

Cybersecurity Law and Policy

Prepared by
Dr. Kamal Alieyan

Lecture 10



The background features a series of vertical panels with rounded ends. The first panel shows hands typing on a laptop. The second panel has a graduation cap icon. The third panel has a play button icon. The fourth panel has a target icon. The fifth panel has an open book icon. The sixth panel has a magnifying glass icon. The seventh panel has a group of people icon. The eighth panel has a bar chart icon. The title text is overlaid on the right side of these panels.

Introduction to Cybersecurity Policies (2)

Lecture 9

Prepared by
Dr. Kamal Alieyan

Lecture Objective



- 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)

Chapter

09

9.1 CYBERSECURITY POLICY

- 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.

Chapter

09

9.1 CYBERSECURITY POLICY

- 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.

9.1 CYBERSECURITY POLICY

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.

9.1 CYBERSECURITY POLICY

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.

9.1 CYBERSECURITY POLICY

- 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.

9.1 CYBERSECURITY POLICY

- 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.

Chapter

09

9.1 CYBERSECURITY POLICY

- 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.

9.2 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.

9.2 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.

9.2 CYBERSECURITY POLICY MAKERS

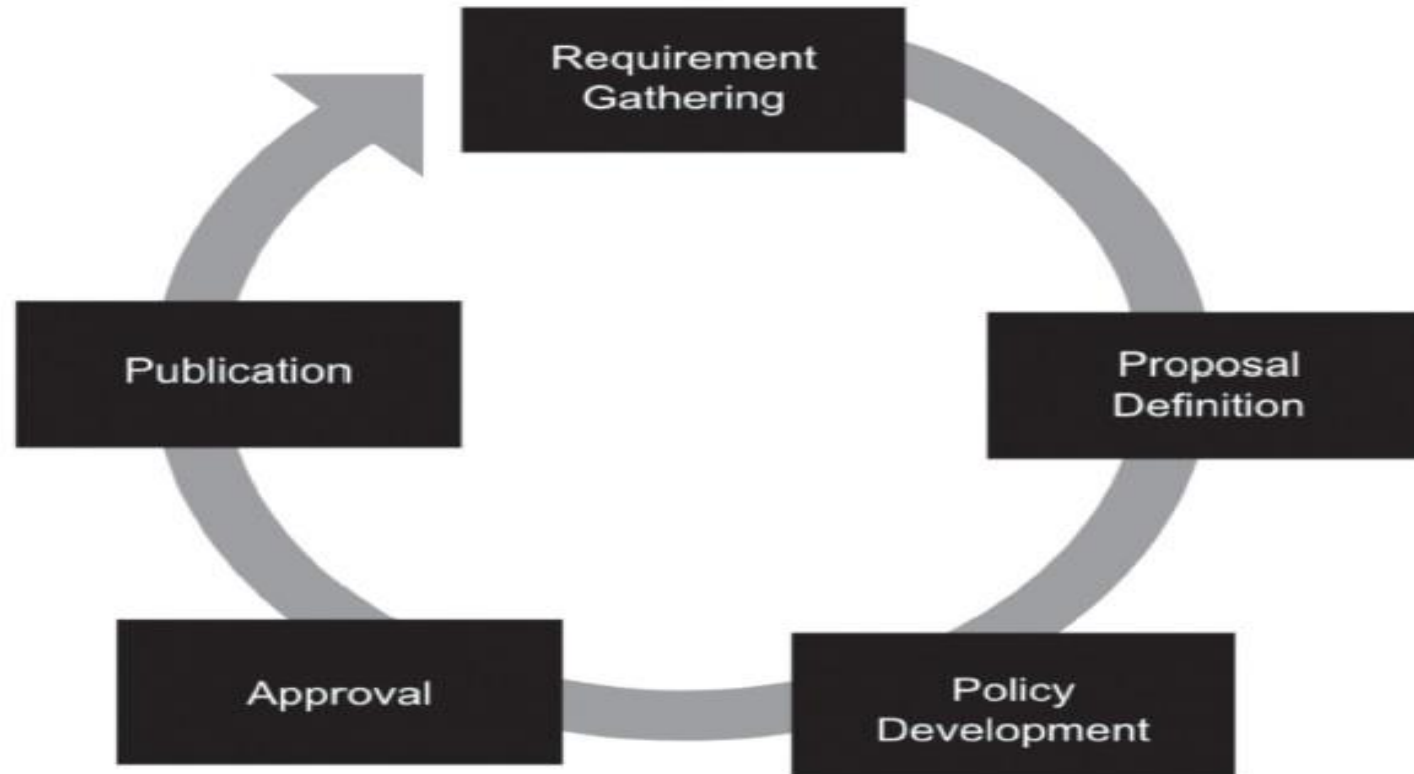


FIGURE 8.1 Security policy development stages.

9.2 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.

9.3 UPDATING AND 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.

9.3 UPDATING AND 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.

9.3 UPDATING AND 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.

9.4 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.

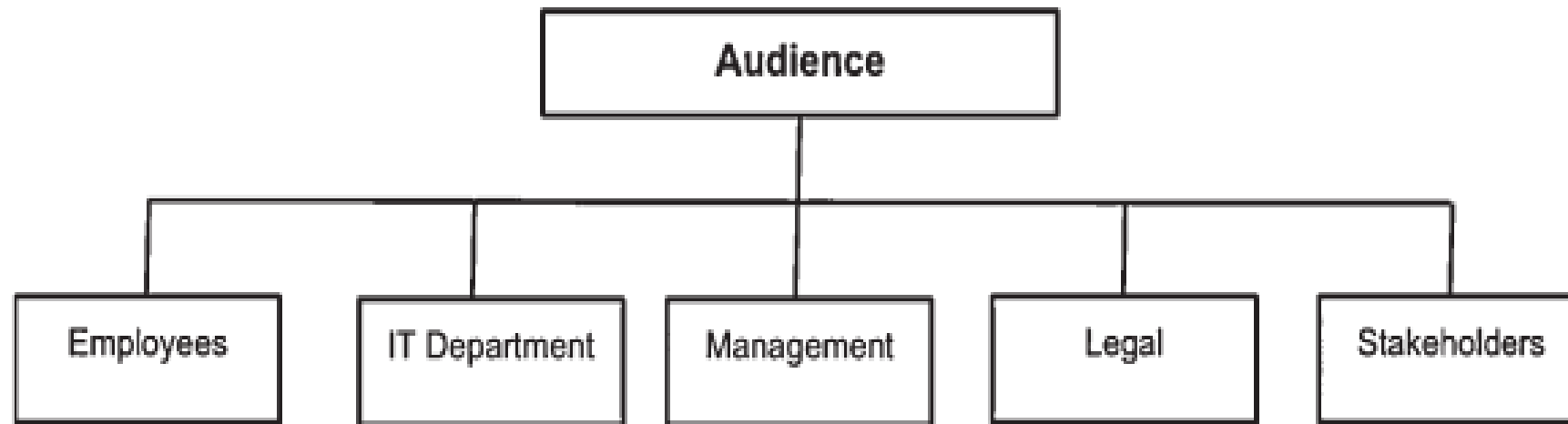


FIGURE 8.2 Cybersecurity policy audience.

9.5 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.

9.5 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.

9.4 CYBERSECURITY POLICY CLASSIFICATION

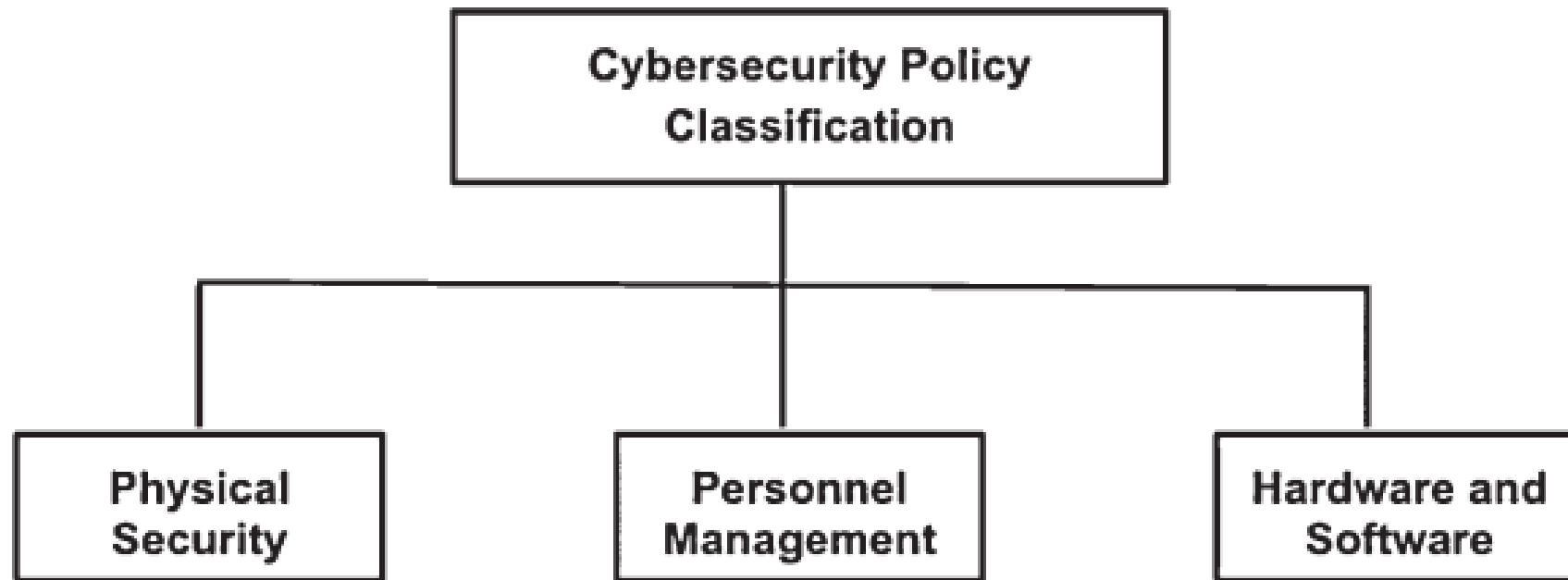


FIGURE 8.3 Cybersecurity policy classification.

Chapter

09

9.6 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.

9.6 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.

9.7 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.

9.7 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.

9.8 CYBERSECURITY POLICY AWAERNESS

- Company employees are often thought of as soft targets to be compromised. This is because the human elements are the least predictable and easiest to exploit.
- Trusted employees may be framed to provide valuable information about a company. Therefore, one of the best methods to combat this exposure of information by employees is cybersecurity training and education.
- It is necessary to make sure that the employees can understand what kind of information they should share and what they must not. This will make the company less vulnerable to risks and cyber-attacks.

- A **good security awareness program** must be conducted periodically. This program must highlight all the current security policies that are commanded to be compliant from employees end.
- Moreover, awareness programs must coordinate correspondence and suggestions to workers about what they ought to and not ought to share with outsiders.
- Hence security policy awareness training and education is necessary for mitigating the threat of information leakage.

Chapter

09

9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES

- Businesses these days run their primary operational processes using cyberinfrastructure.
- As we know, cyber threats and attacks are rising, therefore companies are also investing in better security systems.
- No matter how strong the current cybersecurity plan seems, the reality is that all organizations can possibly be attacked.
- Nowadays, breaches and cyber-attacks are very common. Therefore, there is a need to prepare cybersecurity policies.
- One approach to ensure cybersecurity is to implement the most effective technologies. However, technologies are only effective to a particular extent.
- Technologies are limited to companies and people who are associated with them. Therefore, policy setting and enforcement is a paramount objective for CIOs and Chief Security Officers.

9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES

To write and develop effective cybersecurity policies, the following must be considered :

1. Understanding Own Security:

- Organizations utilize diverse third-party items in various parts of their operations.
- Using an off-the-shelf policy for such products is very common, in spite of the fact that it is not the ideal route for the board to comprehend network security. Instead, organizations must find out what their internal team thinks about their security.
- Essentially, the policy usually comprises mandates made by IT professionals and management. These two parties must analyze the details and need to arrive at a typical decision about the content of the policy.
- Making time as a group to examine policies may assist organizations in understanding the types of information to work with information can be collected and stored.

Chapter
09**9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES**

To write and develop effective cybersecurity policies, the following must be considered :

2. Checking the Compliance:

- Using a security industry standards document is extremely effective in aligning an organization's policy to the recognized standards.
- Additionally, it helps understand all the security compliance requirements in the industry.

3. Considering the Infrastructure:

- A well-planned cybersecurity policy must highlight the systems a business uses to protect its basic and client information.
- An organization needs to work with its IT team to understand the company's capability. This will help evade potential cyber-attacks.
- The policy may explain which programs will be used for security and identify how updates will be made to seal all potential vulnerabilities. It will also help users understand how data may be backed up.

9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES

To write and develop effective cybersecurity policies, the following must be considered :

4. Accountability and its Significance:

- Accountability is one of the most important aspects of ensuring policy. An attack is demanding as it takes time and team effort to manage it.
- Accountability ensures that people become responsible for contacting customers and fixing the problem.
- Accountability measures of an association may likewise incorporate an alternate course of action for cyber-attacks. For example, in a situation where an attack happens and the chief security technician is away, there must be another person to handle the attack.

5. Considering the Employees:

- It is necessary to consider the acceptable use conditions for employees while drafting cybersecurity policies. The smallest of cyber-attacks may be the result of a simple mistake or error made by an employee knowingly or unknowingly. Therefore, an organization must clearly state the best practices for using the company's resources and tools.

9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES

To write and develop effective cybersecurity policies, the following must be considered :

6. Updating Software and Systems

7. Conducting Top-to-Bottom Security Audits:

- It is necessary for organizations to direct a careful security review of its IT resources and practices.
- The audit will be responsible for reviewing the security practices and policies of the central IT systems, as well as the end-user departments and at the edges of your enterprise, which incorporate automated machines and the internet of things (IoT) that an organization could be employing at remote manufacturing plants.
- The audit must take into account the software and hardware techniques the organization needs to ensure better security.
- It should also consider remote site personnel habits and compliance with security policies.

Chapter

09

9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES

To write and develop effective cybersecurity policies, the following must be considered :

8. Social Engineering:

- As part of the end-to-end IT audit, the organization must include social engineering, which reviews whether the employees are exposing loopholes in an organization by exhibiting vulnerability when requested classified data.

9. Demanding Audits from Vendors and Business Partners

10. Providing New and Continuing Security Education:

- Cybersecurity education must be made mandatory for every new employee.

11. Watching the Edge

Chapter
09**9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES**

To write and develop effective cybersecurity policies, the following must be considered :

12. Performing Regular Data Backups:

- In a situation where an organization's data is held hostage or is somehow compromised due to a ransomware attack, a data backup may assist the organization in rolling back to the previous day's data with little loss.

13. Physically Securing the Information Assets:

- Regardless of whether programming, equipment, and system security are set up, it may not support a lot of servers are left unsecured on manufacturing floors and in business units.
- Physical security, which is accessible just to the workforce with trusted status or security clearance, is crucial.
- Security policies and practices must address the physical just as the visual aspects of data.

14. Informing the Board and Chief Executive Officer (CEO)

9.9 WRITING AND DEVELOPING EFFECTIVE CYBERSECURITY POLICIES

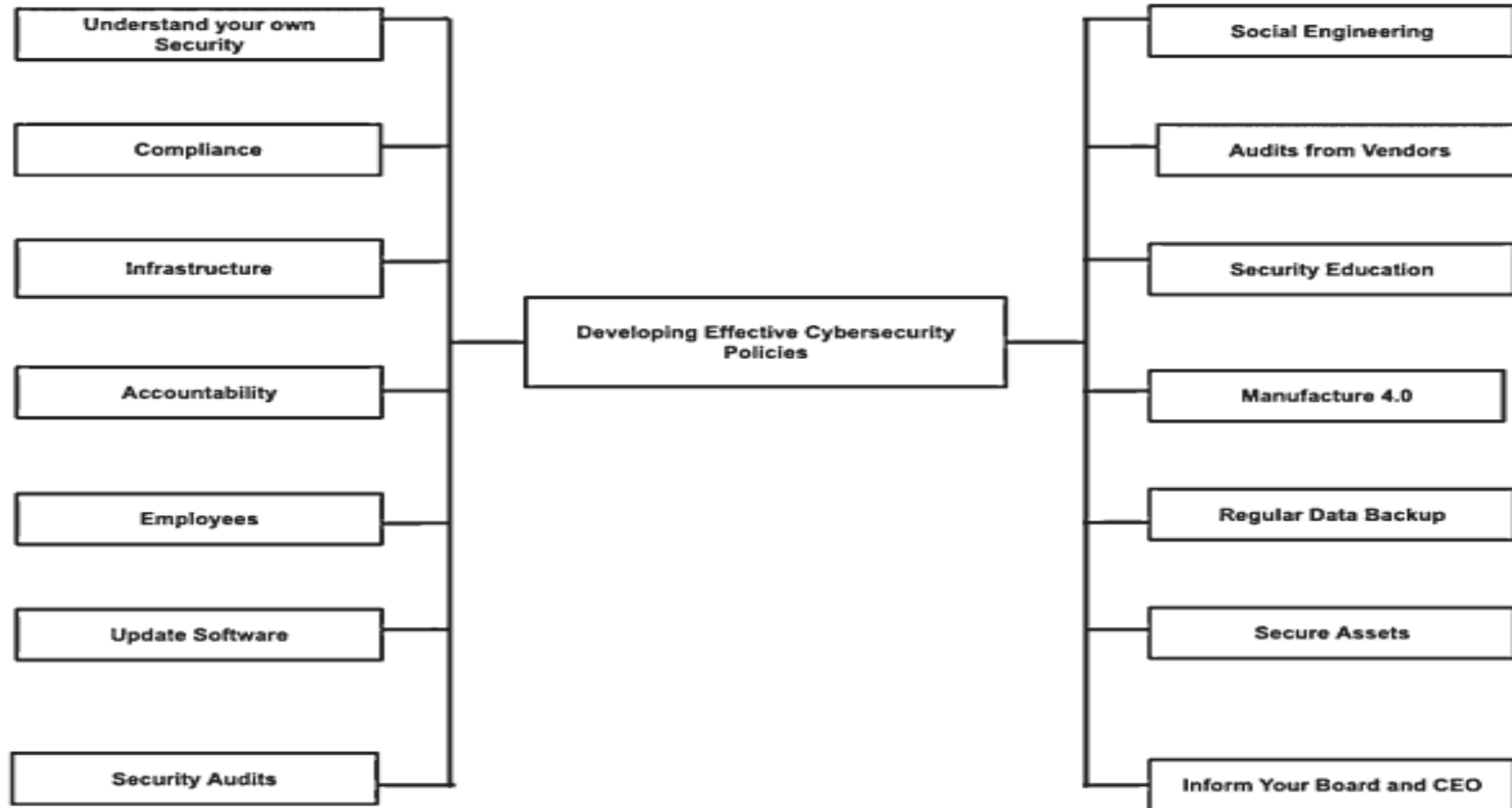


FIGURE 8.4 Developing effective cybersecurity policies.

9.10 TYPES OF CYBERSECURITY POLICIES

- Over time most organizations build and manage security programs.
- To establish the foundation for a security program, companies may first designate an employee to be responsible for cybersecurity.
- This employee will be responsible for drafting a security program which starts with the process of creating a plan.
- The objective of this plan is to manage the company's risk using security technologies and auditable work processes.
- The plan also incorporates documented policies and procedures.
- Security programs are incomplete without policies and procedures.
- Cybersecurity policies can be of many types.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.1 ACCEPTABLE USE POLICY (AUP)

- An acceptable use policy (AUP) or fair use policy, a collection of rules applied by a designer, creator, proprietor, or administrator of a network or website.
- The AUP restricts the manners by which the system, site or framework might be utilized and may have guidelines on how to use these.
- Acceptable use policies are important to the foundation of information security policies.
- New members of an organization are usually asked to sign an AUP before they are given access to its information systems.
- Therefore, an AUP must be concise and clear, yet at the same time, it should cover important **questions on users**, what they are allowed to do with the IT systems and what they are not allowed to do with IT systems.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.1 ACCEPTABLE USE POLICY (AUP)

- The AUP must clearly define the kind of sanctions that will be applied in case a user breaks the AUP.
- The best way to measure and evaluate this policy is by conducting regular audits.
- AUPs must specify imperatives and practices that a worker utilizing organizational IT resources must consent to for accessing the corporate network.
- AUP is basically a standard onboarding policy for new employees who must read and sign the agreement before being provided a network identification.
- It is recommended that organizations IT, security, legal, and HR departments examine what is encompassed in this policy.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.2 ACCESS CONTROL POLICY (ACP)

- Access control pertains to deducing the activities permitted to legitimate users, considering each endeavor by a client to get to an asset in the framework.
- Usually, complete access is granted only after successful authentication of the user.
- Nonetheless, numerous frameworks require more modern and complex control.
- Along with the authentication mechanism, access control deals with how authorizations are organized. In some cases, an authorization may mimic the structure of the organization.
- In other cases, it may be reflective of the sensitivity level of various documents along with the clearance level of the user acquiring those documents.
- In order **to implement an access control system**, organizations need to consider three abstractions: access control approaches, models, and methodologies.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.2 ACCESS CONTROL POLICY (ACP)

- Access control policies (ACP): is a high-level necessities that determine how access is overseen and who may access data under what conditions.
- The ACP features the access available to workers regarding an organization's data.
- ACP incorporates access control standards such as the National Institute of Standards and Technology (NIST's) Access Control and Implementation Guides.
- The policy also mentions network access controls, complexity of corporate passwords, standards for user access, operating system software controls, etc.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.3 CHANGE MANAGEMENT POLICY

- Change management a formal process used for making changes to IT systems.
- Change management is responsible for increasing awareness and understanding of suggested changes across an organization.
- It also ensures that all the modifications made have been thought through and that the change minimizes negative impact on customers and services.
- Change management takes into account the following steps:
 1. **Planning:** Planning the change, which typically includes the execution design, agenda, correspondence plan, test plan, and roll back arrangement.
 2. **Evaluating:** Evaluate the change, which is concerned with determining the risk based on the priority level of service and the nature of the proposed change. It is likewise used to decide the change type, and the change process to utilize.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.3 CHANGE MANAGEMENT POLICY

3. **Reviewing:** Survey change plan with peers and additionally Change Advisory Board as suitable to the change type.
4. **Approving:** Obtain approval of the change by the executives or other appropriate change authority as dictated by change type.
5. **Communicating:** Convey about changes with the suitable gatherings (targeted or campus-wide).
6. **Implementing:** Implement the change.
7. **Documenting:** Document the change and any audit, endorsement data and information related to approval.
8. **Post-Change Reviewing:** Survey the change with an eye to future enhancements.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.4 INFORMATION SECURITY POLICY

- The primary objective of Information security policies is to ensure that all information technology (IT) users that are part of the organization comply with the rules and guidelines with respect to security of information.
- This information is stored digitally in the network.
- It is issued by the company for ensuring that all employees who rely on IT assets within the organization, or its networks, observe the stated rules and guidelines.
- Often employees are asked by the organization to sign a document acknowledging that they will be reading it.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.4 INFORMATION SECURITY POLICY

- This policy is intended for **workers** to understand that they might be considered responsible with respect to sensitivity of the corporate information and IT assets, considering some specific rules.
- Every organization is responsible for protecting its data and controlling its distribution both within and outside the organization.
- For data protection, several techniques may be adopted ranging from encryption of information to authorization by a third party or institution.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.5 INCIDENT RESPONSE (IR) POLICY

- Incident response (IR) policies are responsible for providing an understanding about dealing with certain incidents.
- It is required that the policy identifies an IR team, who must be notified of issues.
- The IR team must also have the knowledge and skills to deal with the issues effectively.
- Some of these issues are viruses, critical system failures, issues relating to unauthorized access, unauthorized changes to systems or data, denial or disruptions of service, or attempts to breach the policies, etc.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.5 INCIDENT RESPONSE (IR) POLICY

- An IR policy must also outline who is responsible for specific tasks in situations of a crisis.
- It may also include related information like:
 - ☐ Who will be responsible for the investigation or analysis of incidents to determine the occurrence of the incident as well as the resulting consequences?
 - ☐ Which individuals or departments will be responsible for fixing specific issues and restoring the system?
 - ☐ Handling of certain incidents.
 - ☐ References to other documentation.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.6 REMOTE ACCESS POLICY

- Remote access policy is a document that highlights and mentions acceptable methods of remotely associating with the internal network of an organization.
- It is useful in large organizations since the networks are dispersed geographically.
- Sometimes these networks extend into insecure network locations like public networks and unmanaged home networks.
- The policy considers every single accessible strategy for remotely accessing internal assets:
 - ☐ Dial-in (serial line internet protocol (IP), point-to-point protocol).
 - ☐ Integrated service digital network/frame relay.
 - ☐ Telnet access from the internet.
 - ☐ Cable modem.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.7 EMAIL/COMMUNICATION POLICY

- A company's email policy may be defined as a document that specifies how representatives can utilize the business' selected electronic correspondence medium.
- This policy incorporates emails, blogs, social media, and chat technologies.
- This policy is responsible for providing rules to representatives on what is viewed as the acceptable and unacceptable utilization of any corporate correspondence technology.
- A viable email strategy will support positive, gainful correspondences while shielding an organization from lawful obligation, reputation damage, and security breaches.
- The following are some guidelines for email policy.
 - ☐ Emails are for business use.
 - ☐ Emails are company property.
 - ☐ Email policy should address company network and security.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.8 DISASTER RECOVERY POLICY

- The CISO and teams manage an incident through the IR policy. The business continuity plan (BCP) gets activated in a situation where an event has a significant business impact.
- The essential goal of this policy is to decide the key methods and resources basic for maintaining minimum business capacities after a catastrophe.
- Some of the best practices to consider for this policy are:
 1. **Preparing for Physical Disasters:** Many companies offer alternative workspaces like desks, computer hardware, and phone/ Internet access so that business can continue running.
 2. **Protecting Against Cyber Disasters:** Cyber disasters typically include major incidents like ransomware attacks and data loss from breaches. For protection against these, the layers of security must include a firewall with Intrusion Detection System/Intrusion Prevention System and solid host-based endpoint protection.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.8 DISASTER RECOVERY POLICY

3. **Ensuring redundancy to eliminate single point of failure.**
4. **Assigning Responsibilities:** Assigning responsibilities to people who will lead initiatives like purchasing new equipment, coordinating alternative office space, and communicating with senior management, clients, and the press is a must.
5. **Testing and reviewing** the disaster recovery plan periodically.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.9 BUSINESS CONTINUITY PLAN (BCP)

- This policy is responsible for the protection of personnel and assets so that they can function efficiently in the event of a disaster.
- Risk may incorporate catastrophic events or natural disasters like fire, flood, or weather-related events, and cyber-attacks.
- After identification of the risks, the plan must:
 - ☐ Determine how the risks can affect operations.
 - ☐ Implement safeguards and procedures for mitigate the risks.
 - ☐ Test procedures to ensure they function.
 - ☐ Review the process to ensure that it is up to date.

9.10 TYPES OF CYBERSECURITY POLICIES

9.10.9 BUSINESS CONTINUITY PLAN (BCP)

- BCPs are an indispensable part of any business. Threats and disruptions may lead to loss of revenue and higher costs, the consequence of which is a drop in profitability.
- Businesses cannot rely on insurance alone since it cannot cover all the costs and the customers who move to the competition.
- The BCP is responsible for coordinating efforts across the organization. It uses the disaster recovery plan for restoring equipment, applications, and information regarded necessary for business coherence.
- BCP's are exceptional to every business. This is because they describe how the organization will operate in the situation of an emergency.

9.10 TYPES OF CYBERSECURITY POLICIES

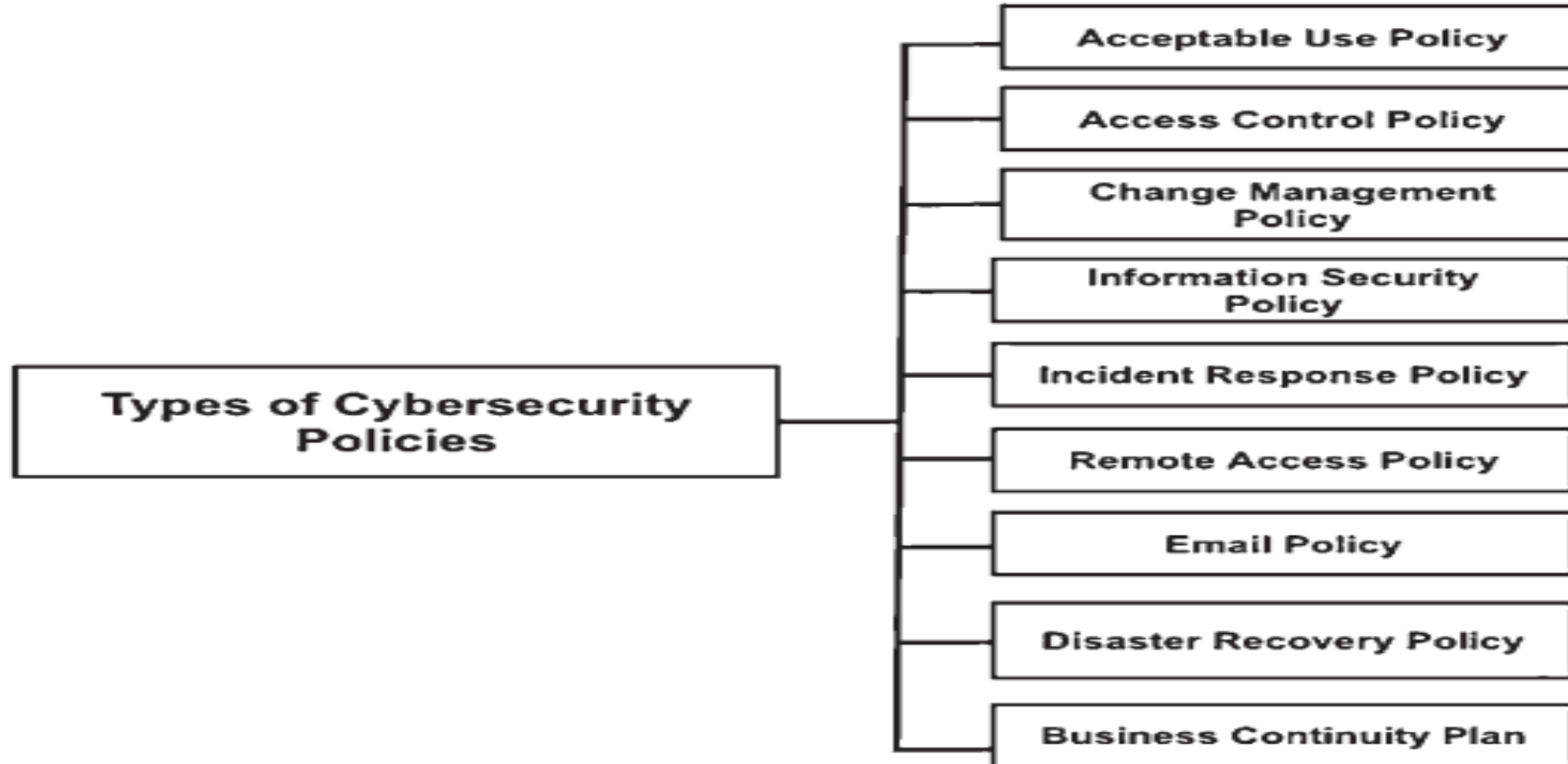


FIGURE 8.5 Types of cybersecurity policies.

9.11 CYBERSECURITY FRAMEWORKS (CSFS)

- A **CyberSecurity Framework (CSF)** defined as a collection of reported methodologies used to characterize policies and procedures with respect to the usage and continuous management of data security controls in an enterprise environment.
- Since CSFs are prioritized, flexible, and cost-effective, they help in promoting the security and flexibility of critical infrastructure (CI) and different sectors critical to the economy and national security.
- Frameworks have been around for quite a while. In financial accounting, frameworks have been used for assisting accountants to monitor monetary exchanges. An accounting framework is worked around ideas like resources, liabilities, expenses, and controls.
- Cybersecurity structures adopt the framework strategy to the work of securing resources.
- The system is created for giving security managers a reliable and systematic way to mitigate cyber risk despite the complex environment.

9.11 CYBERSECURITY FRAMEWORKS (CSFS)

- CSFs are usually compulsory, or if nothing else firmly encouraged, for organizations that need to conform to state, industry, and worldwide cybersecurity guidelines.
- Frameworks can be of a few sorts like:
 1. **Control Frameworks:** These are responsible for developing a basic strategy for the security team. They provide a baseline set of controls and assess the current technical state. These frameworks prioritize control implementation.
 2. **Program Frameworks:** These assess the state of the security program. They are responsible for building a comprehensive security program. They also measure program security/competitive analysis. These frameworks also assure simplified communication between the security team and business leaders.
 3. **Risk Frameworks:** These characterize key process steps to survey/ oversee risk. They structure programs for risk management. Additionally, they can identify, measure, and quantify risk. They prioritize security activities.

9.12 SOME CYBERSECURITY FRAMEWORKS (CSFS)

- A We have familiarized ourselves with the concept of CSFs and their requirements in the Cyberspace.
- While these frameworks vary according to the organizations they are deployed in, there are some frameworks that have been considered very effective over the last few decades.
- In this section, we will be present some of cybersecurity frameworks.

9.12 SOME CYBERSECURITY FRAMEWORKS (CSFS)

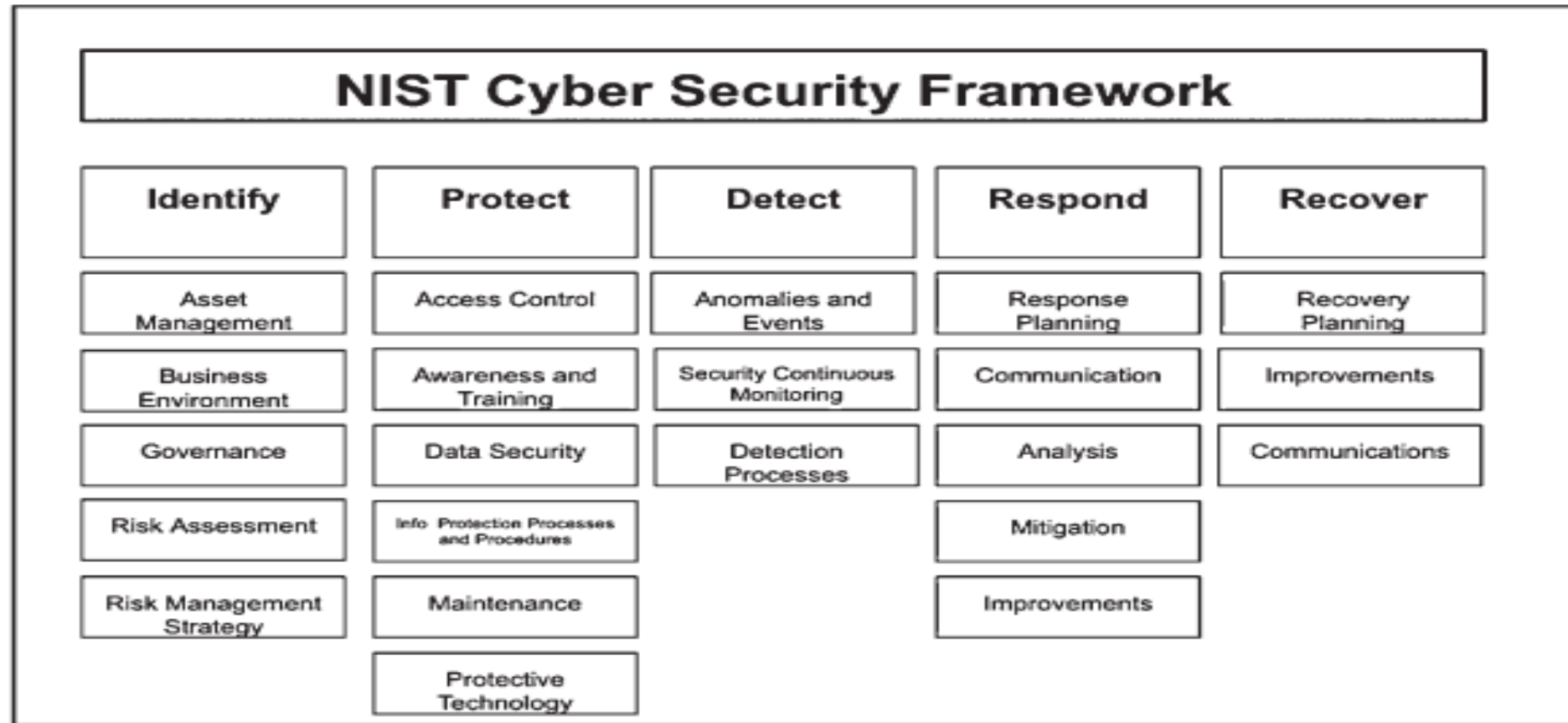


FIGURE 8.7 NIST cybersecurity framework.

9.12 SOME CYBERSECURITY FRAMEWORKS (CSFS)

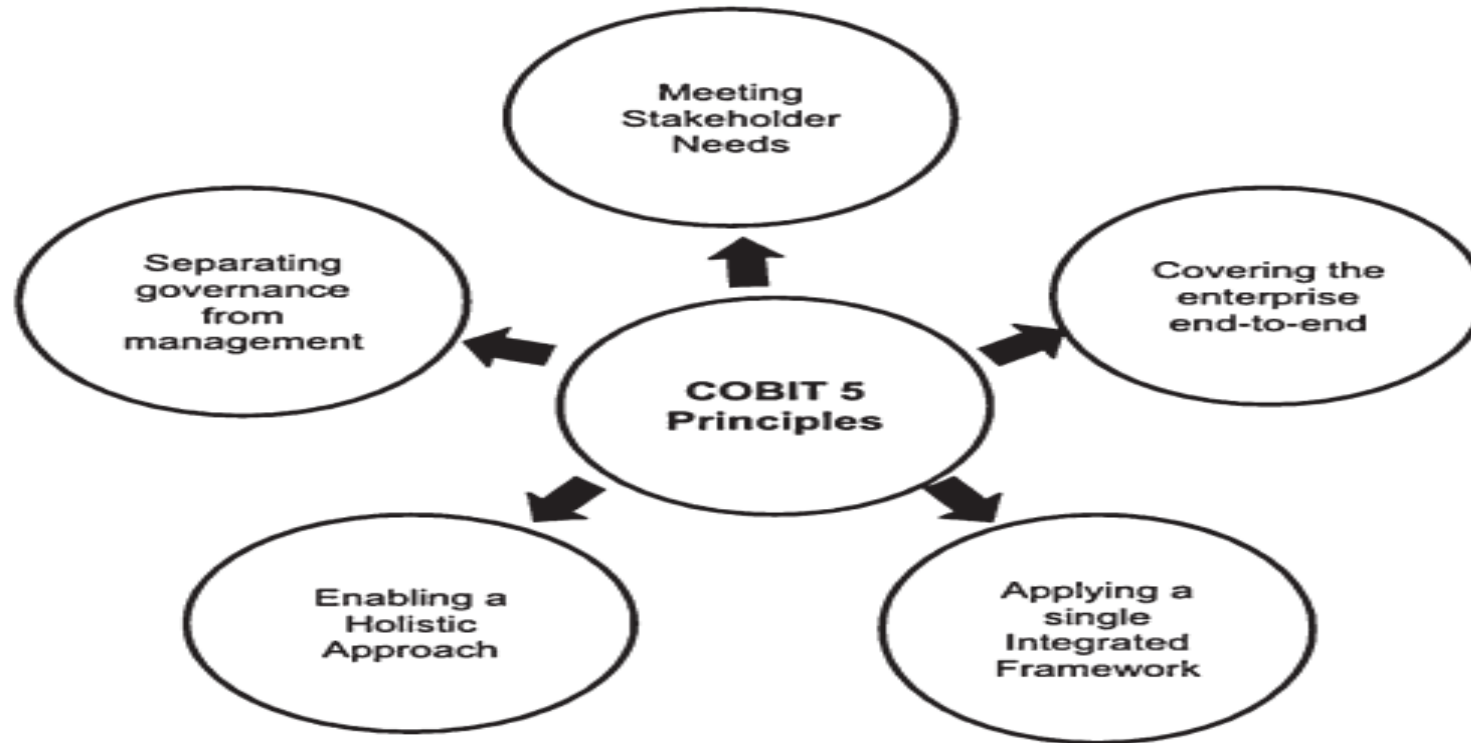


FIGURE 8.8 COBIT 5 principles.

9.12 SOME CYBERSECURITY FRAMEWORKS (CSFS)

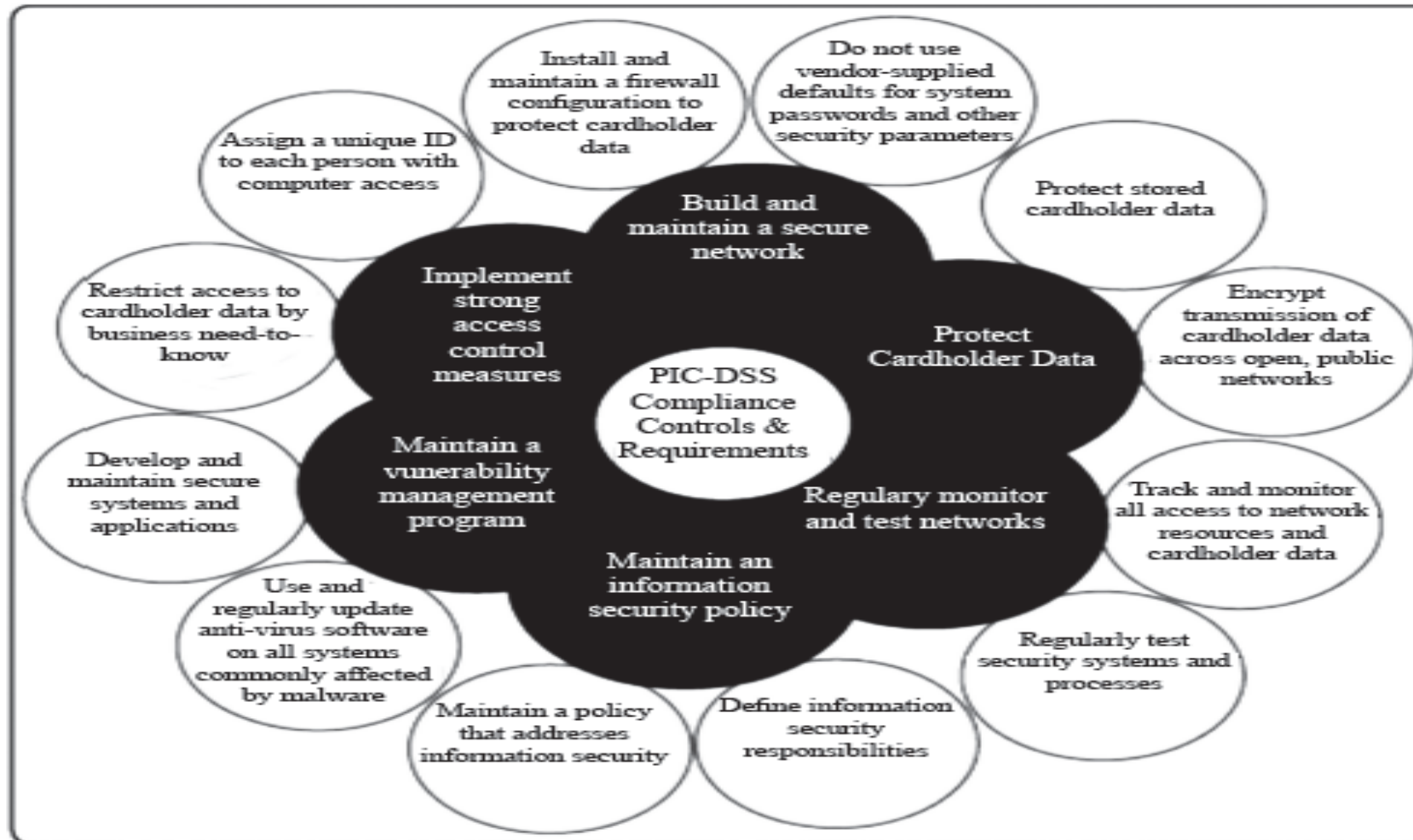


FIGURE 8.15 PCI DSS cybersecurity framework.

9.12 SOME CYBERSECURITY FRAMEWORKS (CSFS)

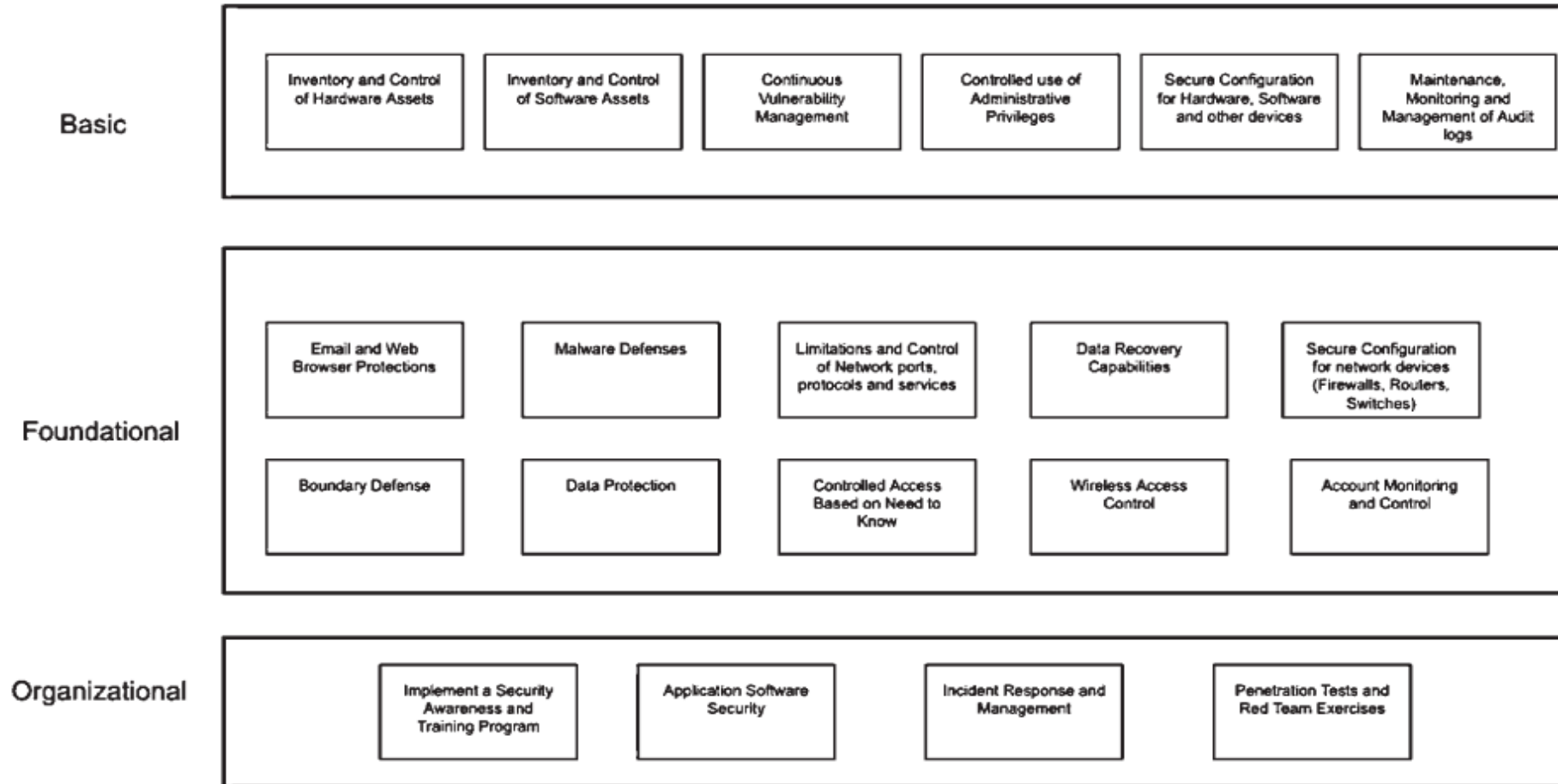


FIGURE 8.16 CIS critical security controls.



Thank You