Chapter 4: Information Security Policy

Gonzalo De La Torre Parra, Ph.D.

Fall 2021

Objectives

- Define information security policy and discuss its central role in a successful information security program
- List and describe the three major types of information security policy and discuss the major components of each
- Explain what is necessary to implement effective policy and what consequences the organization may face if it does not
- Discuss the process of developing, implementing, and maintaining
- various types of information security policies

Case Opener

- Iris was returning from lunch when she ran into Susan Weinstein, one of RWWs senior account executives, who was accompanied by a man Iris didn't know. Susan introduced him as Bob Watson, a prospective client. As they were chatting, Iris noticed Bob's distracted demeanor and Susan's forced smile and formal manner.
- We didn't get the account, Iris real ized.
- A few minutes later, she saw why the meeting between RWW's account executive and prospective client did not go well. In the cubicle across the hall from Susan's office, two programmers were having lunch. Tim had his feet propped up on the desk. In one hand was a half-eaten hamburger; in the other, he held several playing cards. John had made himself comfortable by taking off his shoes. Teetering over an array of a laptop, tablet, and smartphone was a jumbo soft drink threatening a flood of sugary soda water that could inundate the desk.

Case Opener Cont.

- Iris went into her office and pulled up the company's policy manual on the company’s intra net. She was familiar with most of RWW's policies, but for the actions she had in mind, she needed specifics. But RWWs policy and procedure manual did not contain policies about alerting employees to meetings with prospective clients, or playing cards or eating and drinking in the workplace. What was most disconcerting, though, was that it didn't even contain specifics about practices that supported data protection and other information security objectives.

Case Opener Cont.

- Before Iris left that evening, she typed up her notes and scheduled an early morning meeting with her boss, Mike Edwards. As she left for home, she thought, Tim and john playing cards and eating in their office may have cost us a new account. I'll suggest to Mike that it's time for us to reconvene the policy review committee.

What is a policy?

- In business, a statement of managerial intent designed to guide and regulate employee behavior in the organization; in IT. a computer configuration specification used to standardize system and user behavior.
- A manager's or other governing body's statement of intent; as such, a policy (document) actually contains multiple policies (statements).
- Information Security: The document version of the term policy
- Information Technology: computer system configuration.

Information Security Policies

- Written instructions provided by management that inform employees and others in the workplace about proper behavior regarding the use of information and information assets.

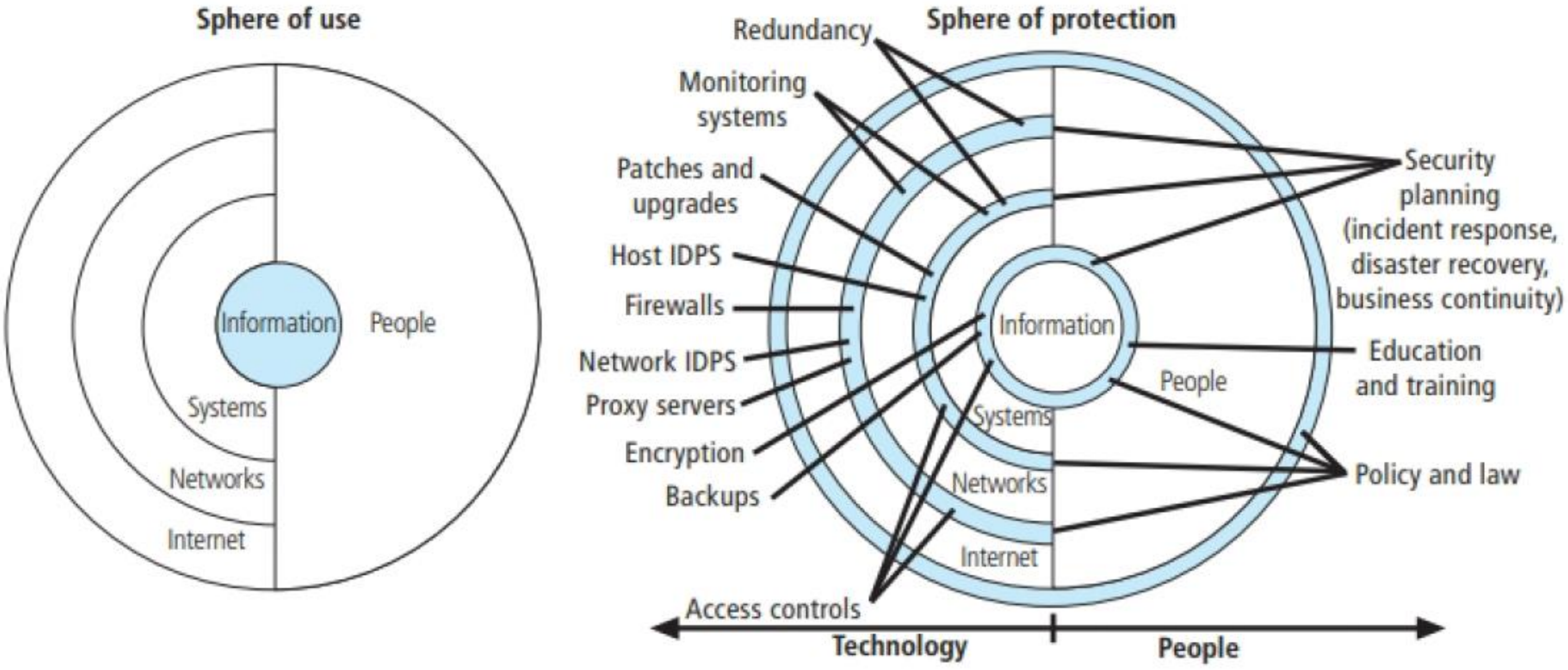
Why do we need a policy?

- A quality information security program begins and ends with policy.
- Information security policies are designed to provide structure in the workplace and explain the will of the organization's management in controlling the behavior of its employees with regard to the appropriate and secure use of its information and information resources. Policy is designed to create a productive and effective work environment, free from unnecessary distractions and inappropriate actions.

Importance of a policy

- A policy may be one of the very few controls or safeguards protecting certain information.

Spheres of Security

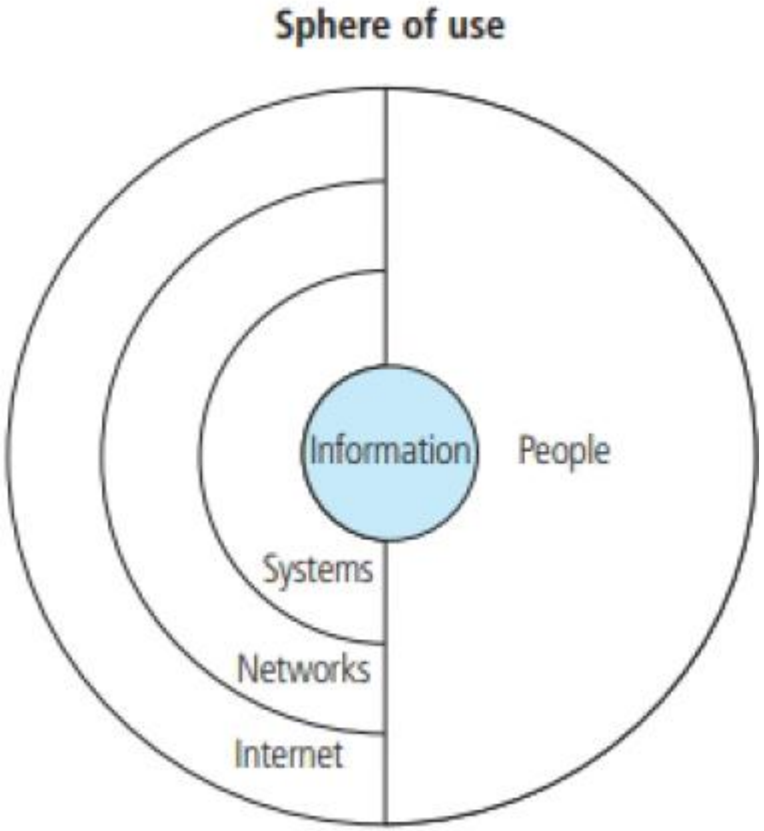


Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

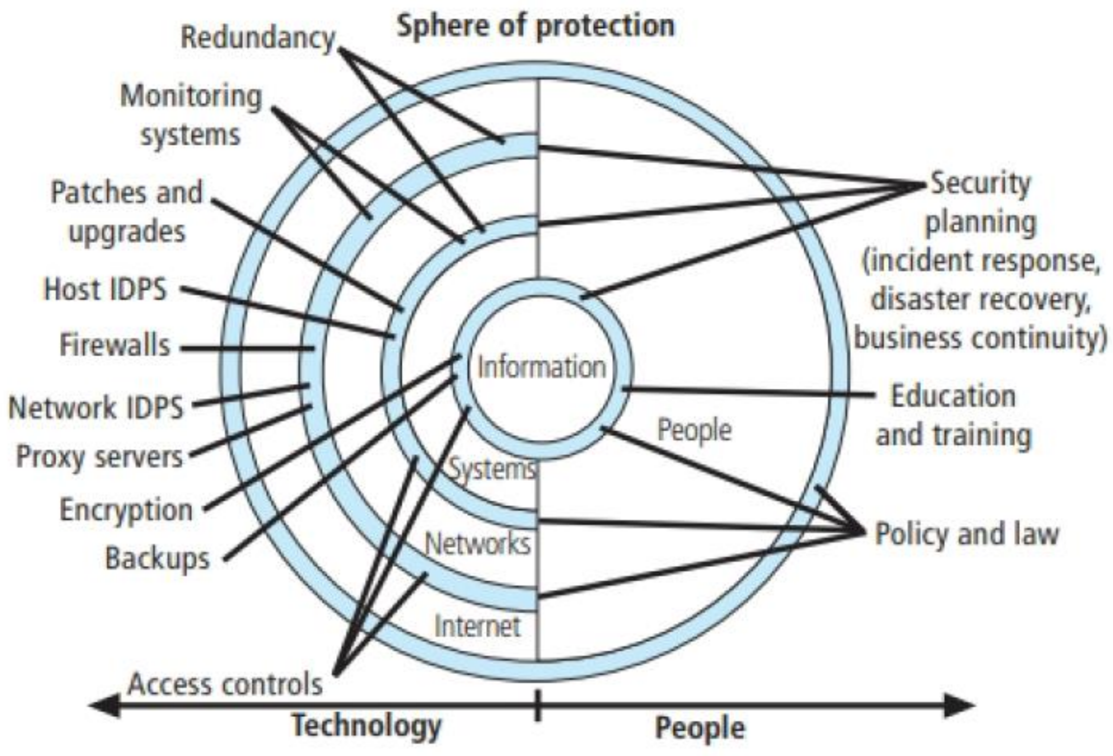
Figure 4-1 Spheres of security

Sphere of Security

- To access information from outside the organization, people must traverse the Internet and go through the organization's perimeter defense (gateway, firewalls, and routers), across the organization's network, into the organization's computer systems, and finally onto the drives physically storing that information.
- This gives the organization several defense points, attack axes, or avenues of approach (however you wish to describe it) it can use to place defensive control safeguards.



- People within the organization, especially employees, unfortunately have much less restricted access to many forms of information, especially when it is in physical form.
- Some access is a direct function of people's job requirements, and other forms are an indirect result of physical access to internal locations, such as meeting rooms, supervisors' offices, and administrative support facilities (including the copy room and mailroom).



Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

Basic rules must be followed when developing a policy

- Policy should never conflict with law.
- Policy must be able to stand up in court if challenged.
- Policy must be properly supported and administered.

Enron scandal (2001)

- The management team at Enron Energy Corporation was found to have lied about the organization's financial records, specifically about reported profits.
- The management team was also accused of a host of dubious business practices, including concealing financial losses and debts.
- The depth and breadth of the fraud was so great that tens of thousands of investors lost significant amounts of money and at least one executive committed suicide rather than face criminal charges.

Arthur Andersen (Accounting Firm)

- Andersen's auditors and information technology consultants claimed that this shredding of working papers was in accordance with Andersen’s established policy.
- The former chief auditor from Andersen was fired after an internal probe revealed that the company shredded these documents, and deleted e-mail messages related to Enron, with the intent to conceal facts from investigators. He pleaded guilty to obstruction of justice, which carries a maximum sentence of 10 years in prison.

Lessons learned?

- An organization must conform to its own policy and that policy must be consistently applied.

IT Policy and Info Sec Policu guidelines

- All policies must contribute to the success of the organization.
- Management must ensure the adequate sharing of responsibility for proper use of information systems.
- End users of information systems should be involved in the steps of policy formulation.

The bullseye model

- An implementation model that emphasizes the role of policy in an InfoSec program.
- Because it provides a proven mechanism for prioritizing complex changes, the bull's-eye model has become widely accepted among InfoSec professionals.
- Issues are addressed by moving from the general to the specific, always starting with policy.
- Focus is on systemic solutions instead of individual problems.

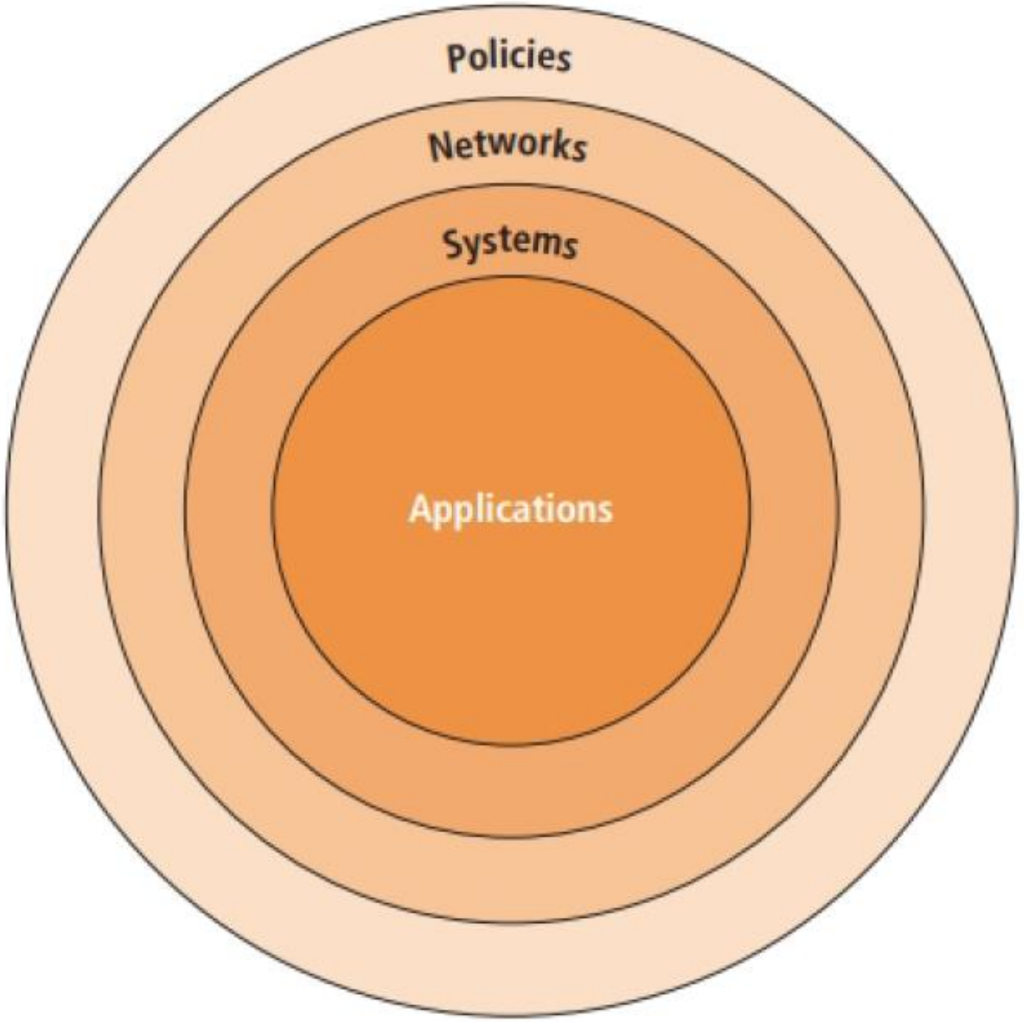


Figure 4-2 Bull's-eye model

The bullseye model

- Policies- This is the outer layer in the bull's-eye diagram, reflecting that it is the initial viewpoint that most users have for interacting with InfoSec.
- It is available from the published documents that express the will of management and seeks to guide user behavior.

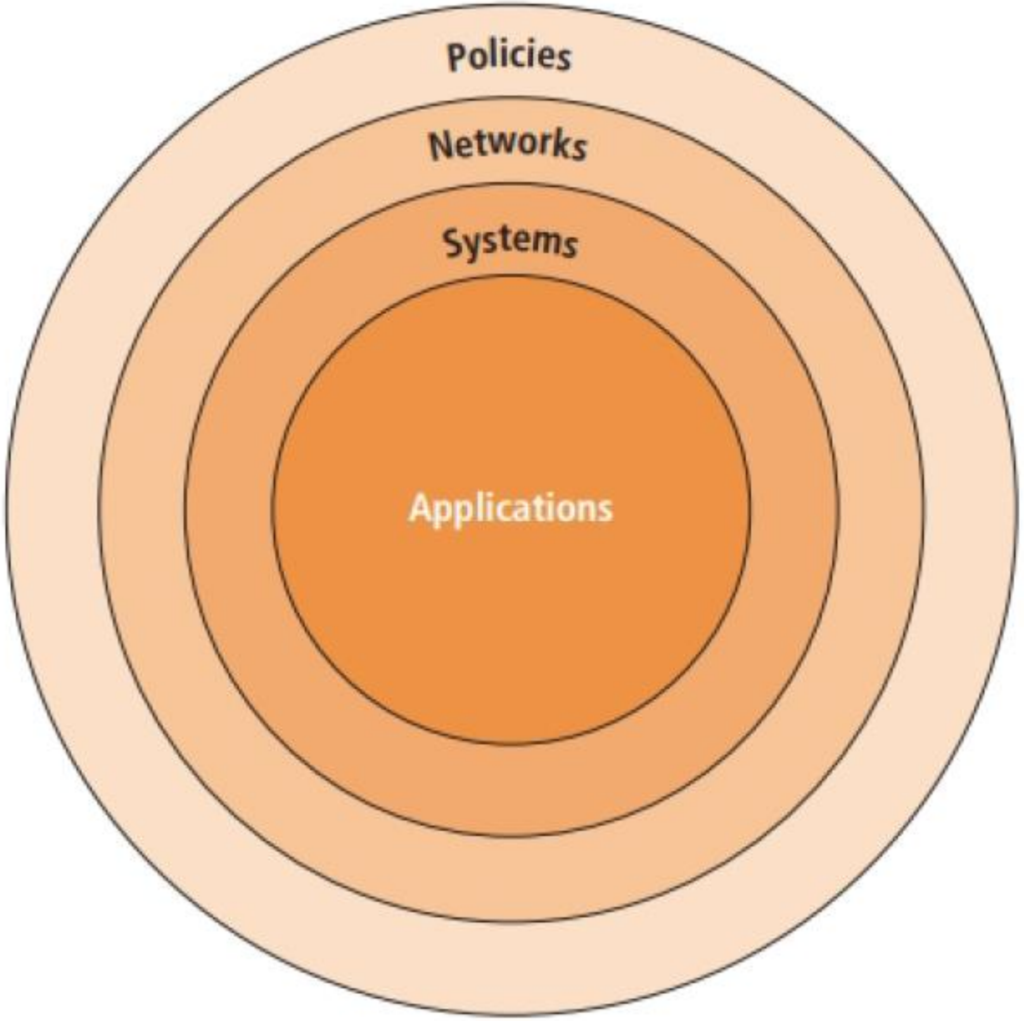


Figure 4-2 Bull's-eye model

The bullseye model

- Networks- This is the environment where threats from public networks meet the organization's networking infrastructure.
- In the past, most InfoSec efforts focused on networks. Until recently, in fact, InfoSec was often thought to be synonymous with network security.

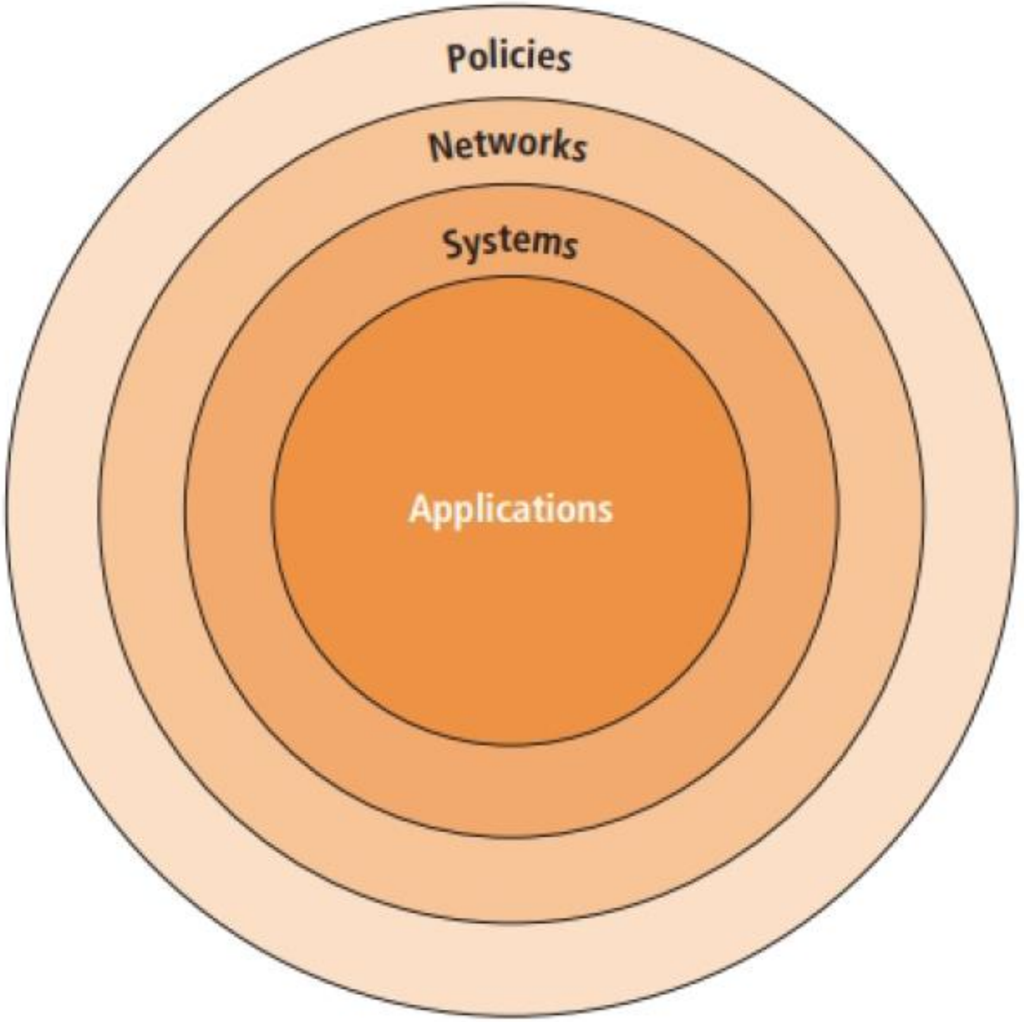


Figure 4-2 Bull's-eye model

The bullseye model

- Systems- These are the collections of hardware and software being used as servers or desktop computers as well as those systems used for process control and manufacturing systems.

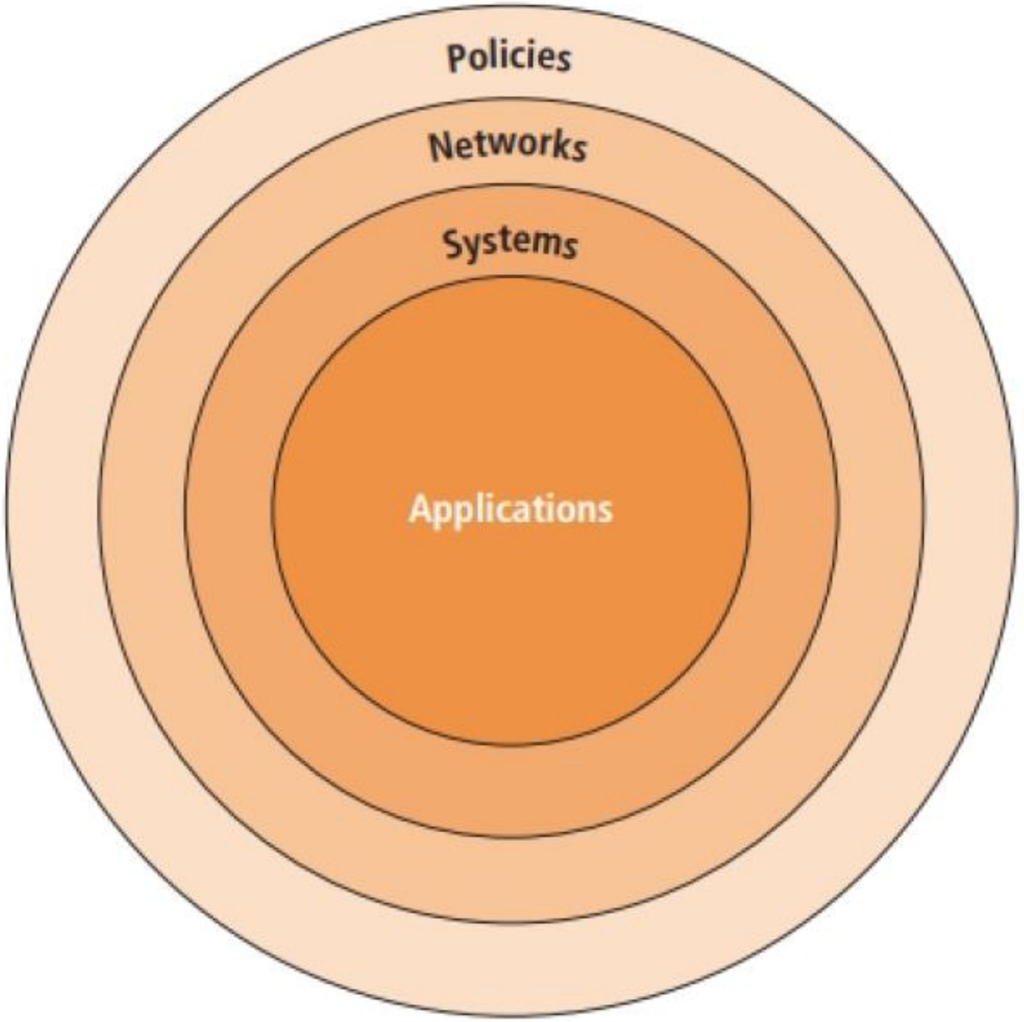


Figure 4-2 Bull's-eye model

The bullseye model

- Applications- These are the application systems, ranging from packaged applications, such as office automation and e-mail programs, to high-end enterprise resource planning (ERP) packages to custom application software or process control applications developed by the organization.

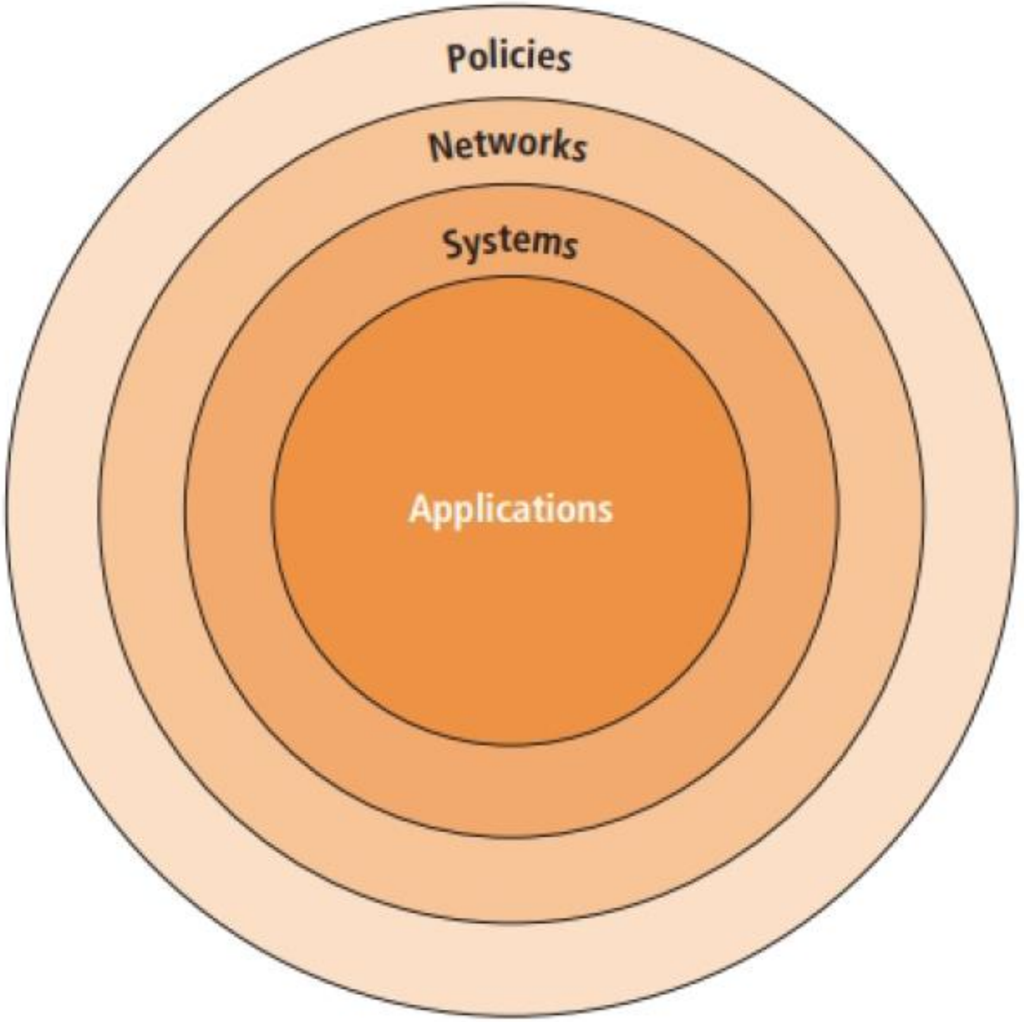


Figure 4-2 Bull's-eye model