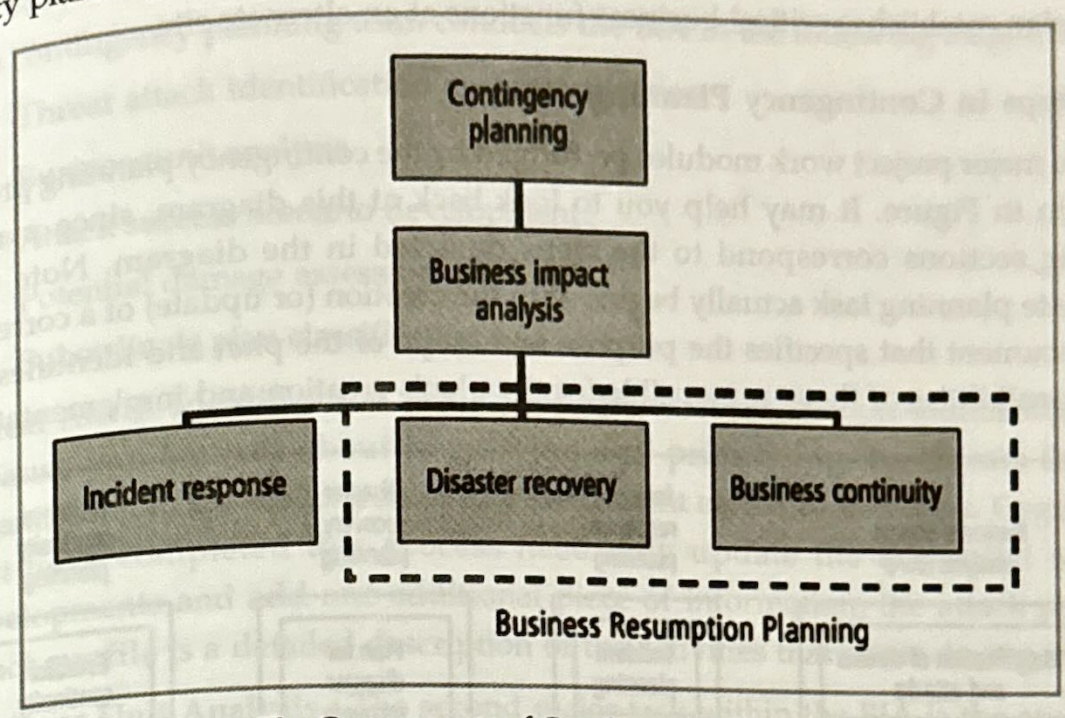

Fig: Components of Contingency Planning

A contingency plan is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization and, subsequently, to restore the organization to normal modes of business operations. The discussion of contingency planning begins with an explanation of the differences among its various elements, and an examination of the points at which each element is brought into play.

An incident is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability. An incident response (IR) plan addresses the identification, classification, response, and recovery from an incident. A disaster recovery (DR) plan addresses the preparation for and recovery from a disaster, whether natural or man-made. A business continuity (BC) plan ensures that critical business functions continue if a catastrophic incident or disaster occurs. The primary functions of these three types of planning are as follows:

1. The IR plan focuses on immediate response, but if the attack escalates or is disastrous (e.g., fire, flood, earthquake, or total blackout) the process moves on to disaster recovery and the BC plan.
2. The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with the BC plan.

3. The BC plan occurs concurrently with the DR plan when the damage is major or ongoing, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.

Major Steps in Contingency Planning

The major project work modules performed by the contingency planning project team are shown in Figure. It may help you to look back at this diagram, since many of the upcoming sections correspond to the steps depicted in the diagram. Note that each subordinate planning task actually begins with the creation (or update) of a corresponding policy document that specifies the purpose and scope of the plan and identifies the roles and responsibilities of those responsible for the plan's creation and implementation.

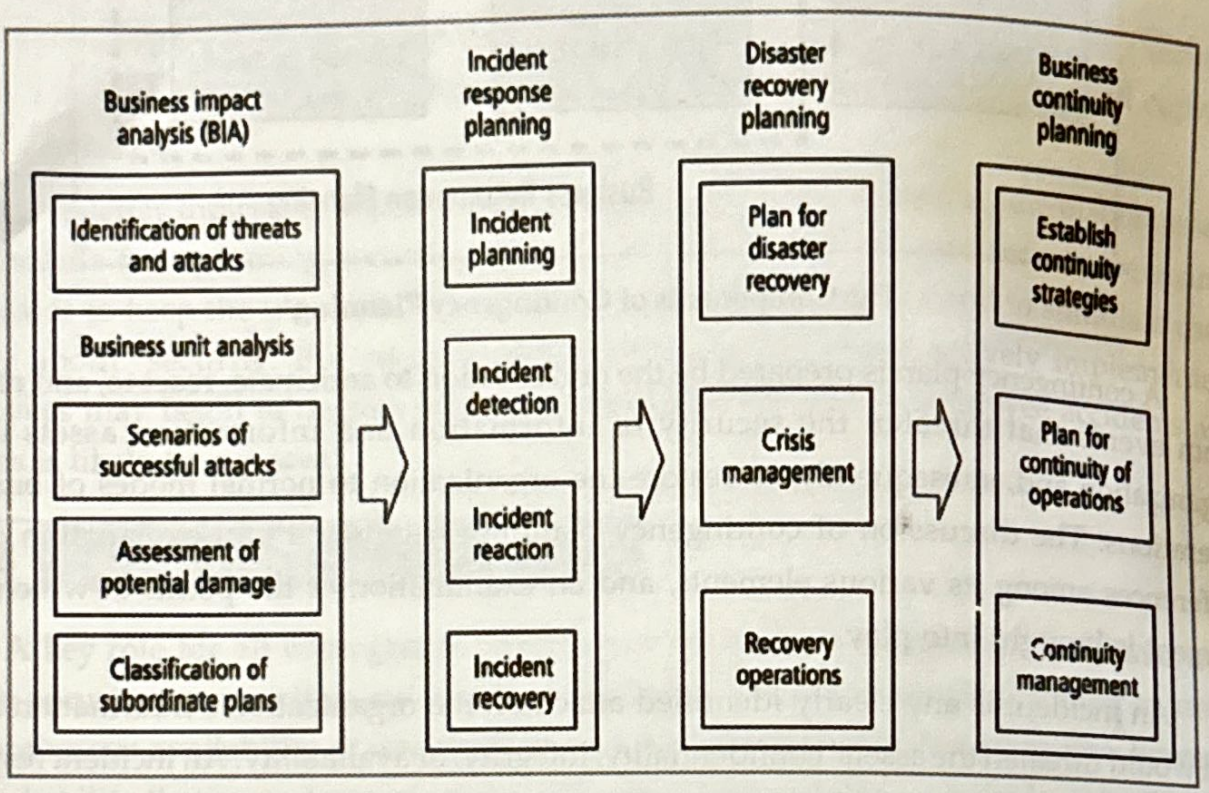

Fig: Major Steps in Contingency Planning

A. BUSINESS IMPACT ANALYSIS

The first phase in the development of the contingency planning process is the **business impact analysis (BIA)**. A BIA is an investigation and assessment of the impact that various attacks can have on the organization. BIA takes up where the risk assessment process leaves off. It begins with the prioritized list of threats and vulnerabilities identified in the risk management process and information about the criticality of the systems involved and a detailed assessment of the threats and vulnerabilities to which they are subjects. The BIA is a crucial component of the initial planning stages, as it provides detailed scenarios of the potential impact each attack could have on the organization. The BIA therefore helps to

determine what the organization must do to respond to the attack, minimize the damage from the attack, recover from the effects, and return to normal operations.

The contingency planning team conducts the BIA in the following stages,

1. Threat attack identification and prioritization
2. Business unit analysis
3. Attack success scenario development
4. Potential damage assessment
5. Subordinate plan classification

1. **Threat Attack Identification and Prioritization :** If this section sounds familiar, it's because you learned about identifying and prioritizing the threats facing the organization in the discussion of risk assessment earlier in this book. Organizations that have completed this process need only update the threat list with new developments and add one additional piece of information, the attack profile. An **attack profile** is a detailed description of the activities that occur during an attack.

2. **Business Unit Analysis :** The second major task within the BIA is the analysis and prioritization of the business functions within the organization to determine which are most vital to continued operations. Each organizational unit must be evaluated to determine how important its functions are to the organization as a whole. For example, recovery operations would probably focus on the IT department and network operation before addressing the personnel department and hiring activities. Likewise, it is more urgent to reinstate a manufacturing company's assembly line than the maintenance tracking system for that assembly line. This is not to say that personnel functions and assembly line maintenance are not important to the business; but the reality is that if the organization's main revenue producing operations cannot be restored quickly, there may cease to be a need for other functions.

3. **Attack Success Scenario Development :** Once the threat attack profiles have been developed and the business functions prioritized, the business impact analysis team must create a series of scenarios depicting the impact of a successful attack from each threat on each prioritized functional area. This can be a long and detailed process, as threats that succeed can affect many functions. Attack profiles should include scenarios depicting a typical attack with details on the method, the indicators, and the broad consequences of the attack.

Once the attack profiles are completed, the business function details can be integrated with the attack profiles, after which more details are added to the attack profile, including alternate outcomes. These alternate outcomes should describe best, worst,

and most likely outcomes for each type of attack on a particular business functional area. This level of detail allows planners to address each business function in turn.

4. **Potential Damage Assessment :** Using the attack success scenarios, the BIA planning team must estimate the cost of the best, worst, and most likely cases. At this stage, you are not determining how much to spend on the protection of information assets, since this was analyzed during the risk management activities. Instead, you are identifying what must be done to recover from each possible case. These costs include the actions of the response team(s), which are described in subsequent sections, as they act to recover quickly and effectively from an incident or disaster. These cost estimates can also inform management representatives from all the organization's communities of interest of the importance of the planning and recovery efforts. The final result of the assessment is referred to as an attack scenario end case.

5. **Subordinate Plan Classification :** Once the potential damage has been assessed, and each scenario and attack scenario end case has been evaluated, a subordinate plan must be developed or identified from among the plans already in place. These subordinate plans take into account the identification of, reaction to, and recovery from each attack scenario. An attack scenario end case is categorized as disastrous or not disastrous. Most attacks are not disastrous and therefore fall into the category of incident. Those scenarios that do qualify as disastrous are addressed in the disaster recovery plan.

   The qualifying difference is whether or not an organization is able to take effective action during the attack to combat its effects. Attack end cases that are disastrous find members of the organization waiting out the attack with hopes to recover effectively after it is over. In a typical disaster recovery operation, the lives and welfare of the employees are the most important priority during the attack, as most disasters are fires, floods, hurricanes, and tornadoes.

B. Incident Response Planning

Incident response planning includes the identification of, classification of, and response to an incident. The IR plan is made up of activities that are to be performed when an incident has been identified. Before developing such a plan, you should understand the philosophical approach to incident response planning. Incident is an attack against an information asset that poses a clear threat to the confidentiality, integrity, or availability of information resources. If an action that threatens information occurs and is completed, the action is classified as an incident. All of the threats identified in earlier chapters could result in attacks that would be classified as information security incidents. For purposes of this discussion, however, attacks are classified as incidents if they have the following characteristics:

1. They are directed against information assets.

2. They have a realistic chance of success.
3. They could threaten the confidentiality, integrity, or availability of information resources.

Incident response (IR) is therefore the set of activities taken to plan for, detect, and correct the impact of an incident on information assets. Prevention is purposefully omitted, as this activity is more a function of information security in general than of incident response. In other words, IR is more reactive than proactive, with the exception of the planning that must occur to prepare the IR teams to be ready to react to an incident.

IR consists of the following four phases:

1. Incident Planning
2. Incident Detection
3. Incident Reaction
4. Incident Recovery

1. **Incident Planning :** Planning for an incident requires a detailed understanding of the scenarios developed for the BIA. With this information in hand, the planning team can develop a series of predefined responses that guide the organization's incident response (IR) team and information security staff. The predefined responses enable the organization to react quickly and effectively to the detected incident. This assumes two things: first, the organization has an IR team, and second, the organization can detect the incident.

The IR team consists of those people who must be present to handle the systems and functional areas that can minimize the impact of an incident as it takes place. Picture a military movie in which U.S. forces have been attacked. If the movie is accurate in its portrayal of IR teams, you saw the military version of an IR team verifying the threat, determining the appropriate response, and coordinating the actions necessary to deal with the situation.

2. **Incident Detection :** Members of an organization sometimes notify systems administrators, security administrators, or their managers of an unusual occurrence. This is most often a complaint to the help desk from one or more users about a technology service. These complaints are often collected by the help desk and can include reports such as "the system is acting unusual," "programs are slow," "my computer is acting weird," or "data is not available." Incident detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly. The mechanisms that could potentially detect an incident include intrusion detection and prevention systems (both host-based and network-based), virus detection software, systems administrators, and even end users.

3. **Incident Reaction :** Incident reaction consists of actions outlined in the IR plan that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident. These actions take place as soon as the incident is over. There are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident. These should be prioritized and documented in the IR plan for quick use in the heat of the moment.

4. **Recovery :** Once the extent of the damage has been determined, the recovery process can begin in earnest. Full recovery from an incident requires that you perform the following:

    1. Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
    2. Address the safeguards that failed to stop or limit the incident, or were missing from the system in the first place. Install, replace, or upgrade them.
    3. Evaluate monitoring capabilities (if present). Improve their detection and reporting methods, or simply install new monitoring capabilities.
    4. Restore the data from backups. Restoration requires the IR team to understand the backup strategy used by the organization, restore the data contained in backups, and then recreate the data that were created or modified since the last backup.
    5. Restore the services and processes in use. Compromised services and processes must be examined, cleaned, and then restored. If services or processes were interrupted during the process of regaining control of the systems, they need to be brought back online.
    6. Continuously monitor the system. If an incident happened once, it can easily happen again. Just because the incident is over doesn't mean the organization is in the clear. Hackers frequently boast of their abilities in chat rooms and dare their peers to match their efforts. If word gets out, others may be tempted to try their hands at the same or different attacks. It is therefore important to maintain vigilance during the entire IR process.
    7. Restore the confidence of the organization's communities of interest. It may be advisable to issue a short memorandum that outlines the incident and assures everyone that it was handled and the damage controlled. If the incident was minor, say so. If the incident was major or severely damaged the systems or data, reassure the users that they can expect operations to return to normal shortly. The objective is not to placate or lie, but to prevent panic or confusion from causing additional disruptions to the operations of the organization.

C. Disaster Recovery Planning

Disaster recovery (DR) planning is the process of preparing an organization to handle and recover from a disaster, whether natural or man-made. The key emphasis of a DR plan is to reestablish operations at the primary site, the location at which the organization performs its business. The goal is to make things whole, or as they were before the disaster.

1. **The Disaster Recovery Plan :** Similar in structure to the IR plan, the DR plan provides detailed guidance in the event of a disaster. It is organized by the type or nature of the disaster, and specifies recovery procedures during and after each type of disaster. It also provides details on the roles and responsibilities of the people involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified. Just as the IR plan must be tested, so must the DR plan, using the same testing mechanisms. At a minimum, the DR plan must be reviewed during a walk-through or talk-through on a periodic basis.

2. **Crisis Management :** Disasters are, of course, larger in scale and less manageable than incidents, but the planning processes are the same and in many cases are conducted simultaneously. What may truly distinguish an incident from a disaster are the actions of the response teams. An incident response team typically rushes to duty stations or to the office from home. The first act is to reach for the IR plan. A disaster recovery team may not have the luxury of flipping through a binder to see what must be done. Disaster recovery personnel must know their roles without any supporting documentation. This is a function of preparation, training, and rehearsal. You probably all remember the frequent fire, tornado, or hurricane drills—and even the occasional nuclear blast drills—from your public school days. Just because you move from school to the business world doesn't lessen the threat of a fire or other disaster.

   The actions taken during and after a disaster are referred to as **crisis management**. Crisis management differs dramatically from incident response, as it focuses first and foremost on the people involved. The disaster recovery team works closely with the crisis management team.

3. **Recovery Operations :** Reactions to a disaster can vary so widely that it is impossible to describe the process with any accuracy. It is up to each organization to examine the scenarios developed at the start of contingency planning and determine how to respond. Should the physical facilities be spared after the disaster, the disaster recovery team should begin the restoration of systems and data to re-establish full operational capability. If the organization's facilities do not survive, alternative actions must be taken until new facilities can be acquired. When a disaster threatens the viability of the organization at the primary site, the disaster recovery process transitions into the process of business continuity planning.

D. Business Continuity Planning

Business continuity planning prepares an organization to re-establish critical business operations during a disaster that affects operations at the primary site. If a disaster has rendered the current location unusable, there must be a plan to allow the business to continue to function.

Not every business needs such a plan or such facilities. Small companies or fiscally sound organizations may have the latitude to cease operations until the physical facilities can be restored. Manufacturing and retail organizations may not have this option, because they depend on physical commerce and may not be able to relocate operations.

1. **Developing Continuity Programs :** Once the incident response and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster. The development of the BC plan is somewhat simpler than that of the IR plan or DR plan, in that it consists primarily of selecting a continuity strategy and integrating the offsite data storage and recovery functions into this strategy.

   Some of the components of the BC plan could already be integral to the normal operations of the organization, such as an offsite backup service. Others require special consideration and negotiation. The first part of business continuity planning is performed when the joint DR/BC plan is developed. The identification of critical business functions and the resources needed to support them is the cornerstone of BC plan.

   When a disaster strikes, these functions are the first to be re-established at the alternate site. The contingency planning team needs to appoint a group of individuals to evaluate and compare the various alternatives available and recommend which strategy should be selected and implemented. The strategy selected usually involves some form of offsite facility, which should be inspected, configured, secured, and tested on a periodic basis. The selection should be reviewed periodically to determine if a superior alternative has emerged or if the organization needs a different solution.

2. **Continuity Strategies :** There are a number of strategies from which an organization can choose when planning for business continuity. The determining factor when selecting from among these options is usually cost. In general, there are three exclusive options: hot sites, warm sites, and cold sites; and three shared functions: time-share, service bureaus, and mutual agreements.

Model for a Consolidated Contingency Plan

To help you understand the structure and use of the incident response and disaster recovery Plans, this section present a comprehensive model that incorporates the basics of

each type of Planning in a single document. It is not uncommon for small- to medium-sized organizations to use such a document. The single document supports concise planning and encourages smaller Organizations to develop, test, and use IR and DR plans. The model presented is based on analyses of disaster recovery and incident response plans of dozens of organizations.

3.6 SECURITY TECHNOLOGY

Introduction

Technical controls are essential to a well-planned information security program, particularly to enforce policy for the many IT functions that are not under direct human control. Networks and computer systems make millions of decisions every second and operate in ways and at speeds that people cannot control in real time. Technical control solutions, properly implemented, can improve an organization's ability to balance the often conflicting objectives of making information readily and widely available and of preserving the information's confidentiality and integrity.

Access Control

Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization—that is, information systems, restricted areas such as computer rooms, and the entire physical location. Access control is achieved by means of a combination of policies, programs, and technologies. Access controls can be mandatory, nondiscretionary, or discretionary.

Mandatory access controls (MACs) use data classification schemes; they give users and data owners limited control over access to information resources. In a data classification scheme, each collection of information is rated, and each user is rated to specify the level of information that user may access. These ratings are often referred to as sensitivity levels, and they indicate the level of confidentiality the information requires. A variation of this form of access control is called **lattice-based access control**, in which users are assigned a matrix of authorizations for particular areas of access. The level of authorization may vary between levels, depending on the classification authorizations individuals possess for each group of information or resources.

Approaches to Access Control

In general, all access control approaches rely on as the following mechanisms:

1. Identification
2. Authentication

3. Authorization
4. Accountability

1. Identification

Identification is a mechanism whereby an unverified entity—called a supplicant—that seeks access to a resource proposes a label by which they are known to the system. The label applied to the supplicant (or supplied by the supplicant) is called an identifier (ID), and must be mapped to one and only one entity within the security domain. Some organizations use composite identifiers, concatenating elements—department codes, random numbers, or special characters—to make unique identifiers within the security domain. Other organizations generate random IDs to protect the resources from potential attackers. Most organizations use a single piece of unique information, such as a complete name or the user's first initial and surname.

2. Authentication

Authentication is the process of validating a supplicant's purported identity. There are three widely used authentication mechanisms, or authentication factors:

a. **Something a supplicant knows:** This factor of authentication relies upon what the supplicant knows and can recall for example, a password, passphrase, or other unique authentication code, such as a personal identification number (PIN). A **password** is a private word or combination of characters that only the user should know.

b. **Something a supplicant has :**This authentication factor relies upon something a supplicant has and can produce when necessary.

c. **Something a supplicant is:** This authentication factor relies upon individual characteristics, such as fingerprints, palm prints, hand topography, hand geometry, or retina and iris scans, or something a supplicant can produce on demand, such as voice patterns, signatures, or keyboard kinetic measurements.

3. Authorization

Authorization is the matching of an authenticated entity to a list of information assets and corresponding access levels. This list is usually an ACL or access control matrix.

4. Accountability

Accountability, also known as auditability, ensures that all actions on a system—authorized or unauthorized can be attributed to an authenticated identity. Accountability is most often accomplished by means of system logs and database journals, and the auditing of these records. Systems logs record specific information, such as failed access attempts and systems modifications. Logs have many uses, such as intrusion detection, determining the root cause of a system failure, or simply tracking the use of a particular resource.

3.6.1 Physical Design

Introduction

As one of the methods of control that go into a well-planned information security program, technical controls are essential in enforcing policy for many IT functions that do not involve direct human control. Networks and computer systems make millions of decisions every second and operate in ways and at speeds that people cannot control in real time. Technical control solutions, properly implemented, can improve an organization's ability to balance the often conflicting objectives of making information more readily and widely available against increasing the information's levels of confidentiality and integrity.

Parts of Physical Design

The physical design of an information security program is made up of two parts:

1. Security Technologies
2. Physical security

Physical design extends the logical design of the information security program which is found in the information security blueprint and the contingency planning elements-and make it ready for implementation. Physical design encompasses the selection and implementation of technologies and processes that mitigate risk from threats to the information assets of an organization assets of an organization.

The physical design process:

1. Selects specific technologies to support the information security blueprint identifies complete technical solutions based on these technologies, including deployment, operations, and maintenance elements, to improve the security of the environment.
2. Designs physical security measures to support the technical solution.
3. Prepares project plans for the implementation phase that follows.

3.6.2 Firewalls

In commercial and residential construction, firewalls are concrete or masonry walls that run from the basement through the roof, to prevent a fire from spreading from one section of the building to another. In aircraft and automobiles, a firewall is an insulated metal barrier that keeps the hot and dangerous moving parts of the motor separate from the inflammable interior where the passengers sit.

A firewall in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world,

known as the untrusted network (for example, the Internet), and the inside world, known as the trusted network. The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices. Firewalls can be categorized by processing mode, development era, or structure.

Firewall Processing Modes

Firewalls fall into five major processing-mode categories:

1. Packet-filtering firewalls
2. Application gateways
3. Circuit gateways
4. MAC layer firewalls
5. Hybrids. Hybrid firewalls

1. **Packet-filtering firewalls :** The packet-filtering firewall, also simply called a filtering firewall, examines the header information of data packets that come into a network. A packet-filtering firewall installed on a TCP/IP- based network typically functions at the IP level and determines whether to drop a packet (deny) or forward it to the next network connection (allow) based on the rules programmed into the firewall. Packet-filtering firewalls examine every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information

2. **Application Gateways** : The application gateway, also known as an application-level firewall or application firewall, is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router. The application firewall is also known as a proxy server since it runs special software that acts as a proxy for a service request.

3. **Circuit Gateways :** The circuit gateway firewall operates at the transport layer. Again, connections are authorized based on addresses. Like filtering firewalls, circuit gateway firewalls do not usually look at traffic flowing between one network and another, but they do prevent direct connections between one network and another. They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall, and then allowing only authorized traffic, such as a specific type of TCP connection for authorized users, in these tunnels. A circuit gateway is a firewall component often included in the category of application gateway, but it is in fact a separate type of firewall.

4. **MAC Layer Firewalls :** While not as well known or widely referenced as the firewall approaches above, MAC layer firewalls are designed to operate at the media access control sublayer of the data link layer (Layer 2) of the OSI network model. This enables these firewalls to consider the specific host computer's identity, as represented by its MAC or network interface card (NIC) address in its filtering decisions. Thus, MAC layer firewalls link the addresses of specific host computers to ACL entries that identify the specific types of packets that can be sent to each host, and block all other traffic.

5. **Hybrid Firewalls :** Hybrid firewalls combine the elements of other types of firewalls – that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways. A hybrid firewall system may actually consist of two separate firewall devices; each is a separate firewall system, but they are connected so that they work in tandem. For example, a hybrid firewall system might include a packet-filtering firewall that is set up to screen all acceptable requests, then pass the requests to a proxy server, which in turn requests services from a Web server deep inside the organization's networks. An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls.

Firewalls Categorized by Generation

Firewalls are also frequently categorized by their position on a developmental continuum – that is, by generation. The first generation of firewall devices consists of routers that perform only simple packet-filtering operations. More recent generations of firewalls offer increasingly complex capabilities, including the increased security and convenience of a DMZ – "demilitarized zone." At present, there are five generally recognized generations of firewalls, and these generations can be implemented in a wide variety of architectures.

1. First generation firewalls are static packet-filtering firewalls – that is, simple networking devices that filter packets according to their headers as the packets travel to and from the organization's networks.
2. Second generation firewalls are application-level firewalls or proxy servers – that is, dedicated systems that are separate from the filtering router and that provide intermediate services for requestors.
3. Third generation firewalls are stateful inspection firewalls, which, as described previously, monitor network connections between internal and external systems using state tables.
4. Fourth generation firewalls, which are also known as dynamic packet-filtering firewalls, allow only a particular packet with a particular source, destination, and port address to enter.

5. Fifth generation firewalls include the kernel proxy, a specialized form that works under Windows NT Executive, which is the kernel of Windows NT. This type of firewall evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack.

Firewalls Categorized by Structure

Firewalls can also be categorized by the structures used to implement them. Most commercial-grade firewalls are dedicated appliances. Specifically, they are stand-alone units running on fully customized computing platforms that provide both the physical network connection and firmware programming necessary to perform their function, whatever that function (static packet filtering, application proxy, etc.) may be. Some firewall appliances use highly customized, sometimes proprietary hardware systems that are developed exclusively as firewall devices.

Other commercial firewall systems are actually off-the-shelf general purpose computer systems that run custom application software on standard operating systems like Windows or Linux/Unix, or on specialized variants of these operating systems. Most small office or residential-grade firewalls are either simplified dedicated appliances running on computing devices or application software installed directly on the user's computer.

1. **Commercial-Grade Firewall Appliances :** Firewall appliances are stand-alone, self contained combinations of computing hardware and software. These devices frequently have many of the features of a general-purpose computer with the addition of firmware based instructions that increase their reliability and performance and minimize the likelihood of their being compromised. The customized software operating system that drives the device can be periodically upgraded, but can only be modified via a direct physical connection or after running extensive authentication and authorization protocols.

   The firewall rule sets are stored in nonvolatile memory, and thus they can be changed by technical staff when necessary but are available each time the device is restarted. These appliances can be manufactured from stripped-down general purpose computer systems, and/or designed to run a customized version of a general-purpose operating system. These variant operating systems are tuned to meet the type of firewall activity built into the application software that provides the firewall functionality

2. **Commercial-Grade Firewall Systems** : A commercial-grade firewall system consists of application software that is configured for the firewall application and run on a

general-purpose computer. Organizations can install firewall software on an existing general purpose computer system, or they can purchase hardware that has been configured to specifications that yield optimum firewall performance. These systems exploit the fact that firewalls are essentially application software packages that use common general-purpose network connections to move data from one network to another.

3. **Small Office/Home Office (SOHO) Firewall Appliances** : As more and more small businesses and residences obtain fast Internet connections with digital subscriber lines (DSL) or cable modem connections, they become more and more vulnerable to attacks. What many small business and work-from-home users don't realize is that, unlike dial-up connections, these high-speed services are always on; therefore, the computers connected to them are much more likely to be visible to the scans performed by attackers than those connected only for the duration of a dial-up session. Coupled with the typically lax security capabilities of legacy home computing operating systems like Windows 95, Windows 98, and even Windows Millennium Edition, most of these systems are wide open to outside intrusion.

Even Windows XP Home Edition, a home computing operating system which can be securely configured, is rarely configured securely by its users. (Newer operating systems like Windows Vista offer the promise of improved security "out of the box.") Just as organizations must protect their information, residential users must also implement some form of firewall to prevent loss, damage, or disclosure of personal information.

4. **Residential-Grade Firewall Software :** Another method of protecting the residential user is to install a software firewall directly on the user's system. Many people have implemented these residential-grade software-based firewalls (some of which also provide antivirus or intrusion detection capabilities), but, unfortunately, they may not be as fully protected as they think.

Firewall Architectures

All firewall devices can be configured in a number of network connection architectures. These approaches are sometimes mutually exclusive and sometimes can be combined. The configuration that works best for a particular organization depends on three factors: the objectives of the network, the organization's ability to develop and implement the architectures, and the budget available for the function. Although literally hundreds of variations exist, there are four common architectural implementations:

1. Packet-filtering routers
2. Screened host firewalls
3. Dual-homed firewalls
4. Screened subnet firewalls

1. **Packet-Filtering Routers :** Most organizations with an Internet connection have some form of a router at the boundary between the organization's internal networks and the external service provider. Many of these routers can be configured to reject packets that the organization does not want to allow into the network. This is a simple but effective way to lower the organization's risk from external attack. The drawbacks to this type of system include a lack of auditing and strong authentication. Also, the complexity of the ACLs used to filter the packets can degrade network performance.

2. **Screened Host Firewalls** : Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall, such as an application proxy server. This approach allows the router to prescreen packets to minimize the network traffic and load on the internal proxy. The application proxy examines an application layer protocol, such as HTTP, and performs the proxy services.

   This separate host is often referred to as a bastion host; it can be a rich target for external attacks and should be very thoroughly secured. Even though the bastion host/application proxy actually contains only cached copies of the internal Web documents, it can still present a promising target, because compromise of the bastion host can disclose the configuration of internal networks and possibly provide attackers with internal information.

3. **Dual-Homed Host Firewalls** : The next step up in firewall architectural complexity is the dual-homed host. When this architectural approach is used, the bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration. One NIC is connected to the external network, and one is connected to the internal network, providing an additional layer of protection. With two NICs, all traffic must physically go through the firewall to move between the internal and external networks. Implementation of this architecture often makes use of NAT.

4. **Screened Subnet Firewalls (with DMZ)** : The dominant architecture used today is the screened subnet firewall. The architecture of a screened subnet firewall provides a DMZ. The DMZ can be a dedicated port on the firewall device linking a single bastion host, or it can be connected to a screened subnet, as shown in Figure. Until

recently, servers providing services through an untrusted network were commonly placed in the DMZ. Examples of these include Web servers, file transfer protocol (FTP) servers, and certain database servers. More recent strategies using proxy servers have provided much more secure solutions.

A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet-filtering router, with each host protecting the trusted network. There are many variants of the screened subnet architecture. The first general model consists of two filtering routers, with one or more dual-homed bastion hosts between them. In the second general model, as illustrated in Figure the connections are routed as follows:

1. Connections from the outside or untrusted network are routed through an external filtering router.
2. Connections from the outside or untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the DMZ.
3. Connections into the trusted internal network are allowed only from the DMZ bastion host servers.

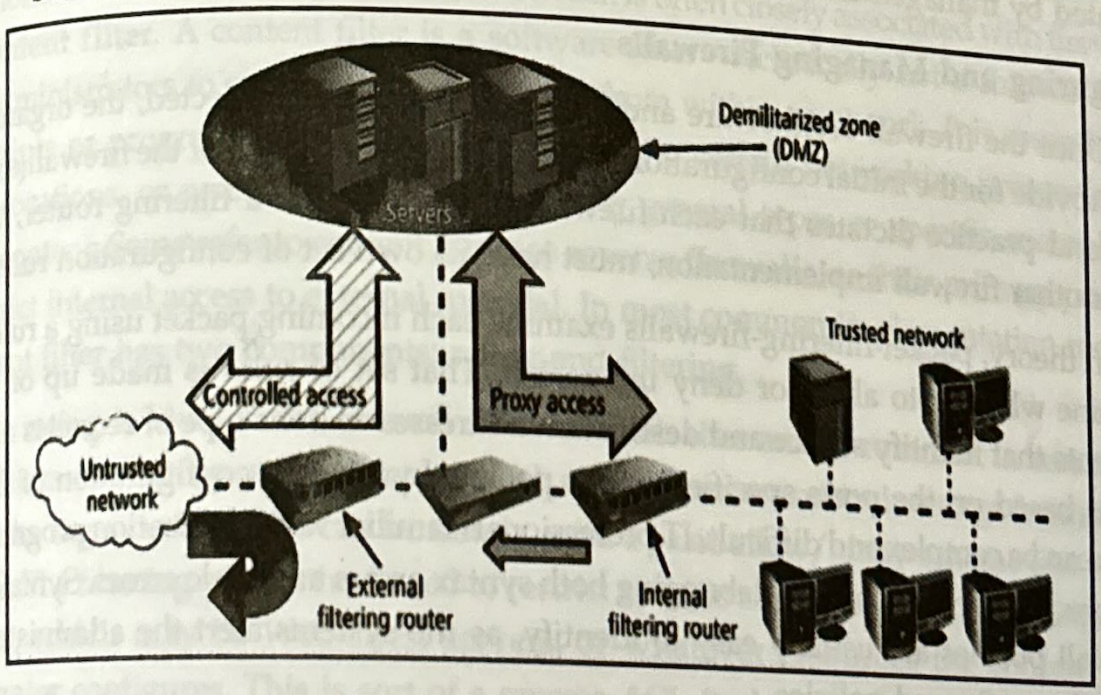

Fig: Screened Subnet (DMZ)

The screened subnet is an entire network segment that performs two functions: it protects the DMZ systems and information from outside threats by providing a network of intermediate security (more secure than the general public networks but less secure than the internal network); and it protects the internal networks by limiting how external connections can gain access to them. Although extremely secure, the screened subnet can be expensive to implement and complex to configure and manage. The value of the information it protects must justify the cost.

Selecting the Right Firewall

When trying to determine which is the best firewall for an organization, you should consider the following questions:

1. Which type of firewall technology offers the right balance between protection and cost for the needs of the organization?
2. What features are included in the base price? What features are available at extra cost? Are all cost factors known?
3. How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?
4. Can the candidate firewall adapt to the growing network in the target organization?

The most important factor is, of course, the extent to which the firewall design provides the required protection. The second most important factor is cost. Cost may keep a certain make, model, or type out of reach. As with all security decisions, certain compromises may be necessary in order to provide a viable solution under the budgetary constraints stipulated by management.

Configuring and Managing Firewalls

Once the firewall architecture and technology have been selected, the organization must provide for the initial configuration and ongoing management of the firewall(s). Good policy and practice dictates that each firewall device, whether a filtering router, bastion host, or other firewall implementation, must have its own set of configuration rules.

In theory, packet filtering-firewalls examine each incoming packet using a rule set to determine whether to allow or deny the packet. That set of rules is made up of simple statements that identify source and destination addresses and the type of requests a packet contains based on the ports specified in the packet. In fact, the configuration of firewall policies can be complex and difficult. IT professionals familiar with application programming can appreciate the difficulty of debugging both syntax errors and logic errors. Syntax errors in firewall policies are usually easy to identify, as the systems alert the administrator to incorrectly configured policies.

However, logic errors, such as allowing instead of denying, specifying the wrong port or service type, and using the wrong switch, are another story. A myriad of simple mistakes can take a device designed to protect users' communications and turn it into one giant choke point. A choke point that restricts all communications or an incorrectly configured rule can cause other unexpected results.

For example, novice firewall administrators often improperly configure a virus-screening e-mail gateway (think of this as a type of e-mail firewall) so that, instead of

screening e-mail for malicious code, it blocks all incoming e-mail and causes, understandably, a great deal of frustration among users.

Configuring firewall policies is as much an art as it is a science. Each configuration rule must be carefully crafted, debugged, tested, and placed into the ACL in the proper sequence– good, correctly sequenced firewall rules ensure that the actions taken comply with the organization's policy.

In a well-designed, efficient firewall rule set, rules that can be evaluated quickly and govern broad access are performed before ones that may take longer to evaluate and affect fewer cases. The most important thing to remember when configuring firewalls is this: when security rules conflict with the performance of business, security often loses. If users can't work because of a security restriction, the security administration is usually told, in no uncertain terms, to remove the safeguard. In other words, organizations are much more willing to live with potential risk than certain failure.

Content Filters

Another utility that can help protect an organization's systems from misuse and unintentional Denial-of-service problems, and which is often closely associated with firewalls, is the **content filter**. A content filter is a software filter–technically not a firewall–that allows administrators to restrict access to content from within a network. It is essentially a set of scripts or programs that restricts user access to certain networking protocols and Internet locations, or restricts users from receiving general types or specific examples of Internet content. Some refer to content filters as **reverse firewalls**, as their primary purpose is to restrict internal access to external material. In most common implementation models, the content filter has two components: rating and filtering.

The rating is like a set of firewall rules for Web sites and is common in residential content filters. The rating can be complex, with multiple access control settings for different levels of the organization, or it can be simple, with a basic allow/ deny scheme like that of a firewall. The filtering is a method used to restrict specific access requests to the identified resources, which may be Web sites, servers, or whatever resources the content filter administrator configures. This is sort of a reverse ACL (technically speaking, a capability table), in that whereas an ACL normally records a set of users that have access to resources, this control list records resources which the user cannot access.

3.6.3 Protecting Remote Connections

The networks that organizations create are seldom used only by people at that location. When connections are made between one network and another, the connections are arranged

and managed carefully. Installing such network connections requires using leased lines or other data channels provided by common carriers, and therefore these connections are usually permanent and secured under the requirements of a formal service agreement. But when individuals—whether they be employees in their homes, contract workers hired for specific assignments, or other workers who are traveling—seek to connect to an organization's network(s), a more flexible option must be provided.

In the past, organizations provided these remote connections exclusively through dial-up services like Remote Authentication Service (RAS). Since the Internet has become more widespread in recent years, other options such as virtual private networks (VPNs) have become more popular.

Remote Access

Before the Internet emerged, organizations created private networks and allowed individuals and other organizations to connect to them using dial-up or leased line connections. (In the current networking environment, where Internet connections are quite common, dial-up access and leased lines from customer networks are used less frequently.) The connections between company networks and the Internet use firewalls to safeguard that interface. Although connections via dial-up and leased lines are becoming less popular, they are still quite common. And it is a widely held view that these unsecured, dial-up connection points represent a substantial exposure to attack.

An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points. A war dialer is an automatic phone-dialing program that dials every number in a configured range (e.g., 555-1000 to 555-2000), and checks to see if a person, answering machine, or modem picks up. If a modem answers, the war dialer program makes a note of the number and then moves to the next target number. The attacker then attempts to hack into the network via the identified modem connection using a variety of techniques.

Dial-up network connectivity is usually less sophisticated than that deployed with Internet connections. For the most part, simple username and password schemes are the only means of authentication. However, some technologies, such as RADIUS systems, TACACS, and CHAP password systems, have improved the authentication process, and there are even systems now that use strong **encryption.**

Virtual Private Networks (VPNs)

Virtual private networks are implementations of cryptographic technology A virtual private network (VPN) is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network.

The Virtual Private Network Consortium (VPNC) (www.vpnc. org) defines a VPN as "a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures." VPNs are commonly used to securely extend an organization's internal network connections to remote locations.

3.6.4 Virtual Private Networks (VPNs)

The VPNC defines three VPN technologies: trusted VPNs, secure VPNs, and hybrid VPNs. A trusted VPN, also known as a legacy VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits. The organization must trust the service provider, who provides contractual assurance that no one else is allowed to use these circuits and that the circuits are properly maintained and protected—hence the name trusted VPN.9 Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet. A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used:

1. Encapsulation of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network and be usable by the server network environment.
2. Encryption of incoming and outgoing data to keep the data contents private while in transit over the public network, but usable by the client and server computers and/or the local networks on both ends of the VPN connection.
3. Authentication of the remote computer and, perhaps, the remote user as well. Authentication and the subsequent authorization of the user to perform specific actions are predicated on accurate and reliable identification of the remote system and/or user.

In the most common implementation, a VPN allows a user to turn the Internet into a private network. As you know, the Internet is anything but private. However, an individual

or organization can set up tunneling points across the Internet and send encrypted data back and forth, using the IP-packet-within-an-IP-packet method to transmit data safely and securely.

VPNs are simple to set up and maintain and usually require only that the tunneling points be dual-homed—that is, connecting a private network to the Internet or to another outside connection point. There is VPN support built into most Microsoft server software, including NT and 2000, as well as client support for VPN services built into XP. While true private network services connections can cost hundreds of thousands of dollars to lease, configure, and maintain, a VPN can cost only a modest amount.

There are a number of ways to implement a VPN. IPSec, the dominant protocol used in VPNs, uses either transport mode or tunnel mode. IPSec can be used as a stand-alone protocol, or coupled with the Layer Two Tunneling Protocol (L2TP).

1. Transport Mode

In transport mode, the data within an IP packet is encrypted, but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contents of the packet. The downside to this implementation is that packet eavesdroppers can still identify the destination system. Once an attacker knows the destination, he or she may be able to compromise one of the end nodes and acquire the packet information from it. On the other hand, transport mode eliminates the need for special servers and tunneling software, and allows the end users to transmit traffic from anywhere. This is especially useful for traveling or telecommuting employees.

There are two popular uses for transport mode VPNs. The first is the end-to-end transport of encrypted data. In this model, two end users can communicate directly, encrypting and decrypting their communications as needed. Each machine acts as the end node VPN server and client. In the second, a remote access worker or teleworker connects to an office network over the Internet by connecting to a VPN server on the perimeter. This allows the teleworker's system to work as if it were part of the local area network.

The VPN server in this example acts as an intermediate node, encrypting traffic from the secure intranet and transmitting it to the remote client, and decrypting traffic from the remote client and transmitting it to its final destination. This model frequently allows the

remote system to act as its own VPN server, which is a weakness, since most work-at-home employees do not have the same level of physical and logical security they would have if they worked in the office.

2. **Tunnel Mode**

Tunnel mode establishes two perimeter tunnel servers that encrypt all traffic that will traverse an unsecured network. In tunnel mode, the entire client packet is encrypted and added as the data portion of a packet addressed from one tunneling server to another. The receiving server decrypts the packet and sends it to the final address. The primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.

IMPORTANT QUESTIONS

1. What is Security policy? Explain about Standards and practices.
2. Explain about Security blue print and Security education.
3. What are the Continuity strategies?
6. What is Security Technology? Explain about Firewalls and VPNs.
7. Explain about Physical design steps and protecting remote connections.