Computer Network Security

Lesson 5

Security Policy & Standards I

Lecturer: Dr. Msagha J Mbogholi, PhD

Flashback from Lesson 4

- Vulnerability assessment can be commonly undertaken through the following steps: Identification of resources, threat identification, vulnerability analysis, risk assessment, remediation
- Assessment techniques are baseline reporting, informal assessment, detailed risk analysis and combined approach
- Tools for assessing vulnerabilities include port scanners, protocol analyzers, vulnerability scanners, honeypots and honeynets.
- Vulnerability scanning is the use of software to scan an existing system for known vulnerabilities and then producing a report of the findings.
- Penetration testing involves 3 steps: black-box, white-box, and gray-box
- Attack mitigation techniques include security posture, configuration of controls, hardening and reporting.

Content

- Policy Related Definitions
- Elements of a Policy
- Policy Types
- Computer Security Program

Part 1

Policy Related Definitions

Definitions

- All organizations need policies in order to have a well structured way of carrying out day to day business. Policies are implemented at national level all the way down to organizational level. Nationally countries have policies that affect the way governments do business, hence the well known term government policy.
- At organizational level this also applies; even as a lay person you will no doubt have heard the term company policy even in supermarkets; you request for a favor and the manager tells you that it is against company policy, or that company policy does not allow for it.
- As a student of information security in networks then, the interest will be in how are policies used in an organization such that the whole system (data, hardware, software, users and network) is well protected. So, what exactly is a policy in this context?

Definitions (cont'd)

- Policy – loosely it can be seen as a rule or law regarding some specific subject or subject area. As is to be expected rules are set by authorities or authority figures/roles. In the context of information security it is a set of goals and beliefs set by top management for the achievement of a certain subject or subject area/objective. All policies should be short and concise.
- General (Master) policy – it is the general program policy that spells out the beliefs and goals of an organization from the top management perspective; it is also known as the enterprise program policy. In the context of system security it is referred to as the security program policy, information management policy, or information security policy. Moreover, it may also contain general policies on other topics of interest such as the conduct of employees. As it is a general declaration it's from here that more specific policies are developed.
- Issue – Specific policy – an issue – specific policy is also known as a topic-specific policy. It deals with specific issues in the organization that are of concern such as internet usage, wireless network usage, email usage, and so on.

Definitions (cont'd)

- System (Application) –Specific policy – this type of policy deals with systems or applications that are of concern to the organization. The policy deals with how they should be set up, used, operated or maintained. For example payroll system policy, SNMP policy, MIS policy, and so on.
- Standards – standards complement 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.
- Procedures – they are step by step instructions that describe in detail how the actions described in the policies and standards will be carried out.
- Baseline – this specifies the minimum acceptable security that all systems within the organization must comply with. (recall the baseline approach described in lesson 4?)
- Guidelines – they are recommendations that provide direction (guides) on how to implement standards and procedures; they can be seen as providing frameworks for the implementation of standards and procedures. As they are recommendations they are not mandatory.

Definitions (cont'd)

- Fig 1 shows how the different terms relate to each other from an organizational perspective

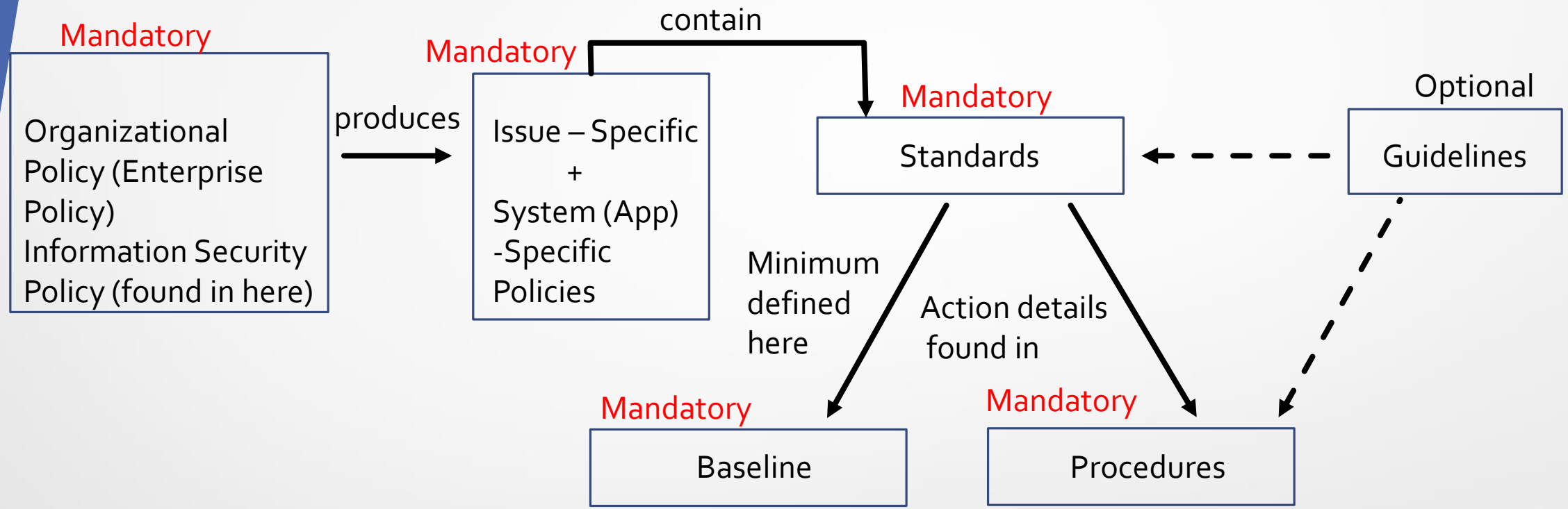

Fig 1. Relationship between policies, standards, procedures and guidelines

Why implement Policies?

- In addition to protecting the organization policies give clear expectations on behavior of employees, goals and expectations of the top management of the organization.
- Organizations are expected to have shown that they have taken necessary steps to protect their systems in the US of A and to show that they have; there are seven elements described by Peltier (2002). They are:

Why implement Policies (cont'd)

- Workforce guidance by establishment of policies, procedures and standards.
- Appointment of executive preferably a CxO to oversee implementation and compliance of organizational policies.
- Establishment of justification when delegating authority to lower level employees.
- Ensure policy adherence is being executed.
- Ensure that standards and procedures are clearly understood by those who are affected.
- Enforcement of policies and clear rules on deterrence.
- Ensuring correction and modification procedures in instances of policy violations.

Part 2

Elements of a Policy

Key ingredients of an Effective Policy

In order for a policy to be deemed effective it should possess the following qualities:

- Be comprehensible – an effective policy should be written in clear and easily understandable language, bearing in mind especially who it is intended for. It is pointless to have a policy written in complex language that the targets can't understand.
- Customized – whereas there are many examples of written policies regarding information security in the public domain (especially the Internet) an effective policy should be written for the particular organization and its circumstances.
- Actionable – recall the acronym SMART? Specific, Measurable, Actionable, Realistic, Time-bound. Right. An effective policy needs be actionable within the confines of the business objectives and mission of the organization. Policies should not be so restrictive as to stifle productivity, and not so lose as to endanger it either; rather a balance should be found.
- Flexible – an effective policy should not be cast in stone such that it is not enforceable. Rather an effective policy should be accommodating to a reasonable degree while still being enforceable. Again, think SMART.

Key ingredients of an Effective Policy (cont'd)

- Give time – for a policy to be effective there is need to give employees a grace period to understand it. In essence this grace period will help employees to understand the standards and procedures in the policy and be in a better position to comply once they have understood it. Win-win right?
- Make expectations clear – an effective policy makes expectations clear; management play a very crucial role in this and they should participate actively in this process.
- Language – just as the wording of the policy should be made comprehensible so too should the deterrence language. The language should be urbane to say the least.
- Support the mission – have you read somewhere that the law was made for man and not the other way around? An effective policy should support the mission, vision, goals and objectives of the organization and not the way around.

Part 3

Policy Types

Introduction

- The different policies found in the enterprise were defined in part 1 of this lesson.
- This part describes in further details what the types of policies are, and what is to be found in them.
- The policies that were defined in part 1 were the master (general) policy, issue-specific policy and system-specific policy.

Master (General) Policy

- The master (general) policy establishes the information security policy to be used across the organization.
- This policy is established by senior management (the Executive) of the organization.
- 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.
- The components of the information security policy are:

Information Security Policy

- Name – the name of the policy; for example, 'Big League Information Security Policy'
- Topic – the objectives of the policy. In this part apart from the objective it is expected that a statement declaring what the topic is all about will also appear here. For example since this is about information security a statement about the necessity of the CIA of the organization to be protected from unauthorized disclosure, access, alteration and modification will suffice.
- Scope – the scope of the policy should be clear in terms of who and what is affected. More specifically it should be specific on who is affected by this policy; is it employees only? Employees and business partners? Employees in a specific division/department in the organization? (as information security may not be required in some parts of the organization). In terms of the 'what', is the policy meant to protect information only, the whole system, the network?
- Responsibilities – specific roles and responsibilities are defined in this section. It is not advisable to mention staff by name as they might not be there tomorrow, or they will have been assigned different roles; this can lead to confusion regarding responsibility. It is therefore advisable to stick to roles in terms of responsibilities. Preferably more than one designation to have responsibility.

Information Security Policy (cont'd)

- Compliance - there are 2 key issues in this section. The first is about who will have the responsibility to ensure compliance to the policy; this is not to be confused with the previous section on roles and responsibilities. In that section all roles were outlined. This section deals specifically with the role(s) responsible for compliance of the policy. The second issue regards the converse which is non-compliance of the policy. What deterrent measures will be put in place in this eventuality.

Issue – Specific Policy

- As defined earlier in the lesson an issue-specific policy deals with issues of specific interest to the organization.
- Specific issues may include usage of the Internet, usage of mobile phones, usage of mass printer, and so on.
- An issue specific policy is different from the information security policy which usually has a wider scope of implementation.
- An issue-specific policy can be issued as is, or the issue can be implemented as a procedure from a standard in some instances.
- Consequently the contents of an issue-specific policy are different from the information security policy.

Issue – Specific Policy (cont'd)

- Name – the name of the issue; this should be worded to be as relevant to the issue the policy is addressing, so that anybody reading it has an idea what the specific issue is from the word go.
- Purpose – the purpose or intention of the policy should be clearly stated. For example ' this policy defines usage of the mass printer on 5th floor of Big League Inc organizational headquarters in Nairobi, Kenya.'
- Responsibilities – just like in the information security policy this section defines the staff responsible for implementing the policy. Again it is advisable to stick to roles rather than individuals.
- Compliance – as this is an issue-specific policy non-compliance will be more specific and therefore it is better to spell out what is acceptable and what is not. For example it is acceptable to use the mass printer for printing of black and white copies exceeding 100 copies and not acceptable to print more than 50 copies of colored materials.
- Point of Contact – who to contact for more information on the policy.
- Revision – a revision number (optional) so that should be the policy be reviewed it can be clearly stated which is the most recent review. This is better than having to redo the whole policy say when management feel some of the parameters like number of copies above can be reviewed upwards or downwards.

System – Specific Policy (cont'd)

- The system-specific policy deals with matters to do with the system or applications.
- The content of the system-specific policy will be similar to issue-specific one, the key difference being that these kinds of policies are specific to applications in use in the organization.
- For example the access rights in the enterprise application will be a system-specific policy. Who has read rights or modification rights in the organizational document management system (DMS) is also a system-specific policy and so on.

Part 4

Computer Security Program

The Purpose

- Once the information security policy has been written and approved by management the next question arises is who will take the lead in its implementation.
- In most organizations a Information Security Manager (ISM) role is established for this purpose.
- The ISM will take the lead in the creation of the computer security program. This program's purpose is to implement the information security policy and all other policies arising therefrom.
- Before establishing the computer security program the ISM must develop documentation clearly stating the mission of the computer security program, preferably in the form of a charter.
- The charter stipulates the purpose, goals and responsibilities of the program. It also shows where it fits in terms of the organization's business goals.

Program Objectives

- The computer security program objectives must align to the organizational objectives, otherwise there is no point to its existence.
- A good place to start in determining organizational objectives is the strategic plan. Organizations will have a short, medium and long term strategic plan.
- It is generally accepted that the long term strategic plan should span 5 years, while medium is about 3 years, and short term is 1 year.
- The computer security program objectives should align to these so that it supports the organization achieve its short, medium and long term goals.
- Other sources of business objectives can also be ascertained through financial reports or even interviewing select staff.

Program Objectives (cont'd)

- The key element being protected by the computer security program is data (information). As earlier alluded to, all networks and computer systems exist for the purpose of processing and disseminating information. The information is what enables the organization to achieve its business objectives.
- An exhaustive computer security program should seek to fulfill this through the information security policy. The program should achieve the following.

Program Objectives

- Enforce the accuracy of the data.
- Protect the CIA of the data.
- Protect the data from all forms of unauthorized disclosure, access and modification.
- Ensure the availability of the data by protecting it from destruction.
- Have a comprehensive DR (disaster recovery) plan in the event that it is needed.
- It should have a comprehensive business continuity plan
- It should prevent access controls in the system from being accessed by unauthorized employees at any given time.

Program Objectives (cont'd)

- Develop security policies and standards that will encourage management support (management support is crucial in implementation)
- Accept responsibility in the event that security breaches of any form occur, thereby protecting management.
- As most losses occur through negligence (errors and omissions) the program should find ways of protecting against this (for example through configuration management controls)

The Charter

- The charter should address the following in its contents; this forms the basis of its layout.
- Goals of the computer security program – these should be concise and clearly show how they align to the information security policy developed by management.
- Description of the program based on the organization's strategy (this shows it aligns with the overall organization mission and vision)
- Responsibilities clearly spelled out (this will be the ISM or equivalent responsibilities)
- In some instances more responsibilities will need to be assigned in order to execute certain policies; this is because despite the information security policy assigning roles it is mostly generalized and to protect organizational assets it may be necessary to do specific assignments.

Charter Example

- The following example adapted from Peltier (2002) is an example of a charter for a medium sized company.
- First Part (Introduction): - sets the tone for the program
- **Introduction**
  This document defines the scope and direction for the computer security program function. The duties and responsibilities set forth will serve as the charter for the program.

Charter (cont'd)

- Responsibilities (2nd part) – for this charter the responsibilities are set out separately, for management and for information security management.

Responsibilities of Management
To fulfill present and future business commitments, steps must be taken to ensure the accuracy, privacy, and security of our computers, communication networks, electronically processed data, and manual data. The responsibility for safeguarding corporate information rests with all employees, but it is the coordinated effort of management and information security that will:
Minimize the probability of security breaches.
Minimize the damage if such a breach occurs.
Ensure the company's ability to recover from damage with minimal disruption of service.
It is a basic management responsibility to protect resources necessary to conduct business. Management is responsible for identifying and protecting hardware, software, and data resources under its control. This task is accomplished by implementing security policies and practicing security procedures commensurate with the value of the asset to the company

Charter (cont'd)

- **Responsibilities of Information Security Management**

Mission
To provide a secure environment for the information assets of the company.

Strategies
Monitor and audit adherence to security policies and procedures on a daily basis.
Maintain an ongoing and corporate wide security awareness program relating to information asset protection.
Act as a catalyst to make security a part of each employee's daily activities.

- .....more strategies outlined here.....

Charter (cont'd)

Key Responsibilities
Establish and enforce the following general data security rules in conjunction with management:
Information shall be created and maintained in a secure environment.
Practices shall be in place to prevent unauthorized modification, destruction, or disclosure of information, whether accidental or intentional.
Safeguards shall be implemented to ensure the integrity and accuracy of vital company information.

…….More responsibilities outlined here…….

- As can be seen from this example the charter clearly explains it purpose, the responsibilities of management in implementation of the information security program, mission and strategies of the program, and a description of all the responsibilities of information security management.
- In a small organization it may be preferred to have information security management as a function of the program rather than an individual role as it set out in other charters.

Charter Example 2

- The content of information security varies even though the document should be guided by ISO 27001. Another example of an ISO 27001 implementation outlines the following:
- Introduction – setting the tone and the management stand regarding the IS management system
- Responsibilities – responsibilities of staff, managers and third parties
- Information security objectives – objectives, necessary actions to implement the objectives, how they will be measured, and who is responsible for each objective.
- Compliance – who is responsible for compliance, and consequences of non-compliance
- Supporting policies – issue-specific and system-specific policies that support the info sec policy.

Charter Examples

- More examples of information security policies and their contents in the public domain can be found at the following urls:
- https://hightable.io/iso-27001-information-security-policy/
- https://isoconsultantkuwait.com/2019/08/02/iso-270012013-clause-5-2-information-security-policies/
- https://www.isms.online/iso-27001/information-security-policy/
- https://popp.undp.org/UNDP_POPP_DOCUMENT_LIBRARY/Public/ICT_Security_Information%20Security%20Policy.docx

Summary

- 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.

References

- 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.