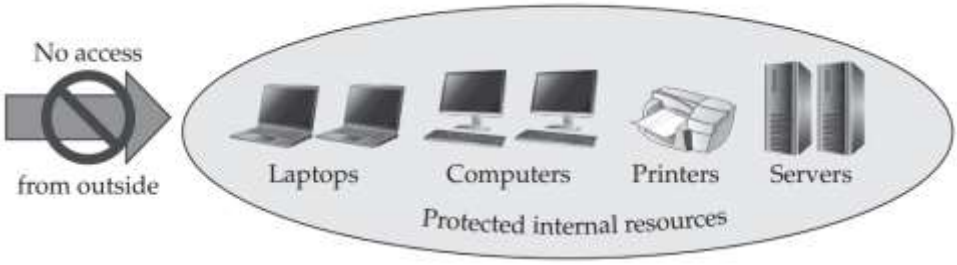
The Importance of Information Security

Information is an important asset. The more information one can have at command, the better one can adapt to the world around. Information can be classified into different categories. This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse. Organizations typically choose to deploy more resources to control information that has higher sensitivity.

Companies may have **confidential information**, such as research and development plans, manufacturing processes, strategic corporate information, product roadmaps. Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company. This type of information is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement (NDA) or equivalent obligation of confidentiality.

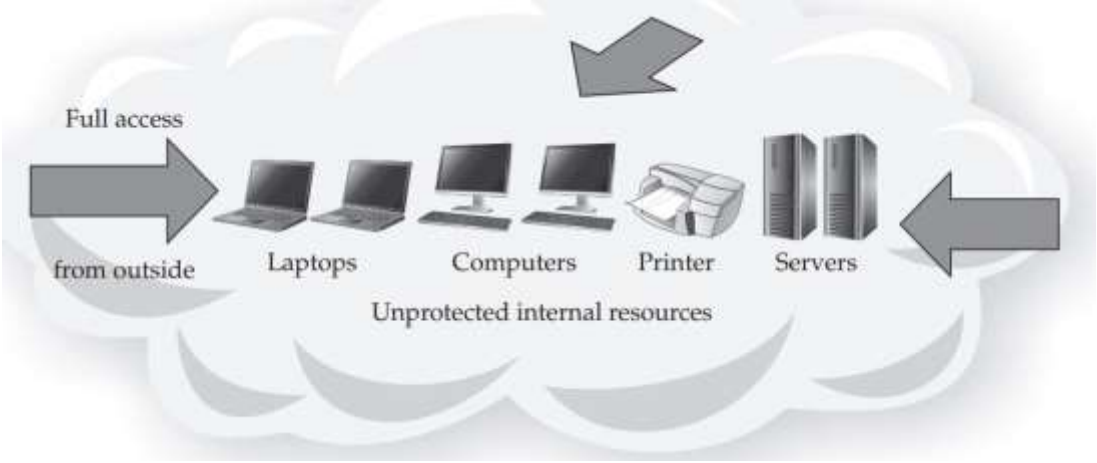
Specialized information or secret information may include trade secrets, proprietary methodologies and practices. If disclosed, this type of information may severely damage the company's competitive advantage. It is usually restricted to only a few people or departments within a company and is rarely disclosed outside the company.

In the early days of networking, individual computers were connected together only in academic and government environments. Thus, at that time, the networking technologies that were developed were specific to academic and government environments. Originally, the **academic security model** was "**wide open**" and the **government security model** was "**closed and locked**."



Original government perimeter blockade model

The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data (for example, by shielding equipment to prevent electromagnetic radiation from being intercepted). This method of protecting assets provided a hard-to-penetrate perimeter.



Original academic open-access model

In the academic world, the goal was to share information openly, so security controls were limited to accounting functions in order to charge money for the use of computer time.

When businesses started to widely embrace the Internet as a sales channel and business tool, a new security model was required. A closed-door approach doesn't work when thousands or millions of people need to have access to the services on network. Likewise, an open-door approach doesn't work for the protection of the privacy of each individual who interacts with the services on the network. E-commerce and business required a more blended approach of providing limited access to data in a controlled fashion, which is a more sophisticated and complex approach than that used by the earlier security models.

As the use of information technologies evolved, the original all-or-nothing approaches to security no longer met the needs of information consumers. So, the practice of network security evolved.

Security implementations that solve specific business problems and produce results that are consistent with clearly identified business requirements produce tangible business benefits by reducing costs and creating new revenue opportunities. Companies that provide access into their network under control allow employees and customers to work together more effectively, enabling the business. Security both prevents unwanted costs and allows greater business flexibility. Thus, security creates revenue growth at the same time as controlling losses.

Security can be thought of in the context of the three Ds: defense, detection, and deterrence—each of which is equally important. Defense reduces misuse and accidents, detection provides visibility into good and bad activities, and deterrence discourages unwanted behavior. A security program that employs all three Ds provides strong protection and therefore better business agility. Strategies are used to manage proactive security efforts, and tactics are used to manage reactive security efforts. Together, well designed security strategy and tactics result in an effective, business-driven security program.