Planning for Security

* Strategic planning starts with the executive level setting a long-term direction for the organization.
* The next step in the strategic plan is to translate these plans into tactical objectives that move toward reaching specific measurable, achievable, and time-bound accomplishments.
* Tactical planning focuses on the short-term (1 or 2 years).
  + Budgeting, resource allocation and personnel are critical components of the tactical plan.
* Managers and employee's use operational plans, which are derived from the tactical plans, to organize the ongoing, day-to-day performance of tasks.
  + Necessary tasks for all relevant departments, as well as communication and reporting requirements.
* The first priority of the CISO and the info sec management team is the creation of a strategic plan to accomplish the organization's info sec objectives.
* 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.
* Standards are more detailed statements of what must be done to comply with policy.
* De facto standards are part of organizational culture.
* De jure standards are published, scrutinized and ratified by a group.
* Mission is a written statement of an organization's purpose.
* Vision is a written statement about the organization's purpose.
* Management must define three types of security policy:
  + Enterprise info sec policies
  + Issue-specific policies
  + Systems-specific policies
* Enterprise info sec policy is based on and directly supports the mission, visiion and direction of the organization and sets the strategic direction, sope and tone for all security efforts.
  + Drafted by the CIO
  + Should include the following elements:
    - Overview of corporate philosophy on security
    - Info on the structure of info sec organization and indivduals who fulfill the info sec role
    - Responsibilities for security members that are shared throughout the organization.
    - Responsibilities for security members that are more specific in nature.
* Issue-specific security policy addresses specific areas, requires frequent updates and contains a statement on the organization's position on a specific instance.
  + Covers:
    - E-mail, use of Internet, specific minimum configs of computers to defend against worms and viruses.
    - Prohibitions on hacking
    - Use of personal equipment on company networks
    - Use of telecommunications technologies
    - Use of photocopy equipment
  + Policy layout?
    - Policy should begin with a statement of clear purpose.
    - The next section should state usage privileges.
    - Then, prohibited uses of equipment.
    - Then, systems management.
    - Then, violations of privacy.
    - Time table for review of policy
    - Limitations of liability
* Systems-specific policy can be separated into two general groups: managerial guidance and technical specifications.
  + Managerial
    - Created to guide the implementation and configuration of technology as well as to address the behavior of people in the organization in ways that support the security of information.
  + Technical
    - Created by system administrators in order to implement the managerial policy. Each type of equipment needs its own policy.
    - Access control lists (ACLs) consist of user access lists, matrices, and capability tables that govern the rights and privileges of users.
    - A capabilities table specifies which subjects and objects users or groups can access.
    - ACLs regulate
      * Who can use, what can be accessed, when the system can be used, where the system can be accessed from.
    - Configuration-rule policies are the specific instructions that govern how a security system reactss to the data it recieves.
  + Combination SysSPs are combinations of managerial and technical.
  + Policy administrator is responsible for the creatino, revision, distrubition and storage of the policy.
  + Encourage staff members to make suggestions to the policy.
* Information Security Blueprint
  + Once an organization has developed its policies it can begin developing a blueprint for the info sec program.
  + After inventory is taken, threats prioritized, a risk assessment(s) and feasibility analysis and CBA must be conducted.
  + Security blueprint is the basis for design, selection and implemnetation 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.
  + Security framework is an outline of the overall informatino security stragey for the organization and a roadmap for planned changes to the info sec environment of the oganzaiton.
* The ISO 27000 Series
  + Refused to adopt it in the US and other countries because:
    - Global info sec community had not defined any jusitifcation for a code of practice.
    - Lacked "necessary measurement precision of a technical standard."
    - No reason to believe it was more useful than any other approach.
    - Not as complete as other frameworks.
    - Hurriedly prepared.
* ISO/IEC 27001:2005
  + Define scope and policy
  + Risks
  + Create risk treatment plans
  + Implement controls
  + Monitor procedures
  + Conduct internal audits
  + Improve and communicate
* NIST Security Models
  + NIST = National Institute for Standards and Technology
  + NIST security principals
    - Security supports the mission of the organization.
    - Security is an integral element of sound management.
    - Security should be cost-effective.
    - Systems owners have security responsibilities outside their own organizations.
    - Security responsibilities and accountability should be made explicit.
    - Security requires a comprehensive and integrated approach.
    - Security should be periodically reassessed.
    - Security is constrained by societal factors.
* Design of Security Architecture
  + Spheres of Security
    - Pg 204, figure 5-8.
* Levels of control
  + Managerial controls
    - Are security processes that are designed by strategic planners and implemented by the security administration of the organization.
  + Operational controls
    - Are management and lower-level planning functions that deal with the operational functionality of security in the irganization, such as disaster recovery and incident response planning.
  + Technical controls
    - Tactical and technical implementations of security in the organization.
* Defense in Depth
  + A layered approach to defense.
  + Organized into policy, training and education and technology as per CNSS model.
* Security perimeter
  + Defines the boundary between the outer limit of an organization's security and the beginning of the outside world.
  + Security domains are areas of trust within which users can freely communicate.
* Firewalls
  + A device that selectively discriminates against information flowing into or out of the organization.
  + Gateway routers purpose is to connect the organization's systems to the outside world, it too can be used as the front-line defense against atacks, as it can be configuared to allow only set types of protocols to enter.
* Proxy Server
  + Performs actions on behalf of another system. When deployed, a proxy server is configured to look like a Web server and is assigned the domain name that users would be expecting to find for the system and its services.
* Intrusion Detection and Prevention Systems
  + Two versions: Host-Based IDPSs and Network-Based IDPSs
  + Host - usually installed on the machines they protect to monitor the status of various files stored on those machines.
  + Network - patterns of network traffic and attempt to dectect unusual acrtivity based on previous baselines.
* Security Education, Training and Awareness Program
  + SETA focuses on enhancing security by doing the following:
    - Improving awareness of the need to protect system resources
    - Developing skills and knowledge so computer users can perform their jobs more securely
    - Building in-depth knowledge, as needed, to design, implement or operate security programs
* Continuity Strategy
  + Incident Response (IR) plan addresses the identification, classificiation, reponse and recovery from an icident.
  + Disaster Recovery plan addresses the preparation for the recovery from a disaster, whether natural or man-made.
  + Business Continuity plan ensures that critical business continue if catastrophe hits.
* Business Impact Analysis
  + Investigation and assessment of the impact that various attacks can have on the organization.
  + Areas that the BIA hits:
    - Threat attack identification and prioritization
      * Attack profile is a detailed description of activities that occur during an attack.
    - Business unit analysis
      * Must determine which areas of the business are the most vital to continued operations.
    - Attack success scenario development
      * Create many scenarios of a successful attack for preparation purposes.
    - Potential damage assessment
      * Using the scenarios, you must estimate the cost of the best, worst and most likely causes.
    - Subordinate plan classification
      * Plan that takes into account the identification of, reaction to, and recovery from each attack scenario.
* IR planning
  + Attacks are classified as incidents if they have the following characteristics:
    - They are directed against info assets.
    - They have a realistic chance of success.
    - They could threaten the confidentiality, integrity or availability of info resources.
  + Consists of four phases:
    - Planning
      * Incident Response plan must be in place. Create a directory of incidents with tabbed sections for each incident. Simply flip to the right page for the right incident.
      * Must be quick and easy to read. Organized very nicely. Have sections for during and after the incident. Also should have procedures to perform before the incident.
      * Must be stored in an easy to find location and the right people should know where to find it.
      * Plan should be tested. Checklist, Structured walkthrough, simulation, parallel, full interruption.
    - Detection
      * Four types of incident indicators: presence of unfamiliar files, presence of execution of unknown programs or processes, unusual consumption of computing resources, unusual system crashes.
      * Types of events: activities at unexpected times, presence of new accounts, reported attacks, notification from IDPS.
      * Definite indicators: use of dormant accounts, changes to logs, presence of hacker tools, notifications by partner or peer, notification by hacker, loss of availability, loss of integrity, loss of confidentiality, violation of policy, violation of law.
    - Reaction
      * Part of the plan that tries to stop the incident, mitigate the impact and provide info for recovery.
      * Alert roster is a document containing contact info for the people to be notified in the event of an incident; note that it should name only those who must respond to the incident.
      * Should always document everything from start to finish of the incident.
      * Incident Containment Strats
        + Pull the plug, not feasible in every case.
        + If the incident is using compromised accounts, disable the account.
        + Bypassing a firewall, reconfigure the firewall to block.
        + Service or process, disable it.
        + Email, application or server taken down.
    - Incident Recovery
      * Incident damage assessment is the rapid determination of the scope of the breach of the confidentiality, integrity, and availability of info and info assets during or must following an incidient.
      * Computer forensics is the processs of collecing, analysizinjg and preserving computer-related evidence.
      * Evidence is a physical object or documented info that proves an action occurred or identifies the intent of a perpetrator.
      * Stages of Recovery:
        + Identify the vulnerabilities that allowed the incident to occur and spread. Resolve them.
        + 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.
        + Evaluate monitoring capabilities (if present). Improve their detection and reporting methods, or simply install new monitoring capabilities.
        + Restore data from backups.
        + Restore services and processes in use.
        + Continuously monitor the system.
        + Restore the confidence of the organization's communities of interest.
* Disaster Recovery Plan comes into effect when the organization is unable to mitigate the impact of an incident during the incident or the level of damage or destruction is so severe that the organization is unable to recover quickly.
  + Steps in the plan:
    - Priorities must be clearly established.
    - Roles and responsibilities must be clearly distinguished.
    - Someone must initiate the alert roster and notify key personel.
    - Someone must be tasked with documenting the disaster.
    - If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations.
* Business Continuity Plan prepares an organization to reestablish critical business operations during a disaster that affect operations at the primary site.
  + Must find temporary facilities that can be used in the case of a disaster.
  + Hot Sites are fully configured computer facilities with all services, communications links and physical plant operations including heating and air conditioning.
  + Warm site provides many of the same services and options of the hot site. However, it typically does not include the actual applications the company needs, or the applications may not yet be installed and configured.
  + Cold site provides only rudimentary services and facilities.
  + Time-shares is a hot, warm or cold site that is leased in conjunction with a business partner or sister organization.
  + Service Bureau is an agency that provides a service for a fee.
  + Mutual agreement is a contract between two or more organizations that psecifices how each will assist the other in the event of a disaster.
* Law Enforcement Involvement