Computer and Network Security

Chapter 18

This presentation covers:

- Building Customer Trust
- Security
- User Education
- Users and User Groups
- Permissions

Qualities of a Good Technician

"Soft skills" as they are known across many industries are essential

Building Customer Trust

- Trust begins with professionalism: Be professional in your attire, attitude, written communication, and oral communication
- Trust also includes being honest with the customer
  - If you are going to be late, let the customer know
  - If you need to do more research, explain the situation
- Trust also involves being honest if you find confidential material
  - Do not use or discuss any material you see while in a customer area
  - If you see confidential material, let the customers know you have seen the material
  - If the material is a password, let them know and recommend that they change the password immediately

Building Customer Trust

- Do not touch or move things or papers in a customer's area
  - Always ask the customer to move or put things away to clear the area you need
  - Do not try to work around a mess; simply explain that you need space to determine and/or repair the problem
- Trust involves giving customers documentation related to the product just installed or replaced
- Trust involves doing what you say you will do
- Trust also involves being honest about billing

Security

Security Policy

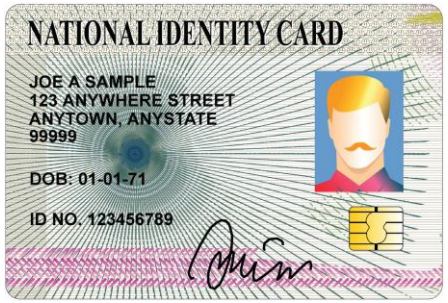
- Management must define and make clear what is acceptable to put on corporate wired or wireless networks and also what is an acceptable, along with the consequences for doing so
- A security policy is one or more documents that provide rules and guidelines related to computer and network security
- Common elements of a security policy are: Physical access, Antivirus, Acceptable use, Password, Email usage, Remote access, and Emergency procedures

Physical Security

- Typical physical security includes door locks, cipher locks, keys, guards, and fences, but physical security regarding computers can mean much more
- Electronic key cards are part of an access control system, which includes the key cards, door readers, and software to control and monitor the system

Physical Security Devices

- Smart card
- Key fob
- RFID
- Badge reader
- Security guard
- Security token
  - Types - authentication token, USB token, hardware token, software token
- Door lock

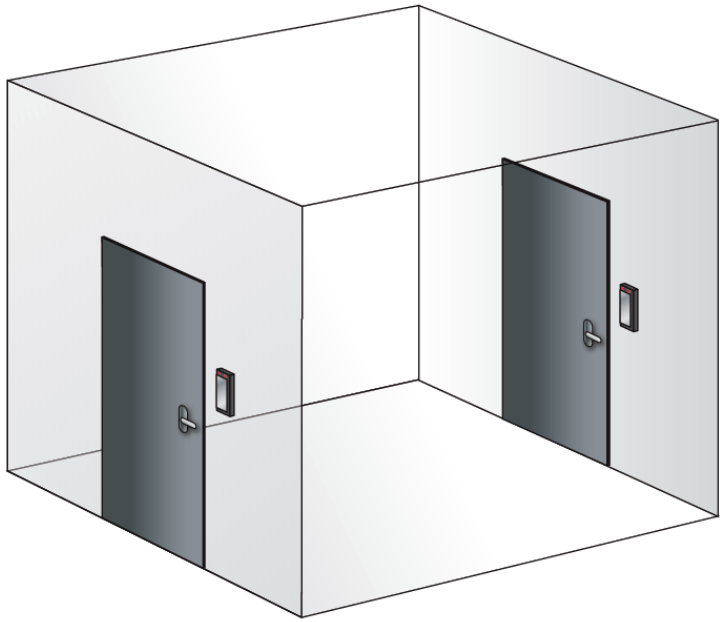


Smart card

Hardware token

Physical Security Devices (cont.)

- Entry control roster
- Biometric lock
- TPM
- Cable lock
- Server lock
- USB lock
- Mantrap



Mantrap

Physical Security Devices (cont.)

- Privacy screen
  - Prevents should surfing
- Tracking module

Document Security

- Keep secure
- Shred
  - Certificate of destruction
  - Proof of incineration
- Be aware of dumpster diving

Authentication

Proving who someone or a device is by using something the user or device has, knows, or is located. Can also be something a person is.

- User authentication/strong passwords: A method of ensuring the person accessing the device or network is a person who is allowed to do so
- Single-factor authentication – username/password
- Multifactor authentication: More than one digital method to verify and identify the person using the device or network resources
  - Software tokens and authenticator apps

Authentication (cont.)

Two server technologies used with authentication

- RADIUS – centralized authentication, authorization, and accounting (AAA) for wired and wireless devices as well as users
- TACACS – supports AAA or just one of these functions

Biometrics

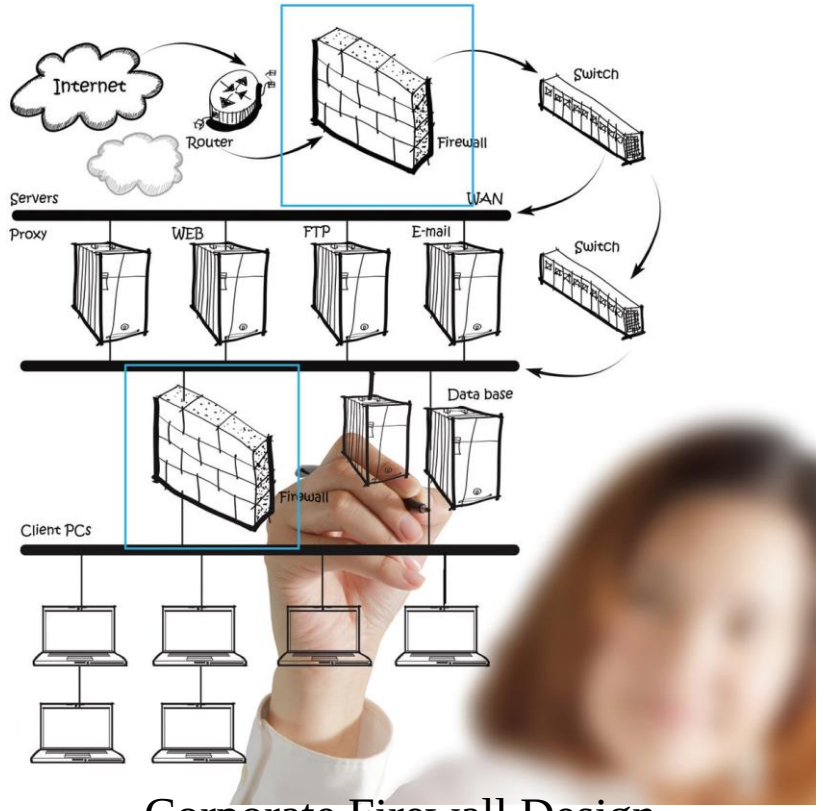
- Biometrics are more secure because a biometric system is more difficult to bypass than a user ID and password
- Biometrics require that the person being authenticated is present when gaining access
- Examples of biometric devices used to allow someone to gain access to a room, locker, or device include: Fingerprint reader/lock, facial recognition, hand scanner, retinal scanner, and voice recognition

Facial Recognition

Logical Security

Logical security - protection through the use of software.

- Antivirus/antimalware: Software to protect the operating system and applications from small programs that wreak havoc on the system, even causing it not to work at all
- Firewall: Hardware device that protects an organization or software available through the operating system or a third-party vendor designed to protect a particular device
- User authentication/strong passwords



Corporate Firewall Design

Logical Security (cont.)

- Multifactor authentication
- Directory permissions: Permissions can be assigned to differentiate between people that just need to see the data or those that need to change or even delete the data
- Virtual private network (VPN): A method of secure connectivity across an unsecure network such as the Internet to a remote location
- Data loss prevention (DLP): Protects corporate data from being sent outside the corporate network

Logical Security (cont.)

- Disabling ports: Computer ports are disabled so that an external device cannot be attached and data transferred
- Access control lists (ACLs): Security rules that permit or deny the type of traffic flowing into a device, out of the device, toward a particular network, or specifying the type of traffic such as HTTP or HTTPS packets
- Port security – Detects when an unauthorized device is plugged into a corporate network port.

Logical Security (cont.)

- Email filtering: Security rules specific to email that processes incoming messages before put-ting into specific users' email inbox that searches for and removes suspicious and harmful emails
- Trusted/untrusted software sources:
  - Windows users commonly have security software that tells them whether a website or a downloaded file is a trusted or untrusted software source
  - Linux users have repositories of open source software that has been approved or tested on specific Linux platforms

Email filtering

BIOS/UEFI Security Settings

- Passwords
  - Supervisor
  - User
- TPM (Trusted Platform Module) – crypto keys
- LoJack – locates a mobile device
- Secure boot – prevents unauthorized OS from loading
- Boot or power-on password – Not the Windows password

Password Security

- Don’t write it down and put in an obvious place
  - Keep digitally through an app or encrypted file
- Number of characters/complexity
  - 8 or more characters’
  - Use upper and lowercase letters
  - Use numerals and special characters
- Format – don’t use consecutive letters or numbers – dictionary attacks can be used
- Expiration
  - Minimum time a user must keep a password before changing
  - Maximum time before requiring a change
- Reuse
- Screen saver/lock computer when away from the desk or inactivity
- Failed attempts – how many times a person is allowed to try a password
- Social – don’t type a password when someone is near
  - Be aware of malicious employees

User Education

- Educating users is a great way to prevent security events and issues
- Training should start when someone is first hired
- New hires should be presented with the acceptable use policy (AUP) previously described
- Users should be reminded that every employee is required to follow corporate end-user policies and apply security best practices with every device used to perform business tasks
- Users should be reminded that if their computer is remotely accessed by a technician, they should close windows that have corporate or personal information prior to agreeing to the remote connection
- Any time that a technician removes a virus or malware from a user device, training should be part of solving the problem

Licensing

- Digital rights management (DRM) is the technology used to implement controls placed on digital media
- Technicians must maintain their professionalism and ethics to ensure that corporate interests are protected

Software Pirate

Licensing (cont.)

- Different software sources:
  - Open source: The original software code is provided.
  - Freeware: Doesn’t cost anything but could include some harmful software.
  - Shareware: Might be free at first but may require later payment; may include only part of a particular software package with the option to buy the rest.
  - Commercial license: Purchased software for a specific number of users and/or machines that may just be one.
  - Personal license: Purchased software for a specific number of users and/or machines that may just be one.

Regulated Data

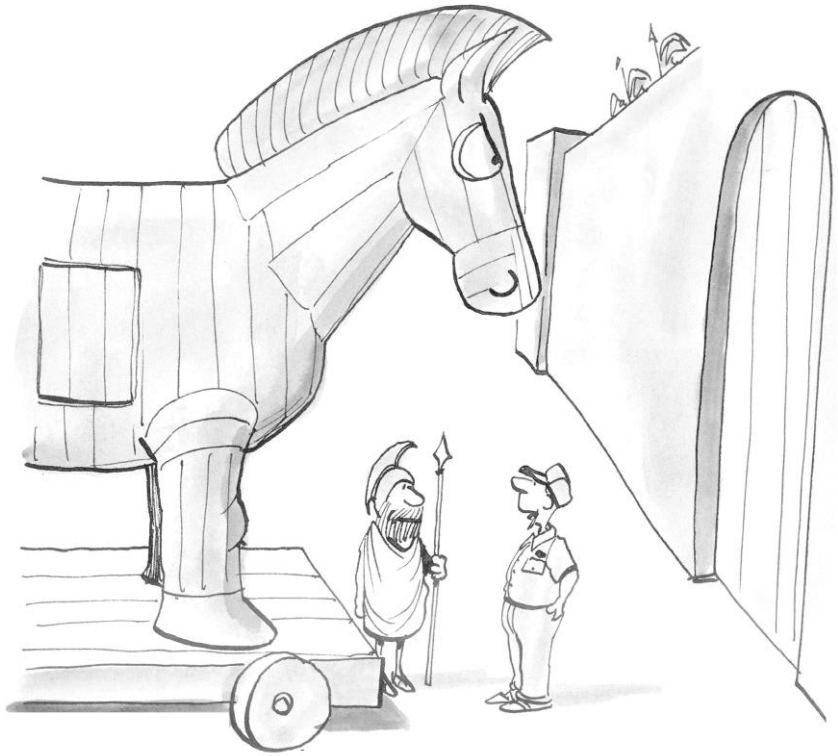
Regulated data is defined by federal law. Types of regulated data include:

- PII (personally identifiable information) – uniquely identifies someone like SSN, employee ID, patient number, password number, user ID
- PCI (payment card information)
- GDPR (European General Data Protection Regulation) – anyone that offers goods or services to residents of EU must comply
- PHI (protected health information)

Security Threats and Vulnerabilities

Malware is software code that is designed to damage a computer system. Types of malware:

- Spyware – collects personal information
- Virus – does something harmful to the computer
- Worm – spreads to other devices
- Trojan – disguises itself as legitimate program

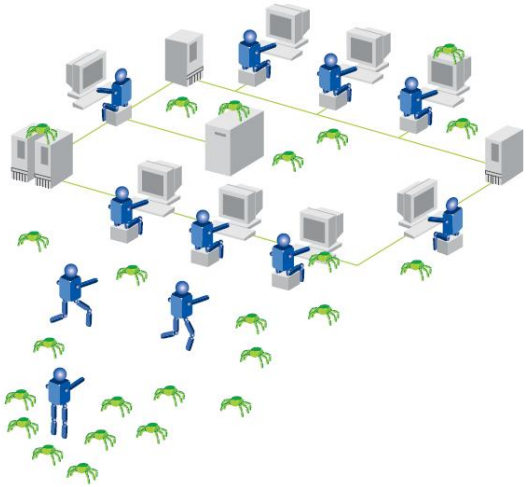


"Sure, bring her in. I've always wanted to work on one of these babies."

Security Threats and Vulnerabilities

Malware (cont.)

- Rootkit – gains access to OS
- Ransomware – requires user to pay money to regain access to the computer
- Keylogger – records every keystroke
- Botnet – software under control of zombie computers (zombies)



Social Engineering

Tricking people into divulging personal or corporate information.

- Impersonation
- Shoulder surfing
- Dumpster diving
- Tailgating or piggybacking – unauthorized person follows an authorized person
- Phishing (pronounced fishing) – attempts to get info via email
- Spear phishing – attempts to get info with some information provided about you

Security Attacks

- Attacks can come from outside or from within a corporate network
- Types of network attacks include:
  - Access
  - Backdoor
  - Botnet
  - Brute force
  - Dictionary
  - DoS (Denial of Service)
  - DDoS (Distributed Denial of Service)
- MitM (Man-in-the-Middle)
- Rainbow table
- Reconnaissance
- Replay
- Smurf
- Spoofing
- TCP/IP hijacking
- Vulnerability scanner
- Zero day attack
- Zombie

Workgroups and Domains

- A workgroup/HomeGroup is a LAN in which each computer maintains its own networked resources
- A domain environment is used in medium to large companies where servers are used to authenticate users

Protecting Access to Local and Network Resources

- Authentication is used to determine what network resources can be used
- Authorization is the part of the operating system or network controls that grant access to specific resources such as files, folders, printers, video conferencing equipment, scanners, and so on, on a computer system or network

Windows Default Users/Groups

- Administrator (user): Has total control of the computer; best practice is to rename the account and password protect it; create another user account that belongs to the administrator group, and has a complex password
- Administrators (group): A user account that has been created and placed in this group that has total control of the computer
- Guest (user): A member of the Guest group; disabled by default; no default user rights
- Guests (group): Used by those that do not have an account on the computer; normally does not require a password; best practice is to disable

Windows Default Users/Groups (cont.)

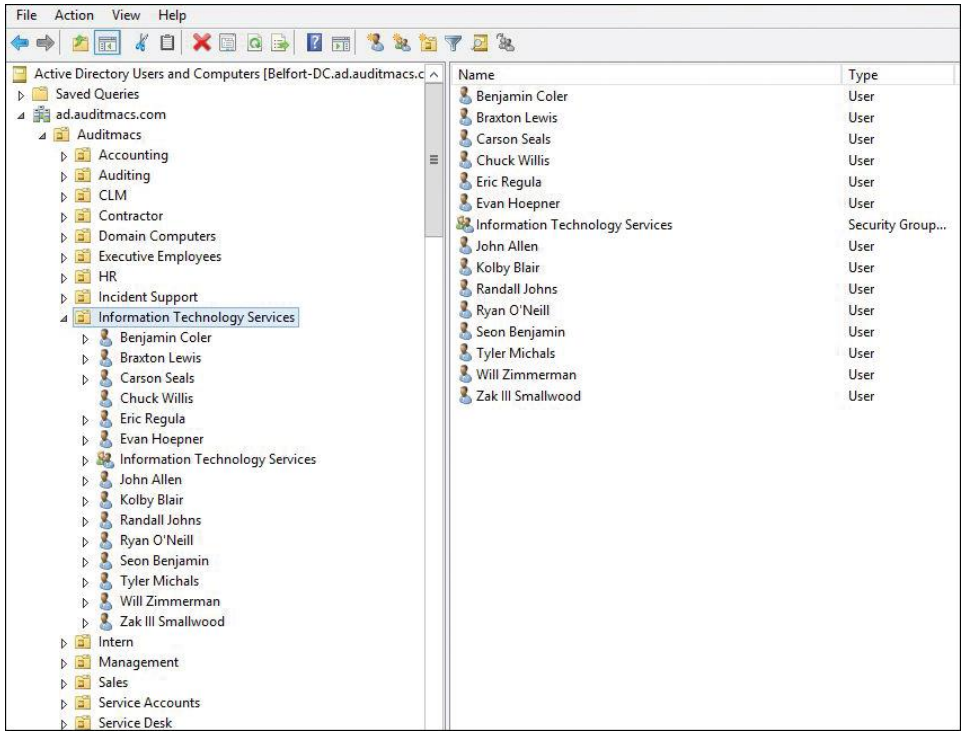
- Standard user (user): Default type of account created when you create a common corporate staff worker; the user is required to request an administrator to make changes to software, hardware, or security settings
- Backup operators (group): Can back up and restore files and folders regardless of permissions assigned; cannot change security settings; can access the computer from a remote location
- Power users (group): Same as a Standard user account (change things like time zone or date/time)
- Users (group): Can perform common tasks and create local groups, but cannot share folders or printers

Windows Default Users/Groups (cont.)

- Remote desktop users (group): Can log on to the computer from a remote location
- Offer Remote Assistance Helper (group): Can use the Remote Assistance program to help the computer user
- Network Configuration Operators (group): Can make TCP/IP changes and release/renew IP addresses
- Performance Log Users (group): Can manage local or remote performance logs and alerts

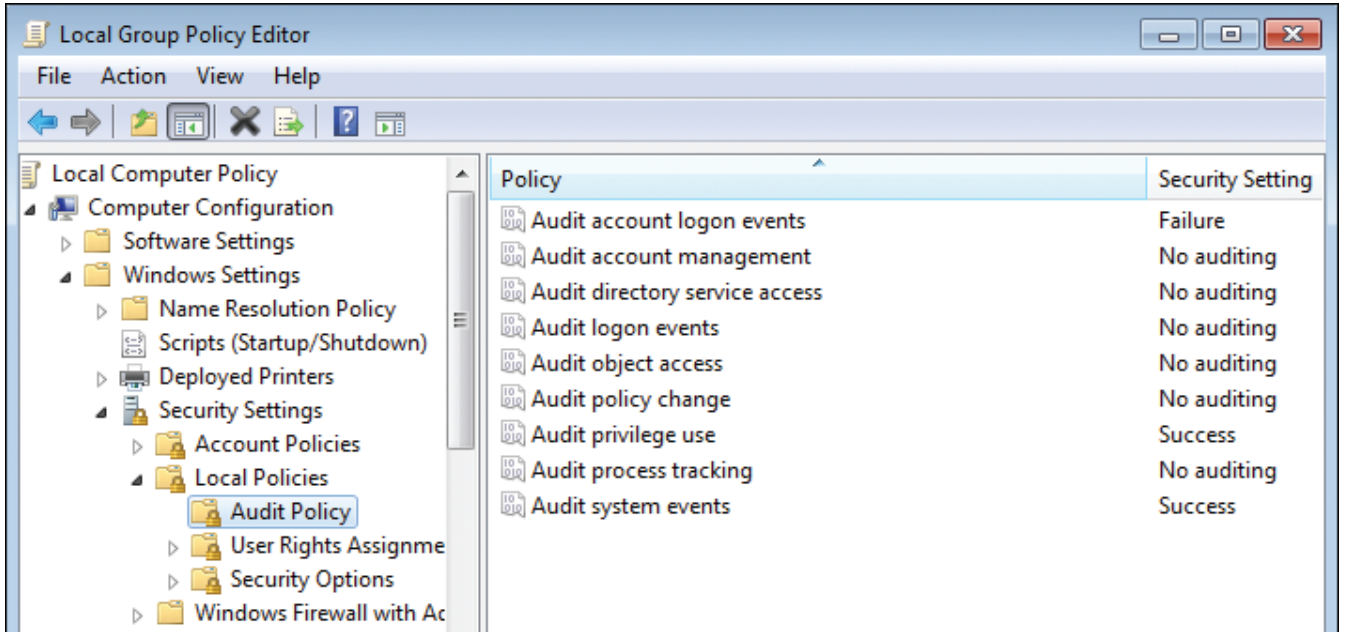
Active Directory

> Users placed in groups for administration and security such as controlling login scripts.



Local and Group Policies

- Policies can be applied at the domain level (group policy) and/or at the local level through the local security policy.



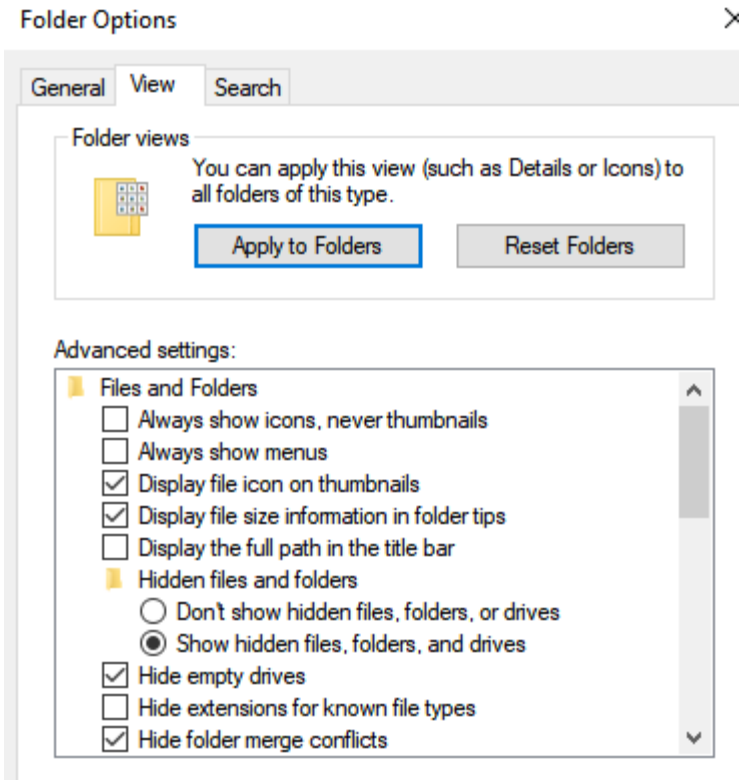
Permissions

- Permissions control what can or cannot be done (permit or deny access) to files, folders, and devices from a remote connection
- Network administrators and end users can set permissions on folders, and these permissions may affect another user's access to files and folders
- Two types of permissions can be assigned in Windows:
  - Share permissions: Share permissions provide and/or limit access to data across a network; are the only way to secure network resources on FAT16 or FAT32 drives
  - NTFS permissions: provide tighter control than shared folder permissions.; can be used only on NTFS drives

Folder Options

Because of quarantined files or the need to check system files, a technician is required to be familiar with Windows Explorer/File Explorer display options.

- In Windows 7 *Windows Explorer* > *Organize* > *Folder and search options* > *View* tab.
- In Windows 8 and 10 *File Explorer* > *View* > *Options* > *Change folder and search options* > *View* tab.



Protecting the Operating System and Data

Several chapters have contained important security-related tips, steps, and information related to protecting the operating system and data.

Items that pertain specifically to the security of the operating system and data:

- Use the NTFS file system
- Ensure that operating system and application service packs and updates are applied regularly (good patch management)
- Have an alternative boot source (such as optical disc, flash drive, another hard drive, and operating system discs)

Protecting the Operating System and Data (cont.)

- Install antivirus software with the latest virus definitions
- Encrypt data that needs to be protected
- Optionally, place operating system files and data files on separate hard drive partitions
- Some firmware or driver versions may cause security issues. Keep the versions updated
- If using virtualization, don’t forget that each virtual machine needs the same protection as an individual computer.

Protecting the Operating System and Data (cont.)

- If the computer you use does not need to share files or a printer with others on the network, use the Network and Sharing Center Control Panel and disable file and print sharing
- To create a shared folder that is not seen by any others across the network, add a $ (dollar sign) to end of the share name
- Use the System Restore program to control restore points before installing new software or hardware
- Disable ports through the system BIOS/UEFI BIOS

Backup/Restore

- Backup data routinely and test the backups
- Local storage – CDs, DVDs, BDs, flash drives, external hard drives
  - Advantage - Control the security and the cost
  - Disadvantage – Must store and maintain the media
- Cloud storage
  - Can be free or for a charge
  - Security is a concern
  - Restoration requires connectivity to the cloud storage

AutoRun and AutoPlay

- Disable AutoRun to prevent software form automatically starting from an optical disk, flash drive, or external drive.
- AutoPlay is how a music or movie disc will automatically start playing as soon as it is inserted
- Use `gpedit.msc` > *Administrative Templates* > *Windows Components* > *Autoplay Policies* to disable

Mechanical Hard Drives

- Use a drive overwrite program – rewrites the drive with all 1s or all 0s
- Use a drive wipe program – may not be good for highly sensitive data
- Use a low-level format utility from the manufacturer
- Use SDelete utility from Microsoft
- Use the `format` and `cipher` commands
- For sensitive data – use secure erasing software, degaussing, drilling through platters, or special hard drive destruction machine.

Internet Security

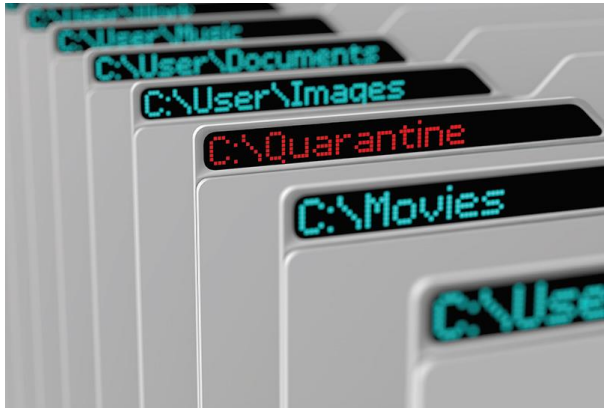
- No system should connect to the Internet without antivirus and antimalware software installed
- Pay attention to the security alerts provided by antivirus and antimalware software, browser applications, and the operating system
- For antimalware, Microsoft provides for free the Malicious Software Removal Tool through Windows 7 updates
- Microsoft 7, 8, and 10 come with Windows Defender, which works with Internet Explorer/Edge to warn for spyware

Internet Security (cont.)

- The Microsoft Security Baseline Analyzer (MBSA) identifies security misconfigurations on computers
- Configure your browser to display a security warning or that you are asked or warned of potential security threats
- Windows Defender can be customized as to when updates are downloaded and how often it scans the computer

Malware Removal

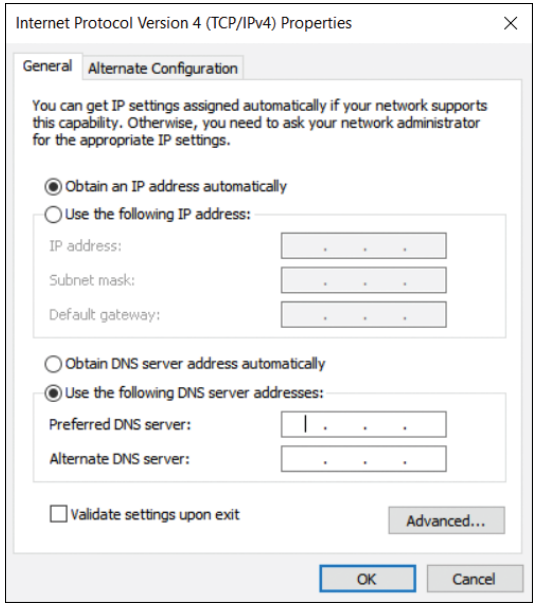
1. Identify malware symptoms and log all actions performed.
2. Quarantine the infected system. Disconnect it from the network. Do not power off or reboot the computer.
3. Notify the appropriate personnel per the security policy.
4. For Windows computers, disable System Restore.
5. Remediate the infected system.
6. Schedule antivirus/antimalware scans and run updates.
7. For Windows computers, re-enable System Restore and create a new restore point.
8. Educate the user.



DNS Issues

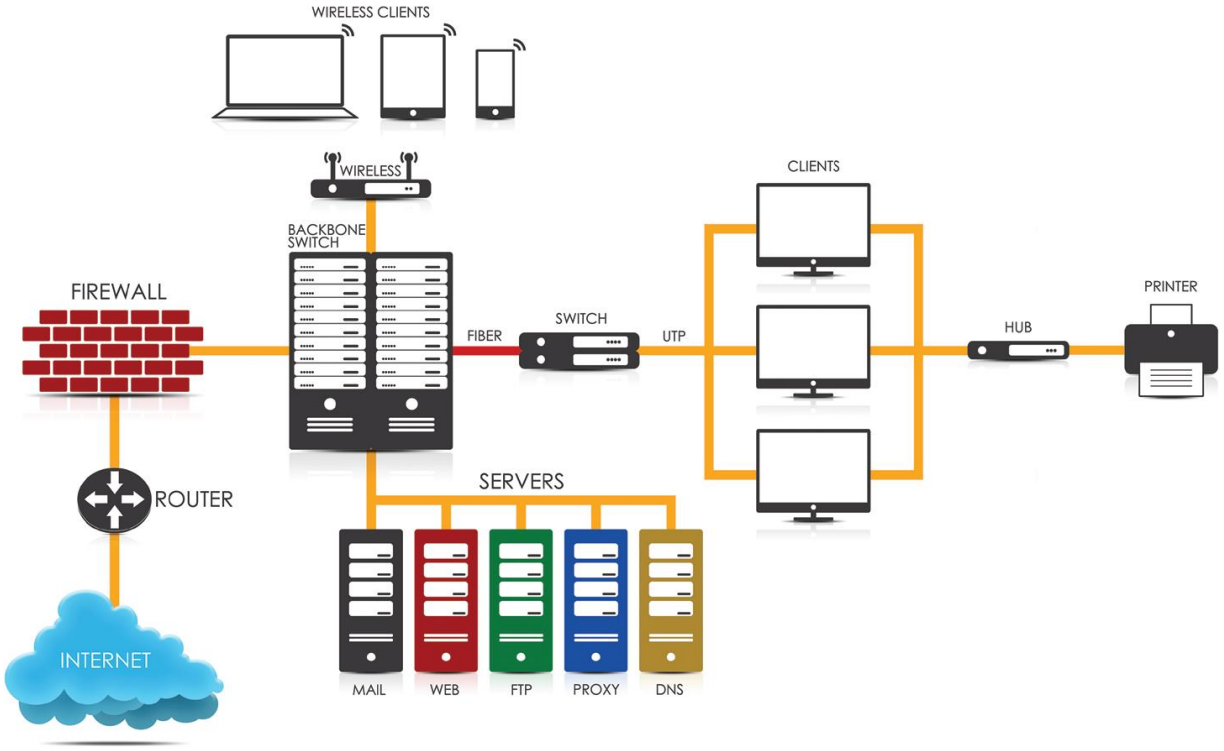
DNS translates a URL to an IP address.

- If the browser is redirected to an unusual website, change the DNS configuration to another DNS server.
- OpenDNS offers free and fee-based configurations.
  - 208.67.222.222
  - 208.67.220.220
  - 208.67.222.220
  - 208.67.220.222
- Clear the browser history/cache
- Clear the DNS cache - `ipconfig /flushdns`



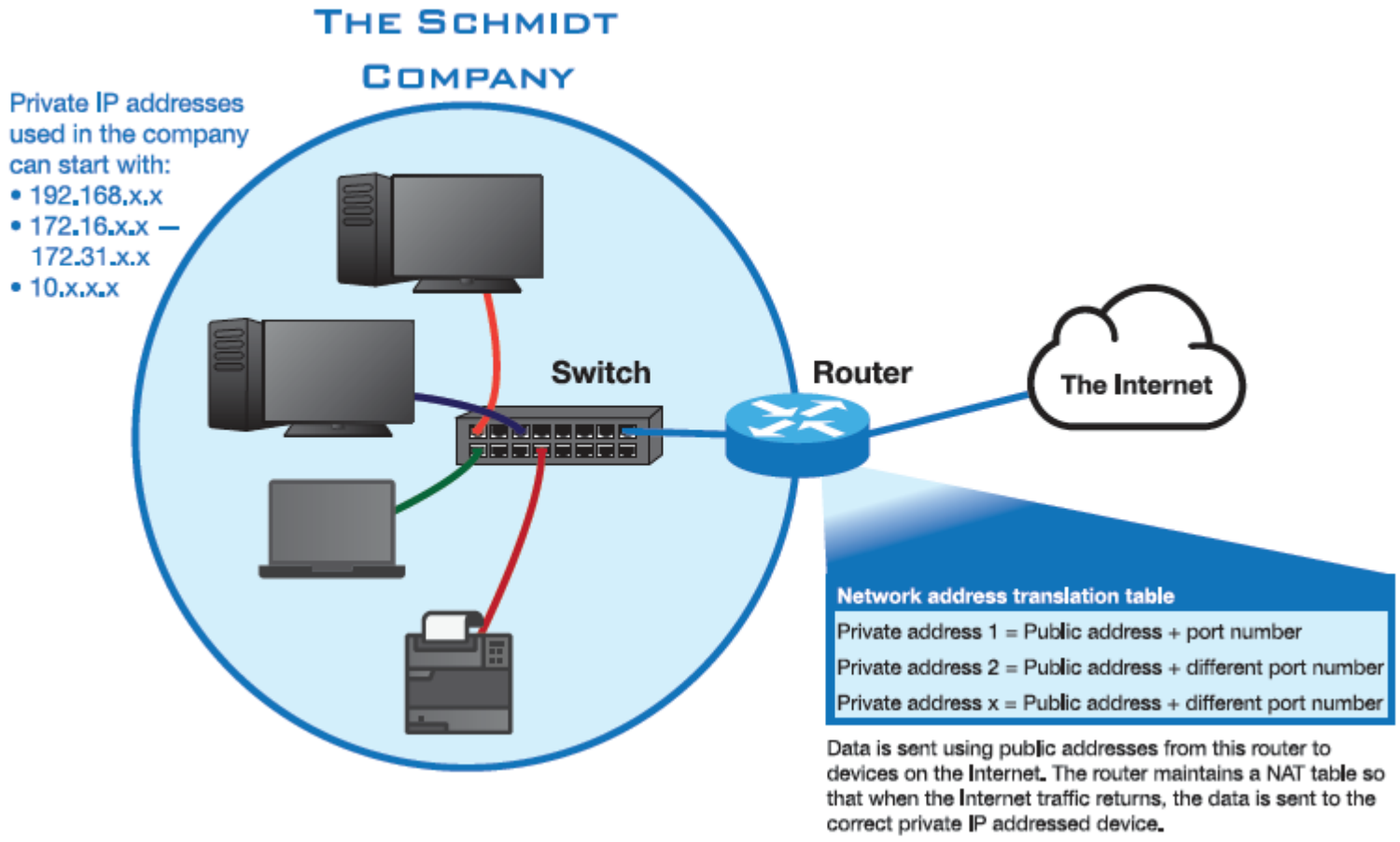
Proxy Servers

Acts as an agent between an application such as a web browser and a remote server. Can also cache frequently accessed web pages for speedier access.



NAT (Network Address Translation)

Translates private IP addresses to public ones that can be routed on the Internet. Tracks by port numbers.



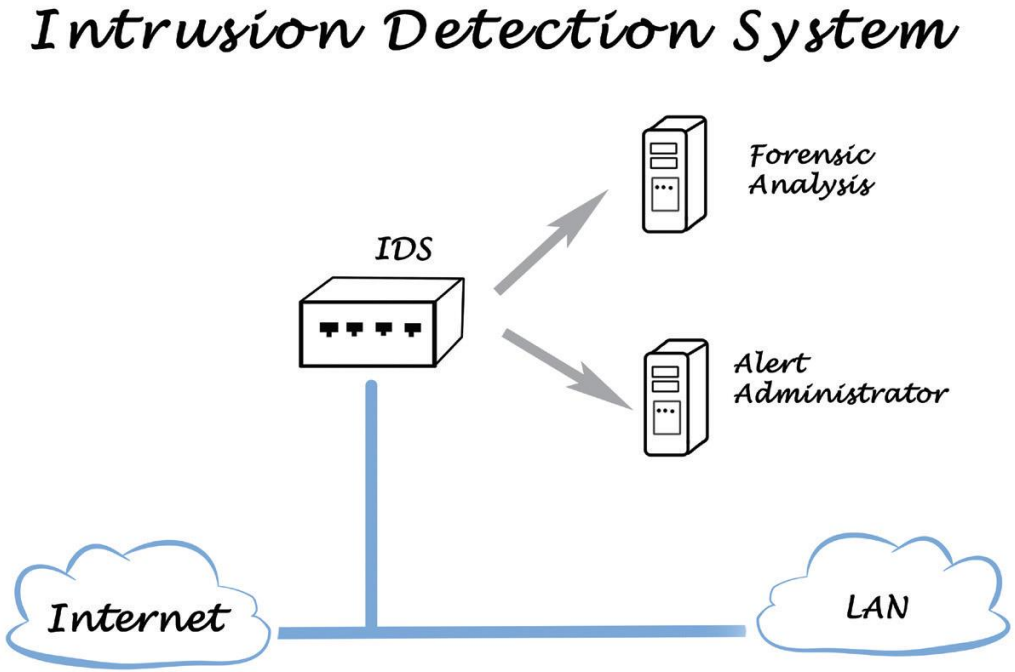
Remote Access to Network Devices

TABLE 18.14 Remote access protocols and security concerns

Remote access protocol	Description	Security concerns
RDP (Remote Desktop Protocol)	Creates a peer-to-peer remote desktop connection from one computer to a remote computer. You might have to enable port forwarding (see Chapter 13, "Networking") and allow port 3389 in order to connect to the remote device.	Reported security issues should be taken into consideration before using RDP.
SSH (Secure Shell)	Uses port 22 to securely log in to a remote network device.	An alternative to Telnet that includes strong encryption within the secure channel created between devices.
Telnet	Uses port 23 to access a remote device on the network, such as a router, a server, an access point, or a switch.	Telnet uses clear text to send data and passwords. Telnet should not be used unless the network device supports no other remote access protocol.

Internet Appliances

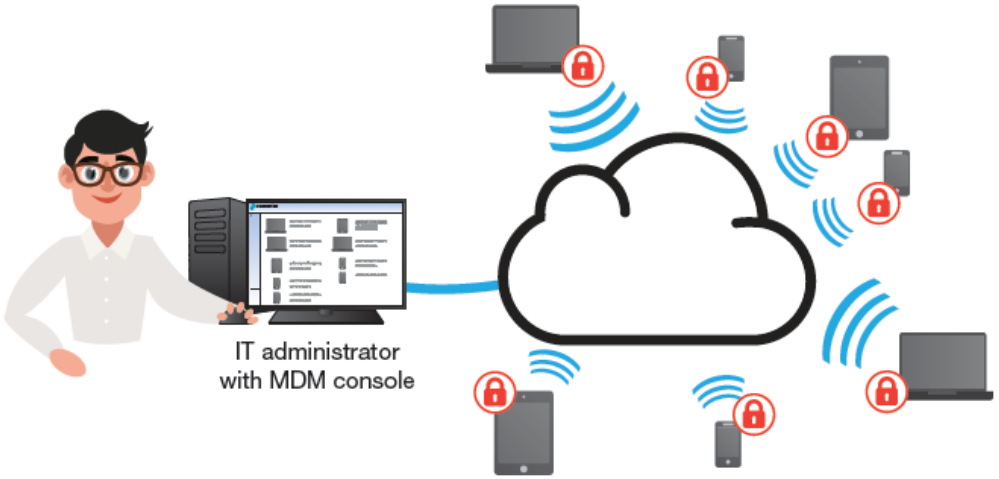
- End-point management server – to discover and manage devices
- UTM (unified threat management) – provides multiple security functions including firewall and content filtering
  - Content filtering screens data for specific suspicious web addresses, email, or files



- IDS (intrusion detection system) – passive system that scans for malicious traffic
- IPS (intrusion prevention system) – active system that takes action when a security risk is detected

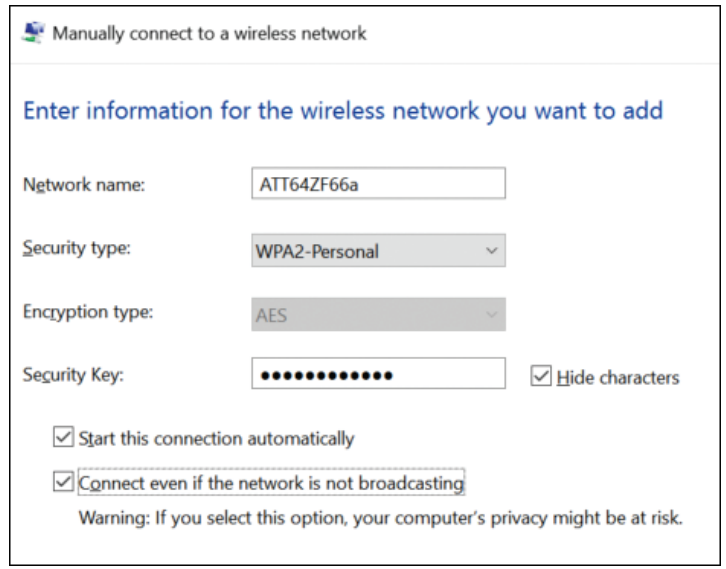
Mobile Device Management (MDM)

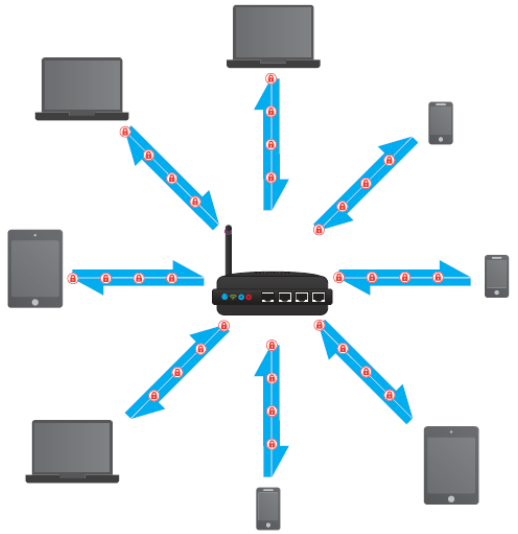
- Used to view and manage mobile devices
- Sample MDM policies
  - Software/firmware installation
  - System updates
  - Backup process
  - VPN connectivity
  - Password storage
  - How to report lost or stone devices
  - Steps to take when a security breach occurs
  - Data storage



Wireless Security

- Mobile device security setting must match AP setting
  - WEP
  - WPA
  - WPA2 – most common
  - TKIP
  - AES
  - WPS – avoid using





Wireless Security (cont.)

- MAC Address Filtering
  - Manually enter the MAC address of any wireless device allowed on the wireless network
- Beware AP default settings – change as soon as you configure for the first time.
- SSID broadcasting – sends out a beacon frame of the SSID (unique wireless network identifier)
  - Can disable, but you must manually configure every wireless device if you do.

Security Incident Reporting

1. Identify the issue (virus, spyware or grayware, phishing, child exploitation, or software piracy).
2. Report the issue through the proper channels.
3. Preserve the data/device by documenting the incident. Use a chain-of-custody form that travels with the data/device.

- Report the incident to your supervisor if you do not know what to do.

Computer Terms

Refer to the glossary terms at the end of the textbook chapter. Review Chapter 18 and become familiar with the terms.

This PPT deck was developed

to support instruction of

The Complete CompTIA A+ Guide to IT Hardware and Software 8th Ed.