CH 7: Policies to Protect Data

- Implement Security Best Practices
- Implement Data Protection Policies
- Protect Data During Incident Response

Topic A: Implement Security Best Practices

CompTIA

Authentication

Authentication factor: Information used to identify a user.

Access control depends on credentials being known only to the account holder.

Use various authentication factors:

Something you know

Something you have

Something you are

Something You Know: Strong Passwords

Strong passwords

8 – 14 characters for regular user accounts, longer for administrative accounts

No single words

Mixed case

Use easily memorized phrase

Don't write down passwords or share passwords

Change the password periodically

Password management

Single sign on

Avoid using work passwords for personal accounts

Implement BIOS/UEFI passwords

Something You Have: Smart Cards and Tokens

RFID: A chip allowing data to be read wirelessly.

Key fob: A chip implanted in a plastic fob.

- Smart card is "**something you have**"
  - Chip contains authentication data
  - Card reader reads the data to authenticate the user
  - Can be a contactless card using RFID

- Token-based technology
  - SecurID token from RSA
  - Contained in a key fob
    - Generates random number code
    - Synchronized to code on the server
    - One-time password

Something You Are: Biometrics

- Something you "are"
  - Fingerprint
  - Signature
  - Iris or retina
  - Facial recognition
  - Voice

[illegible]

- Biometric data is scanned and recorded in a database.
- User is rescanned to access resources and compared to database record.
- False negatives and false positives can occur.

Multifactor Authentication

- Single factor can be easily compromised
- Two-factor and three-factor authentication is much stronger
  - Must use different authentication factor types

- **Two-factor authentication**: An authentication scheme that requires validation of two authentication factors.
- **Three-factor authentication:** An authentication scheme that requires validation of three authentication factors.

Software Tokens

Replay attack: Where the attacker intercepts some authentication data and reuses it to try to re-establish a session.

System grants token to remember the user's authentication

If not securely designed, token can be captured by a third party

Token based authorization:

- Used in SSO
- Domain logins use Kerberos
- Implemented as cookies on the web

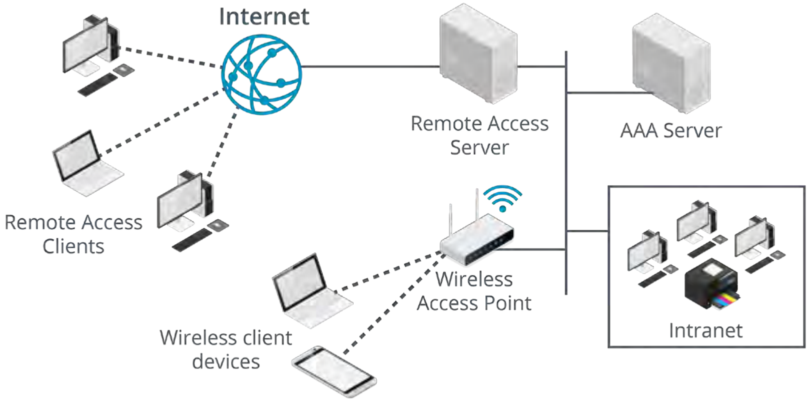
Software tokens can use digital signing

Should be designed to prevent replay

Remote Authentication

- **Remote Authentication Dial-in User Service:** (**RADIUS**) Used to manage remote and wireless authentication infrastructure.

- **Terminal Access Controller Access Control System:** (**TACACS+**) An alternative to RADIUS.



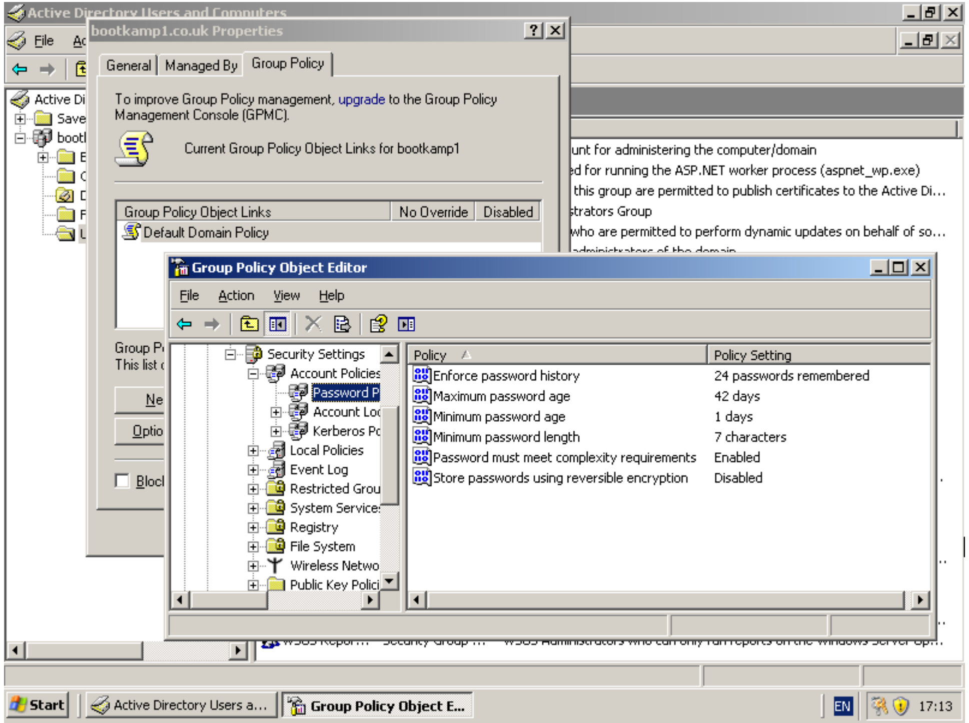
Password and Account Policies

Access Control List: (**ACL**) The permissions attached to or configured on a network resource

- Many authentication systems still password based
- Use policies to enforce ACLs:
  - Require passwords
  - Change default admin user name
  - Change default user passwords
  - Disable guest account
  - Restrict user permissions (least privilege)
- **Use Local Security Policies**
- Use Group Policy Objects in domains

Password Protection Policies

- Minimum password length
- Complexity requirements
- Maximum password age
- Password history
- Minimum password age
- User cannot change password
- Password never expires



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

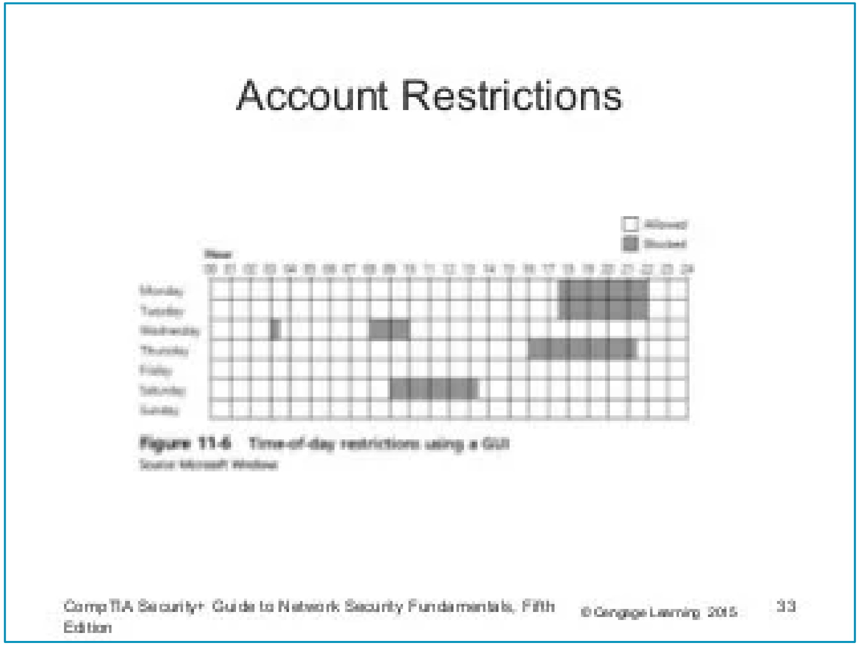
Current Group Policy Object Links for bootkamp1

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Restrictions

- Logon Time Restriction
- Station Restriction
- Concurrent Logons
- Account Expiration Date
- Disable Account
- Failed Attempts Lockout



Account Restrictions

Figure 11-6 Time-of-day restrictions using a GUI

Source: Microsoft Windows

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition © Cengage Learning 2015 33

Desktop Lock and Timeout

After logon, system trusts workstation implicitly

Someone else could use the system if left unlocked

Lunchtime attack

Lock workstations whenever unattended

Windows key + L

Set screensaver to require password on resume

System displays the screensaver after set inactivity time

Locks the desktop after inactivity time

Guidelines for Implementing Security Best Practices

- Enforce use of ACLs through Local Security Policy or Group Policy Objects.
- Enforce the use of strong passwords through GPOs.
- Implement account restrictions.
- Require users to lock unattended systems.
- Implement timeouts for unattended systems.

Guidelines for Implementing Security Best Practices

- Consider using multifactor authentication.
- Create secure passwords.
- Consider password protecting BIOS/UEFI.
- Take measures to prevent software tokens from being used in replay attacks.
- Consider using RADIUS in VPN implementations and TACACS+ for authenticating administrative access to routers and switches. test

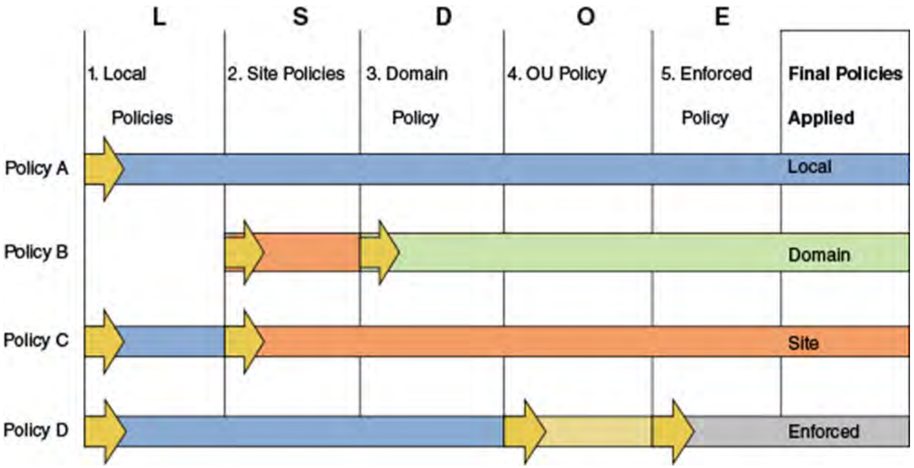
Guidelines for Implementing Security Best Practices

Which Policy Wins

- onetime policies overlap or conflict

Order in which policies are applied; the last policy applied wins

- Local
- Site
- Domain
- OU
- Enforced



L S D O E

1. Local Policies

2. Site Policies

3. Domain Policy

4. OU Policy

5. Enforced Policy

Final Policies Applied

Policy A — Local

Policy B — Domain

Policy C — Site

Policy D — Enforced

Discussing Security Best Practices Implementation

- **What constitutes a strong password?**

- **ANSWER:**
  - Something easy to remember but difficult to guess. A password should be sufficiently long and mix alphanumeric and punctuation characters and case.

Discussing Security Best Practices Implementation

- **How does a smart card provide authentication?**

- **ANSWER:**
  - It contains a chip that can store the user's account and credentials securely in a digital certificate that the logon provider trusts. Therefore, possession of the device is confirmation of identity.

Discussing Security Best Practices Implementation

- **Why should use of a smart card be protected by a PIN?**

- **ANSWER:**
  - To prevent misuse of the card if it is lost or stolen.

Discussing Security Best Practices Implementation

- **What are the drawbacks of biometric authentication technologies?**

- **ANSWER:**
  - Users find it **intrusive**, it is relatively **expensive** (compared to password-based authentication), and there are risks from **false positives** and false negatives.
  - Some implementations of biometric methods can be vulnerable to spoofing, such as using a photograph to pass through a facial recognition system.

Discussing Security Best Practices Implementation

- **What type of biometric recognition is most suitable for integrating with a laptop computer?**

- **ANSWER:**
  - Finger or thumbprint readers are generally the simplest type of device. Facial recognition using a built-in camera is also becoming popular.

Discussing Security Best Practices Implementation

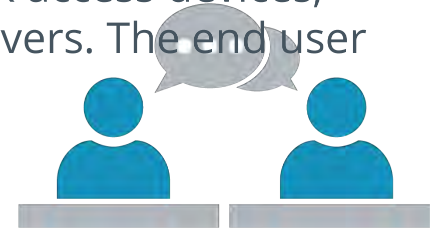
- **What general methods can be used to prevent a replay attack against a software token?**

- **ANSWER:**
  - Using coding techniques to accept a token only once or restrict the timeframe in which a token can be used.

Discussing Security Best Practices Implementation

- **In AAA architecture, what type of device might a RADIUS client be?**

- **ANSWER:**
  - AAA refers to Authentication, Authorization, and Accounting.
  - When the role is played by a Remote Access Dial-in User Service (RADIUS) server, the server processes authentication and authorization requests.
  - The clients submitting the requests to the server are network access devices, such as routers, switches, wireless access points and VPN servers. The end user devices connecting to them are referred to as supplicants.



Discussing Security Best Practices Implementation

- **What type of account policy can protect against password-guessing attacks?**

- **ANSWER:**
  - A lockout policy (disables the account after a number of incorrect logon attempts).

Topic B: Implement Data Protection Policies

Data Policies

Information Content Management: (**ICM**) The process of managing information over its lifecycle, from creation to destruction.

- Documents are classified based on sensitivity levels:
  - Unclassified: there are no restrictions
  - Classified: internal use only/official use only
  - Confidential: information is highly sensitive, viewing only by approval
  - Secret: Viewing is severely restricted.
  - Top Secret: the highest level of classification
- Confidential, secret, and top-secret information should be securely protected (encrypted) for storage and transmission.

PII

Personally Identifiable Information: (PII) Data that can be used to identify or contact an individual.

- Some information becomes PII based on how it is used, including:
  - Social security number
  - Date of birth
  - Email address
  - Phone number
  - Address
  - Biometric data

COMMON TYPES OF PII
NAME
ALIAS
POSTAL ADDRESS
UNIQUE PERSONAL IDENTIFIER
ONLINE IDENTIFIER
IP ADDRESS
EMAIL ADDRESS
ACCOUNT NUMBER
SOCIAL SECURITY NUMBER
DRIVER'S LICENSE
PASSPORT NUMBER
PHONE NUMBER

PII

PHI:

- Anonymizes data
- Highly sensitive and unrecoverable; cannot be changed

PCI DSS:

- Identifies steps to take if cardholder data is stored
- Specific cyber-security controls

Protected Health Information: (PHI) Information that identifies someone as the subject of medical and insurance records, plus associated hospital and laboratory test results.

Payment Card Industry Data Security Standard: (**PCI DSS**) A standard for organizations that process credit or bank card payments.

Browser Protection Policies

- Extension
  - Script that uses the browser application programming interface (API) to implement new or modified functionality
- Plug-in
  - Executable designed to handle a specific type of object embedded on a web page
  - Generally deprecated due to risks from vulnerabilities
- Apps, default search provider, and themes
- Trusted versus untrusted sources
  - Browser plug-in store/marketplace

Browser Protection Policies

- Sign-in and browser data synchronization
- Password managers

- Settings page
  - Ellipsis (...) or Hamburger (☰) menu
  - chrome://settings
    edge://settings
    about:preferences

Browser Protection Policies

- Transport Layer Security (TLS) and digital certificates
- HTTPS browser validation
  - Padlock icon
  - High assurance certificates
- Trusted root certificate updates
  - Windows Update
  - Separate per-browser stores

Browser Privacy Settings

- Site privacy and content controls
  - Cookie policy and tracking protection
  - Pop-up blocker
  - Ad blockers

- Browser cache
  - Clearing cache and browsing data
  - Private/incognito browsing mode

ACLs and Directory Permissions

Permissions: Rights granted to access files and folders.

Access Control List: (**ACL**) The permissions attached to or configured on a network resource.

Access Control Entries: (**ACE**) Within an ACL, the records of subjects and the permissions they hold on the resource.

Permissions are usually implemented as ACL attached to a resource.

Windows has two permission types:

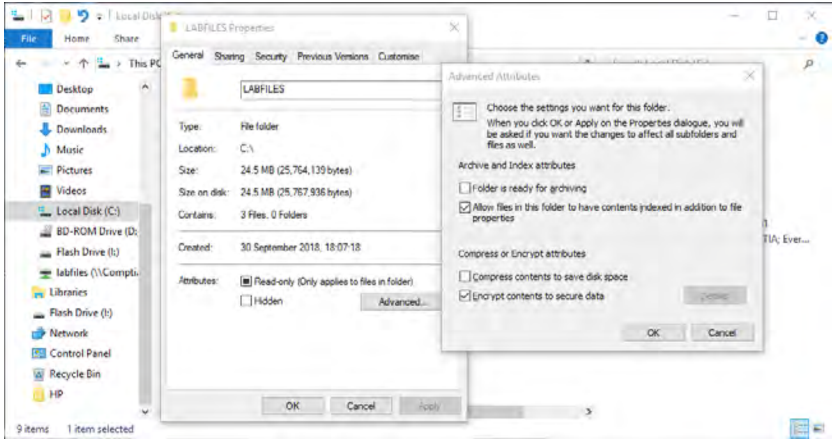
- File system permissions enforced by NTFS
- Share-level permissions

Linux uses the same set of permissions at the local level and over the network.

Data Encryption

must be in a bussines edtion or enterprise

Encrypting File System: (EFS) Under NTFS, files and folders can be encrypted to ensure privacy of the data.



LABFILES Properties

General | Sharing | Security | Previous Versions | Customise

LABFILES

Type: File folder

Location: C:\

Size: 24.5 MB (25,764,139 bytes)

Size on disk: 24.5 MB (25,767,936 bytes)

Contains: 3 Files, 0 Folders

Created: 30 September 2018, 18:07:18

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

Advanced... | OK | Cancel | Apply

Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialogue, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

□ Folder is ready for archiving

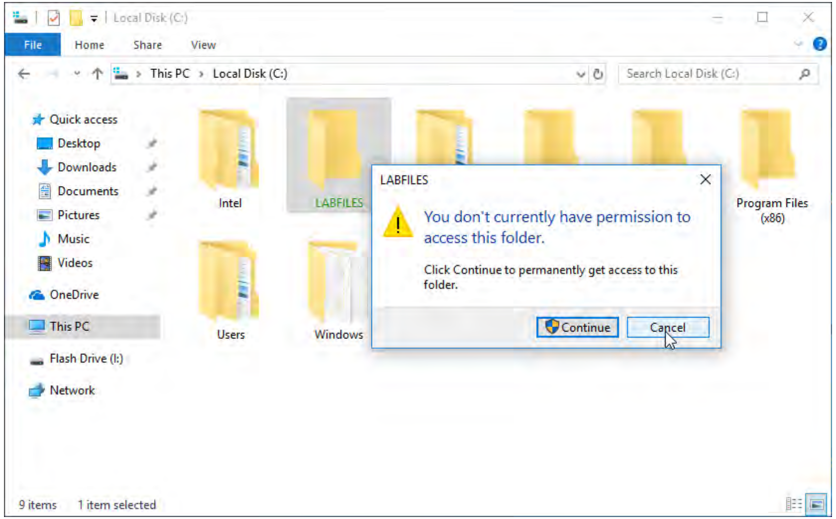
☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Details | OK | Cancel



LABFILES

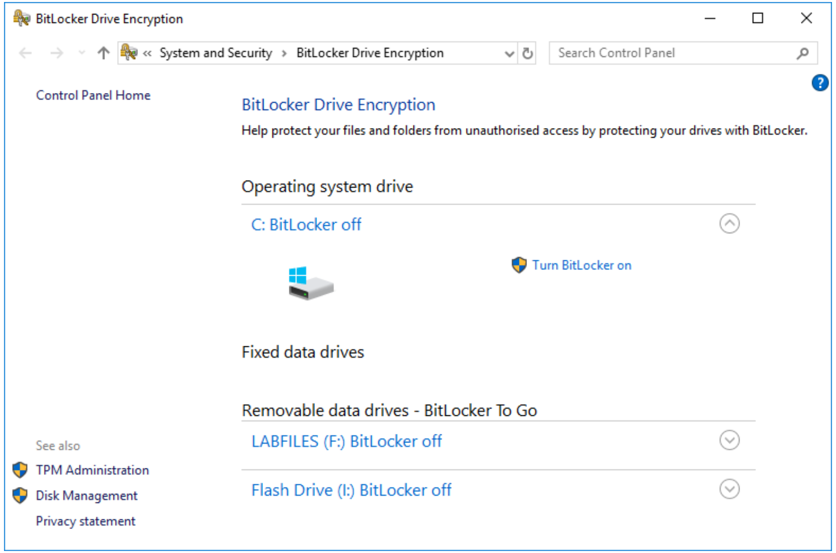
You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.

Continue | Cancel

Full Disk Encryption

Full Disk Encryption: (FDE) Encryption of all data on a disk.



BitLocker Drive Encryption

BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

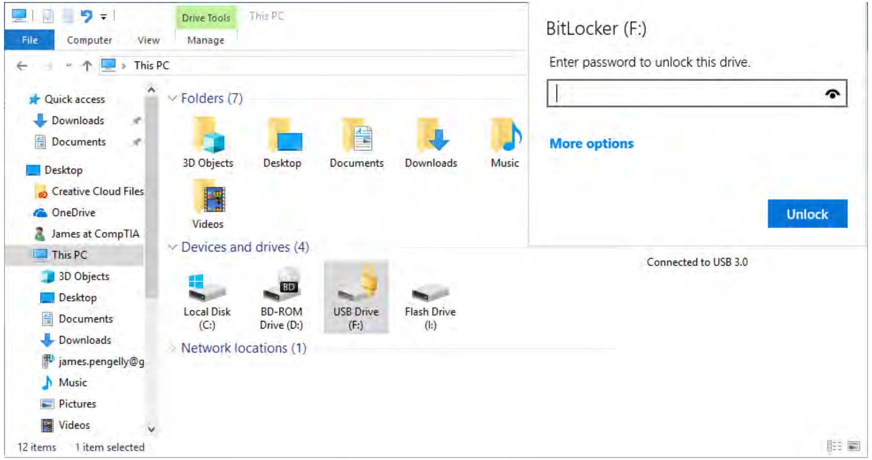
Turn BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

LABFILES (F:) BitLocker off

Flash Drive (I:) BitLocker off



BitLocker (F:)

Enter password to unlock this drive.

Data Loss Prevention (DLP)

Data Loss Prevention: (DLP) Software that can identify data that has been classified and apply fine-grained user privileges to it.

- Policy server: to configure confidentiality rules
- Endpoint agents: to enforce policy on client computers
- Network agents: to scan communications at network borders and interface

Software Licensing and DRM

End User License Agreement: (EULA) The agreement governing the installation and use of proprietary software.

- Most AUPs prohibit abuse of Internet services to download games or obscene content
- Must accept the EULA when installing software
- Software often activated using a product key
- Each computer requires licensed software in most cases
- Types of licenses include:
  - **OEM**
  - **Retail**
  - **Volume**
  - **Server**

Software Licensing and DRM

Shareware: Software you can install free of charge for a **limited time** or with limited functionality.

Freeware: Software that is available for download and use free of charge.

Open source: Programming code used to design the software is freely available.

Digital Rights Management: (**DRM**) Copyright protection technologies for digital media.

Guidelines for Implementing Data Protection Policies

- Classify documents based on how sensitive they are.
- Protect PII, PHI, and PCI data.
- Implement permissions as ACLs attached to resources.
- Use full disk, folder, and file encryption.
- Implement a data loss prevention policy.
- Follow all software licensing agreements and DRM.

Discussing Data Protection Policies

- **Why should PII be classed as sensitive or confidential?**
- **ANSWER:**
  - Disclosing Personally Identifiable Information (PII) may lead to loss of privacy or identity theft. There may be legal or regulatory penalties for mishandling PII.

Discussing Data Protection Policies

- **What is PHI?**
- **ANSWER:**
  - Protected Health Information (PHI) is data such as medical records, insurance forms, hospital/laboratory test results, and so on.

Discussing Data Protection Policies

- **True or false? The encryption applied by EFS can be overridden by the local administrator account.**

- **ANSWER:**
  - False—only the user can decrypt files, via their account password or a backup key. In a Windows domain, administrators can be configured key recovery agents but the local administrator does not have this right automatically. This means that the disk cannot be connected to a different computer to circumvent the protection afforded by encryption.

Discussing Data Protection Policies

- **What is the function of a TPM in relation to Windows' BitLocker feature?**

- **ANSWER:**
  - A Trusted Platform Module can store the disk encryption key to tie use of the disk to a particular computer.

Discussing Data Protection Policies

- **You are advising a customer on purchasing security controls. What class of security technology prevents users from sending unauthorized files as email attachments?**

- **ANSWER:**
  - Data Loss Prevention (DLP).

CompTIA

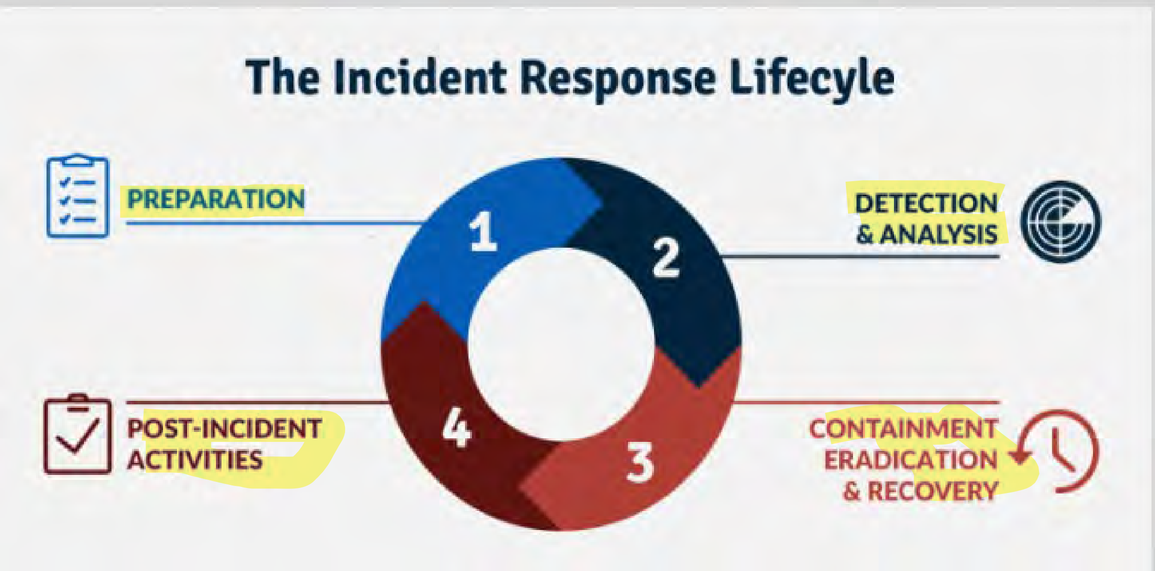
Discussing Data Protection Policies

- **What type of software license is locked to a single hardware device?**

- **ANSWER:**
  - Original Equipment Manufacturer (OEM).

Topic C: Protect Data During Incident Response

test


The Incident Response Lifecyle
PREPARATION
1
DETECTION & ANALYSIS
2
CONTAINMENT ERADICATION & RECOVERY
3
POST-INCIDENT ACTIVITIES
4

Incident Response Policies

Security incidents might include:

- Computer or network infected with virus, worms, Trojans
- Evil twin Wi-Fi access point
- DoS attack
- Unlicensed software
- Finding prohibited material on a PC

Security incident handling lifecycle:

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activity

Incident Response Documentation

- Preparation is key to effective response.
- Documented policies and procedures for dealing with security breaches.
- Personnel and resources to implement the policies.
- Clear lines of communication.
  - Reporting incidents.
  - Notifying affected parties as part of incident management.
- Contact information and alternative communication channels.
- Review and update periodically or after a trigger event.
  - Staff changes.
  - Deployment of new network or security systems.
  - Changes in legal or regulatory requirements.

First Responders

Incident: Something that is not normal and disrupts regular operations in the computing environment.

Computer Security Incident Response Team: (**CSIRT**) Team with responsibility for incident response.

- Categorize and prioritize incident types.
- CSIRT : (Computer Security Incident Response Team)
  - Provide the range of decision making and technical skills needed to respond to incidents.
  - Mix of senior decision makers, managers, and technicians.
- Employees at all levels must be trained to recognize and respond to actual or suspected security incidents.

Data and Device Preservation

Forensics: The process of gathering and submitting computer evidence to trial.

Latent: Evidence that cannot be seen with the naked eye and instead must be interpreted using a machine or process.

- Collection of evidence:
  - What evidence must be collected?
  - How should evidence be collected?

CompTIA

Data and Device Preservation

- General procedure:
  - Document crime scene
  - Interview witnesses
  - Gather evidence from the live system
  - Use forensic tools
  - Make cryptographic hash of collected data
  - Shut down or power off system
  - Place evidence in tamper-proof bags

Chain of Custody

Chain of custody: Documentation attached to evidence from a crime scene detailing when, where, and how it was collected, where it has been stored, and who has handled it subsequently to collection.

- Evidence must conform to valid timeline.
- Digital information must be tightly controlled against tampering.
- Each step should be documented and recorded.
- After evidence is bagged, must not be handled or inspected except in controlled circumstances.
- Use Chain of Custody form to record:
  - When, where, who collected evidence.
  - Who handled it subsequently.
  - Where it is stored.

Discussing Data Protection During Incident Response

- **What is incident reporting?**

- **ANSWER:**
  - The process of identifying security breaches (or attempted breaches and suspicious activity) to security management personnel.

Discussing Data Protection During Incident Response

- **Why are the actions of a first responder critical in the context of a forensic investigation?**

- **ANSWER:**
  - Digital evidence is difficult to capture in a form that demonstrates that it has not been tampered with. Documentation of the scene and proper procedures are crucial.

Discussing Data Protection During Incident Response

- **What does Chain of Custody documentation prove?**
- **ANSWER:**
    - Who has had access to evidence collected from a crime scene and where and how it has been stored.