

“Security policies define the rules that regulate how an organization manages and protects its information and computing assets to achieve security objectives. Security policies that are documented, well known, and visibly enforced establish expected user behavior and serve to inform users of their obligations for protecting computing assets. Users include all those who access, administer, and manage your systems and have authorized accounts on an organization’s systems. They play a vital role in implementing security policies.

“A policy must be enforceable to achieve its objectives. In most organizations, the administrators responsible for the technological aspects of information security do not have the authority to enforce security policies. It is therefore necessary to educate management about security issues, the need for policies in specific topic areas such as acceptable use, and then to obtain a commitment to support the development, deployment, maintenance, and enforcement of those policies” [Allen 01].

“Two-thirds of [CIO.com] survey respondents (600 IT professionals) said their company did not have a well-defined company-wide security policy or plan in place, and the majority of those surveyed lack data-handling guidelines and policies.

“In close to half of the companies, employees are provided with information about security policy. However, familiarity with the company’s security policies is required of employees in less than one-third of the companies surveyed.

“In close to one-third of the companies surveyed, the organization’s critical information is accessible directly via the Internet. Servers that store critical information communicate directly with other systems that are accessible via the Internet in more than half of the companies.

“Employees have access to critical data when they don’t necessarily need access. Results of our survey showed that overall, a greater percentage of employees were allowed to access the company’s critical information than needed.

“Half of the companies in our survey have no system in place to determine if the company’s infrastructure is under attack. More than half of the respondents said their company has no automatic procedure or alert in place for escalating security-related events (breach, unauthorized access, or suspicious activity). The majority of companies we surveyed wouldn’t know they were attacked or hacked for 24 hours” [Ware 01].

Real World Problem Cases Caused By Missing Policies: <<http://www.baselinesoft.com/whatif.html>>

Lack of Acceptable Use Policy:

“A clerk spent a great deal of time surfing the Internet while on the job. Because there was no policy specifying what constituted excessive personal use, management could not discipline this employee. Then management discovered that the clerk had downloaded a great deal of pornography. Using this as a reason, management fired him. The clerk chose to appeal the termination with the Civil Service Board, claiming that he couldn't be fired because he had never been told that he couldn't download pornography. After a Civil Service hearing, the Board ordered him to be reinstated with back pay.

Lack of Personnel Management and Least Privilege Policy:

“The manager of data processing took a job with a competing law firm. Because his former employer had nobody who could do the job that he did, they kept him on as a contractor. On a part-time basis, he would perform systems management tasks. In order to do these tasks he needed full privileges on the former employer's network. One day the former employer learned that the manager's new employer was opposing them in a high-visibility lawsuit. Could the former data processing manager gain access to the shared legal strategy files for this case on the network? The answer was yes, but nobody knew whether the manager had exploited these capabilities because no data access logs were being kept. This situation could have been avoided if the former employer had policies about conflicts of interest, system access privileges, and keeping logs.

Lack of Account Management Policy:

“A local newspaper had no policy requiring the termination of user-ID and password privileges after an employee left. A senior reporter left the newspaper, and shortly thereafter, the newspaper had trouble because the competition consistently picked-up on their exclusive stories (scoops). An investigation of the logs revealed that the former employee had been consistently accessing their computer to get ideas for stories at his new employer.

Lack of Virus Alert Handling Policy:

“A virus hoax sent by email through the Internet indicated that if people receive a message with the heading “Join the Crew,” they should not read it. The hoax went on to state that this email would erase a hard drive if ever it should be displayed. Thinking that they were doing others a favor, 10% of the staff at a large manufacturing company broadcast the hoax to all the people they knew. Because no policy defined how they should handle these warnings, they flooded the company's internal networks with email and caused a great deal of technical staff time to be wasted unnecessarily.

Lack of Employee Data Protection Policy:

“Because it had no policy requiring employee private data to be encrypted when held in storage, a large manufacturing company found itself facing a public relations problem. A thief made off with a computer disk containing detailed personal data and bank account information on more than 20,000 current and former employees. The press speculated that this could be used to facilitate identity theft, including application for credit cards in the names of other people. The event precipitated a massive notification process including recommendations on changes to bank account numbers.

Lack of [Privacy] Policy Enforcement:


“A Navy enlisted man registered with an Internet online service company and filled out a profile form, which indicated that he was gay. An employee at the service company, after an inquiry from the Navy, shared this profile information with the Navy's “top brass.” Based on this information, the enlisted man was given a dishonorable discharge. The enlisted man sued the Navy for violating its own “don't ask, don't tell” policy, and won an honorable discharge with retirement benefits as a result. The online service company publicly stated that its employee had violated “the privacy policy,” but this policy had been

Student Workbook – Module 3: Policy Formulation and Implementation

violated on multiple occasions before including top management's publicly stated intention to sell customer home telephone numbers to telephone marketers. At least the service firm now admits that it has a policy.”

Two examples from an administrator’s perspective:

- Lack of Vulnerability Analysis Policy: There are a number of anecdotal cases of an administrator using password cracking tools (to test whether or not users are following the password policy) or network mapping software (to check for open ports and update network topologies) and then getting fired or suspended for inappropriate access or system disruption when using these tools
- Lack of Network Traffic Policy: It is extremely difficult, if not impossible, to configure a firewall properly if security policies have not been created. A firewall is, by definition, an enforcer of security policies.



Networked Systems Survivability

Instructional Objectives

Describe the importance of establishing, deploying, maintaining, and enforcing information security policies

- Identify characteristics of an effective security policy

Provide understanding of administrator's role in policy formulation and implementation

© 2002 Carnegie Mellon University Module 3: Policy Formulation and Implementation – slide 2

An administrator's job, in large part, is to keep the organization's computing infrastructure up and running in a secure manner. But what does this mean? Security policy guides both this process and an administrator's decisions and actions by defining requirements that must be fulfilled. Some occasions when a security policy could help guide actions include:

- adding new users to the system or removing users no longer employed by the organization
- adding, updating, or migrating to a new asset or to a new asset configuration (e.g., a new operating system)
- configuring a firewall or intrusion detection system including what alerts are high priority
- monitoring system, network, file and directory, and user activities including determining what constitutes suspicious behavior

Policies, when written properly, clearly articulate roles, responsibilities, and authority to act, and, as a result, protect and guide administrators.

This module will assist an administrator in answering the following questions:

- How should I think about security policies and their implementation?
- What is a useful framework for making security policies real in my organization's infrastructure?
- How can the presence of policies protect me?
- How can the absence of policies hurt me?
- How do I go about making changes in policies based on my operational experience?
- What are the consequences for not complying with policies? What is my role in ensuring policy compliance and taking action in the event of non-compliance?

Overview

Information security policies

- Participants, characteristics, and topics

Role of administrators

Security requirements are satisfied by:

- performing asset and risk management as describe in Module 2
- establishing, deploying, maintaining, and enforcing information security *policies* defining, deploying, and maintaining a *roadmap* for policy implementation that is reflected in infrastructure design and operations
- ensuring that *roles and responsibilities* are clearly defined including those of administrators

Security requirements derive from an organization’s mission and business objectives. These objectives provide a strategic understanding of what information assets need to be protected from compromise, damage, and loss. Performing risk management (including preparation, assessment, mitigation, and monitoring as described in Module 2) adds clarity and detailed guidance for information asset protection. Risk assessment is used to identify critical assets, identify threats to those assets, and formulate asset protection strategies based on identified risks. The presence of security policies demonstrates due diligence in the protection of information assets, which is critical for mitigating legal liability.

Using explicit and implicit security requirements and the enhanced understanding resulting from risk management processes, responsible parties can develop and maintain security policies and responsive infrastructure designs that satisfy these requirements.

Policies are used to guide organizational decisions and behavior. Effective security policies are viewed by users (including administrators) as effective and useful, not as barriers to getting the job done.

Security is a requirement of infrastructure design, not an “after the fact” add-on. Security policies cannot be directly implemented; they are typically too high level. Policy requirements, reflected in design decisions, are made real in an operational infrastructure through subsequent detailed design activities, development, and technology selection and implementation. There is a logical progression of actions to take where a roadmap can assist an administrator in ordering and prioritizing such actions.

If an organization can make the difficult strategic decisions on information security up-front, it makes the implementation of the rest of the program that much easier. Sponsored, comprehensive, and up-to-date policies are critical in meeting an organization’s security requirements. There must be a clear, implemental, traceable path from policy specification to policy implementation. These artifacts enhance communication between members of Information Security teams, executive management, and key stakeholders, and they provide a common understanding of the foundations required for more effective information security [Palmer 01].

Importance of an Information Security Policy

The key directive for taking action to implement an organization's security requirements

In the absence of an organization- or site-wide security policy, decisions are often made tactically, bottom-up, and with a short-term, crisis focus



© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 4

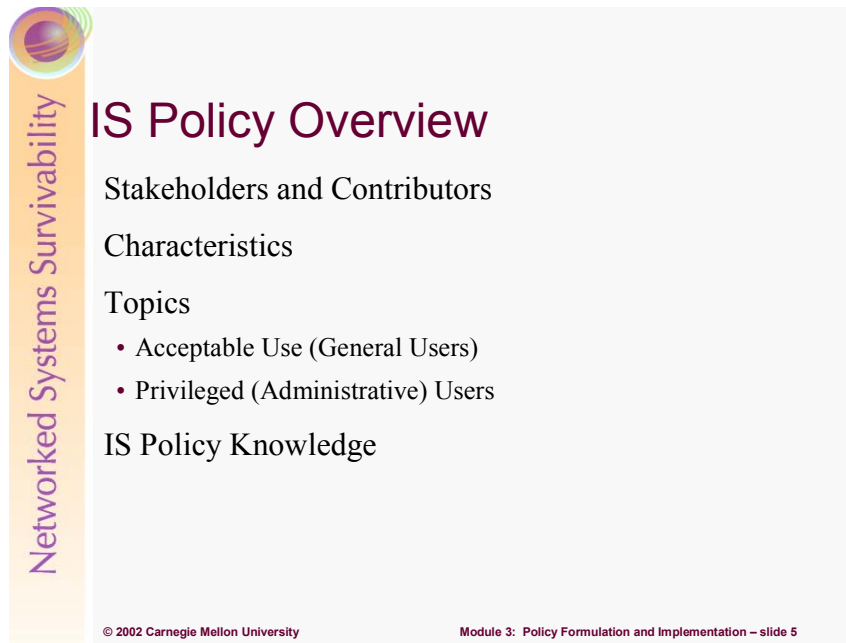
As a case in point, it is essential that those responsible for your organization's information assets be adequately prepared to know what constitutes a breach to security and to detect if any such breaches have occurred. Without advance planning, policy deployment, and preparation, it will be difficult, if not impossible, to determine

- if there has been – or still is – an intruder
- the extent of the damage caused by the intrusion
- how to return affected systems to a known, trusted state
- roles, responsibilities, and the authority to act

Most organizations have to experience a significant security event, or observe this happening to one of their major competitors or peer organizations, before those responsible recognize the need for comprehensive planning and preparation. If, for example, you depend on your public Web site to conduct a high volume of business transactions or communication, simple Web site defacement or a more serious denial-of-service attack can cause such a loss of customer and public confidence that they permanently take their business elsewhere.

Federal, state, and local laws and regulations with which you need to comply are constantly evolving. New and updated technologies are regularly released. Intruder attack methods and the damage they cause are constantly evolving, posing new threats to your information assets. So as part of conducting normal day-to-day business, you need to have processes in place to keep information security policies and their implementation up to date. These changes serve as immediate, updated “marching orders” for the way the organization does business [Allen 01].

Having an effective IS policy in place should be considered a prerequisite for being in business. Having a bad policy or no policy, while buying and installing security solutions such as firewalls and intrusion detection systems, is like having cops, courts, and prisons, but no laws [McBride 02].



Networked Systems Survivability

IS Policy Overview

- Stakeholders and Contributors
- Characteristics
- Topics
 - Acceptable Use (General Users)
 - Privileged (Administrative) Users
- IS Policy Knowledge

© 2002 Carnegie Mellon University Module 3: Policy Formulation and Implementation – slide 5

This section describes attributes of security policies including:

- the identification and involvement of stakeholders (those who have a vested interest in a policy's specification and enforcement) and contributors (those who participate in policy development, deployment, and maintenance)
- characteristics of an effective policy (such as clearly defined roles and responsibilities and being stated at a high enough level to allow for a range of implementation solutions)
- the topics that most security policies should address
- the questions an organization should ask to determine if employees understand its security policies and if their behavior is consistent with these policies

Policies Defined

Senior Management Statement of Policy

- Acknowledgement
- Support
- Commitment

Regulatory

Advisory

Informative



© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 6

Policies define the rules that regulate how an organization manages and protects its information and computing assets in order to achieve their survivability objectives. Policies that are documented, well known, and visibly enforced establish expected user behavior and serve to inform them of their obligations for protecting the organization's information assets. Users include all those who access, administer and manage, or have authorized accounts on an organization's system. A policy must be enforceable to achieve its objectives.

Survivability policies are less implemented and deployed than traditional security policies. As a result, we will concentrate on security policies, with the understanding that most of the practices are the same when developing and deploying policies that deal with overall mission survivability.

Information security policies define the organization's rules and expectations regarding access, protection, and accountability of information assets and resources. Security policies are imperative for a sound security implementation. Ideally, policies should be written first, and then where prudent, have technology implemented to enforce them; however this is often not the case. Policies may be a requirement of government or regulatory functions and may be essential during a disaster. They may also provide protection from liabilities or form a basis for certain security controls.

Policies are considered the highest level of documentation from which standards, guidelines, and procedures are formed. The higher level policies are created first for strategic reasons and the more tactical elements can follow.

Policy creation begins with the Senior Management Statement of Policy. This general, high level statement contains the following elements:

- An acknowledgement of the importance of the computing resources to the business model
- A statement of support for information survivability throughout the enterprise
- A commitment to authorize and manage the definition of the lower level standards, procedures, and guidelines.

The senior management's statement of commitment is important to the survivability initiative's success. Management must understand how important planning, controls and protections are to the company's survival. Senior management must publicly support the implementations throughout the organization.

Student Workbook – Module 3: Policy Formulation and Implementation

There is much evidence, both statistical and anecdotal, that many senior managers are not taking the issue of security seriously. For instance an Information Week survey of 1,271 computer managers found that only 22 percent believed that their senior managers thought that information security was "extremely important". Senior managers, they felt, were more concerned with the 'bottom line' issues of reducing costs and improving competitiveness. These are obviously worthwhile - and indeed vital - business goals, but there seems to be an ignorance amongst many senior managers (who may well have climbed to the top before their business was as dependant on the PC as it is today) that effective security can reduce costs [3].

Regulatory policies are security policies that an organization is required to implement, due to compliance, regulation, or other legal requirements. [1]. Organizations with public interest usually use regulatory policies which are detailed and specific to the industry in which it operates. The main purpose of regulatory policies is to ensure the organization is adhering to standard operating procedures or policies in their specific industry.

The growth of computer hacking, Trojan horses, emergence of the virus threat, and the growing dependencies of computer usage has led to the creation of the Computer Misuse Act. Implementation of this Act in similar forms varies from country to country, with more widespread enactment annually. Among other topics, the act covers the following:

- Unauthorized access to computer programs or data.
- Unauthorized access with intent to commit further offence.
- Unauthorized modification of the contents of any computer, with intent to impair operation or hinder or impair reliability [4].


Advisory policies are security policies that are strongly suggested but not mandatory. However, there may be defined consequences for failure to follow them. Most entities will want their personnel to consider these policies mandatory. This is a broad category where most policies will fall.

Informative policies exist to inform the reader. These policies contain no specified requirements and are general enough to be distributed to external customers or vendors without compromising confidentiality.

Networked Systems Survivability

Policy Elements

- Standards**
 - Use of specific technologies
- Guidelines**
 - Methodologies of securing systems
- Procedures**
 - Detailed steps to follow



© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 7

Policies are considered the first and highest level of documentation and are distinct from standards, guidelines and procedures. Standards, guidelines, and procedures are the next level down from policies, and are the elements that contain the details of the policy. These details include how the policies should be implemented and what standards and procedures should be used. Generally, policies should be broad enough so that the underlying standards guidelines and procedures can be changed without having to change the overall policy.

These three elements of a policy are separate yet related documents. Many companies create one document that satisfies all of these. However, it is important to keep them separate. Having the elements separate from the policy makes physical distribution easier. Each element serves a different function and is tailored for different audiences. This modular approach makes updating the policy much easier because each element is kept separate.

A *standard* is typically a collection of system-specific or procedural-specific requirements that must be met by everyone [5]. They are used to state the use of technologies in a uniform way. Specifying uniform methodologies for security controls through standards is beneficial for an organization. Standards are usually required for consistency. Here is an example of a standard: “all systems will be Windows 2000 professional or higher and shall be configured to connect to the organizational domain.”

Guidelines are a collection of system or procedural recommendations for best practice. They are not requirements to be met, but are strongly recommended. Guidelines are much more accommodating, taking into account and adjusting for the varying nature of information systems. Guidelines may be used to indicate how standards are developed. Effective security policies make frequent references to standards and guidelines that exist within an organization. An example guideline might be: “To avoid losing data, personnel should save their important files out to their network share at regular intervals.”

Some policies, such as password policies, may contain both standards and guidelines. The guidelines they detail are not suggested as many guidelines are; they are mandatory and carry consequences for failure to follow. An example policy which contains both standards and guidelines can be found at:

http://www.sans.org/newlook/resources/policies/Password_Policy.pdf

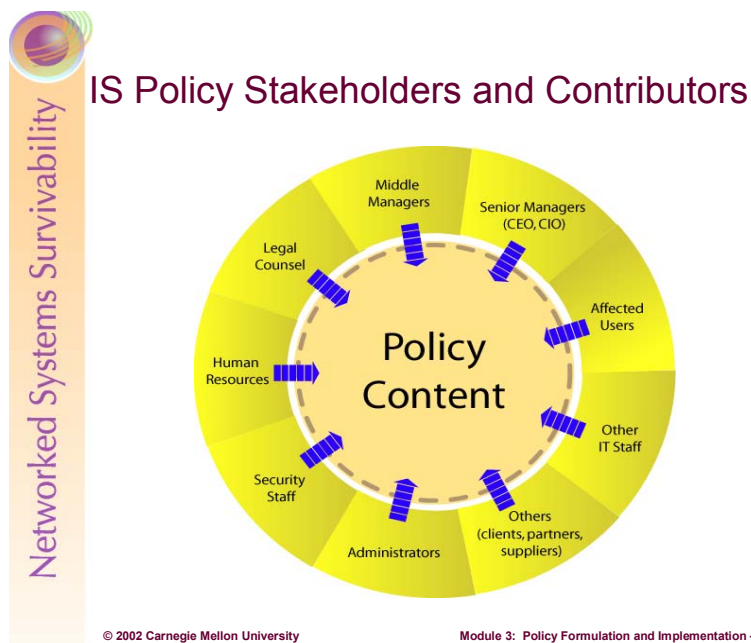
Procedures embody the detailed steps that are followed to perform a specific task [1]. These are usually very detailed actions that personnel are required to follow. The purpose of procedures, the lowest level in

Student Workbook – Module 3: Policy Formulation and Implementation

the policy chain, is to provide direction for applying the previously created policies, standards, and guidelines. Procedures include methods for proper handling of sensitive information, and instructions for what to do in the event of an information security incident.

Well documented procedures are critical to ensuring the survivability of an organization. Step-by-step instructions for routine tasks like system backups and restores, making changes to firewall access control rules, etc. should be followed and updated as appropriate. This also provides for continuity when faced with turnovers in IT personnel.

Baselines are used to ensure security is being implemented throughout the organization consistently. Standards are developed once a baseline is created and the security architecture of an organization is designed.



“As a general rule, policies are more successful if they are developed in cooperation with the people to whom they apply. **Users**, for example, are in the best position to evaluate how various policy statements might affect how they perform their work. Although **middle or senior managers** may be responsible for setting overall information security policies, they need to collaborate with **administrators, IT staff, security staff, and users** in order to define reasonable technological and procedural protection measures for information assets.

“When a new policy is first adopted in an established organization, not everyone will want to make the behavioral changes to comply with it. The responsible **executive** must be sure to explain the motivation for the policy. Peers, including those who participated in the development of the policy, can help accomplish this” [Allen 01].

The single most commonly expressed barrier to an effective information security program’s adoption (including security policies) is the absence of visible, active **senior executive** sponsorship. The role of senior managers is to actively sponsor and endorse security policies. They make the connection between policies and the organization’s mission and objectives. They generate awareness through words and actions, thereby reinforcing the importance of security policies. They assign organizational ownership and responsibility for critical assets.

“**Legal counsel** are responsible for ensuring that security policies

- are legally defensible and enforceable
- comply with organization-wide policies and procedures
- reflect known, generally-accepted business practices demonstrating the exercise of due care
- conform to federal, state, and local laws and regulations
- protect the organization from being held legally responsible in the event of compromise
- require the preservation of critical evidence including a defensible, documented, chain of custody for all artifacts that may be used in legal proceedings” [Allen 01]

The **Human Resources** Department is responsible for ensuring that user/employee rights are properly represented and reflected in security policies as well as ensuring HR’s ability to legally enforce and act upon the consequences for policy non-compliance.

Student Workbook – Module 3: Policy Formulation and Implementation

Middle managers have much the same role as senior managers but often at a more operational level. They need to ensure that their staff members understand and are acting in a manner consistent with security policies. An **IT middle manager** has a much larger role in policy formulation, ensuring that policy statements can be reasonably and effectively implemented.

Typically the security department has ongoing responsibility for creating and maintaining the organization's security policy including standards, guidelines, and procedures that derive from the policy. **Security staff** is responsible for ensuring that security requirements as expressed in policy can be carried out and are being carried out (through, for example, reviews and audits). For the purposes of this module, security staff also includes one or more CSIRTs (Computer Security Incident Response Teams), responsible for ensuring that actions required to detect and respond to a security incident are properly reflected in security policies.

Affected users advise on how security policies may affect their ability to do their work, helping to ensure the proper balance between required infrastructure operational capabilities and the need to operate securely.

Other IT staff (excluding administrators) are often involved in policy formulation and review based on the topic under consideration. If they have responsibility for a critical asset (such as a customer database) or are on the firing line responding to user questions and complaints (such as help desk staff), they need to have a voice in how policies are described and implemented, much the same as affected users.

Outside parties (such as vendors, contractors, partners, and suppliers) have a role to play in policy formulation in areas that describe third-party access to networks and data. Outside parties that can access your organization's networks need to demonstrate their ability to comply with your policies.

Administrators play the critical role of ensuring that policy language is clear and can be implemented at a reasonable cost. Administrators need to ensure that policy topics they require to do their jobs are included, and that they are comprehensive, complete, and accurate. One example is an administrator's authority to act in the event of a security incident (including different actions for different types of incidents) and where they need to obtain management concurrence before taking action, such as taking a system or network off line [Wood 01b].



Characteristics of an Effective IS Policy

- Traceable to the organization's mission and objectives; long-term focus
- Clearly defined scope and language; concise
- Involves stakeholders and affected parties
- Addresses what, not how
- Realistic – balances protection with productivity; enforceable
- Role-based
- Documented, up-to-date
- Visible and actively enforced; demonstrated senior management sponsorship
- Accompanied by awareness and training sessions

© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 9

Traceable, long-term focus: The relationship between an organization's mission and objectives and security policy should be clearly articulated and communicated. Policies should remain relevant and applicable for a substantial period of time, until objectives or requirements change.

Clearly defined scope: If this has not been done elsewhere, security policies should identify what critical information assets are to be protected and at what level. This includes what assets the policy affects and to whom and what parts of the organization it applies. Site-specific policies or tailored versions of organization-wide security policies may be required to meet the needs of a specific site. Policies need to be stated simply and in plain English.

Involves stakeholders, affected parties: The parties described in the previous slide are actively involved when and where they need to be.

Addresses what, no how: Policies should be stated at the level of principles, objectives, priorities, and strategies. Each policy statement should allow for a range of interpretations and implementations.

Realistic: Policies support accomplishing the organization's objectives. By the same token, they must be realistic, balancing the need for protection with the need for users to be productive without undue barriers, and able to be implemented, maintained, and enforced for a reasonable cost.

Role based: Security policies should clearly define roles, responsibilities, accountabilities, and authorities to act. Authority needs to be commensurate with responsibility and accountability. Roles to be covered may include members of boards of directors or other oversight committees, executive and senior managers, middle managers, legal counsel, security officers, human resources, IT managers, and representatives of administrator and key user groups. Policies articulate the role and companion responsibilities that each of these positions has in ensuring that the policy is followed. They describe the enforcement mechanisms that are used to ensure that these roles and responsibilities are carried out. Policies should describe key decisions and scenarios under which authority to act is granted to specific roles.

Documented, up-to-date: Security policies are written down, communicated, and disseminated. All employees understand that these are living documents to which they are held to account. There is a known, visible organizational process and point of contact for sending policy updates, improvements, and suggestions. Policies are periodically reissued and redistributed. New policy information is included in

Student Workbook – Module 3: Policy Formulation and Implementation

ongoing awareness and training sessions. Where appropriate, policy implementations are regularly tested and evaluated.

Visible and actively enforced: As stated earlier, senior managers actively sponsor and endorse security policies. They regularly make the connection between policies and the organization's mission and objectives. They generate awareness through words and actions, thereby reinforcing the importance of security policies. An example would be the inclusion of security policies as a regular topic at senior staff meetings and in program/project reviews.

Awareness and training: All users understand the part they are required to play in ensuring policy compliance. They understand and respect the consequences for non-compliance. To ensure user acceptance of any policies that require their compliance, you may consider requiring each user to sign a statement acknowledging that he or she understands the policy and agrees to follow it. The Human Resources department often administers this process.

Policies should include provisions for handling exceptions or waivers to the policy under well-described, well-bounded conditions.



The policy topics that your organization chooses to address depend on your mission, objectives, requirements, and needs. The topics indicated above are a candidate set, examples of which can be found in a number of sources.

A minimum set of topics suggested by Wood includes [Wood 01a]:

- responsibility for information security including involved personnel (and their roles) and involved systems
- user identification including password policy and protection
- release of information
- network connections, access (internal, external, Internet), and monitoring
- system access control privileges
- acceptable use (see later slide)
- information backup
- contingency planning
- physical security

Here are some excerpts from the Department of the Navy’s (DON) 1995 SECNAV INSTRUCTION 5239.3 under which USMC falls [Bowes 95]:

“Fundamental INFOSEC Policy:

- Data processed, stored, and transmitted by information system shall be adequately protected with respect to requirements for confidentiality, integrity, availability, and privacy
- All DON information systems shall be protected by the continuous employment of appropriate safeguards

Classified information processed or stored by DON information systems shall be safeguarded as required by that level of classification

Student Workbook – Module 3: Policy Formulation and Implementation

“Training:

- All individuals operating DON information systems will be afforded appropriate training and awareness information commensurate with their duties, responsibilities, and the level of information protection required

“Responsibilities:

- The Assistant Secretary of the Navy (ASN) for Research, Development, and Acquisition (RD&A) shall issue the appropriate DON policies and guidance, providing implementation details and procedures for the INFOSEC program
- The Commandant of the Marine Corps (CMC) shall ensure that Designated Approving Authorities (DAAs) are identified and security services provided for Marine Corps information systems
- All action addresses shall implement this guidance within their organizations. All developing and operating activities shall budget for, fund, and execute the actions necessary to comply with this instruction and the implementing documents that support it.”

As another example from the slide, communications policy describes guidelines for establishing communication contacts, channels, and mechanisms, particularly when dealing with a security incident. This includes communication up and down the chain of command, and when, if ever, it is appropriate to bypass levels in the chain (vertical communication); notification of managers and peers at the same level (horizontal communication); the involvement of public relations for interfacing with the press and public; communication with Internet service providers, help desk personnel, legal counsel, investigations groups, law enforcement agencies, and users. Mechanisms may include verbal conversations (phone, face-to-face), email, pagers, and other forms of written correspondence such as fax, meetings, whether these occur onsite or offsite, and whether they require secure means of communication using various forms of encryption, scrambling, or jamming. This description may need to include communication scenarios to help better describe how channels and mechanisms may be used.

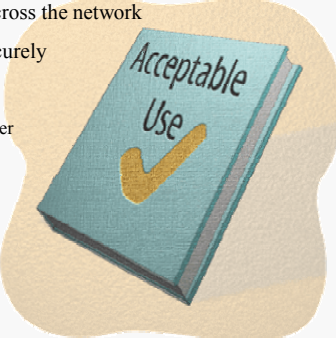
For further information, refer to:

- [Wood 01a]. Additional topics in this reference include Web pages, firewalls, employee surveillance, electronic commerce, digital signatures, computer viruses, encryption, contingency planning, logging controls, Internet, intranets, privacy, outsourcing security functions, CSIRT teams, microcomputers, local area networks, password selection, electronic mail, data classification, telecommuting, telephone systems, portable computers, and user training
- [van der Walt 01] “Introduction to Security Policies,” a Security Focus article in four parts
- [Allen 01], specifically all practice Policy Considerations sections and Appendix B

Networked Systems Survivability

Acceptable Use Policy Topics

- Compliance with your password policy
- Hardware changes a user may or may not make
 - Modem restrictions and use
- Software a user may or may not install or remove
- Information a user may or may not transmit across the network
- User responsibilities to operate a computer securely
 - Virus scanning and eradication
 - Restrictions on opening email attachments
 - Shutting down or locking an unattended computer
- Prohibitions against
 - Sharing of accounts
 - Breaking into accounts and systems
 - Cracking passwords
 - Disruption of service
 - Conduct of personal business



© 2002 Carnegie Mellon University Module 3: Policy Formulation and Implementation – slide 11

The purpose of an acceptable use policy is to identify and encourage user behavior that can enhance security and discourage or prohibit user behavior that can reduce or breach security. Users need to know the information assets that require protection and their responsibilities with respect to that protection. The security of many computing assets (desktops, laptops, peripherals, personal digital assistants, etc.) and their access to an organization's infrastructure are ultimately the responsibility of users. If users don't understand their security responsibilities and the organization's expectations, the technological measures used to enforce security policies will likely be ineffective [Allen 01].

An acceptable use policy describes what a user is authorized to do and not do as a computer professional, and the conditions under which a user can act with authority.

In addition to the topics listed above, additional acceptable use topics include:

- special considerations for laptop and home computer use including mechanisms for remote access
- physical theft, sabotage, or intentional destruction of computing equipment
- enabling and use of active program scripting/mobile code (ActiveX, Java, JavaScript, VBS)
- prohibiting the use of company computing resources for illegal or illicit communications or activities (porn surfing, email harassment) [Briney 01]

Refer to [Allen 01], specifically Policy Considerations Sections 2.7.4, 2.8.7, and Section 2.15 Develop and Roll Out an Acceptable Use Policy for Workstations (UW).

Refer to [Wood 01a], specifically Section 1.1.1.1.1, Password and User ID Construction; Section 1.2.1, Computer Viruses and Worms; Section 1.3.3.4, Data Classification System Implementation; Section VI, Sample Telecommuting & Mobile Computer Security Policy; Section IX, Sample Electronic Mail Security Policy; and Section XI, Sample Internet Security Policy.



Policy Topics for Privileged (Administrative) Users

- Authority and conditions for monitoring user activities (e.g., reading user email)
- Accessing protected programs or files
- Disrupting or terminating service under specific conditions
- Adding and changing users, user groups, user privileges, and authentication mechanisms
- Authority and conditions for using vulnerability testing, penetration testing, and password cracking tools
- Enforcing acceptable use policy provisions and prohibitions

Administrators typically have an increased level of privilege (access, enforcement) over normal users. With this increased level of access comes greater responsibility, accountability, and authority. These rights and privileges need to be articulated in security policy language specifically directed to administrators. This policy should be carefully drafted and reviewed by administrators to ensure that it fully describes the rights and protections they require to perform their job responsibilities.

IS Policy Knowledge

Any user (all levels, all privileges) should be able to answer the following questions:

- Where are your organization's IS policies defined?
- Who is involved in establishing IS policy?
- Who is responsible for monitoring IS policy compliance?
- To whom is the IS policy disseminated? How? How is receipt acknowledged?
- How often is the IS policy updated? How are updates disseminated and acknowledged?
- To whom do you submit suggested IS policy changes?



Can you answer these for your organization?

© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 13

To emphasize the current state of security policy knowledge, we restate the summary findings from the survey described at the beginning of this module:

“A recent survey of 600 IT professionals by the CIO Security Worksheet showed that

- nearly two-thirds of the respondents (66%) said that their organizations did not have defined security policies
- less than one-third (32%) said that employees are required to review and be familiar with the organization's security policies/guidelines
- only 23% indicated that their employees receive training or information sessions on security.”
- <<http://www.humanfirewall.org/rhfwm.htm>>

For security policy to be part of an organization's way of doing business, senior managers, middle managers, security trainers, security staff, and administrators must periodically ask all users (and themselves) these questions and receive satisfactory and correct responses. Indications of lack of awareness and knowledge serve as a signal for improvements in the security training program.

Importance of Planning for Policy Implementation

To meet policy requirements, security must be designed in from the beginning.

But policy statements cannot be directly implemented.

- A more detailed description is required
- Implementations are likely derived from standards, guidelines, procedures, best practices, and administrator experience

In the absence of a policy implementation plan that is reflected in infrastructure design and operations, the following situations occur:

- The organization and its information assets are vulnerable
- Only band-aid, point solutions are available
- Administrators continually make adhoc decisions, play catch-up

Security is a requirement of infrastructure design, not an “after the fact” add-on. Security policies cannot be directly implemented; they are typically too high level. Policy requirements, reflected in design decisions, are made real in an operational infrastructure through subsequent detailed design activities, development, and technology selection and implementation. There is a logical progression of actions to take where a plan can assist an administrator in ordering and prioritizing such actions.

Without a plan, policy implementers run the risk of deploying a piecemeal solution that only addresses specific needs, not the overall security “architecture” required to effectively meet policy requirements. Keep in mind the adage “security is only as strong as its weakest link.” Having only comprehensive perimeter protection in place by deploying properly configured firewalls and intrusion detection systems has historical precedent with the Maginot Line in World War II. Localized security technologies produce a “fingers in the dike” solution and often result in crisis management and a high degree of vulnerability. The absence of a plan perpetuates erroneous silver bullet thinking (the latest, hot security technology will protect our infrastructure from today’s threats), wastes precious resources, and undermines an administrator’s ability to make the case for improvement when the latest technology fails to protect in the face of a new attack.

Review Questions

1. What is the role of risk management in the formulation of IS policy?
2. Who needs to participate in policy formulation? enforcement?
3. What are three characteristics of an effective IS policy?
4. What topics might you expect to see covered in a general security policy? in an acceptable use policy?
5. What questions should users be able to answer about their organization's IS policy? Can you answer these questions about yours?
6. What is an example of an administrator action in each category?
7. What is an administrator's role in IS policy formulation and enforcement?

© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 15

1. What is the role of risk management in the formulation of IS policy?

Performing risk management adds clarity and detailed guidance for information asset protection. Risk assessment is used to identify critical assets, identify threats to those assets, and formulate asset protection strategies based on identified risks. Protecting critical information assets is one of the primary purposes of IS policy.

2. Who needs to participate in policy formulation? enforcement?

Senior managers (CEO, CIO), middle managers including the IT manager, legal counsel, human resources, security staff, administrators and other IT staff, affected users, affected third parties (contractors, vendors, suppliers, partners)

3. What are three characteristics of an effective IS policy?

- Realistic – balances protection with productivity
- Visible and actively enforced with demonstrated senior management sponsorship
- Accompanied by regular awareness and training sessions

4. What topics might you expect to see covered in a general security policy?

- Staff roles and responsibilities including involved systems
- Password policy and protection
- Network connectivity and access (internal, external, Internet), and monitoring
- System access control privileges including special administrator privileges
- Information backup
- Contingency planning and disaster recovery
- Physical security

in an acceptable use policy?

- Compliance with the organization's password policy
- Hardware changes a user may or may not make including modem restrictions and use

Student Workbook – Module 3: Policy Formulation and Implementation

- Software a user may or may not install or remove
 - Information a user may or may not transmit across the network
 - User responsibilities to operate a computer securely including virus scanning and eradication
 - Prohibitions against sharing accounts and conducting personal business
5. What questions should users be able to answer about their organization's IS policy? Can you answer these questions about yours?
- Where are your organization's IS policies defined?
 - Who is involved in establishing IS policy?
 - Who is responsible for monitoring IS policy compliance?
 - How do you acknowledge you have received and read your IS policies and all applicable updates?
6. What is an example of an administrator action in each category?
- Data security – apply access control lists to objects
 - Host security – use a minimum essential configuration
 - (Internal) Network security – enable secure remote administration of services and infrastructure
 - Internet security – patch and update Internet and public services
 - Intrusion detection and response – inspect system and network logs for unexpected behavior
7. What is an administrator's role in IS policy formulation and enforcement?
- Content contributor for procedures, processes, and tools
 - Enforcer in areas of responsibility
 - Trainer

Summary

Information security policies

- Participants, characteristics, and topics

Role of administrators

© 2002 Carnegie Mellon University

Module 3: Policy Formulation and Implementation – slide 16

References

[Allen 01] Allen, Julia. *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley, 2001.

[Bowes 95] Bowes, W.C. “Department of the Navy Information Systems Security (INFOSEC) Program” memorandum. SECNAV INSTRUCTION 5239.3. Secretary of the Navy, 14 July 1995.

[Briney 01] Briney, Andy. “2001 Industry Survey.” *Information Security Magazine*. October, 2001. Available at <http://www.infosecmag.com/articles/october01/images/survey.pdf>.

[Guttman 97] Guttman, B. & Bagwill, R. *Internet Security Policy: A Technical Guide -Draft*. Gaithersburg, MD: NIST Special Publication 800-XX. Available at <http://csrc.nist.gov/isptg/html/> (1997).

[IETF 97] Internet Engineering Task Force Network Working Group. Edited by Barbara Fraser. *RFC 2196 Site Security Handbook*. Available at <ftp://ftp.isi.edu/in-notes/rfc2196.txt> (1997).

[McBride 02] McBride, Patrick, et al. *Secure Internet Practices: Best Practices for Securing System in the Internet and e-Business Age*. Boca Raton, FL: Auerbach, 2002.

[Palmer 01] Palmer, Malcolm, et al. “Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age.” *Information Systems Security*. Auerbach Publication, May/June 2001.

[van der Walt 01] van der Walt, Charl. “Introduction to Security Policies” *Security Focus*, 2001. Available in four parts:

Part One: An Overview of Policies at <http://www.securityfocus.com/cgi-bin/infocus.pl?id=1193>

Part Two: Creating a Supportive Environment at <http://www.securityfocus.com/cgi-bin/infocus.pl?id=1473>

Part Three: Structuring Security Policies at <http://www.securityfocus.com/cgi-bin/infocus.pl?id=1487>

Part Four: A Sample Policy at <http://www.securityfocus.com/cgi-bin/infocus.pl?id=1497>

[Ware 01] Ware, Lorraine Cosgrove. “CIO Research Reports: CIO Security Worksheet.” *CIO.com*. August 12, 2001. Available at <http://www2.cio.com/research/surveyreport.cfm?id=21>.

[Wood 01a] Wood, Charles Cresson. *Information Security Policies Made Easy Version 8*. Pentasafe Security Technologies, Inc., 2001. Ordering information available at <http://www.pentasafe.com>.

[Wood 01b] Wood, Charles Cresson. *Information Security Roles and Responsibilities Made Easy*. Pentasafe Security Technologies, Inc., 2001. Ordering information available at <http://www.pentasafe.com>.

Student Workbook – Module 3: Policy Formulation and Implementation

References:

- [1] *The CISSP Prep Guide*, Krutz, R, Vines, R., Wiley 2001
- [2] *Outsourcing Managed Security Services*, Allen, J., Gabbard, D., May, C, 2002
- [3] <http://www.scmagazine.com/scmagazine/november/cover/cover.html>
- [4] <http://rr.sans.org/legal/regulatory.php>
- [5] <http://www.sans.org/newlook/resources/policies/#name>
- [6] *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, Ron Ross and Marianne Swanson, NIST Special Publication 800-37
- [7] Collaborative Security Strategies in an Outsourced, Cross-Agency Web System Roopangi Kadakia October 15, 2001
- [8] *Computer Security Basics*, Russell, D. and Gangemi, G.T, O’Rielly 1991