Security Policy Roadmap - Process for Creating Security Policies

Information is an important business asset and is valuable to an organization. Thus, it needs to be protected to ensure its confidentiality, integrity and availability. The very first thing in information security is to set up policies and procedures on how to protect information. This paper presents a systematic approach in developing computer security policies and procedures. All the processes in the Policy Life Cycle will be discussed. In particular, it will list all the issues and factors that must be considered wh...

Security Policy Roadmap – Process for Creating Security Policies
Chaiw Kok Kee
Version 1

Abstract

Information is an important business asset and is valuable to an organization. Thus, it needs to be protected to ensure its confidentiality, integrity and availability. The very first thing in information security is to set up policies and procedures on how to protect information. This paper presents a systematic approach in developing computer security policies and procedures. All the processes in the Policy Life Cycle will be discussed. In particular, it will list all the issues and factors that must be considered when setting up the policies. It makes some recommendations and suggestions on relevant areas and produces a framework for setting security policies and procedures.

Identifying safeguards and controls that protects information from security threats can be time-consuming that needs a lot attention and planning. As a result, the ISO 17799 is used as a security checklist to help in developing the policies and measuring its compliancy. This policy will then reflect the business and technical needs of the multiple business units and users within the organization.

1. Introduction

Organizations face security threats from a wide range of sources and are vulnerable to attacks such as computer viruses, hacking and denial of service attacks. Information security by technical means is not sufficient and needs to be supported by policies and procedures.

Security policies are the foundation and the bottom line of information security in an organization. A well written and implemented policy contains sufficient information on what must be done to protect information and people in the organization. Security policies also establish computer usage guidelines for staff in the course of their job duties.

System administrators and business owners have to acknowledge the fact that security threats exist and how to prevent and respond to them. Identifying and implementing suitable controls requires careful planning and participation of all employees in the organization is also vital for the success of information security management. Therefore, depending on the company's size, financial resources, and the degree of threat, we have to set up a security policy that finds the right balance between the overreacting and the vulnerable of exposing your system to any and every hack. The objective of a well written and implemented security policy is improved information availability, integrity and confidentiality, from both inside and outside the organization.

One approach to setting security policies and procedures is suggested by the following steps:

- Identify all the assets that we are trying to protect.
- Identify all the vulnerabilities and threats and the likeliness of the threats happening.
- Decide which measures which will protect the assets in a cost-effective manner.
- Communicate findings and results to the appropriate parties.
- Monitoring and review the process continuously for improvement.

2. ISO 17799

ISO 17799 provides a comprehensive set of guidelines and controls comprising best practices in information security whereby it can be used as a basis to develop security policy. The ISO 17799 defines 127 security controls which are grouped into 10 sections can be used as a security checklist to assist us in defining our policy. However, not all of the controls defined will be relevant to the organization.

As part of the preparation process, a questionnaire consisting of all relevant security controls defined in ISO 17799 is created. The checklist must be designed according listing all the recommended best practices from ISO 17799 and at the same time gathering data whether it is being implemented in the organization, who is the process owner and how it is being done. A good questionnaire should have the 5Ws and 1H – What? Who? Where? When? Why? and How?

This questionnaire will be use to understand the organization's security posture and to suggest areas where policy is needed.

3. Security Policy Pre-Work

To develop an enterprise-wide security policy, we need a thorough understanding of the organization. We have to consider the goals and direction of the organization. The policy that we are going to develop must also conform to existing policies, rules, regulations and laws that the organization is subject to.

Firstly, we need to appoint a person with enough status to own and implement the policy. This is to appoint an Information Security Officer who may be a full time specialist or existing person given this responsibility. Getting the right set of people involved from the beginning is critical to the success of the project and acceptance of the policy. It is a joint effort by the technical personnel, process owner and decision makers who have the authority to enforce the policy. The right level of authority on policy decision is required to ensure that the policy is well written and supported as it affects all employees in the organization.

4. Information Gathering

We will start will identify all the assets that we are trying to protect and its likely threats and vulnerabilities. This includes getting business owners to answer the ISO 17799 questionnaire, analysis of the questionnaire and conducting interviews with process owners.

4.1. Identify Assets

Start by identifying all critical business processes in the organization. The ISO 17799 checklist also provides a list of business processes that needs to be considered. Once we have identified all the business processes, create a list of assets used by those critical processes. These include physical assets, such as servers, routers and information on network services, remote access locations, what information travels over the network, who, what and when data can be accessed etc. The asset list should be exhaustive and cover all key assets but manageable. Including everything make the entire process unwieldy and unlike to be completed.

Next, quantify their importance by placing a value on the assets. This will help us prioritize the items. It is vital to involve business process owner at this stage to give a more accurate data on the value of the processes and its assets.

Example of a list of assets and its associate value:

Webserver	$10,000
Database	$100,000
Mail server	$10,000

4.2. Identify Vulnerabilities and Threats

Carefully analyze all the processes to identify threats and vulnerabilities. Consider also the probability of any of the vulnerabilities being exploited. There are many tools available to analyze your systems for vulnerabilities producing a report of known vulnerabilities found on your system. Use this as your starting point and follow-up with a manual review of all the systems and applications.

Beside electronic risk, consider physical risks such as stealing magnetic tape too.

Example of a list of potential threats and its probability of happening:

Unauthorized user modifying the database	30%
Denial-of-service on the Web server	80%
Virus	90%

4.3. Evaluation of Measures and Controls

Look at each threat and brainstorm about potential safeguards and controls as well as their associated cost. Also note the risk reduction of the threat if the safeguard and control is implemented.

Example of a list of potential controls and their associated costs:

Threat	*Possible Controls*	*Cost*	*Risk reduction*
Unauthorized user modifying the database	Strong access controls	$25,000	80%
Denial-of-service on	Firewall	$10,000	60%

the Web server			
Virus	E-mail anti-virus	$5,000	70%
	Client anti-virus	$10,000	80%
	Strong policies on e-mail attachment	$500	60%

Next, analyze the list of control options for each threat taking into consideration the costs, risk reduction, probability of the threat happening and the value of the assets. Decide which control is best to implement for each threat, or may none at all (if it costs more to protect a threat that is unlikely to happen).

Finally, document the assessment process and results. Having a good documentation of the process and result will make the review process in the future easier.

5. Define Roles and Responsibilities

Different roles should be defined in your organization to group employees based on their job functions. These roles should include human resources, accounts, marketing, development, quality assurance, system support, contractors, etc. Each group requires different access privilege level to access resources to perform its job function.

You need to decide who can access to what and what specific privileges they need. You will also need to balance between protection and productivity.

6. Communicate Findings

Communicate the results to the appropriate parties highlighting the risks and vulnerabilities. The findings and recommendations must be communicated to management or business owner to ensure that the computer security policy created will implement measures that will protect the organization in the most cost-effective manner.

Recommended policy and procedures must be approved by decision makers and representatives from all the stakeholder groups such as employee union and legal. This is to ensure that the new policy conforms to the law and regulations.

7. Writing Policy

Policies and its supporting processes are developed based on the findings and accepted recommendations to reduce the risks posed by the threats. The first thing to remember when writing policy is to write them in an easy-to-understand language and do not make them too complicated. Our policies should also be written using the SMART rule. They must be **S**pecific, **M**easurable, **A**greeable, **R**ealistic and **T**ime-bound.

Writing a policy from scratch can be a daunting task. However, there are numerous Internet sites that provide excellent information about creating a policy document. Some may come with a policy template or example where you may tailor to your organization's need. The paper, "A System Security Policy for You", written by David Milford provides a good reference and suggested a format a Security Policy.

Another cost effective way is to procure a set of pre-written policies and then customize to our organization's needs. RUSecure's Information Security Policies is a comprehensive Security Policy template from Glendalesystems.com Ltd which can be downloaded and purchased from http://www.information-security-policies-and-standards.com/ is a good choice because of its compliancy with ISO 17799.

The RUSecure Information Security Policy covers the following issues and contains the following contents.

- **Securing Hardware, Peripherals And Other Equipment**
  - Purchasing and Installing Hardware
  - Cabling, UPS, Printers and Modems
  - Consumables
  - Working Off Premises or Using Outsourced Processing
  - Using Secure Storage
  - Documenting Hardware
  - Other Hardware Issues
- **Controlling Access To Information And Systems**
  - Controlling Access to Information and Systems
- **Processing Information And Documents**
  - Networks
  - System Operations and Administration
  - E-mail and the Worldwide Web
  - Telephones & Fax
  - Data Management
  - Backup, Recovery and Archiving
  - Document Handling
  - Securing Data
  - Other Information Handling and Processing
- **Purchasing And Maintaining Commercial Software**
  - Purchasing and Installing Software
  - Software Maintenance & Upgrade
  - Other Software Issues
- **Developing And Maintaining In-House Software**
  - Controlling Software Code
  - Software Development
  - Testing & Training
  - Documentation
  - Other Software Development
- **Combating Cyber Crime**
  - Combating Cyber Crime
- **Complying With Legal And Policy Requirements**
  - Complying with Legal Obligations
  - Complying with Policies
  - Avoiding Litigation
  - Other Legal Issues

- **Planning For Business Continuity**
    - Business Continuity Management (BCP)
- **Addressing Personnel Issues Relating To Security**
    - Contractual Documentation
    - Confidential Personnel Data
    - Personnel Information Security Responsibilities
    - HR Management
    - Staff Leaving Employment
    - HR Issues Other
- **Controlling E-Commerce Information Security**
    - E-Commerce Issues
- **Delivering Training And Staff Awareness**
    - Awareness
    - Training
- **Dealing With Premises Related Considerations**
    - Premises Security
    - Data Stores
    - Other Premises Issues
- **Detecting And Responding To IS Incidents**
    - Reporting Information Security Incidents
    - Investigating Information Security Incidents
    - Corrective Activity
    - Other Information Security Incident Issues
- **Classifying Information And Data**
    - Setting Classification Standards

Study the pre-written Security Policy and customize the policies to the recommended and approved policies excluding areas which are not relevant. The completed draft Security Policy must be reviewed by the appropriate parties such as executive, IT and Security management, human resources, legal staff and employee union. The draft should be amended to reflect the feedbacks and corrections and finally endorsed by management as part of the company's policy for all employees to follow.

8. Implementation

The endorsed final copy of Security Policy must be made easily available to all employees. It must be communicated to all users formally and users are to acknowledge that the policy is read and understood by signing and agree to comply with it.

The key to acceptance and compliance with security policies is education. Educating employees on the need for security and keeping them involved in the policy development process is important to keep them from finding ways to avoid policies and rendering them ineffective. Seminars and awareness campaigns help to educate the importance of security, especially on password selection, screen locking, document labeling, and physical (door) security.

The Security Policy must be incorporated into the company's Employee Handbook as a Code of Practice for all employees. It can also be published onto the company's intranet whereby it is available to all employees. Security tips can be printed on posters, e-mails, screensavers and mouse pads to remind employees of importance of security.

Finally, top management should set an example of how to follow the security policies.

9. Compliancy and Enforcement

We must develop a method to measure compliance with the policy. This may include the setting up of auditing team to ensure that the policy is enforced. The auditors who are responsible for monitoring compliance with the security policy should be independent of the persons implementing the policy. The best person to perform this task cost effectively is the internal auditors. The internal audit may audit employees on a regular basis to ensure that all employees understand and aware of the policies. Krishni Naidu's paper on "How to Check Compliance with your Security Policy" provides a good reference and procedures on how to design audit procedures.

Tools may be used to check computer and network log files. Various monitoring tools can be used to monitor the system and review log files for intrusion and proper usage by users.

The policies must be enforced in a strictly manner and noncompliance should be punished. Once a culprit is identified, the organization may choose to take disciplinary actions spelt out in the security policy.

10. Monitoring and Review

It is important to monitor and review the above process continuously for improvement as new threats are being discovered. This includes changes in the organization resulting in new threats. Controls have to be modified as necessary to minimize any new threat introduced.

As time goes by, it is crucial to maintain the relevancy of the security policies. New policies may be added when necessary. Obsolete policies must also be removed.

11. Conclusion

The basic goals of security are availability, confidentiality and integrity. We must determine what we need to protect, what threats we are protecting it from and how to protect it. In the process of identifying the risk, always remember to rank the risks by level of severity and priority. This will ensure that we make wise cost-effective decision and should not spend more to protect something than it is actually worth.

Once you have a security policy, follow through. Review the policy regularly to assess changing conditions, and ensure that the policy is updated to adapt to the change. Make the overall security policy the responsibility of one person with enough status in the company to enforce the rules. Don't hand this important job over to a junior member of the IT staff.

12. References

1. International Organization for Standardization, BS ISO/IEC 17799:2000 -- Information technology – Code of practice for information security management, 1st edition, 2000-12-01.

2. Dr. Hartley, Bruce V.. "You Need a Corporate Security Policy". Business Security Advisor magazine. June 1998. URL: http://www.advisor.com/Articles.nsf/aidp/HARTB03 (27 Sept. 2001).

3. Glendalesystems.com Ltd. RU Information Security Policies. Version 2.0. 2001. URL: http://www.information-security-policies-and-standards.com/ (24 July 2001).

4. Internet Security System (ISS). Creating, Implementing and Managing the Information Security Lifecycle – Security Policy, E-Business and You. URL: http://www.iss.net/customer_care/resource_center/whitepapers (25 Sept. 2001).

5. Milford, David. "A System Security Policy for You". 25 April 2001. URL: http://www.sans.org/infosecFAQ/policy/sys_sec.htm (7 Aug. 2001).

6. Sun. "How to Develop a Network Security Policy". An Overview of Internetworking Site Security. URL: http://www.sun.com/software/white-papers/wp-security-devsecpolicy (29 Sept. 2001).

7. Naidu, Krishni. "How to Check Compliance with your Security Policy". 30 Jan. 2001. URL: http://www.sans.org/infosecFAQ/policy/compliance.htm (7 Aug. 2001).

8. Andress, Mandy. Surviving Security: How to Integrate People, Process, and Technology. Sams Publishing. 2001. 30-73.

Last Updated: July 8th, 2011

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tokyo Summer 2011	**Tokyo, Japan**	**Jul 25, 2011 - Jul 30, 2011**	**Live Event**
SANS Boston 2011	**Boston, MA**	**Aug 06, 2011 - Aug 15, 2011**	**Live Event**
SANS Virginia Beach 2011	**Virginia Beach, VA**	**Aug 22, 2011 - Sep 02, 2011**	**Live Event**
SANS Ottawa 2011	**Ottawa, ON**	**Aug 28, 2011 - Sep 02, 2011**	**Live Event**
Security Architecture: Baking Security into Applications and Networks 2011	**Washington, DC**	**Aug 29, 2011 - Aug 30, 2011**	**Live Event**
SANS Melbourne 2011	**Melbourne, Australia**	**Sep 05, 2011 - Sep 10, 2011**	**Live Event**
SANS Delhi 2011	**Delhi, India**	**Sep 12, 2011 - Sep 17, 2011**	**Live Event**
SANS Network Security 2011	**Las Vegas, NV**	**Sep 17, 2011 - Sep 26, 2011**	**Live Event**
2011 European Digital Forensics and Incident Response Summit	**London, United Kingdom**	**Sep 21, 2011 - Sep 27, 2011**	**Live Event**
SANSFIRE 2011	**OnlineDC**	**Jul 15, 2011 - Jul 24, 2011**	**Live Event**
SANS OnDemand	**Books & MP3s Only**	**Anytime**	**Self Paced**