Lecture Notes

On

Cyber Security

University Academy
Teaching | Training | Informative

By

Mr. Sandeep Vishwakarma

Assistant Professor

Dr. A.P.J. Abdul Kalam

Technical University,Lucknow

UNIT – 4

Security Policy

Security policy is the statement of responsible decision makers about the protection mechanism of a company crucial physical and information assets. Overall, it is a document that describes a company's security controls and activities. Security policy does not specify a technological solution, instead, specifies sets of intentions and conditions that will aid to protect assets along with its proficiency to organize business.

Policy Makers

Security policy development is a joint or collective operation of all entity of an organization that is affected by its rules. In general, security policies should not be developed by IT team itself as it is a responsibility of everyone that has a stake in the security policy should be involved in its development so that they could too, mold the policy according to their requirement. During policy creating following entity typically involves;

1. **Board:** Company board members must render their advice to some form of a review of policies in response to exceptional or abnormal running condition of business.
2. **IT Team:** IT team members usually are the biggest consumers of the policy information in any company, as it involves making standard around the usage of the computer system, especially security controls.
3. **Legal Team:** This team ensure the legal points in the document and guide a particular point of appropriateness in the company.
4. **HR Team:** HR team typically obtain a certified T&C certificate from each employee that they have read and understood the stipulated policy, as the HR team deals with reward and punishment related issues of employees to implement discipline.

An IT security policy should:

1. Protect people and information
2. Set the rules for expected behavior by users, system administrators, management, and security personnel
3. Authorize security personnel to monitor, probe, and investigate
4. Define and authorize the consequences of violations
5. Help minimize risk
6. Help track compliance with regulations and legislation
7. Ensure the confidentiality, integrity and availability of their data
8. Provide a framework within which employees can work, are a reference for best practices, and are used to ensure users comply with legal requirements

Development of Security Policy:

A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.

Planning for Security -

- Creation of information security program begins with creation and/or review of organization's information security policies, standards, and practices
- Then, selection or creation of information security architecture and the development and use of a detailed information security blueprint creates plan for future success
- Security education and training to successfully implement policies and ensure secure environment

Definitions

- **Policy**: course of action used by an organization to convey instructions from management to those who perform duties
    - Organizational rules for acceptable/unacceptable behavior
    - Penalties for violations
    - Appeals process
- **Standards**: more detailed statements of what must be done to comply with policy
- **Practices, procedures and guidelines** effectively explain how to comply with policy

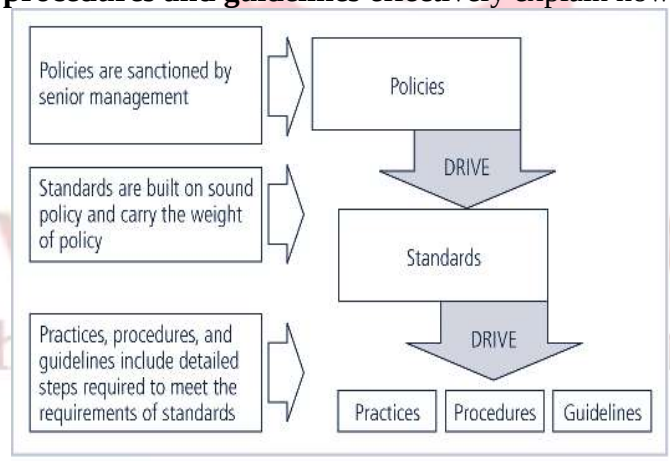

FIGURE 5-1 Policies, Standards, and Practices

Why Policy?

- A quality information security program begins and ends with policy
- Policies are least expensive means of control and often the most difficult to implement
- Some basic rules must be followed when shaping a policy:
    - Never conflict with law
    - Stand up in court
    - Properly supported and administered
    - Contribute to the success of the organization

- Involve end users of information systems

The principles here are based upon the following goals:

- Ensure the availability of data and processing resources.
- Provide assurance for the confidentiality and integrity of customer data and allow for the compartmentalization of risk for customers and your organization.
- Ensure the integrity of data processing operations and protect them from unauthorized use.
- Ensure the confidentiality of the customer's and your processed data, and prevent unauthorized disclosure or use.
- Ensure the integrity of the customer's and your processed data, and prevent the unauthorized and undetected modification, substitution, insertion, and deletion of that data.

Security Policy Fundamentals

This section provides basic information on the purpose, goal, definition, and implementation of a security policy.

Purposes of a Security Policy: The primary purpose of a security policy is to inform users, staff, and managers of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets. The policy should specify the mechanisms through which these requirements can be met.

Security Policy Goals: The goal of the security policy is to translate, clarify and communicate management's position on security as defined in high-level security principles. The security policies act as a bridge between these management objectives and specific security requirements.

Definition of a Security Policy: A security policy is a formal statement of the rules through which people are given access to an organization's technology, system and information assets. The security policy defines what business and security goals and objectives management desires, but not how these solutions are engineered and implemented.

The characteristics of good security policies are:

- They must be **implementable** through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods.
- They must clearly define the areas of **responsibility** for the users, administrators, and management.
- They must be **documented**, **distributed**, and **communicated**.

Policy Flexibility: A successful security policy must be flexible. In order for a security policy to be viable for the long term, a security policy should be independent of specific hardware and software decisions, as specific systems choices change rapidly. In addition, the mechanisms for updating the policy should be clearly spelled out. This includes the process, the people involved, and the people who must sign-off on the changes.

Security Policy Communication: Once security policies have been established, they must be disseminated to all appropriate users, staff, management, vendors, third party processors, and

support personnel. Given the nature of your enterprise, it may also be necessary to communicate some or all policies to customers as well.

Policy Management: To ensure that your policies do not become obsolete, you should implement a regular review process of them. That process should include some form of update

mechanism so that changes in your organization's operating environment can be quickly translated into your security policy.

Roles and Responsibilities: The development of security policies is predicated upon the participation of various organizations. In general, it is recommended that the following areas participate in this development effort:

- Business management
- Technical management
- Data security
- Risk management
- Systems operations
- Application development
- Network engineering
- Systems administration
- Internal audit
- Legal
- Human resources

Security Policy Structure: The basic structure of a security policy should contain the following components:

- A statement of the issue that policy addresses.
- A statement about your position on the policy.
- How the policy applies in the environment.
- The roles and responsibilities of those affected by the policy.
- What level of compliance to the policy is necessary?
- What actions, activities and processes are allowed and which are not.
- What are the consequences of non-compliance?

WWW Policy:

A cyber security policy outlines the assets you need to protect, the threats to those assets and the rules and controls for protecting them and your business. The policy should inform your

employees and approved users of their responsibilities to protect the technology and information assets of your business. Some of the issues the policy should cover are:

- the type of business information that can be shared and where
- acceptable use of devices and online materials
- Handling and storage of sensitive material.

The World Wide Web is a system for exchanging information over the Internet. The Web is constructed from specially written programs called *Web servers* that make information available on the network. Other programs, called *Web browsers*, can be used to access the information that is stored in the servers and to display it on the user's screen.

It also poses profound security challenges. In order of importance, these challenges are:

1. An attacker may take advantage of bugs in your Web server or in CGI scripts to gain unauthorized access to other files on your system, or even to seize control of the entire computer.
2. Confidential information that is on your Web server may be distributed to unauthorized individuals.
3. Confidential information transmitted between the Web server and the browser can be intercepted.
4. Bugs in your Web browser (or features you are not aware of) may allow confidential info on your Web client to be obtained from a rogue Web server.
5. Because of the existence of standards and patented technologies, many organizations have found it necessary to purchase specially licensed software. This licensed software, in turn, can create its own unique vulnerabilities.

Email Security

Email security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.

An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.

Email security is a broad term that encompasses multiple techniques used to secure an email service. From an individual/end user standpoint, proactive email security measures include:

- Strong passwords
- Password rotations
- Spam filters
- Desktop-based anti-virus/anti-spam applications

Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address. It also implements firewall and

software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.

Security Services over Email:

Privacy: No one should read message except recipient
Authentication: Recipient should know exactly who the sender is **Integrity**: Recipient should be able to tell whether message was altered in transit

Non-repudiation: Recipient can prove that the sender really sent **it Proof of submission**: Verification to the sender that the mailer got **it Proof of delivery**: Verification to sender that the recipient got it **Message flow confidentiality**: Eavesdropper cannot determine the sender's ID **Anonymity**: Ability to send so recipient does not know sender **Containment**: Ability to keep secure messages from "leaking" out of a region **Audit**: Logging of events having relevance to security **Accounting**: Maintain usage statistics (might charge for service) **Message sequence integrity**: Sequence of messages have arrived in order, without loss

Email Security PGP (Pretty good Privacy)

- Combines best features of secret and public key cryptography.Compresses plaintext befor-e encryption.
- Compression saves transmission time and disk space and strengthens cryptography: thwarts cryptanalysis techniques which exploit patterns found in plaintext to crack the cipher.
- Creates session key: random, onetime number, and encrypts.
- Encrypts session key with recipient's public key.
- Encrypted session key and message are sent to recipient.
- Recipient applies private key to encrypted session key.
- Recipient uses session key to decrypt message, then decompresses.

Policy Review- Process

The Policy Owner is responsible for conducting a comprehensive review of their policies. The purpose of the review is to determine:

1. If the policy is still necessary and accurate;
2. If the policy should be combined with another policy or if it should be rescinded;
3. If the policy is up to date with current laws and regulations and Regents policies;
4. If changes are required to improve the effectiveness or clarity of the policy;

Policy Review Steps:

- Policies for review are identified by the policy owner.

- The policy owner examines their policies and procedures, considering comments captured through the comment boxes on the policy and related documents (available under the maintenance tab) as well as feedback obtained through their other mechanisms, such as meetings, comments from the Diversity Community of Practice, and help line.
- The policy is revised as needed, using track changes.
- The management does a preliminary review of the form and policy, and provides suggestions. The Director forwards the revised policy and form to the committee members for review.

Effective security policies are the foundation for an effective security program, as it helps to clarify the security goals of an organization in relation to its business processes, technical mechanisms and personnel behavior. A good security policy can help to ensure that systems are utilized in the intended manner; and control legal liability.

a) Corporate Policies:

Usually, a documented set of broad guidelines, formulated after an analysis of all internal and external factors that can affect a firm's objectives, operations, and plans. Formulated by the firm's board of directors, corporate policy lays down the firm's response to known and knowable situations and circumstances. It also determines the formulation and implementation of strategy, and directs and restricts the plans, decisions, and actions of the firm's officers in achievement of its objectives. Also called company policy.

The corporate policies develop the principles set in the company's corporate governance system & contain the guidelines that govern the action as well as of their directors, officers & professionals. The links that provides access to the full text or a summary of the corporate policies are corporate governance & regulatory compliance policies, risk policies, social responsibility policies.

A corporation's security policy indicates that confidential information should be properly protected. Guidelines are recommended actions & operational guides to users, IT staff, operations staffs and others when a specific standard does not apply. Whereas standards are specific mandatory rules, guidelines are general approaches that provide the necessary flexibility for unforeseen circumstances.

Procedures are detailed step by step tasks that should be performed to achieve a certain goal. The step can apply to users, IT staff, operations staff, security members & others who may need to carry out specific tasks. Procedures are considered the lowest level in the policy chain because they are closest to the computers and users provides detailed steps for configuration and installation issues. Procedures tell how the policy standards & guidelines will actually be implemented in an operating environment.

b) Sample security policy:

A security policy is the essential basis on which an effective & comprehensive security program can be developed. This critical component is the primary way in which the agency security plan is translated into specific, measurable and testable goals & objectives.

The security policies must establish a consistent notion of what is and what is not permitted with respect to control of access to your information resources. They must bond with the business, technical, legal, & regulatory environment of your agency.

To implement security education, training and awareness programs is needed. These are control measures designed to reduce accidental security breaches by employees. Security education and training builds on the general knowledge the employees must possess to do their jobs familiarizing them with the way to do their jobs security.

c) Publishing & Notification Policy:

Publishing & notification security policy is a commonly used pattern for inter-object communication. Eg. Publish systems provided by message oriented software vendors or in system and device management domains. This notification pattern is increasingly begin used in a web services context.

Notification may have specifications that define a standard web services approach to notification using a topic based publish pattern. It can be standard message exchanges to be implemented by service providers that wish to participate in point to point notification, standard message exchange for a notification service provider allowing publication of messages from entities that are not themselves service providers, operational requirements expected of service providers and requestors that participate in notification. The notification documents may include publish-subscribe notification for web services.

Evolving Technology Security

Technology is evolving at a rapid pace, and so is the rate at which cyber crimes are committed. Cybercriminals keep finding new ways to hack, even as technologists scramble to fix the previous loses. Such is the importance of cyber security in this digital age that it has learned to evolve with technology, albeit the hard way. Luckily, as technology advances so is the ability to predict cyber-attacks and weed out cyber security threats. Here is a list of 5 technologies that have changed cyber security.

Corporate Security Breaches

There is a common saying in ethical hacking- "It only takes an employee to open one phishing ***email*** to bring the whole corporate security down". It is not a shocker, therefore, when we say that most of the corporate security breaches are a result of hackers exploiting employees through *social engineering* and scams. Hackers are becoming only more and more adept at finding breaches and backdoors in corporate security systems, more so with the advancement of digital technology, leaving no data to be really secure.

Identity Fraud

Social media has evolved so much and has made itself a part and parcel of people's everyday lives that the security concerns revolving around it have gone into the shadows. In fact, they are the biggest threat to online security, what with the sheer amount of information an average user shares online.

It has become the breeding ground for Cybercriminals, who are increasingly using this data to engage in identity theft schemes, stealing personal email accounts, work email accounts and banking information.

Mobile security

As new ***mobile*** technology emerges every day, so are mobile cyber security threats. Again, it is a case of hacking personal data. At the pace in which mobile technology and usage are growing, there is little chance that cyber security could keep up. Hence, for every new phone, tablet or smart device a person buys, more is the opportunity for a cyber-criminal to hack into. As mobile devices can universally plug into any port for sharing, malware issues are just multiplying.

Cloud storage

Digital storage of data is common these days. So more and more companies are shifting to ***cloud computing*** to increase efficiency and lower costs involved with maintenance. While this method is a relatively low risk, as individual organizations can skip the complexities of designing their own cyber security systems, the onus is on service providers to install certain sophisticated security measures to protect data on the cloud. Anything on a network is hackable!

Secure configuration management (SCM)

Assures systems are set up and maintained so as to minimize risk while still supporting the essential business functions of the system. In small organizations, SCM can seem simple, but it's quite complicated for enterprises that operate larger, more complex technology environments consisting of numerous systems, asset owners, and applications, all of which have differing configuration states and business requirements. For this reason, enterprises should consider investing in technology that automates the assessment, monitoring, and management of configurations across all systems.

Outsourcing:

An increasing number of organizations are outsourcing security to reduce costs and raise security standards. Businesses have various options for outsourcing security – including opting for managed and hosted services. These are ideal for organizations without the necessary tools, resources and budgets to tackle these issues in-house. A common way to outsource is to use a managed security service provider (MSSP) that can provide a range of services including enterprise grade content filtering, VPNs and data backup. We look at the best practices for outsourcing security and the steps on where to begin.