



Romel Cabiling ▾



Home

Home > My courses > 121 - ITSP2B > 04 Understanding Security Policies I > Lesson Proper for Week 4

Lesson Proper for Week 4

UNDERSTANDING SECURITY POLICIES

A security policy is used by the company's staff, IT users, and administrators, and so on. A security policy must be enforced on an organization's network so it helps them to protect the network from potential attack and threats.

The following should be considered before creating a security policy:

- A security policy can be formed to balance access and security, and to minimize risk
- A security policy created should not replace the thoughts of the user
- When a potential threat is identified, a security policy must be created in such a way that it can be changed

Also, the policies created should define the following:

- Aims of the policy
- Actions by the policy
- The device on which the policy is configured
- Consequences if there is a failure in the policy

1. Need for a Security Policy



A security policy plays a vital role in the deployment of a network topology. A security policy helps network administrators to prioritize their administration role. A proactive security policy protects the intellectual property of a company from several potential attacks/threats. This also helps the organization to introduce rules and regulations to the user, about how they should make use of their IT equipment.

A security policy helps baseline security terms to reduce the risk of losing an organization's artifacts. It provides an understanding for security administrators as to what steps they should take if there is a security violation, and what the consequences of the violation should be.

Five Steps for a Security Policy

There are important steps to be followed to implement a security policy:

Identifying a risk: Identifying an issue in the current environment involves understanding the use of resources by a legitimate or authorized user. The risk in the network can be identified by the use of good monitoring and reporting tools.

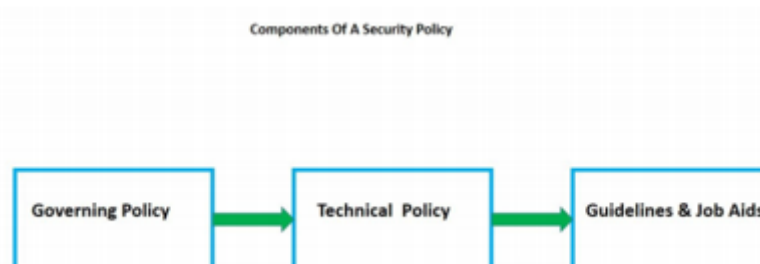
Conducting analysis: A proper and efficient analysis should be conducted to understand the use of secure hardware and software used in the organization. Even ""too much is too bad,"" so administrators should take care to check that a high level of security does not disturb the smooth running of the business.

Drafting a language: A rule or a language should be drafted and the administrator should make sure that the policies are read and agreed to by all the users inside the organization. In the case of enterprise companies, administrators can use a manual or automated tool to help the user sign the policy. There are some tools available on the internet to test the user's knowledge of the policy.

Performing a legal review: A legal review can also be done to understand the perfect nature of the policy created, which will clearly explain the consequences if the user violates it.

Deploying an appropriate policy: An appropriate policy is required to be deployed to explain the preceding factors.

Security Policy Components



The following is an overview of each of the three components of a security policy:



- **Governing policy:** The governing policy talks about the concept and importance of the security information at a very high level and defines the stance of the organization on security policies. Governing policies are also created in alignment with other company policies, so they support most components of the security policy. The governing policy is mostly read and signed by the management users and it is also agreed to by the end users.
- **Technical policy:** These policies are used in most technical aspects of an IT environment and also cover some of the aspects and topics within the governing policy. Examples of technical policies are policies created for the use of an operating system, application, network, and handheld devices, such as mobiles, PDAs, and tablets.
- **Guidelines and job aids:** Guidelines and job aids are the documentation that offers a step-by-step outline to implement a specific security policy, depending on the analysis. Job aids act as a backup when a user or member of IT leaves the company and none of the intellectual properties are maintained safely. Thus guidelines and job aids help the organization maintain security. An example is a document that explains how to install a software application on an end user machine.

A. Best example for a security policy – a password policy

A password policy is created to provide the ability for the user to change their account password. To achieve this, a policy should be created that defines a secure password for the systems. The following are the steps to be followed to create a password policy:

Set password history: Password history keeps track of old passwords to ensure they are not repeated.

Maximum and minimum password age: The second factor in the password policy is deciding how long users can keep their passwords before they expire. The intention of this is to make the users change their password periodically.

Minimum password length: This configures the minimum number of characters for a password. Best practice is to have at least 8 to 14 characters.

Complexity of the password: The important factors in configuring complex passwords are that passwords should have a minimum of eight characters, which consist of numbers, symbols, and lowercase and uppercase letters.

B. How to develop a policy

Developing a policy is an art where multiple blocks are assembled together into a framework. This takes a lot of time and several revisions. There are two different approaches used to deploy a policy. One approach is the top-down approach and the other is the bottom-up approach. Also, make sure that the new policy balances the current practices of the organization. Finally, the policy should be efficient and it should contain mechanisms to protect the organization against different types of potential attack.



Risk is the possibility of a vulnerability getting exploited. Risk can also be defined as a threat or attack that can cause damage to the business or the organization.

Risk Analysis

It is used to forecast any possible risks that may arise within the organization in terms of assets usage, policy weakness, and so on. The impact would be in terms of financial loss, any critical data loss, and other concerns.

Benefits of Risk Analysis

The following are benefits of risk analysis:

- Business continuity can be smooth
- All stakeholders are well-informed about the risk and its consequences so that they try to take proactive steps in their respective roles against the risk
- From a network security perspective, it basically helps to manage assets and safeguard them from specific attacks

There are two ways in which risk analysis are implemented:

- Quantitative risk
- Qualitative risk

A. Quantitative Risk

This method of analysis tries to put in some numbers so that there are some analytical values to identify the risks involved.

Let's discuss the terminologies involved in the risk calculation:

Asset Value (AV): The cost of an asset. For example, a router is an asset and the cost to purchase, install, and maintain it would be referred to as the asset value for the router.

Exposure Factor (EF): The amount the loss could have incurred on an asset. For example, the risk assessment team might check the EF due to a natural catastrophe affecting the server farm and at what percentage.

Single Loss Expectancy (SLE): The single instance of a threat on an asset and the loss incurred from it.

Annualized Rate of Occurrence (ARO): The rate of the threat occurrence on a per-annum basis.

Annualized Loss Expectancy (ALE): The loss to the organization due to a threat occurring on a per-annum basis.



B. Qualitative Risk

This method of risk analysis is more useful in a scalable environment where assets keep growing. It may be difficult to use the quantitative method here because the calculations never end.

The good thing about qualitative risk analysis is that it can be implemented regardless of the size of the business or the assets that have to be protected. Further, this method has more descriptive scales of risk analysis, such as low, medium, or high, instead of analytical analysis. For these scales to be defined, a tool called **the risk assessment matrix** could be used. The analysis is also done based on the attributes and instincts of the organization's top management; that is, every organization base in their assets level and scaling factor can define the scale of the risk.

3. Vulnerability

A vulnerability can be defined as a flaw or weakness in the system that an attacker can use to attack the system/network. A vulnerability in the system/network can be caused as a result of a malicious attack, or it can be triggered accidentally because of the failure in the policy implementation. Vulnerabilities can also occur due to the installation of a new software update, due to the installation of unlicensed third-party tools, and so on.

There are two different terms to be remembered: bug and vulnerability. Both of these terms are similar, which explains the weakness in the programming. A bug may not be risky for the product, and the attackers may not use this to attack, but a vulnerability can create a way for the attackers to gain access to the system/network. Thus a vulnerability should be addressed and patched as soon as possible.

The following are some of examples of vulnerability exploits:

- An attacker installs malware to export sensitive data using a buffer overflow weakness. Using that malware, the attacker convinces the user and opens an email message.
- An employee of an organization copies an encrypted, hardened program to a USB drive and tries to crack it at his home.

Typically, network vulnerabilities are classified into three primary types:

- Technology weaknesses
- Configuration weaknesses
- Security policy weaknesses

A. Weakness in Technology

Network technologies naturally have weaknesses that can be exploited by an attacker. Some of them are as follows:

TCP/IP protocol: Protocols, such as HTTP and FTP, are generally not secure because they are not encrypted.

Protocols, such as SMTP and SNMP, are insecure because SNMP queries are allowed to flow through a firewall and security systems as the scanners in the remote can acquire the filter rules.

Operating system: Most operating systems have several known security problems.



Network equipment: Weakness in password protection, authentication, and holes in firewalls are some examples of vulnerabilities in network devices.

B. Weakness in Configuration

These are some common errors that network administrators make while configuring the network device:

- **Unfastened user accounts:** Attackers use several snooping tools to snoop the username and passwords exposed insecurely
- **Passwords and system accounts:** If administrators use easily guessed passwords without any special characters, hackers may also use this to exploit the network
- **Misconfiguration in internet services:** If JavaScript is turned on in web browsers, attackers can run an attack on the system
- **Misconfiguration in network equipment:** Configuration mistakes while configuring an access list, routing protocols, and firewall rules, and a lack of encryption can cause vulnerability

C. Weakness in a Security Policy

Mistakes in a security policy may increase the chance of vulnerabilities. Some policy weaknesses are as follows:

- **Lack of security policy:** If a particular issue has not been addressed during creation, a security policy can allow hackers to attack.
- **Policy weakness for hardware and software installation:** Installing unapproved or unlicensed third-party software and making unapproved changes in the network topology can allow an attacker to exploit the network.

Understanding vulnerabilities and taking the proper action to protect them are very important steps in mitigating threats to an organization. A vulnerability in the network may occur due to the following reasons:

- A weakness in the network/system
- Flaws in the policy
- Misconfigurations
- Weaknesses in the protocol
- Physical access to network resources
- Human mistakes
- Malicious software

There are some tools that help administrators perform an analysis:

Common Vulnerabilities and Exposures (CVE): This is a very famous database that provides some of the most common identifiers used to enable the exchange of data between different security products and also helps to evaluate the tools and services of an organization.



National Vulnerability Database (NVD): This US government database contains several standards of vulnerability management. The NVD also provides vulnerability management, security measurement, and compliance. This contains the checklist of security principles, a list of software weaknesses, and so on.

◀ Preliminary Activity for Week 4

Jump to...



Analysis, Application, and Exploration for Week 4 ▶



Navigation

Home

 Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants

 Grades

General

01 Exploring Security Threats


02 Delving into Security Toolkits

03 Intrusion Prevention System

04 Understanding Security Policies I

 Preliminary Activity for Week 4

 **Lesson Proper for Week 4**

 Analysis, Application, and Exploration for Week 4

 Generalization for Week 4

 Evaluation for Week 4

 Assignment for Week 4

05 Understanding Security Policies II

06 - Preliminary Examination

07 Deep Diving into Cryptography

08 Deep Diving into Cryptography: Types of Cipher

09 Implementing the AAA Framework

10 Implementing the AAA Framework: Implementing A...

11 Securing the Control and Management Planes



12 - Midterm Examination
13 Protecting Layer 2 Protocols
14 Protecting the Switch Infrastructure
15 Exploring Firewall Technologies I
16 Exploring Firewall Technologies II
17 Cisco ASA
121 - WEB101 / CCS3218
Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment



A banner for Bestlink College of the Philippines (BCP) featuring a blue-tinted image of a modern building. The text is overlaid on the image. At the top right, it says "visit www.bcp.edu.ph". The main headline in large red letters reads "Enrollment registration is now Ongoing". Below this, in white text on a blue background, it says "For 2nd Semester SY 2021 - 2022". Underneath that, in white text on a dark blue background, it says "We are accepting new students, returnees and transferees." On the right side, there is a quote: "Be trained to be the best, Be linked to success" next to the BCP logo. At the bottom left, there is an email icon and the address "bcp-inquire@bcp.edu.ph". At the bottom right, there is a phone icon and the numbers "(8)442-8601 | (8)518-8050".

visit www.bcp.edu.ph

Enrollment registration is now Ongoing

For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.





"Be trained to be the best,
Be linked to success"



 bcp-inquire@bcp.edu.ph

 (8)442-8601 | (8)518-8050

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)

