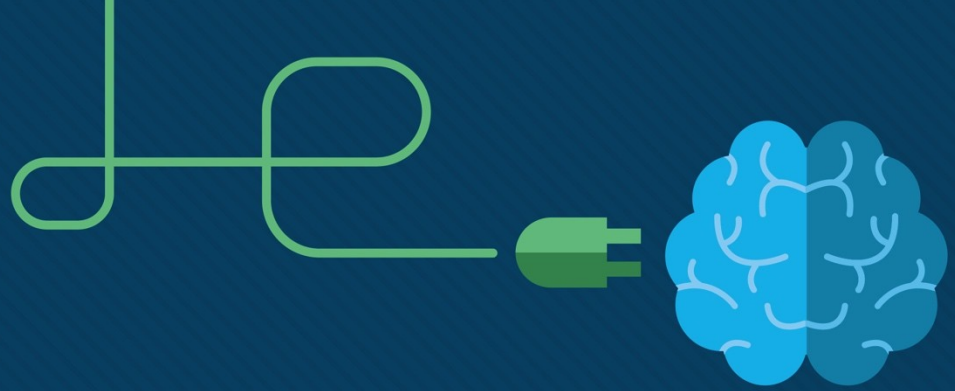


Chapter 14: The IT Professional

IT Essentials v8.0

Chapter 14 - Sections & Objectives

- 14.1 Communication Skills and the IT Professional
  - Explain why good communication skills are a critical part of IT work.
    - Explain the relationship between good communication skills, troubleshooting, and professional behavior.
    - Use communication skills and professional behavior while working with a customer.
    - Explain why professional behavior at work is important.
    - Perform good customer communications while on a call.
- 14.2 Operational Procedures
  - Explain how to manage change and unplanned disruptions in a business environment.
    - Compare and contrast different types of IT and business documentation.
    - Describe how change is managed in an IT environment.
    - Explain measures taken by IT organizations to reduce the impact of unplanned outages or data loss.

Chapter 14 - Sections & Objectives (Cont.)

- 14.3 Ethical and Legal Issues in the IT Industry
  - Explain appropriate behavior when faced with the legal and ethical issues that arise in the IT industry.
    - Describe ethical and legal issues in the IT industry.
    - Describe procedures for dealing with inappropriate content.

- 14.4 Call Center Technicians
  - Explain the call center environment and technician responsibilities.
    - Describe the responsibilities of different types of call center technicians.
    - Describe the basic commands and operation of scripts in different environments.

14.1 Communication Skills and the IT Professional

Relationship Between Communication Skills and Troubleshooting

To troubleshoot a computer, you need to learn the details of the problem from the customer. Most people who need a computer problem fixed are probably feeling some stress. If you establish a good rapport with the customer, the customer might relax a bit. A relaxed customer is more likely to be able to provide the information that you need to determine the source of the problem and then fix it.

Relationship Between Communication Skills and Professional Behavior

- If you are talking with a customer in person, that customer can see your body language. If you are talking with a customer over the phone, that customer can hear your tone and inflection. Customers can also sense whether you are smiling when you are speaking with them on the phone. Many call center technicians use a mirror at their desk to monitor their facial expressions.
- Successful technicians control their own reactions and emotions from one customer call to the next. A good rule for all technicians to follow is that a new customer call means a fresh start. Never carry your frustration from one call to the next.

Know, Relate, and Understand

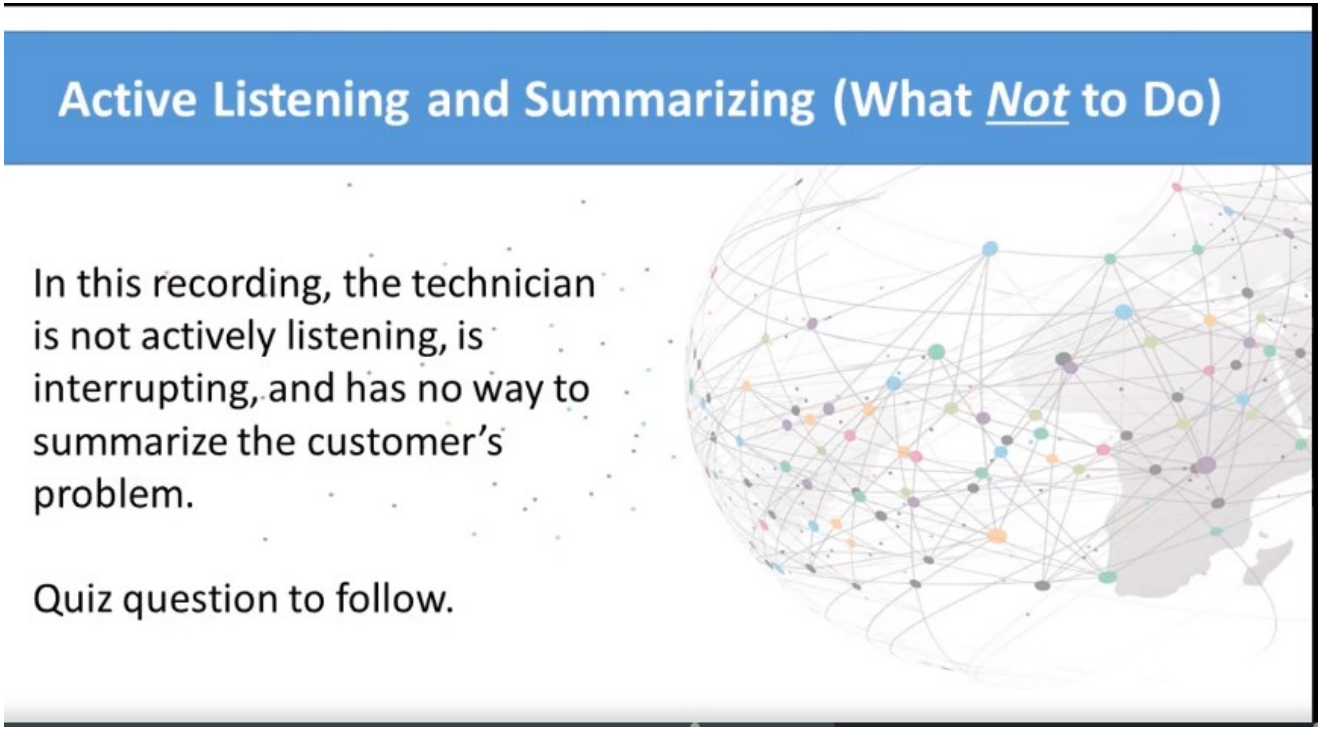
One of first tasks as a technician is to identify customer's computer problem. The table summarizes the three general rules for talking with a customer:

Rule	Definition	Example
Know	Call your customer by his or her name. Ask if there is any name in particular that they prefer you use.	For example, if the customer tells you her name is Mrs. Johnson, ask if that is what she prefers to be called by you. She may say yes, or she may give you her first name. In any case, only use the preferred name with your customer.
Relate	Create a one-to-one connection between you and your customer.	For example, find something you may have in common (without giving too much information). If you hear a dog barking in the background of the call and you have a dog, then briefly ask about their dog. If you have had to call customer support for your own computer, mention that you understand how frustrating this can be and that you will do everything you can to help them. Do not lose control of the call.
Understand	Determine your customer's level of knowledge about the computer to help you best communicate with them.	For example, a customer who is very new to computers will not be likely to know all of the jargon that you use every day, so you should use the most common words you can think of to describe aspects of their computer. A more experienced customer probably knows some of the same jargon that you use.

Active Listening

- Allow the customer to tell the whole story. During the time that the customer is explaining the problem, occasionally interject some small word or phrase, such as “I understand,” or “Yes.”
- Do not interrupt the customer to ask a question or make a statement. Listen carefully when your customers speak, and let them finish their thoughts.
- An open-ended question usually involves information about what the customer was doing, what they were trying to do, and why they are frustrated.
- After listening to the customer explain the whole problem, summarize what the customer has said.
- Follow-up questions should be targeted, closed-ended questions based on the information that you have already gathered. Closed-ended questions should focus on obtaining specific information. The customer should be able to answer a closed-ended question with a simple “yes” or “no” or with a factual response, such as “Windows 10.”

Video Demonstration – Active Listening and Summarizing



Using Professional Behavior with the Customer

When dealing with customers, it is sometimes easier to explain what you should not do. The following list describes things that you should not do when talking with a customer:

- Do not minimize a customer's problems.
- Do not use jargon, abbreviations, acronyms, and slang.
- Do not use a negative attitude or tone of voice.
- Do not argue with customers or become defensive.
- Do not say culturally insensitive remarks.
- Do not disclose any experiences with customers on social media.
- Do not be judgmental or insulting or call the customer names.
- Avoid distractions and do not interrupt when talking with customers.
- Do not take personal calls when talking with customers.
- Do not talk to co-workers about unrelated subjects when talking with the customer.
- Avoid unnecessary holds and abrupt holds.
- Do not transfer a call without explaining the purpose of the transfer and getting customer consent.
- Do not use negative remarks about other technicians to the customer.

Tips for Hold and Transfer

- When dealing with customers, it is necessary to be professional in all aspects of your role.
- You must handle customers with respect and prompt attention.
- When on a telephone, make sure that you know how to place a customer on hold, as well as how to transfer a customer without losing the call.

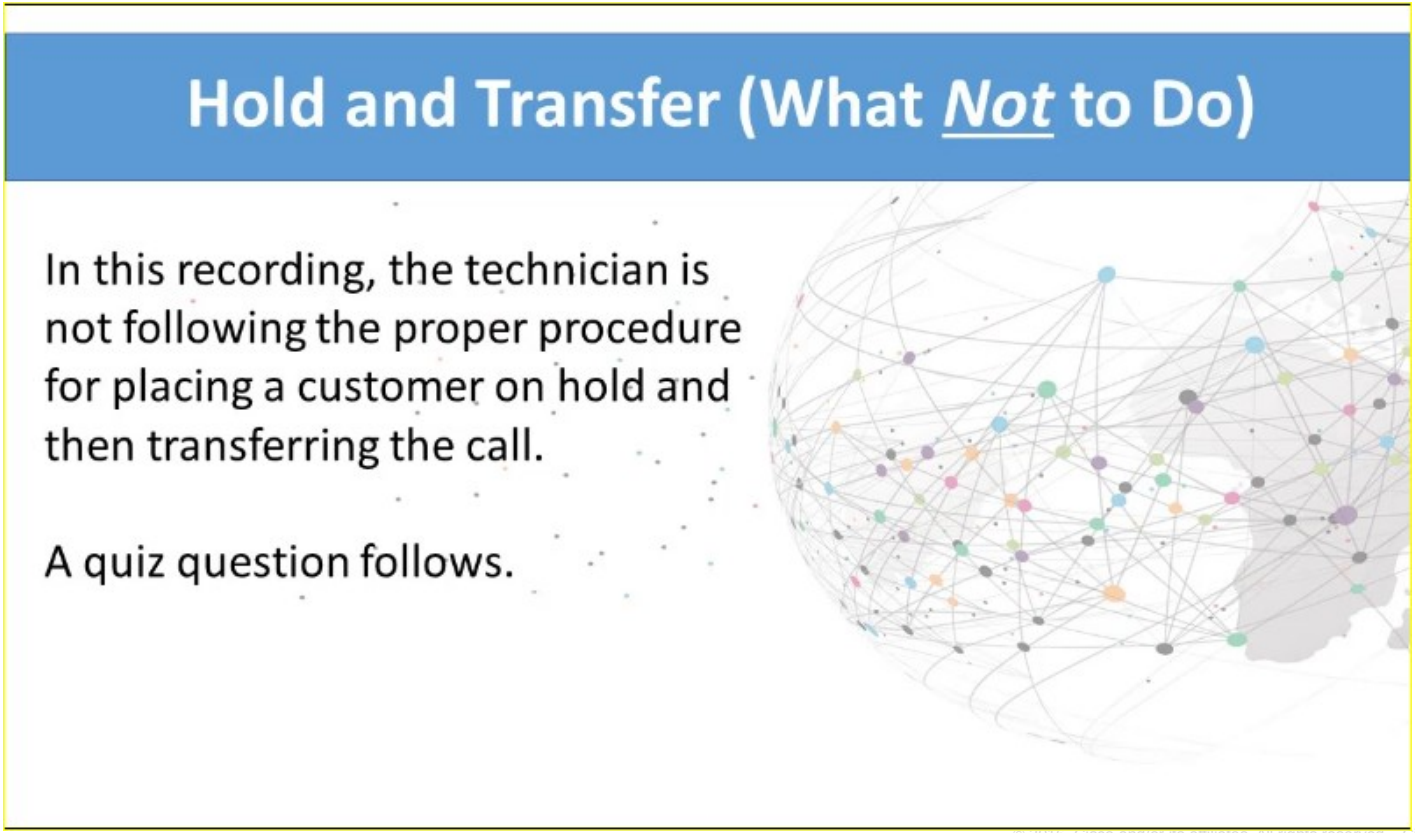
How to Put a Customer On Hold

Do	Do Not
• Let the customer finish explaining the problem. • Say that you must put the customer on hold and explain why. • Ask the customer for permission to put the call on hold. • When the customer agrees, thank the customer and explain that you expect to be back in just a few minutes. • Explain what you will be doing during that time. • If, after placing the call on hold, it takes longer to return to the customer than expected, quickly get back on the call to explain the situation to the customer. • Always thank the customer for their patience as you work to fix their problem.	• Interrupt the customer. • Put a customer on hold without an explanation. • Put a customer on hold without the customer's consent. • Assume that your time is more valuable than the customer's time.

How to Transfer a Call

Do	Do Not
• Let the customer finish explaining the problem. • Say that you must transfer the call and why. • Tell the customer the name and number of the person they will be speaking with. • Ask the customer for permission to transfer the call. • When the customer agrees, thank the customer and begin the transfer. • Tell the new technician who will be receiving the transfer your name, the ticket number, and the customer's name.	• Interrupt the customer. • Transfer the call without an explanation. • Transfer the call without the customer's consent. • Assume that your time is more valuable than the customer's time.

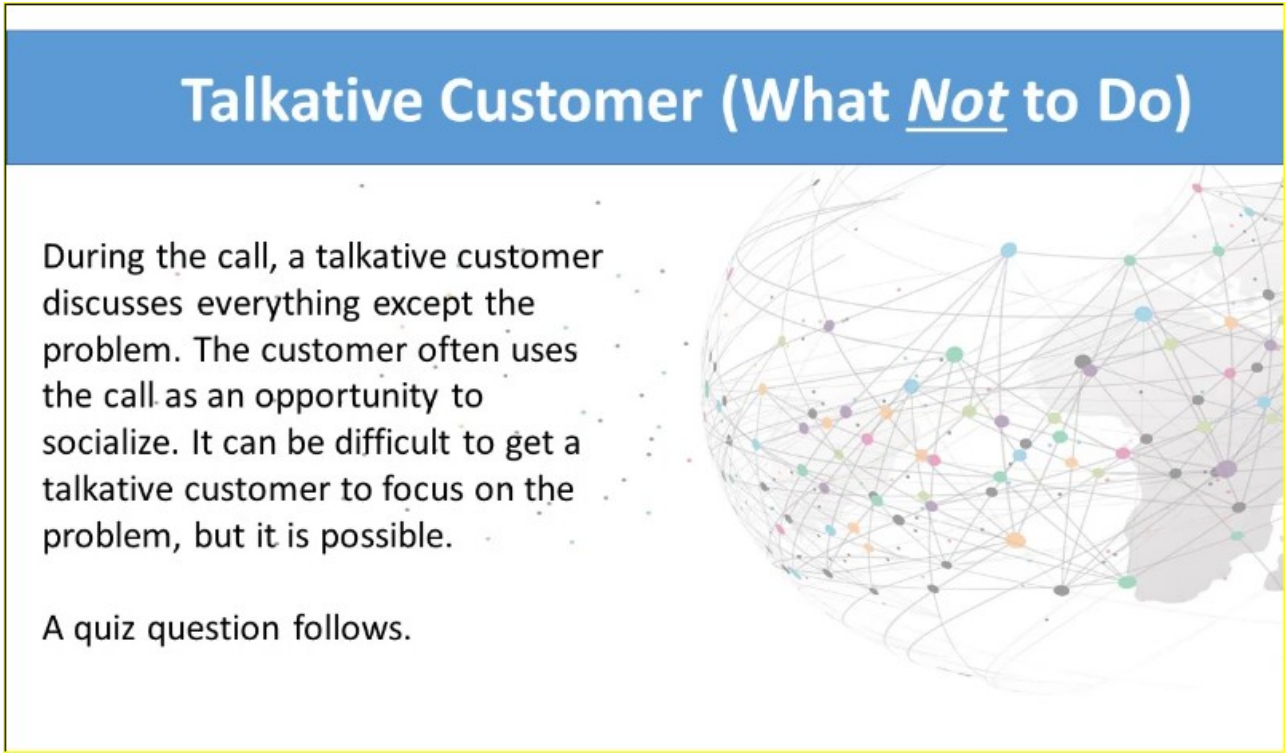
Video Demonstration - Hold and Transfer



Keeping the Customer Call Focused

- **Use proper language** – Be clear and avoid technical language that the customer might not understand.
- **Listen and question** – Listen carefully to the customer and let them speak. Use open and closed ended questions to learn details about the customer's problem.
- **Give feedback** – Let the customer know that you understand the problem and develop a friendly and positive conversational manner.

Video Demonstration – The Talkative Customer



Video Demonstration – The Rude Customer

Rude Customer (What *Not* to Do)

A rude customer complains during the call and often makes negative comments about the product, the service, and the technician. This type of customer is sometimes abusive and uncooperative and gets aggravated very easily. The first recording is of a support technician who is ***not*** using professional behavior with a customer.

A quiz question follows.

Video Demonstration – The Knowledgeable Customer

Knowledgeable Customer (What *Not* to Do)

A knowledgeable customer wants to speak with a technician who is equally experienced in computers. This type of customer usually tries to control the call and does not want to speak with a level one technician. The first recording is of a support technician who is ***not*** using professional behavior with a customer.

A quiz question follows.

Video Demonstration – The Angry Customer

Angry Customer (What *Not* to Do)

An angry customer talks loudly and often tries to speak when the technician is talking. Angry customers are usually frustrated that they have a problem and upset that they have to call somebody to fix it. The first recording is of a support technician who is ***not*** using professional behavior with an angry customer.

A quiz question follows.

Video Demonstration – The Inexperienced Customer

Inexperienced Customer (What *Not* to Do)

An inexperienced customer has difficulty describing the problem. These customers are sometimes not able to follow directions correctly and not able to communicate the errors that they encounter. The first recording is of a support technician who is ***not*** using professional behavior with this inexperienced customer who does not know jargon. The technician is also being demeaning.

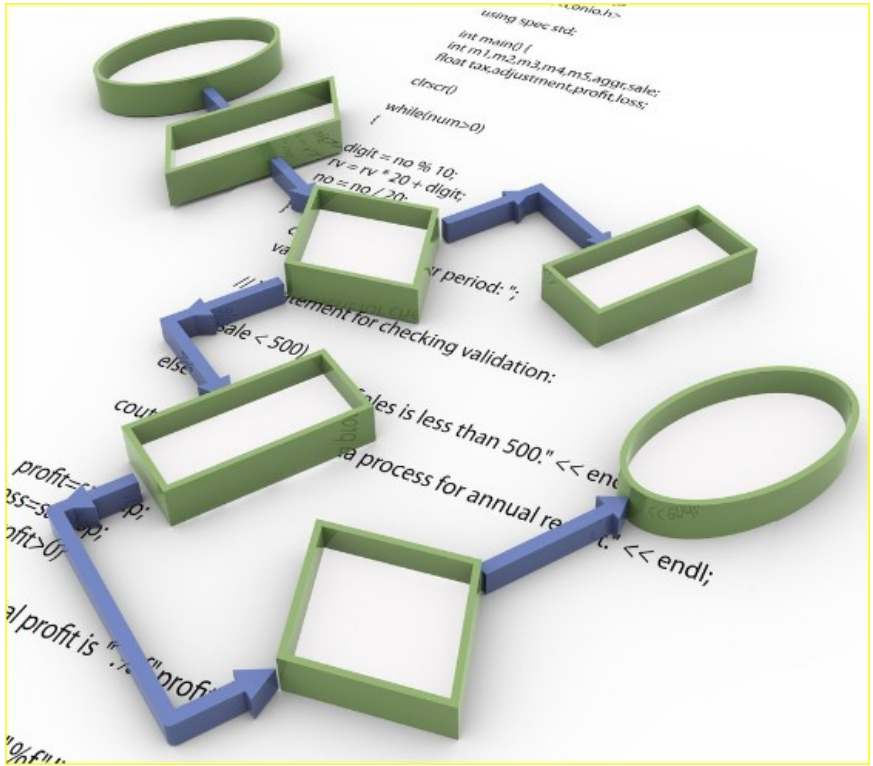
A quiz question follows.

14.2 Operational Procedures

Documentation Overview

Purposes for documentation include:

- Providing descriptions for how products, software, and hardware function through the use of diagrams, descriptions, manual pages and knowledgebase articles.
- Standardizing procedures and practices so that they can be repeated accurately in the future.
- Establishing rules and restrictions on the use of the organization's assets including acceptable use policies for internet, network, and computer usage.
- Reducing confusion and mistakes saving time and resources.
- Complying with governmental or industry regulations.
- Training new employees or customers.



IT Department Documentation

- Keeping documentation current is a challenge for even the best managed IT departments.
- In general, IT documentation falls into four categories: Policies, Operations, Projects, and User Documentation.

Policy Documents

- Acceptable use policies that describe how technology is to be used within the organization.
- Security policies that outline all aspects of information security, including password policies and security incident response methods.
- Regulatory compliance policies which describe all federal, state, local and industry regulations that apply to the organization.
- Disaster recovery policies and procedures that provide detailed plans for what must be done to restore services in the event of an outage.

Operation and Planning Documents

- IT strategy and planning documents outline the near- and long-term goals of the department.
- Proposals for future projects and project approvals.
- Meeting presentations and minutes.
- Budgets and purchasing records.
- Inventory management, including hardware and software inventories, licenses, and management methods, such as the use of asset tags and barcodes.

IT Department Documentation (Cont.)

Project Documents

- User requests for changes, updates or new services.
- Software design and functional requirements, including flow diagrams and source code.
- Logical and physical network topology diagrams, equipment specifications, and device configurations.
- Change management forms.
- User testing and acceptance forms.

User Documentation

- Features, functions, and operation of software, hardware, and services provided by the IT department.
- End-user manuals for hardware and software.
- Help desk ticket database with ticket resolutions.
- Searchable knowledgebase articles and FAQs.

Report and Procedures

- **Acceptable use policy (AUP)** - an agreement between two or more parties that defines the appropriate user access to resources or services.

- **Incident report, also known as an after-action report (AAR)** - can be used to document an episode of a critical and major incident, such as a security breach. The purpose of the report is to identify potential issues, provide insight for improvements, and allow prompt corrective action to prevent a similar event in the future.

- **Standard operating procedures (SOP)** - step-by-step instructions to guide employees on how to use computers and networked services efficiently, securely, and are informed of expected responsibilities. The main goals of the SOP are to establish uniformity across the company, create high-quality work consistently, and reduce miscommunications.

User Checklists

SOP can also be in the form of user checklists. Two examples of user checklists are:

- **New-user setup checklist** – a formal onboarding process helps new hires or employees changing job roles. Some of typical process can include:
  - Setting up the user accounts with the necessary permissions and security clearance
  - Assigning devices and receiving training as necessary
  - Learning about security policy and data privacy agreements

- **End-user termination checklist** - When an employee retires, changes job roles, or leaves the organization, the end-user termination checklist should be part of the off-boarding process. Some of typical process can include:
  - Take back the device and wipe all data from the device.
  - Transfer or release software licenses.
  - Deactivate account access and remove all account permissions.

Knowledge Base and Articles

A knowledge base is a centralized repository of articles and documents that allow users to create, share, and manage knowledge across the organization. The articles in the knowledge base can provide these common types of data:

- Answers to frequently asked questions (FAQs)
- Troubleshooting scenarios
- Internal database to support self-service support
- Training documents
- Links to external legitimate and verifiable knowledge base articles

Regulatory Compliance Requirements

Federal, state, local, and industry regulations can have documentation requirements over and above what is normally documented in the company's records. Regulatory and compliance policies often specify what data must be collected and how long it must be retained. A few of the regulations may have implications on internal company processes and procedures. Some regulations require keeping extensive records regarding how the data is accessed and used.

Failure to comply with laws and regulations can have severe consequences, including fines, termination of employment, and even incarceration of offenders.

Asset Databases

- Asset management is the tracking and management of assets to ensure that they are used properly, maintained, upgraded, and disposed of responsibly at the end of their lifecycles.
- The organization needs an inventory of all the deployed hardware assets along with the consumables, spare components in case of hardware failures, and software assets, such as warranty information, licenses, and intellectual property (IP).

- **Database system** - many software solutions are available for businesses to manage and track their assets. Asset management software can improve the visibility and management of the assets to reduce hardware and software costs.

- **Asset tags and IDs** - working in conjunction with an asset management database system, can provide up-to-date and accurate information about an asset. An asset tag identifies the equipment with a unique serial number, barcode, QR code, or radio frequency ID (RFID) and is typically adhered to the asset.

Asset Procurement

Procurement life cycle

- **Planning** – Analysis of the organization's current and future needs combined with potential asset impact on business, network, daily operations and implemented devices is needed before requesting a new or upgraded asset.
- **Procurement** – A budget is determined, and a supplier or vendor is identified to deliver the asset.
- **Deployment** – The procured asset can be installed or integrated with the other tools in the business.
- **Maintenance** – Provisions should be made to keep your assets in operating condition to optimize their use.
- **Disposal** – When an asset has reached the end of life, the asset should be sanitized of any data. The sanitized asset can be sold, recycled, donated, or destroyed.

- **Warranty and licensing**

For each hardware asset, the invoice, warranty, support contract, and vendor contact information should be readily available. For each software asset, License information, subscription-based details, and number of allotted users or devices should be readily available.

Asset Procurement (Cont.)

Assigned users

- Depending on the type of assets, the assets can be assigned to individuals or shared within the entire organization.

- Typical assets managed by individual accounts:
  - Workstations
  - Laptops
  - Mobile devices, like smartphones and tablets
  - Software license Shared assets managed by individuals or security groups within a department:
    - Servers
    - Routers
    - Switches
    - Access points

Change Control Process

CHANGE CONTROL WORKSHEET

NAME OF PROJECT		DATE CREATED	
PROJECT MANAGER		DATE APPROVED	
TECHNICIAN		DATE STARTED	
STAKEHOLDERS		DATE COMPLETED AND ACCEPTED	

PROJECT DESCRIPTION	
PROPOSED CHANGE	*A detailed description of the proposed change.*
PURPOSE OF CHANGE	*A detailed overview of the reasons this change is necessary.*
SCOPE OF CHANGE	*Descriptions of all of departments and/or services that will be impacted by this change.*
INTENDED OUTCOME	*Overview of benefits resulting from change.*
ESTIMATED TIME FRAME	*Timeframes for preparation, notification, implementation, testing and approval.*
RISK ANALYSIS	*Detailed analysis of potential risks involved with this change.*
BACK-OUT OR RECOVERY	*Detailed steps needed to return system to operational status if the change fails.*

PROJECT IMPLEMENTATION PLAN	
PLAN FOR CHANGE	*Steps necessary to prepare for change.*
PLANNED IMPLEMENTATION STEPS	*Steps to perform change.*
ACTUAL STEPS PERFORMED	*Detail of the actual implementation of the change. If any unplanned steps are necessary to complete the change, or if there are steps that cannot be completed for any reason, note them here.*
DOCUMENTATION AND FOLLOW-UP	*Provide a list of current documentation that needs to be updated as a result of this change.*

Disaster Recovery Overview

A disaster recovery plan is a comprehensive document that describes how to restore operation quickly and keep critical IT functions running during or after a disaster occurs. The disaster recovery plan can include information such as offsite locations where services can be moved, information on replacing network devices and servers, and backup connectivity options.

Some services may even need to be available during the disaster in order to provide information to IT personnel and updates to others in the organization. Services that might need to be available during or immediately after a disaster include:

- Web services and internet connectivity.
- Data stores and backup files.
- Directory and authentication services.
- Database and application servers.
- Telephone, email and other communication services.

Preventing Downtime and Data Loss

Backup Storage Method	Advantages	Disadvantages
Cloud backups	• Reliability – cloud providers use the latest technology and can offer other related services, such as compression and encryption. • Scalability – cloud backups scale easily, so a business doesn't need to worry that it doesn't have the storage capacity or media if their data files increase in size. • Accessibility – cloud backup files are available anywhere the Internet is accessible.	• Time – backing up data and restoring files are dependent on the speed and reliability of the Internet connectivity. In the event of a regional natural disaster, network congestion may cause intermittent connectivity. • Discontinuation of service or increase in pricing.
Local backups	• Local control of where data files reside and who has access to them. • Accessibility – in the event of a disaster that impacts network connectivity, locally stored backup media may be more accessible. • Speed of file restores – locally attached media restore times are usually faster than over the Internet.	• Scalability – keeping local backups often requires manual intervention and handling of the media. The media itself has storage limitations that may cause issues as data file sizes increase. • Off-site storage requirements, fire protection, and environmental controls.

Elements of a Disaster Recovery Plan

There are five major phases of creating and implementing a disaster recovery plan:

Phase 1 - Network Design Recovery Strategy
Phase 2 - Inventory and Documentation
Phase 3 - Verification
Phase 4 - Approval and Implementation
Phase 5 - Review

14.3 Ethical and Legal Considerations

Ethical and Legal Considerations in IT

Respect your customers, as well as their property. Computers and monitors are property, but property also includes any information or data that might be accessible, for example:

- Emails
- Phone lists and contact lists
- Records or data on the computer
- Hard copies of files, information, or data left on a desk

Before accessing computer accounts, including the administrator account, get the permission of the customer.

Personal Identifiable Information (PII)

Examples of PII include, but are not limited to:

- Names, such as full name, maiden name, mother's maiden name, or alias
- Personal identification numbers, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number, address information, such as street address or email address
- Personal characteristics, including photographic images (especially of the face or other identifying characteristics), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)

PII violations are regulated by several organizations in the United States, depending on the type of data.

The EU General Data Protection Regulation (GDPR) also regulates how data is handled for personal data, including financial and healthcare information.

Payment Card Industry (PCI)

Payment Card Industry (PCI) information is considered personal information that needs to be protected.

The PCI Security Standards Council was formed in 2005 by the 5 major credit card companies in an effort to protect account numbers, expiration dates, magnetic strip and chip data for transactions around the globe.

For more information on PCI, visit www.pcisecuritystandards.org.

Protected Health Information (PHI)

- Protected Health Information (PHI) is another form of PII that needs to be secured and protected.
- PHI includes patient names, addresses, dates of visits, telephone and fax numbers, and email addresses.
- With the move from paper copy records to electronic records, Electronic Protected Health Information (ePHI) is also regulated.
- Penalties for breaches of PHI and ePHI are very severe and regulated by the Health Insurance Portability and Accountability Act (HIPAA).

Lab – Investigate Breaches of PII, PHI, PCI

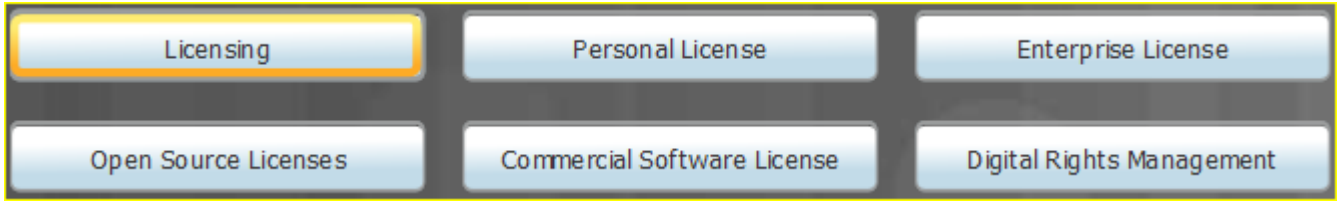
In this lab, you will investigate breaches of PII, PHI, and PCI by searching the Internet and then recording your findings.

Legal Considerations in IT

The laws in different countries and legal jurisdictions vary, but generally, actions such as the following are considered to be illegal:

- It is not permissible to make any changes to system software or hardware configurations without customer permission.
- It is not permissible to access a customer's or co-worker's accounts, private files, or email messages without permission.
- It is not permissible to install, copy, or share digital content (including software, music, text, images, and video) in violation of copyright and software agreements or the applicable law. Copyright and trademark laws vary between states, countries, and regions.
- It is not permissible to use a customer's company IT resources for commercial purposes.
- It is not permissible to make a customer's IT resources available to unauthorized users.
- It is not permissible to knowingly use a customer's company resources for illegal activities. Criminal or illegal use typically includes obscenity, child pornography, threats, harassment, copyright infringement, Internet piracy, university trademark infringement, defamation, theft, identity theft, and unauthorized access.
- It is not permissible to share sensitive customer information. You are required to maintain the confidentiality of this data.

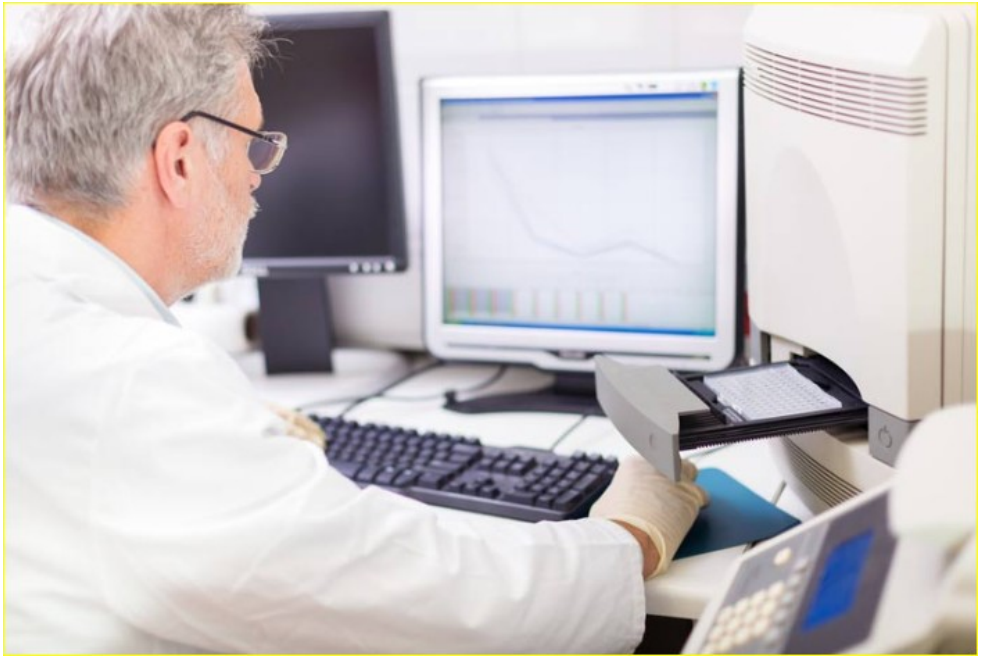
Licensing



- It is illegal to use licensed software without the appropriate license.
- An example of a personal software license is an End User License Agreement (EULA).
- An enterprise license is a software license held by a company for its employees to use.
- Open-source licensing is a copyright license for software that allows developers to modify and share the source code that runs the software.
- If you use software to make money, you must pay for a commercial license.
- Digital rights management (DRM) is software that is designed to prevent illegal access to digital content and devices.

Computer Forensics

Data from computer systems, networks, wireless communications, and storage devices may need to be collected and analyzed in the course of a criminal investigation. The collection and analysis of data for this purpose is called computer forensics. The process of computer forensics encompasses both IT and specific laws to ensure that any data collected is admissible as evidence in court.



Data Collected in Computer Forensics

Two basic types of data are collected when conducting computer forensics procedures:

- **Persistent data** - Persistent data is stored on a local drive, such as an internal or external hard drive, or an optical drive. When the computer is turned off, this data is preserved.

- **Volatile data** - RAM, cache, and registries contain volatile data. Data in transit between a storage medium and a CPU is also volatile data. If you are reporting illegal activity or are part of an incident response team, it is important to know how to capture this data, because it disappears as soon as the computer is turned off.

Cyber Law

- Cyber law is a term to describe the international, regional, country, and state laws that affect computer security professionals.
- IT professionals must be aware of cyber law so that they understand their responsibility and their liability as it relates to cybercrimes.
- Cyber laws explain the circumstances under which data (evidence) can be collected from computers, data storage devices, networks, and wireless communications. They can also specify the manner in which this data can be collected.
- In the United States, cyber law has three primary elements:
  - Wiretap Act
  - Pen/Trap and Trace Statute
  - Stored Electronic Communication Act

IT professionals should be aware of the cyber laws in their country, region, or state.

First Response

- First response is the term used to describe the official procedures employed by those people who are qualified to collect evidence.
- Routine administrative tasks can affect the forensic process. If the forensic process is improperly performed, evidence that has been collected might not be admissible in court.
- You may be the person who discovers illegal computer or network activity. Do not turn off the computer. Volatile data about the current state of the computer can include programs that are running, network connections that are open, and users who are logged in to the network or to the computer. This data helps to determine a logical timeline of the security incident. It may also help to identify those responsible for the illegal activity.
- Be familiar with your company's policy regarding cybercrimes. Know who to call, what to do and, just as importantly, know what not to do.

Documentation

If you discover illegal activity on a computer or network on which you are working, at a minimum, document the following:

- Initial reason for accessing the computer or network
- Time and date
- Peripherals that are connected to the computer
- All network connections
- Physical area where the computer is located
- Illegal material that you have found
- Illegal activity that you have witnessed (or you suspect has occurred)
- Which procedures you have executed on the computer or network

Chain of Custody

- To prove the chain of custody, first responders have documentation procedures in place that track the collected evidence.
- These procedures also prevent evidence tampering so that the integrity of the evidence can be ensured.
- Incorporate computer forensics procedures into your approach to computer and network security to ensure the integrity of the data.
- These procedures help you capture necessary data in the event of a network breach. Ensuring the viability and integrity of the captured data helps you prosecute the intruder.

14.4 Call Center Technicians

Call Centers

- A call center environment is organized and professional.
- Customers call in to receive computer-related help.
- The workflow of a call center starts with calls from customers displayed on a callboard.
- Level one technicians answer these calls in the order that the calls arrive. If the level one technician cannot solve the problem, it is escalated to a level two technician.
- The technician must supply the level of support that is outlined in the customer's Service Level Agreement (SLA).
- A call center might exist within a company and offer service to the employees of that company as well as to the customers of that company's products.
- Alternatively, a call center might be an independent business that sells computer support as a service to outside customers.
- In either case, a call center is a busy, fast-paced work environment, often operating 24 hours a day.

Call Centers (Cont.)

Computers in call centers have support software that technicians use to manage many of their job functions:

- Log and Track Incidents
- Record Contact Information
- Research Product Information
- Run Diagnostic Utilities
- Research a Knowledge Base
- Collect Customer Feedback

Each call center has business policies regarding call priority. Consider this sample chart of how calls can be named, defined, and prioritized.

Call Prioritization

Name	Definition	Priority
Down	The company cannot operate any of its computer equipment.	1 (Most Urgent)
Hardware	One (or more) of the company's computers is not functioning correctly.	2 (Urgent)
Software	One (or more) of the company's computers is experiencing software or operating system errors.	2 (Urgent)
Network	One (or more) of the company's computers cannot access the network.	2 (Urgent)
Enhancement	There has been a request from the company for additional computer functionality.	3 (Important)

Level One Technician Responsibilities

- Call centers sometimes have different names for level one technicians. These technicians might be known as level one analysts, dispatchers, or incident screeners.
- The primary responsibility of a level one technician is to gather pertinent information from the customer.

Information Checklist

- Contact information
- What is the manufacturer and model of computer?
- What OS is the computer using?
- Is the computer plugged in to the wall or running on battery power?
- Is the computer on a network? If so, is it a wired or wireless connection?
- Was any specific application being used when the problem occurred?
- Have any new drivers or updates been installed recently? If so, what are they?
- Description of the problem
- Priority of problem

Level Two Technician Responsibilities

- Call centers sometimes have different names for level two technicians.
- These technicians might be known as product specialists or technical-support personnel.
- The level two technician is usually more knowledgeable and experienced than the level one technician or has been working for the company for a longer period of time.
- When a problem cannot be resolved within a predetermined amount of time, the level one technician prepares an escalated work order.
- The level two technician receives the escalated work order with the description of the problem and then calls the customer back to ask any additional questions and resolve the problem.
- Level two technicians can also use remote access software to connect to the customer's computer to:
  - update drivers and software
  - access the operating system
  - check the BIOS
  - gather other diagnostic information to solve the problem

Level Two Technician Responsibilities (Cont.)

The level one technician prepares an escalated work order.

Work Order

Company Name: Cisco Systems, Inc.
Contact: Office Manager
Company Address: 170 West Tasman Drive, San Jose, CA 95134
Company Phone: 408-526-4000

Generating a New Ticket

Category	HW	Closure Code		Status	Open
Type	Laptop	Escalated?	Y	Pending	
Item	Laptop	Business Impacting:	○ Yes ◉ No	Pending Until Date	
Summary	Won't Boot				
Case ID	Cisco001	Connection Type	Wireless network connection		
Priority	Medium			Environment	Mobile
User Platform	Windows 7				

Problem Description
User complains that the laptop won't boot up.
No software was added recently. No operating system changes have been made.
No peripherals have been added.

Problem Solution
The level one technician was unable to resolve the problem within 10 minutes.
The work order is being escalated to a level two technician.

Lab – Remote Technician – Fix a Hardware Problem

In this lab, you will gather data from the customer, and then instruct the customer to fix a computer that does not boot.

Lab – Remote Technician – Fix an Operating System Problem

In this lab, you will gather data from the customer, and then instruct the customer to fix a computer that does not connect to the network.

Lab – Remote Technician – Fix a Network Problem

In this lab, you will gather data from the customer, and then instruct the customer to fix a computer that does not connect to the network.

Lab – Remote Technician – Fix a Security Problem

In this lab, you will gather data from the customer and instruct the customer to fix a computer that cannot connect to a workplace wireless network.

Script Examples

- A script file is a simple text file written in scripting languages to automate processes and tasks on various operating systems.
- A script file might be used to automate the process of performing a backup of a customer's data or run a list of standard diagnostics on a broken computer.
- The script file can save the technician a lot of time, especially when the same tasks need to be performed on many different computers.
- You should also be able to identify the many different types of script files because a script file may be causing a problem at startup or during a specific event.

Script Examples (Cont.)

```
@echo off
echo My first batch script!!
echo My hostname is: %computername%
pause
```

The four lines of this Windows batch script do the following:

1. Turn off automatic echoing output at the terminal.
2. Echo the sentence, "My first batch script!!" to the terminal.
3. Echo "My hostname is:" followed by the variable %computername% to the terminal.
4. Pause the script with a prompt of "Press any key to continue..."

Windows batch script

```
#!/bin/bash
echo My first batch script!!
echo My hostname is: $(hostname)
sleep 2
```

The four lines of this Linux shell script do the following:

1. Identify the shell that the script will be using.
2. Echo the sentence, "My first batch script!!" to the terminal.
3. Echo "My hostname is:" followed by the variable $(hostname) to the terminal.
4. Pause the script for two seconds.

Linux shell script

Script Languages

Script Types

Scripting Language	Extensions	Description
Windows Batch File	.bat	Windows command-line interpreted language
PowerShell	.ps1	Windows task-based command-line shell and scripting language
Linux Shell Script	.sh	Linux shell interpreted language
VBScript	.vbs	Windows visual basic script
JavaScript	.js	Client-side scripting language that runs in the browser
Python	.py	An Interpreted, object-oriented, high-level language

A scripting language is different than a compiled language because each line is interpreted and then executed when the script is run.

Script Syntax

Scripting Language	Comment Syntax
Windows Batch File	REM comment
PowerShell	# comment or <# comment #>
Linux Shell Script	# comment
VBScript	` comment
JavaScript	// comment
Python	# comment

Various comments found in scripts based on the script type

Basic Script Commands

Windows

SCRIPTING LANGUAGE	COMMAND	OUTPUT
Windows Batch File	dir	View the contents of the current directory
Windows Batch File	cd	Change directories
Windows Batch File	mkdir	Make a directory
Windows Batch File	cls	Clear the screen
Windows Batch File	date	Display / set the date
Windows Batch File	copy	Copy a file or files

Linux

SCRIPTING LANGUAGE	COMMAND	OUTPUT
Linux Shell Script	ls	View the contents of the current directory
Linux Shell Script	cd	Change directories
Linux Shell Script	mkdir	Make a directory
Linux Shell Script	clear	Clear the screen
Linux Shell Script	date	Display / set the date
Linux Shell Script	cp	Copy a file or files

Variables/Environmental Variables

Variables

Variables are designated places to store information within a computer. A primary function of computers is to manipulate variables. Some variables are environmental, which means that they are used by the operating system to keep track of important details such as: username, home directory, and language. Some useful Windows environmental variables are %SystemDrive% (the drive where the system folder is) and %WinDir% (exactly where the Windows folder

Environmental Variables

The figure is of a shell script depicting environmental variables. The Linux variables PWD, LANGUAGE, and SHELL were preset when the user logged into this terminal. To view a list of all environmental variables use the env command.

Variable Type

The figure on this page is a table of variable types.

Some scripting languages require that variables are defined as being integers (numbers), characters, strings or something else. In code, a string usually contains multiple characters but can also use numbers and spaces. Often, when defining a string, quotes are used to denote the beginning and end of the string, for example, " Dan sold 3 cars yesterday"

DATA TYPE	DESCRIPTION	EXAMPLE
int	Integer Numbers	-1,0,1,2,3
float	Numbers with Decimals	1234.5678
char	A Single Character	S
string	Multiple Characters	He77o!
bool	True or False	True

Conditional Statements

Conditional Statements

Conditional statements are needed for scripts to make decisions. These statements usually come in the form of an if-else or a case statement. In order for these statements to make a decision, a comparison must be made using operators. The syntax of these commands will vary, depending on the Operator language.

If-Then Statements

This figure is of a shell script determining if it is morning or afternoon.

In this script, the date command is cut until only the hour remains, and the result is placed in a variable. The if statement compares the variables $TIME and $NOON using the -ge operator to determine if the output is going to say “afternoon” or “morning”

Relational Operators

This figure is a list of relational operators in various scripts.

When making a mathematical comparison, use relational operators. Other types of operators include arithmetic (+, -, *, /, %), logical (and, or, not), assignment (+=, -+, *=), and bitwise (&, |, ^).

OPERATOR	BATCH	POWERSHELL	BASH	PYTHON
Equal	== EQU	-eq	-eq	==
Not Equal	!= NEQ	-ne	-ne	!=
Less Than		-lt	-lt	<
Greater Than	>GTR	-gt	-gt	>
Less Than or Equal To	<=LEQ>	-le	-le	<=
Greater Than or Equal To	>=GEQ	-ge	-ge	>=

Loops

Loops

In order to repeat commands or tasks a loop can be used. The three main types of loops found in scripts are the For loop, the While loop, and the Do-While loop.
The For loop repeats a section of code a specified number of times. The While loop checks a variable to verify that it is true (or false) before repeating a section of code. This is known as a pre-test loop. Finally, the Do-While loop repeats a section of code, then checks a variable to verify that it is true (or false). This is known a s a post-test loop.

For Loops

This figure is of a shell script which outputs five binary numbers. The For loop in this script repeats a sequence exactly five times. The variable NUMBER1 is randomly generated to be between 0 and 255. The variable NUMBER2 is the binary conversion of NUMBER1. The spacing between the commands “for” and “done” are optional in some languages, but they help the programmer to understand what code is contained in the loop.

While Loops

This figure is of a shell script which runs until a randomly chosen number is greater than 8.
In this script, the loop keeps running until a random number is chosen which is greater than eight. Notice how the variable NUMBER was set to 1 before the loop started. This was to prevent the test in the next line [$NUMBER -le 8] from failing.

Do While Loops

This figure is of a shell script determining if a vowel or consonant is used.
Unlike most compiled languages, several scripting languages lack a Do-While loop. In this case, we are emulating the post-test function using an If statement within the loop followed by a Break statement.

Lab – Writing Basic Scripts in Linux, Windows, Python, and JavaScript

In this lab, you will write some basic scripts in different scripting languages to help understand how each language handles automating tasks

14.5 Chapter Summary

Chapter 14: The IT Professional

- Explain why good communication skills are a critical part of IT work.
- Explain how to manage change and unplanned disruptions in a business environment.
- Explain appropriate behavior when faced with the legal and ethical issues that arise in the IT industry.
- Explain the call center environment and technician responsibilities.