Computer Network Security

Lesson 6

Security Policy & Standards II

Lecturer: Dr Msagha J Mbogholi, PhD

Flashback from Lesson 5

- There are 3 types of policies – general, issue-specific and system – specific
- Standards and procedures complement policies in their implementation
- An effective policy should be comprehensible, customized, actionable, flexible, give time, make expectations clear, language (clearly worded and not in the form of a riot act), support the mission.
- The master policy will state the purpose of the information security policy, where it will be applied in the organization, who has responsibility for its implementation, and who is responsible for ensuring compliance.
- An issue-specific policy deals with issues of specific interest to the organization
- The system-specific policy deals with matters to do with the system or applications.
- The information security charter stipulates the purpose, goals and responsibilities of the computer security program. It also shows where it fits in terms of the organization's business goals.

Content

- Policy Requirement Exceptions
- Specific Information Security Policies
- Standards and Procedures

Part 1

Policy Requirement Exceptions

Policy Requirement Exceptions

- In lesson 5 there were 3 different types of policies that were discussed. These were the general(master) policy, issue-specific policy and system (application) –specific policy.
- It was also explained that the Information Security policy is produced from the master policy.
- All policies have requirements. A requirement is something that is needed in order to implement the policy.
- There are times when an exception to the requirements occurs; perhaps it is not practical to implement as a necessary component can't be found, or some other reason.
- At such times an exception must be developed, stating why the requirement can not be fulfilled. An exception therefore fills the gap between the requirement and the policy itself.

Policy Requirement Exceptions (cont'd)

- Placing it contextually it can be seen as follows:
- Information security policy = policy requirements (+ policy exceptions)
- In the absence of exceptions the information security policy will contain all requirements without exception.
- There are 3 ways to document an exception.

Documenting Exceptions

- With Requirement adjustments – in this case the exception to the requirements is allowed based on an adjustment to the requirement to accommodate the exception. For example service on the departmental printers will be done every 3 months instead of every 6 months.
- Redress mechanisms – in this case a requirement is set in the policy but acknowledges that it cannot be met. The policy then sets an exception that offers redress in the event that the requirement cannot be met. For example an employee requires a smart card to access the server room; however, due to organizational constraints, the exception allows the use of a password to access the server room instead.
- Risk based control – in this case a requirement is set in the policy but due to certain constraints it cannot be implemented. In this instance an exception is implemented that balances the risk of not implementing that requirement. For example in the server room above there is a requirement that the web cam stays on whenever an administrator is working on the server. However the hardware did not come with a webcam and an exception is made since the risk is low; it is reasonable to expect that with the current security measures in place only authorized personnel can access the server room in the first place.

Part 2

Specific Information Security Policies

Introduction

- In every organization the information security policy will be developed from the master policy.
- The information security (infosec) policy is unique to every organization as an organization will have its own strategy, goals and objectives. The information security policy supports the strategy, goals and objectives of the organization.
- Within the infosec policy is actually a set of policies collectively making up this one document.
- These policies are divided into 4 distinct groups as described in fig 1.

InfoSec Policies

- The hierarchy can be illustrated in terms of the targets of the policies themselves and are grouped as enterprise level, security program level, user security level, and system and controls level policies.

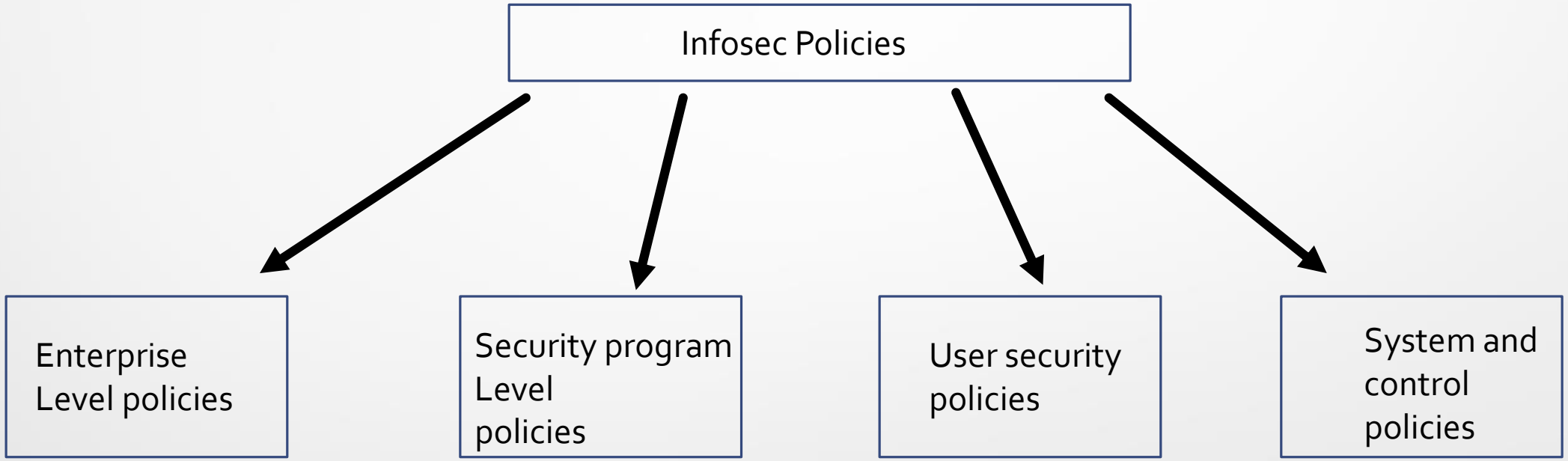

Fig 1. Information Security Policies (Hierarchy)

Enterprise level Policies

- These policies are found at enterprise level. At this level the very definition of what data is valuable and sensitive to the enterprise is described.
- It is also at this level that the information security group described in lesson 5 is found.
- The roles and responsibilities for the information security function are also defined here. Recall in the example in lesson 5 the role was assigned to a department and not a designated individual role?
- There are 2 fundamental policies found at this level.

Information classification Policy

- Information classification and handling policy – it is also known as the data classification and handling policy.
- This policy defines what is deemed sensitive data across the enterprise, who is responsible for it and what are the minimum acceptable controls for protecting the data.
- It is worth noting that in the context of the system the data in reference is electronic data. However, the policy should apply to all data (electronic or hard) across the enterprise.

Information classification Policy

- Structure: the general structure of this policy might vary from enterprise to enterprise. However, there are 3 common ingredients to all information classification policies.
- Data classification levels - the four common classifications of data are public, internal use, restricted and confidential. In other environments data is also further classified in levels such as high, medium or low security; yet in others a further classification of proprietary is included. As can be easily deduced what is more important in classification is to let users know which group particular data types belong to. The most appropriate way to do this is to give examples of data that belong to each of the identified classifications.
- Responsibilities – Responsibilities in this area may include the owner and the custodian of the information. They should be listed and their roles made clear.
- Information rules – rules have to be put in place to stipulate how each of the identified classifications will be treated. For example it is logical to label data in terms of sensitivity. In an electronic environment such data can be either visibly tagged with a label or color signifying its sensitivity. The rules should also describe how such information will be transmitted (use of tunneling protocols or cryptography), how it should be stored, and how it should be disposed of.
- There are many information classification policies available in the public domain, together with some templates that can be used for the same. A good example can be found in https://www.uottawa.ca/administration-and-governance/information-classification-and-handling-policy

Information Security Program Policy

- This is a key policy that establishes the information security program, its staff, and required controls.
- Structure – the common components of the information security program are:
- Roles – this part specifies who (roles) and what (responsibilities) is involved in the establishment and management of the information security group. The roles described should start from the most senior team member to the lowest key role.
- Policies – it should be specific in describing required policies, standards and procedures.
- Security plan – Leighton (2016) asserts that "The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the nation if the plan is implemented as intended."

Information Security Program Policy (cont'd)

- Risk management – all controls for risk assessment for the enterprise information systems should be identified in this section.
- Testing – the policy should define the controls for testing, monitoring and evaluation across the enterprise.

Security Program level Policies

- These are the policies that will be written once the security program has been established.
- The purpose of these policies is to guide the security program activities.
- These policies can be divided into 3 groups.

Incident Response Policy

- This policy deals with how to handle security related incidents when they occur.
- Key to the policy is understanding what an incident is in the first place (identifying it), how to respond to it, and by extension how to manage and control it.
- This gives skeleton structure on what to find in an incident response policy.

Incident Response Policy

- Structure: the structure of the policy may vary but based on the description the following components will be found:
- Training – required training for identified staff, thereby creating awareness of their roles, how to identify incidents, and how often the training should take place.
- Testing – testing of response plan and its accompanying logistical parameters.
- Handling – details of who should handle the incident and how it should be handled.
- Monitoring – the monitoring capabilities of the enterprise, who should be doing it, and what software will assist in the process.
- Response plan – details of the response plan.

Contingency Plan Policy

- A contingency plan is one that is put in place to handle unexpected eventualities (outcomes that have not been planned for).
- The contingency plan should not be developed in isolation; rather it should work in tandem with disaster recovery planning, information security program policy and business continuity planning.
- SP 800-34 specifies the elements that should be addressed by contingency plan policies.

Contingency Plan Policy

- SP 800-34 identifies the following elements that should be addressed by a contingency plan policy:
- Roles and responsibilities – the roles of all key members of the contingency plan together with their responsibilities
- Scope – which applications and departments are covered in the contingency plan.
- Resource requirements – which resources are required across the targeted applications and departments to effect the contingency plan
- Training requirements – the specific kind of training required for key roles and other roles in the policy, specifying what exactly they require to be trained on and how often.

Contingency Plan Policy

- Exercise and testing schedules – when the contingency plan will be rehearsed (practiced) together with testing schedules determining frequencies.
- Plan maintenance schedule – a maintenance schedule of the contingency plan components, for example applications
- Minimum frequency of backups and storage of backup media. – a determination of how often backups and storage will occur as part of the contingency plan.

Personnel Security Controls Policy

- Personnel security though sometimes not given the attention it deserves is a key issue. In the discussion on threats one of the most challenging threats that was identified was insider threats.
- The issue of personnel is discussed in several SP documents, 800-73, 800-76 and 800-78.
- The policy should ensure that all users are aware of their responsibilities, and that they are qualified for the roles that they have been hired in.
- Additionally there should be measures in place to reduce the risk of theft, fraud, or even misuse or abuse. The measures should purpose to ensure the following:

Personnel Security Controls Policy

- Job descriptions and terms and conditions of employment should spell out responsibilities explicitly.
- All employees and other users of the system (including contractors) should be thoroughly vetted using an established vetting process.
- Users should sign an agreement stating they have understood their roles and responsibilities; the agreement should also be in the form of a non-disclosure agreement to protect the information any user may come across intentionally or unintentionally in the course of their duty.
- The information security policy should contain all the roles and responsibilities of system users.

Personnel Security Controls Policy

- Structure: considering the foregoing requirements different organizations will have different structure of the personnel security controls policy. However, the following are to be found in all personnel security controls policies:
- Position classification – it should classify personnel positions in terms of their sensitivity and describe the different controls for those positions.
- Vetting – it should describe the procedures for vetting of all potential employees, and actions to be taken based on the screening. Further the policy should specify how often rescreening should be done in the event of successful employment.
- Separation – the policy should clearly state what should happen to protect the system and its information when an employee separates from the enterprise.
- Sanctions – the policy should ensure sanctions to ensure compliance with it.

User Security Policy

- The user security policy is used to express what users can and cannot do in the information system environment.
- SP 800-53 specifies the rules and behaviors of users and it is a required control (PL-4) in that document.
- SP 800-18 specifies the rules to be followed or adopted for each information system. The topics that need to be addressed are:

User Security Policy

- SP 800-18 topics that should be addressed:
- User roles, responsibilities and use of the system should be clearly defined and described.
- Means of access and limits (if any) on interconnections should be described.
- Acceptable use behavior and violation of it should be made explicitly clear
- Clear list of policies applicable to the system that users must follow.

User Security Policy

- When composing an acceptable user policy (AUP) the following should be examined:
- Content – as there are no clear guidelines as to exact content of the AUP guidance may be gotten from SP 800-53 and applicable country laws.
- Content organization is also not explicit though the sequence may follow that of other policies. However, the following order is recommended.

User Security Policy

- Structure: recommendations on structure of AUP are –
- Expected code – how the user should behave with respect to the system
- Unacceptable behavior – what is not allowed with respect to the system
- Notifications – a notification of ownership of the system in its entirety (including data and any other component deemed to be part of the system in the notification), and a requirement (like a checkbox) requiring the user to acknowledge this. The system will only allow the user to access it after ticking the checkbox.
- Others – a section for any other additional information or exceptions.

System and Control Policies

- These are policies that deal with the system and its controls. Due to ever changing technology these policies need keen monitoring and updating to keep up.
- These are some of the most sensitive policies to deal with as shall be clearly seen.
- There are 4 key policies in this domain.

Network Security Policy

- The policy should address the following:
- Network architecture controls – should define boundary protection (use of packet filtering or software/hardware firewalls) and any architectural implementations such as DMZs
- Server controls – description of minimum security configurations for the network/domain server(s).
- Service controls – security mechanisms for static information, for example, encryption and for information in transit, for example, SSL and other tunneling protection.

Authentication Policies

- These policies can be written in diverse ways. However, the policies should purpose to capture the following:
- Unique identification of users – so no user can authenticate themselves using other user's credentials.
- Authentication types and multifactor authentication – use of different authentication mechanisms such as biometric authentication, and using multifactor authentication (implementation of layering principle)
- Device identification – identification of devices uniquely as they join the network.

Access Control Policies

- This policy is guided by SP800-12 and SP 800-100.
- Topics that are addressed by this policy include:
- Enforcement of access control
- Operational procedures
- Privilege levels
- Use of session locks
- Use of system notifications
- Rules of network access (restrictions on internal and external network access)

Security Audit Policy

- This policy specifies the different security events that should be audited. The security events are normally categorized.
- Consequently the issues that need to be addressed by the policy are:
- Required audit events
- Contents of the audited events
- Audit records storage (where should they be stored)
- Reviews of audit records
- Report generation
- Audit record protection

Security Audit Policy Example

- In https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies some event categories that can be audited in Windows 10 are suggested. These are:
- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

Part 3

Standards and Procedures

Standards

- In lesson 5 the role of standards was explained as complementing policies by describing the rules, steps, guidelines and actions to be implemented in order for the policy to be effective. The steps/actions described in a standard are mandatory.
- For a standard to be successful, there must be overall commitment to it (and by extension the policy it complements) by all who have a role in it. Secondly standards cannot be cast in stone and therefore must be reasonable, adaptable and current.
- Procedures were described as step by step instructions that describe in detail how the actions described in the policies and standards will be carried out.
- An format of a standard (and accompanying procedure) is as follows:

Standards (and Procedures) Format

- Policy –
- Standard –
- Procedure –
- This format in some books is referred to as PSP

Standards (and Procedure) Example

- Policy – it is the policy to process exams as quickly as possible
- Standard – all departments must process exams within 10 days
- Procedure –
  - Day 1 -6 : marking of scripts and entry into the system
  - Day 7: submission of scripts and grade sheets to examination officer
  - Day 8: departmental exam board meets for moderation
  - Day 9: corrections entered into the system by examiners
  - Day 10: results leave department for onward processing.

Summary

- Information security policy = policy requirements (+ policy exceptions)
- There are 3 ways to document an exception: With Requirement adjustments, redress mechanisms and risk based control
- Within the infosec policy is actually a set of policies collectively making up this one document. These policies are divided into 4 distinct groups: organizational level policies, security program level policies, user security policies, and system and control policies
- The format of a standard and by extension procedure is threefold: - Policy description, description of the standard, and steps that make up the procedure.

References

- Gantz, S. D., Philpott, D. R., & Windham, D. (2013). *Fisma and the Risk Management Framework: The new practice of Federal Cyber Security*. Elsevier/Syngress.
- Landoll, D. J. (2016). *Information security policies, procedures, and standards: A practitioner's reference*. CRC Press, Taylor & Francis Group.
- Peltier, T. R. (2002). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach, NY.
- Dansimp. (n.d.). *Basic security audit policies (Windows 10) - windows security*. (Windows 10) - Windows security | Microsoft Docs. Retrieved October 8, 2021, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies.