

Cybersecurity Law, Policy and Ethics

Prepared by **Dr. Kamal Alieyan**

Lecture 09

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Introduction to Cybersecurity Policies



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Lecture Objectives

- To understand the overall idea of policies in cyberspace.
- To know the role of people who are associated with cybersecurity policies like policymakers and policy audiences.
- Different types of policies.
- Some very famous cybersecurity policy frameworks.

Lecture Topics

- 8.1 CYBERSECURITY POLICIES
- 8.2 CYBERSECURITY POLICY MAKERS
- 8.3 UPDATING AND AUDITING CYBERSECURITY PROCEDURES
- 8.4 CYBERSECURITY POLICY AUDIENCE
- 8.5 CYBERSECURITY POLICY CLASSIFICATION
- 8.6 CYBERSECURITY POLICY AUDIT
- 8.7 CYBERSECURITY POLICY ENFORCEMENT
- 8.8 CYBERSECURITY POLICY AWARENESS
- 8.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES
- 8.10 TYPES OF CYBERSECURITY POLICIES
- 8.11 CYBERSECURITY FRAMEWORKS (CSFS)
- 8.12 SOME CYBERSECURITY FRAMEWORKS (CSFS)

8.1 CYBERSECURITY POLICIES

- A Cybersecurity is a global issue.
- Risk management at the enterprise level is a big concern, hence every employee in an organization including IT professionals and managers must be concerned about security.
- One of the effective ways of educating employees on the significance of security is a **cybersecurity strategy** that clarifies an individual's responsibilities for protecting IT systems and data.
- **Cybersecurity policies** are responsible for setting the standards of behavior for activities like encrypting email attachments and restricting the use of social media.
- Cybersecurity policies are significant as cyberattacks and data breaches are potentially costly.
- Many times, employees are the weak links in an organization's security. This is because employees may share passwords, click on malignant URLs and links, use unapproved cloud applications, and disregard to encode confidential records.

8.1 CYBERSECURITY POLICIES

- All this may lead to catastrophic effects in cyberspace.
- However, improved cybersecurity policies may be useful for a better understanding of how to maintain the security of data and applications by the employees and consultants.
- **Cybersecurity policies are a must in organizations and public companies** that are associated with industries like healthcare, finance, or insurance.
- In these organizations, cost as well as reputation are at stake, and there are heavy penalties paid if their security infrastructure and procedures are found to be inadequate.
- Cybersecurity policies promote the public image and credibility of an organization. Often customers, partners, shareholders, and prospective employees demand evidence that the organization is capable of protecting its sensitive data.
- It might be hard for an association to demonstrate its capacity if it does not have a cybersecurity policy.

8.1 CYBERSECURITY POLICIES

Definition of Cybersecurity Policy:

- A cybersecurity policy is the statement of responsible decision-makers about the protection methodology of an organization's vital physical and data resources.
- It may be thought of as a document that describes a company's security controls and activities.
- Although security policies do not determine technological solutions, they characterize sets of expectations and conditions that may assist in protecting assets along with its proficiency to organize business.

8.1 CYBERSECURITY POLICIES

Definition of Cybersecurity Policy(2):

- Ideally, a **security policy** defined as the essential manner by which organization prospects for security are converted into explicit, quantifiable objectives.
- These policies are used to assist users in building, installing, and maintaining systems, so that they do not have to make those decisions by themselves.
- Policies are written to offer guidance about the kind of behavior and resource uses may be required in acceptable from the employees of an organization. It also states what is forbidden to wield.

8.1 CYBERSECURITY POLICIES

- A **Cybersecurity procedures** define the rules for the number of employees, consultants, partners, board members, and other end-users who access online applications and web assets, send information over communication networks, and in any case practice dependable security.
- Usually, the first part of a cybersecurity policy defines the overall security expectations, jobs, and duties in the association. Stakeholders incorporate outside consultants, IT staff, financial staff, etc.
- This section characterizes the jobs and obligations or information responsibility along with accountability of the policy.
- The policy may also include sections with respect to other areas of cybersecurity. These sections may highlight requirements for antivirus software or the use of cloud applications.

8.1 CYBERSECURITY POLICIES

- In order to incorporate guidelines and procedures for large organizations or those in regulated industries, a cybersecurity policy may be several pages long.
- In the case of small organizations, it may be only a few pages long and must cover fundamental security best practices.
- Such practices may incorporate:
 - ☐ Rules for utilizing email encryption.
 - ☐ Steps for accessing work applications remotely.
 - ☐ Rules for making and securing passwords.
 - ☐ Rules on the use of social media.

8.1 CYBERSECURITY POLICIES

- Cybersecurity policies must be irrespective of their length and must highlight the areas of primary importance in the organization.
- It might incorporate security for the most delicate or managed information, or security to address the reasons for earlier information breaches.
- Risk analysis may be used to highlight areas to prioritize in the policy.
- The policy must be simple and easy to read.
- The policy encompass technical information for referred to reports, particularly if that information requires periodic updating.
- In a situation where policy must specify employees encrypting all personally identifiable information (PII), it does not have to highlight the particular encryption programming to utilize or the means for encoding the information.

8.2 CYBERSECURITY POLICY MAKERS

- Security policy development is undertaken by different entities in an organization who collectively provide inputs for the policymaking process.
- Anyone who has a stake in the security policy must be involved in the process of policymaking. This is because policies must be developed according to the requirements of various people in an association.
- Creation of policy is witnessed by the following entities:
 - ☐ **Board:** Company board members need to present their expertise for reviewing existing policies and suggesting new ones. Keeping in mind the running conditions of business of the organization, policies can be drafted.
 - ☐ **IT Team:** Since policy involves developing standards around the usage of computer systems, especially security controls, IT team members happen to be the biggest consumers of the policy information in an organization.

8.2 CYBERSECURITY POLICY MAKERS

- ❑ **Legal Team:** This team ensures the legal points in the document and also guides a specific purpose of appropriateness in the organization.
- ❑ **Human Resources (HR) Team:** This team is responsible for obtaining a certified Terms and Conditions certificate from every representative that they have perused and perceived the specified policy. This is on the grounds that the HR group manages prize and discipline-related issues of workers to execute discipline.
- Security policymakers must know that picking a policy and validating it are two different things. Choosing a policy is a simple task with respect to analyzing the effectiveness of it.

8.2 CYBERSECURITY POLICY MAKERS

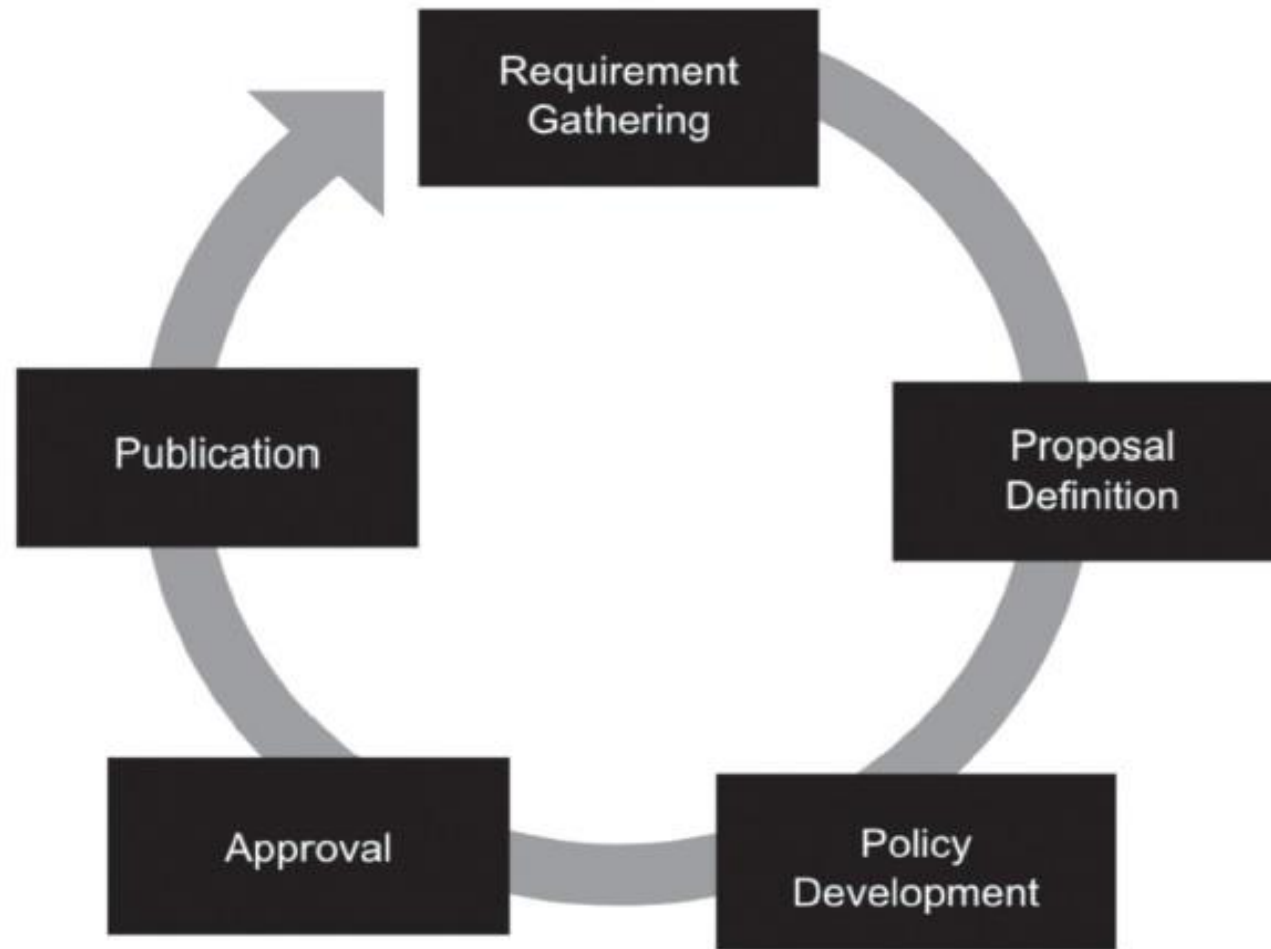


FIGURE 8.1 Security policy development stages.

8.2 CYBERSECURITY POLICY MAKERS

- The IT department, often the **Chief Information Officer (CIO)** or **Chief Information Security Office**, is fundamentally liable for all information security policies.
- On the other hand, stakeholders add to the policy, contingent upon their aptitude and jobs inside the association.
- In situations where personnel are invited to participate in policy development, it is important to consider who is the most critical to the success of the policy.
- A department manager or business executive who enforces policy or provides resources for implementing it may be an ideal participant.

8.3 UPDATING AND AUDITING CYBERSECURITY PROCEDURES

- A **policy** may be defined as a guiding principle that may be used to set direction in an organization.
- A policy is a course of action for guiding and influencing decisions.
- Policies are used for making decisions with respect to specific circumstances.
- Policymaking must take into account the overall framework of objectives, goals, and management philosophies as stated by the senior management.
- A **procedure** is a specific method of achieving something. It ought to be planned as a progression of steps to be followed as a steady and monotonous methodology or cycle to achieve a final product.

8.3 UPDATING AND AUDITING CYBERSECURITY PROCEDURES

- Since technology is consistently changing, there is a need to update cybersecurity procedures regularly, ideally once a year.
- Also, establishing an annual review and update process and involving key stakeholders is a must. When reviewing an information security policy, an organization must contrast the policy's rules and the real acts of the association.
- A policy audit or survey can be helpful in pinpointing rules that no longer address current work processes.

8.3 UPDATING AND AUDITING CYBERSECURITY PROCEDURES

- **Audit** assist in identifying where better enforcement of the cybersecurity policy is needed.
- Three important **policy audit goals** are as follows:
 - ☐ Comparing the organization's cybersecurity policy to actual practices.
 - ☐ Determining the organization's exposure to internal threats.
 - ☐ Evaluating the risk of external security threats.
- An updated cybersecurity policy may be an essential security resource for all organizations without which it is possible for end-users to make mistakes that may result in data breaches.
- An irresponsible attitude may cost an organization significantly in terms of fees, fines, loss of public trust, settlements, and brand degradation.
- Hence it is mandatory to create and maintain policies that can help prevent such adverse outcomes.

8.4 CYBERSECURITY POLICY AUDIENCE

- Cybersecurity policy holds true for all senior administration, workers, investors, experts, and service providers who use organization resources.
- The security policy must be understandable to its audience. This may be achieved by ensuring that the policies are concise and readable.
- This will make it easier for employees to adhere to the policies and fulfill their defined roles.
- In other words, the security policy incorporates all employees, hardware, software, consultants, service providers who use company assets.
- These assets may be in the form of computer networks, data information or any information that may prove to be valuable to the business.

8.4 CYBERSECURITY POLICY AUDIENCE

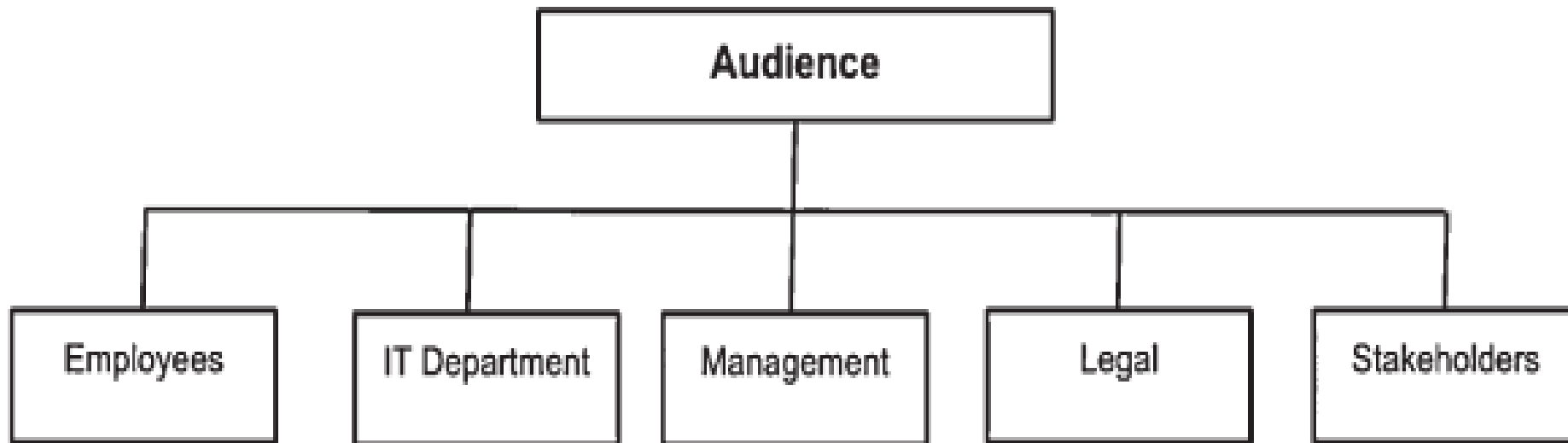


FIGURE 8.2 Cybersecurity policy audience.

8.5 CYBERSECURITY POLICY CLASSIFICATION

- Each association commonly has **three policies**.
- The **first** one is drafted on paper, **second**, one is in employees minds, and the **last one is executed**.
- The security policies are essential to the hierarchy of management control that addresses its audience regarding what must be conducted by the specified terms and requirements of an organization.
- The policy generally requires what must be done. However, it does not address how it should be done.
- Security policies may be informative, regulative, and advisory.

8.5 CYBERSECURITY POLICY CLASSIFICATION

- The **policy** subdivided into the following categories as:
 - ☐ **Physical Security:** It mandates what protection mechanisms must be enforced to safeguard the physical asset of both employees and management. It applies to the prevailing facilities that include doors, entry points, surveillance, alarm, etc.
 - ☐ **Personnel Management:** These are responsible for telling their workers how to lead or work every day and conduct business exercises in a safe way. It may take into account password management, confidential information security, etc., and it may apply to individual employees.
 - ☐ **Hardware and Software:** It specifies the administrator about the type of technology that may be used. It also defines how network control ought to be arranged and applies to framework and system managers.

8.5 CYBERSECURITY POLICY CLASSIFICATION

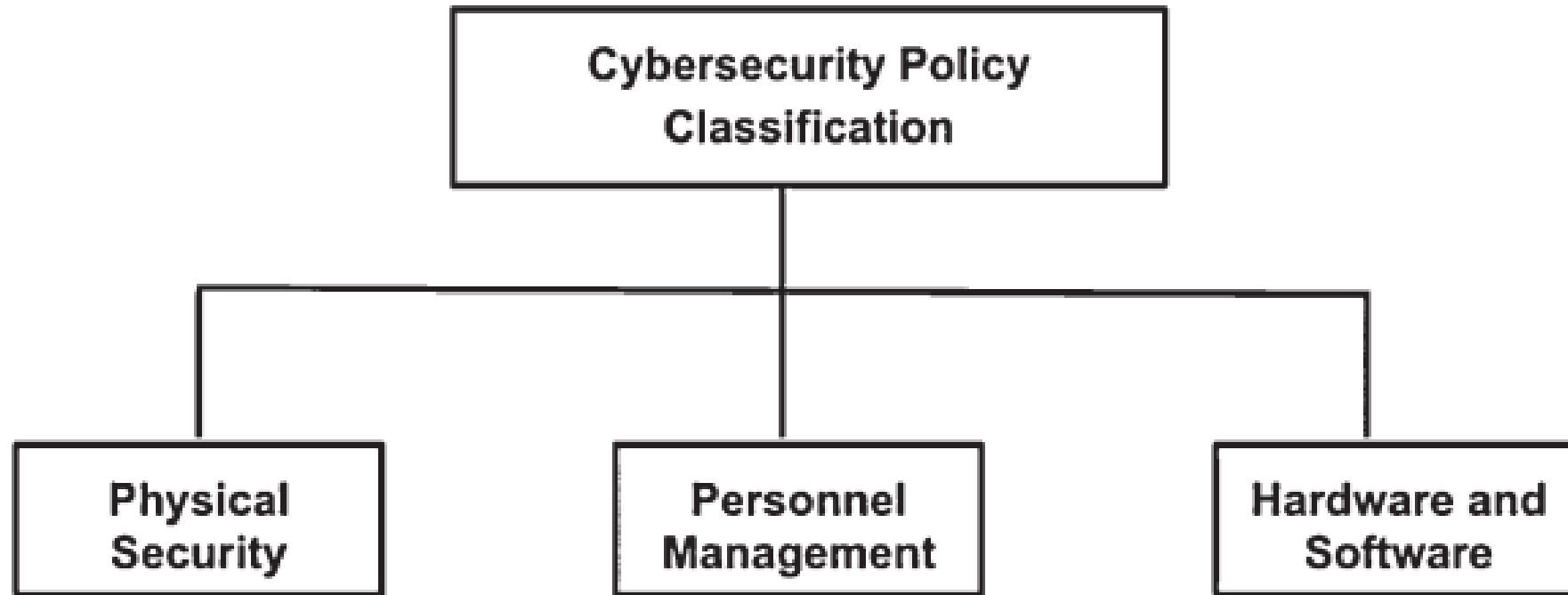


FIGURE 8.3 Cybersecurity policy classification.

8.6 CYBERSECURITY POLICY AUDIT

- Security documents may be thought of as living documents. Hence, it is mandatory to update them at specific intervals with respect to altering business and customer specifications.
- After the establishment of policies, they become operational, following which an audit may be performed.
- **Audits** are usually performed by outsiders or insider agencies for comparing existing practices to the intentions of the policy.
- Security policy audits to help the organization to see better the threat the organization is prone to and the adequacy of the current protection.
- The primary goal of the security audit is to bring all the security policies as closely as possible.
- **Security auditing** may be thought of as a high-level investigation of the current project progress.
- It also analyzes the company posture by testing information security related to existing policy compliance.

8.6 CYBERSECURITY POLICY AUDIT

- Auditing is performed from time to time because it is necessary to contrast existing practices against a security strategy. This may be useful for substantiating and verifying the effectiveness of security measures.
- **Security reviews** are helpful for giving the organization confirmation of best practices that already exist.
- A successful security audit focuses on:
 - ☐ Comparing security policy with the actual practice in place.
 - ☐ Determining an organization's exposure to threats internally.
 - ☐ Determining the exposure of an organization externally.

8.7 CYBERSECURITY POLICY ENFORCEMENT

- Upholding security policies may ensure consistency with the standards and practices directed by the organization. This is because policy, procedures do not work if they are violated.
- **Enforcement** consider the most significant aspect of a company since it is responsible for dissuading anyone from deliberately, accidentally violating policy rules.
- System administrator-level enforcement guarantees appropriate support and forestalls privilege escalation, and employees level enforcement monitors whether assurance of daily working activities actually comply with the policies.

8.7 CYBERSECURITY POLICY ENFORCEMENT

- Nonetheless, there is a need to keep up an appropriate balance between positive and negative reinforcement.
- The best employees that abide by rules are rewarded from time to time for increasing their motivation and boosting up their morale high in positive enforcement.
- On the other hand, in negative enforcement, strict compliance of policies takes the form of threat to the employees.

THANK YOU

