Chapter 13: Incident Preparation and Investigation

Business Continuity Planning

- **Business continuity** is the ability of an organization to maintain its operations and services in the face of a disruptive event or disaster
- **Business continuity planning** is the process an organization undertakes in advance to determine a plan of action in the event of a disaster
  - The outcome of this planning is a **business continuity plan** (**BCP**), which is a strategic document that provides alternative modes of operation for business activities

Business Continuity Planning

- A BCP should include the following elements:
  - High availability
  - Scalability
  - Diversity
  - On-prem and cloud
- **Continuity of operation planning** (**COOP**) is a federal initiative that is intended to encourage organizations to address how critical operations will continue under a broad range of negative circumstances

Business Continuity Planning

- A **business impact analysis** (**BIA**) identifies business processes and functions and then quantifies the impact a loss of these functions may have on business operations
- A BIA is designed to identify those processes that are critically important to an enterprise
  - It will help determine the **mission-essential function** (the activity that serves as the core purpose of the enterprise
  - Another goal of a BIA is to identify the **single point of failure** of a system

Business Continuity Planning

- A subset of a BCP is called a **disaster recovery plan** (**DRP**)
  - It is a written document that details the process for restoring IT resources following an event that causes a significant disruption in service
- One topic of a DRP is the sequence in restoring systems (**restoration order**)
- Factors that affect the restoration order include dependencies, importance of processes, and alternative business practices

Incident Response Planning

- Step to take in preparation for an incident:
  - Create an incident plan
  - Perform testing exercises
  - Study attack frameworks
- An **incident response plan** is a set of written instructions for reacting to an information security incident and should contain the following:
  - Definitions, incident response teams, and reporting requirements

Incident Response Planning

- It is important to test an incident response plan by conducting simulated **testing** exercises to make necessary adjustments
- An information security **framework** is a series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment
  - Frameworks can be studied about how attacks occur, called exploitation frameworks

Resilience Through Redundancy

- **Capacity planning** is the process of forecasting the need for future resources
  - It involves calculating the following:
    - Future human resources (**people capacity planning**)
    - Predicting the number of devices needed (**technology capacity planning**)
    - The size of the network (**infrastructure capacity planning**)

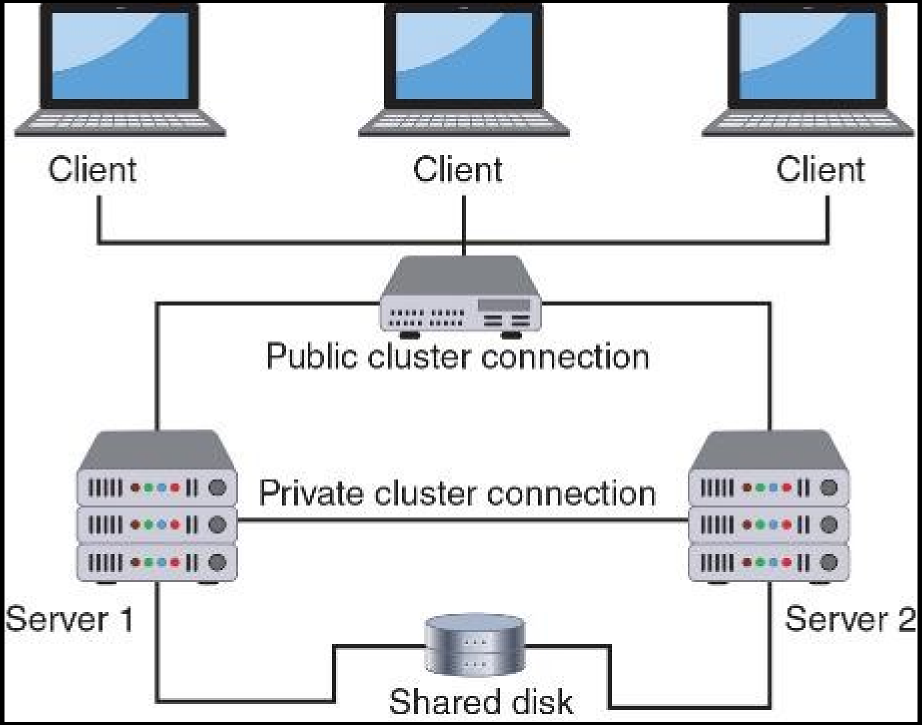
Resilience Through Redundancy

- Using multiple different devices to host or serve an application or a service is known as **platform diversity**
- Equipment **redundancy** can provide **resilience** in the case of a cyberattack
- Resilience through redundancy can also aid in incident preparation
  - It usually involves duplicated servers, drives, networks, power, sites, clouds, and data

Servers

- There needs to be **high availability** in servers so that they are always accessible
- One approach is to design the network infrastructure so that multiple servers are incorporated into the network but appear to users as a single resource
    - **Clustering** combines two or more devices to appear as a single unit
- A server cluster is the combination of two or more servers interconnected to appear as one

Server Cluster



Servers

- There are two types of server clusters:
  - In an asymmetric server cluster, a standby server exists only to take over for another server in the event of its failure
  - In a symmetric server cluster, every server in the cluster performs useful work
    - If one server fails, the remaining servers continue to perform their normal work as well as that of the failed server
- Virtualization has impacted the number of server clusters that are needed for server redundancy

Drives

- **Hard disk drives** (**HDDs**) use spinning platters, actuator arms with read/write heads, and motors to store and retrieve data
- **Solid-state drives** (**SSDs**) stores data on chips instead of magnetic platters
  - SSDs are more resistant to failure and are more reliable than HDDs
- Some organizations maintain a stockpile of HDDs as spare parts to replace failures
- **Mean time between failures** (**MTBF**) refers to the average amount of time until a component fails, cannot be repaired, or must be replaced

RAID

- **RAID** (**Redundant Array of Independent Drives**) uses multiple hard drives for increased reliability and performance
  - It can be implemented either through software or hardware
- Software-based RAID is implemented at the OS level
- Hardware-based RAID requires a specialized hardware controller
- There are several RAID configurations (called levels)
  - Nested levels can combine other RAID levels (RAID level 10 is a combination of RAID Level 0 and Level 1)

SAN Multipath

- A **storage area network** (**SAN**) is a dedicated network storage facility that provides access to data storage over a high-speed network
  - They consolidate different storage facilities that appear to the server as a single pool of locally attached devices
- “Multipath” is a technique for creating more than one physical path between devices and a SAN
  - If one path is interrupted, multipath would redirect the broken connection to another path

Networks

- A redundant network waits in the background during normal operations and uses a replication scheme to keep its copy of the live network information current
  - A redundant network ensures that network services are always accessible
- Switches and routers can have a primary active port as well as a standby failover network port for physical redundancy
- Load balancers can provide a degree of network redundancy by blocking traffic to servers that are not functioning

Power

- An **uninterruptible power supply** (**UPS**) is a device that maintains power to equipment in case of an interruption in the primary electrical power source
- With an **off-line UPS**, if power is interrupted, the UPS quickly begins supplying power to the equipment
  - When power is restored, the UPS switches back to standby mode
- An **on-line UPS** is always running off its battery while the main power runs the battery charger
  - It can clean the electrical power before reaching the server

Sites

- A **hot site** is generally run by a commercial disaster recovery service that allows a business to continue computer and network operations to maintain business continuity
- A **cold site** provides office space, but the customer must provide and install all the equipment needed to continue operations
- A **warm site** has all the equipment installed but does not have active Internet or telecommunications facilities and does not have current backups of data

Clouds

- The following are two considerations for cloud resilience:
  - The location of the data stored in the cloud
  - Spread cloud computing across multiple cloud providers (**multicloud systems**)
- An advantage of multicloud is the organization is able to tolerate a critical issue that could occur with a single cloud provider

Data

- Resilience for data is achieved by copying data
- Two calculations are used regarding when data copies should be performed
  - **Recovery point objective** (**RPO**) is the maximum length of time that an organization can tolerate between copies
  - **Recovery time objective** (**RTO**) is the length of time it will take to recover the data that has been copied

Data

- A **backup** is a single scheduled event where data is copied and then stored so that it can be used in the event of a disaster
  - Copies can be stored onsite or offsite
- There are two techniques for data **replication**
  - A **snapshot** takes a “picture” of the state of the data repeatedly so that data can be restored from a specific point in time
  - **Journaling** makes a copy of the data whenever a change to the data occurs

Incident Investigation

- **Root-cause analysis** (**RCA**) is the process of discovering the origin (root) cause of the security event
- Incident investigation involves analyzing data sources and performing a digital forensics investigation

Data Sources

- A **log** is a record of events that occur
- Security logs can reveal the type of attack that was directed at the network and how it circumvented existing security defenses
- Several problems associated with log management are due to the following:
  - Multiple devices generate logs
  - Very large volume of data
  - Different log formats

Data Sources

- Data accumulated from a **vulnerability scan** can provide useful information
- A **SIEM dashboard** can provide information collected from its sensors
  - This includes alerts, trends, sensitivity, and correlation data
- Network Internet Protocol (IP) monitors can also provide insight into an incident by creating **automated reports** on activity without the need for a user to manually analyze the data
  - sFlow is a **packet capture** protocol that generates information based on capturing packets

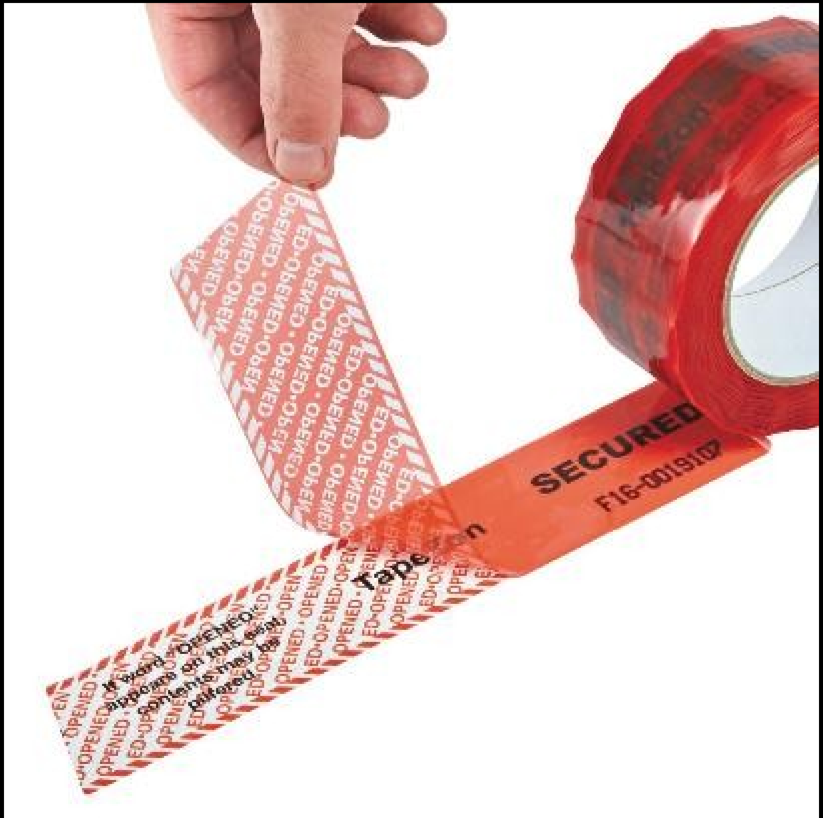
Digital Forensics

- Digital forensics is an important part of incident investigation
- **Forensics** is the application of science to questions that are of interest to the legal profession
- **Digital forensics** involves the retrieval of difficult-to-obtain data, which is usually hidden, altered, or deleted by the perpetrator
  - A digital forensics specialist searches for evidence pertaining to a cybercrime or to damage that occurred during a cyber incident
- **E-discovery** is the electronic counterpart of manually sifting through documents in discovery

Forensics Procedures

- Secure the Scene
  - Contact a digital forensics incident response team and secure the scene immediately to avoid contamination
- Preserve the Evidence
  - Ensure that important proof is not corrupted or destroyed
  - Evidence should be placed in bags that have tags or identifying labels that record a description of the item, a numeric identifier, date, collection location, and other relevant information

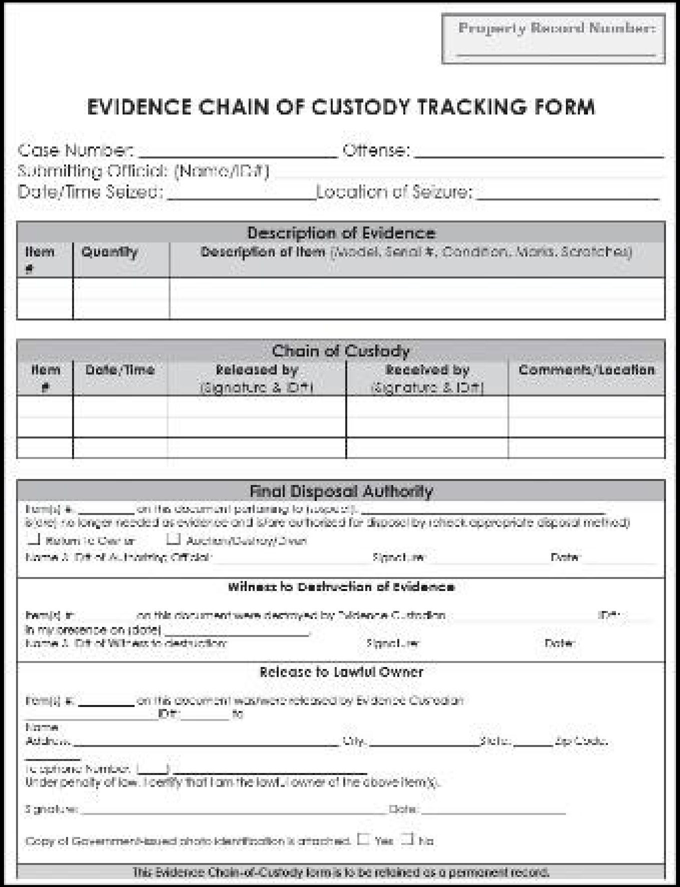
Tamper-Evident Tape


If word "OPENED" appears on this seal contents may be altered
SECURED
F16-0019107
OPENED

Forensics Procedures

- Document Chain of Custody
  - The chain of custody documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence
- Examine for Evidence
  - When examining a device for evidence, there are specialized tools that should be used to gather evidence (**acquisition**)
  - Software digital forensics tools can capture a system image or a snapshot of the current state of all current settings and data

Chain of Custody Form



Property Record Number: ____________

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: ____________________ Offense: ____________________

Submitting Official: (Name/ID#) ____________________

Date/Time Seized: ______________ Location of Seizure: ______________

Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority

Item(s) #: ________ on this document pertaining to (suspect): ______________________________

is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

□ Return to Owner □ Auction/Destroy/Divert

Name & ID# of Authorizing Official: ______________ Signature: ______________ Date: ________

Witness to Destruction of Evidence

Item(s) #: ________ on this document were destroyed by Evidence Custodian ______________ ID#: ______

In my presence on (date) ______________.

Name & ID# of Witness to destruction: ______________ Signature: ______________ Date: ________

Release to Lawful Owner

Item(s) #: ________ on this document was/were released by Evidence Custodian

______________ ID#: ________ to

Name

Address: ______________________________ City: ______________ State: ______ Zip Code: ________

Telephone Number: (____) ______________________

Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: ______________________________ Date: ______________

Copy of Government-issued photo identification is attached. □ Yes □ No

This Evidence Chain-of-Custody form is to be retained as a permanent record.

Forensics Procedures

- Examine for Evidence (continued)
  - Two common forensic software suites are EnCase and FTK Imager
  - Mobile device forensics tools are designed to perform forensics on smartphones, tablets, and other similar devices
  - When examining devices, it is crucial to follow a specific order (called an **order of volatility**: see Table 13-6 on the next slide)
- Generate a Report
  - A detailed written description of the acquisition and analysis of the evidence is required (**reporting**)

Forensics Procedures

Order	Examples	Description
1	Registers and CPU cache	Registers and the CPU cache are extremely volatile and change constantly
2	Routing tables, ARP cache, process table, kernel statistics, RAM	The network routing and process tables have data located on network devices that can change quickly while the system is in operation, and kernel statistics are moving between cache and main memory, which make them highly volatile, RAM is lost if power is lost
3	Temporary file systems	Temporary file systems are not subject to the degree of rapid changes as the prior elements
4	Hard drive	Hard drive data is relatively stable
5	Remote logging and monitoring data	Although remote logging and monitoring are more volatile than hard drive data, the data on a hard drive is considered more valuable and should be preserved first
6	Physical configuration and network topology	These items are not considered volatile and do not have a significant impact on an investigation
7	Archival media	Data that has been preserved in archival form is not volatile