Tool Descriptions:

	**User Training:** This often makes the difference between success and failure of an overall security strategy because users are positioned to be the first line of detection for many attacks. A well-trained user base will be able to recognize when something unusual is occurring, know what to do, and how to report the security problem to those who can investigate further. Training is automatically placed for you in their labeled locations separately from your network diagram.
	**Redundant System**: Duplicated critical portions of your network hardware and software and are typically maintained in "standby" status or even in parallel operation during normal system operation. In the event of a successful attack on your network (or other system failure), redundant system function will independently permit rapid restoration of your networks operation. Redundant systems are placed automatically for you in their labeled locations separately from your network diagram.
	**Access Control**: Restricts access to your Information System resources to those users, programs, processes, and other systems that have specific authorization for their use. Access control is placed on the server.
	**Anti-Virus Program**: Anti-virus safeguards include prevention, detection, containment, and recovery measures. The anti-virus program represents a combination of procedures and software that detects and removes most known viruses. Anti-virus protection is placed on the server and individual workstations.
	**Backups**: These are hardware, software, and procedures used to mitigate the consequences of accidental, natural, or manmade damage that can affect your network and users. In using the backup defensive tool, copies of files and programs are maintained and updated to facilitate systems and information recovery. Backups are placed on the server and individual workstations.
	**Disconnection**: This is a combination of hardware and software that denies external attackers (or the effects of their attack) entrance to a network through the link protected by disconnection capability. This permits continued functioning of your information systems exclusive of that link. Disconnection features are placed on routers.
	**Encryption**: This converts, by means of a cryptographic system, original information (plain text) into transformed information (cyphertext), for transmission over one of your external links. Cyphertext usually has the appearance of random, unintelligible data. Without the method to decrypt the encrypted data, this information is of little use to an attacker. Encryption is placed on routes.
	**Firewall**: This limits access for information transfer between networks in accordance with local security policy. Your firewall protects your network integrity by controlling information flow over networks external linkages, thus restricting external access to your network. Firewalls are placed on the external links of the routers being protected.
	**Intrusion Detection Software**: Collects data on user (and intruder) activity and performs analyses to detect security attacks, unauthorized activity, and network abuse. Intrusion Detection is designed to give you real-time warning and may automatically react to any computer misuse it detects. Intrusion Detection is placed on the server.

Other Installation

Headquarters

Other Installation

Internet

Router

Router

Server

Dept. Lan

Dept. Lan

Router

Dept. Lan

Department Lan

Printer

User Training

Redundant Systems

Other Installation

Headquarters

Other Installation

Internet

Router

Router

Dept. Lan

Server

Department Lan

Printer

User Training

Redundant Systems

Router

Dept. Lan

Dept. Lan

Tool	Workstation	Server	Router	Universal
Access Control	x			
Antivirus	x	x		
Backups	x	x		
Disconnection			x	
Encryption			x	
Firewall			x	
Intrusion Detection	x			
Redundant System				x
User Training				x

Strategy	Description
Allocation Policy	Networks are subject to a wide spectrum of possible security threats, from corporate espionage, to curious browsing to malicious hacking, and criminal fraud. When allocating Resource Units, one viable strategy is to select a wider range of defenses at lower and less costly effectiveness ratings during you first quarter and plan to upgrade in the future when more RUs are available.
Mitigation Tools	No defense can be one hundred percent effective. Sooner or later, your information system will be successfully attacked, and when that happens, the best you can hope for is to minimize the effects of attack on your system. There are three particular tools that can mitigate these effects and speed the restoration of network operations: Backups, User Training, and Redundant Systems.
Prevalence of Viruses	Many information system security experts believe that the most prevalent threat to information systems is a virus attack. Therefore, you would be wise to acquire the most effective Antivirus tool you can afford. For best effect, use the Antivirus defense first on your network's server and then, as more RUs become available, place additional Antivirus tools on individual workstations.
Value of Training	Trained users are your first line of defense for your information system's security. User Training is more than instruction on the use of hardware and software. Users who understand and employ good security policies and practices will be better able to recognize potential security problems and react appropriately when problems occur. In addition to preventing some attacks from succeeding, having well-trained users can mitigate the consequences of attacks and may even make certain types of attack -- particularly virus attacks-- less likely to occur.
Trust Relationships	Today's information systems environment is a sprawling, decentralized collection of networks crossing numerous organizational boundaries. Critical to your information system's operation in this environment are the trust relationships you establish between your network and others'. These trust relationships may be formal, specified by policy or directive, like your relationship to another installation; or they may be informal, built on personal relationships with other system administrators, perhaps colleagues in charge of other networks at your own installation. There will also some network connections, such as the Internet, in which you should have no trust at all. The less trusted the system, the more important it is to have extensive, higher grade defenses in place.
Network Security Priorities	As a System Administrator or Security Officer, you must be concerned with all the elements of information system security, with a focus on the resulting total security to the network itself. Because the server and routers are so central to the protection of department information, you will want to give them the priority when purchasing and deploying tools—before you armor each individual workstation.

Attack	Description	Consequences	Countermeasures
Data Modification	Change or destroy information on a system	• Can't get information. • Get false information from our own data files.	• Intrusion detection • Access control • Backup (2) • User Training (2)
Data Theft	Steal sensitive information without owner knowing about it	• Competitor or bad guy gets information. • We don't know that someone has the information.	• Intrusion detection • Access control • User Training (2) • Backup (2)
Flooding	Bombards system with more messages or information than it can handle	• System cannot process all the data coming in or it processes this information and ignores other important processing tasks. • Results in denial of service to valid users.	• Firewall • Redundant Systems (2)
Imitation or Spoofing	Pretends to be a valid user by using a stolen UserID and password or by "hijacking" a valid session	• Bad guy can get into a computer to steal data, destroy data, or take control of system, but looks like a valid user.	• Encryption • Access Control • User Training (2)
Jamming	Electronically disrupt transmission signals	• Information coming in over communications lines is incorrect or can't be understood.	• Disconnection • Redundant Systems (2)
Mole	A trusted person of an organization gives information to an outsider	• Competitor or bad guy gets information • We don't know that someone has the information.	• Access Control • User Training (2)
Packet Sniffer	Tools collect information from network such as UserID, passwords, contents of E-mail messages, credit card numbers.	• Attacker can get valid UserIDs and passwords that enable him to legally log onto a system. • Confidential information is read by unauthorized persons.	• Encryption • User Training (2)
Social Engineering	Information obtained by talking with people, obtaining their trust, and tricking them to give out information, like passwords.	• Passwords and other confidential information may be given to an unauthorized person.	• User Training
Virus	Malicious program that reproduces by attaching itself to a computer program.	• Destroys information on a system or makes it run very slowly.	• Anti-virus software • User Training (2) • Backup (2) • Redundant Systems (2)