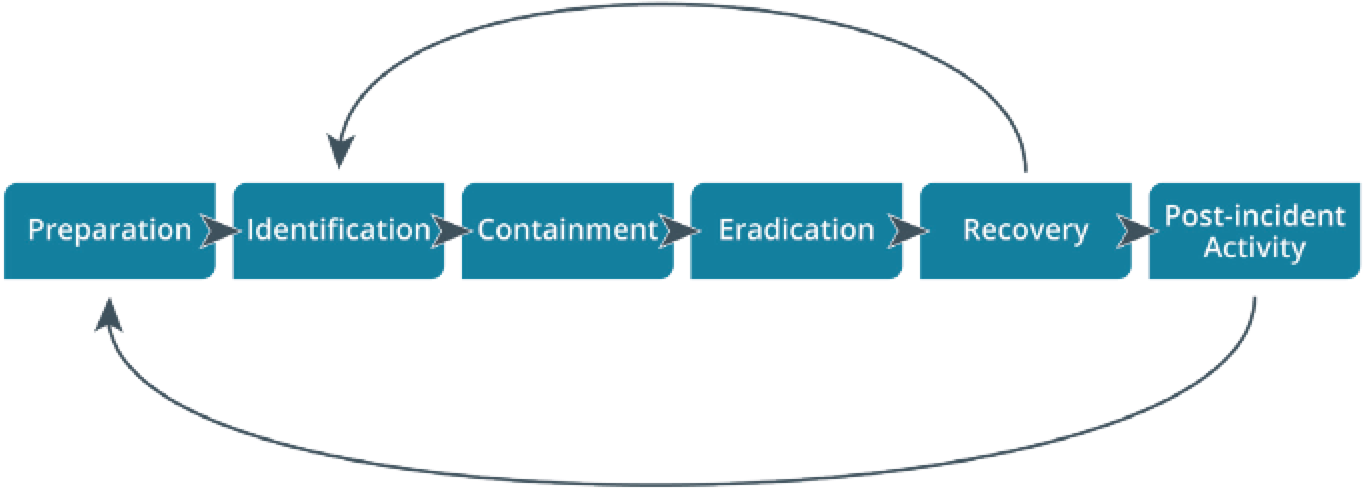
Unit - 5

Incident response : incident response procedures, utilize appropriate data sources for incident response, apply mitigation controls

Digital forensics : digital forensics documentation, digital forensics evidence acquisition

Cyber security Resilience : redundancy strategies, implement backup strategies, cyber security resiliency strategies, physical site security controls, physical host security controls

Incident Response Process



Phases in incident response.

- Preparation—make the system strong to attack in the first place.
- Identification—determine whether an incident has taken place.
- Containment—limit the scope and extent of the incident.
- Eradication—once the incident is contained, restore the affected system to a secure state by applying secure configuration settings and installing patches.

- Recovery—with the cause of the incident eradicated, the system can be reintegrated into the business process that it supports.

- Lessons learned—analyze the incident whether procedures or systems could be improved and this phase feed back into a new preparation phase in the cycle.

Cyber Incident Response Team

- Reporting, categorizing, and prioritizing (triage)
- CIRT/CERT/CSIRT/SOC
- Management/decision-making authority
- Incident analysts
- 24/7 availability
- Roles beyond technical response
  - Legal
  - Human Resources (HR)
  - Marketing

Communication Plan and Stakeholder Management

- Secure communication between the trusted parties.

- Trusted parties might include both internal and external stakeholders.

Incident Response Plan

- An **incident response plan (IRP)** lists the procedures, contacts, and resources available to responders for various incident categories.
- The CSIRT should develop profiles or scenarios of typical incidents (DDoS attack, virus/worm outbreak, data exfiltration by an external adversary, data modification by an internal adversary, and so on).
- This will guide investigators in determining priorities and remediation plans.

- There are several factors that can affect this process:
  - Data integrity
  - Downtime
  - Economic/publicity
  - Scope
  - Detection time
  - Recovery time

Incident Response Exercises

- Training on specific incident response sce
  - **Tabletop**—this is the least costly type of training. The facilitator presents a scenario and the responders explain what action they would take to identify, contain, and eradicate the threat. The training does not use computer systems.narios can use three forms:

- Walkthroughs—in this model, a facilitator presents the scenario as for a tabletop exercise, but the incident responders demonstrate what actions they would take in response. Unlike a tabletop exercise, the responders perform actions such as running scans and analyzing sample files.

- Simulations—a simulation is a team-based exercise, where the red team attempts an intrusion, the blue team operates response and recovery controls, and a white team moderates and evaluates the exercise.

Incident Response, Disaster Recovery, and Retention Policy

- Disaster recovery plan—Disaster recovery requires considerable resources, such as shifting processing to a secondary site.
- **Business continuity plan (BCP)**—this identifies how business processes should deal with both minor and disaster-level disruption.
- **Continuity of Operation Planning (COOP)**—this terminology is used for government facilities, COOP refers specifically to backup methods without IT support.

Incident Identification

- **First Responder**
- When a suspicious event is detected, which person can take charge of the situation and formulate the appropriate response. This person is referred to as the **first responder**.
- **Analysis and Incident Identification**
- The responsible person(s) must analyze the event to determine whether a genuine incident has been identified and what level of priority it should be assigned. Analysis will depend on identifying the type of incident and the data or resources affected (its scope and impact).

SIEM Dashboards

- SIEM dashboards are one of the main sources of automated alerts.

Trend analysis

- **Trend analysis** is the process of detecting patterns or indicators within a data set over a time series and using those patterns to make predictions about future events.

Logging Platforms

- Log data from network appliances

Network, OS, and Security Log Files

- Network logs are generated by appliances such as routers, firewalls, switches, and access points.

Metadata

- **Metadata** is the properties of data as it is created by an application, stored on media, or transmitted over a network. A number of metadata sources are likely to be useful when investigating incidents, because they can establish timeline questions, such as when and where, as well as containing other types of evidence.

Incident Containment

- **Isolation-Based Containment**
- Isolation involves removing an affected component from whatever larger environment it is a part of.

- **Segmentation-Based Containment**
- Segmentation-based containment is a means of achieving the isolation of a host or group of hosts using network technologies and architecture. Segmentation uses VLANs, routing/subnets, and firewall ACLs to prevent a host or group of hosts from communicating outside the protected segment.

Incident Eradication and Recovery

- After an incident has been contained, you can apply mitigation techniques and controls to eradicate the intrusion tools and unauthorized configuration changes from your systems.
- Eradicating malware, backdoors, and compromised accounts from individual hosts is not the last step in incident response.
- You should also consider a recovery phase where the goal is restoration of capabilities and services.
- This means that hosts are fully reconfigured to operate the business workflow they were performing before the incident.

Firewall Configuration Changes

- ingress filtering is a technique used to ensure that incoming packets are actually from the networks from which they claim to originate. This can be used as a countermeasure against various spoofing attacks where the attacker's packets contain fake IP addresses.
- Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another.

Content Filter Configuration Changes

- Update or revoke certificates
  - Remove compromised root certificates from trust stores
  - Revoke certificates on compromised hosts

Security Orchestration, Automation, and Response

- SOAR is designed as a solution to the problem of the volume of alerts overwhelming analysts' ability to respond, measured as the mean time to respond (MTTR).

Digital **forensics**

- Digital **forensics** is the practice of collecting evidence from computer systems to a standard that will be accepted in a court of law.
- Forensics investigations are most likely to be launched against crimes arising from insider threats, notably fraud or misuse of equipment.

Digital Forensics Reports

- A digital forensics report summarizes the significant contents of the digital data and the conclusions from the investigator's analysis.

E-Discovery

- **E-discovery** is a means of filtering the relevant evidence produced from all the data gathered by a forensic examination and storing it in a database in a format such that it can be used as evidence in a trial.

Video and Witness Interviews

- Investigators must capture every action they take in identifying, collecting, and handling evidence.

Event Logs and Network Traffic

- A Retrospective Network Analysis (RNA) solution provides the means to record network events at either a packet header or payload level.

Data Acquisition and Order of Volatility

- **Acquisition** is the process of obtaining a forensically clean copy of data from a device held as evidence.

- **Data acquisition** is also complicated by the fact that it is more difficult to capture evidence from a digital crime scene than it is from a physical one.

- The general principle is to capture evidence in the **order of volatility**, from more volatile to less volatile.

Digital Forensics Software

- Digital forensics software is designed to assist the acquisition, documentation, and analysis of digital evidence.

System Memory Acquisition

- **Live Acquisition :** A specialist hardware or software tool can capture the contents of memory while the host is running. Unfortunately, this type of tool needs to be preinstalled as it requires a kernel mode driver to dump any data of interest.

- **Crash Dump:** When Windows encounters an unrecoverable kernel error, it can write contents of memory to a dump file at C:\Windows\MEMORY.DMP.

Disk image acquisition

- Disk image acquisition refers to acquiring data from nonvolatile storage.
- Nonvolatile storage includes hard disk drives (HDDs), solid state drives (SSDs), firmware, other types of flash memory (USB thumb drives and memory cards), and optical media (CD, DVD, and Blu-Ray).
- This can also be referred to as device acquisition, meaning the SSD storage in a smartphone or media player.
- Disk acquisition will also capture the OS installation, if the boot volume is included.

Preservation and Integrity of Evidence

- It is vital that the evidence collected at the crime scene con

- A cryptographic hash of the disk media is made, using either the MD5 or SHA hashing function. form to a valid **timeline**.

- A bit-by-bit copy of the media is made using the imaging utility.

Risk Management Processes

- **Risk management** is a process for identifying, assessing, and mitigating vulnerabilities and threats to the essential functions that a business must perform to serve its customers.

- **Risk Types**
- **Assessment of Risks: quantitative, qualitative**

Risk Management Strategies

- How to prioritize
- How to mitigate

Risk Avoidance and Risk Transference

- How to avoid the risk

- How to transfer or share the risk (means assigning risk to a third party, such as an insurance company)

Risk Acceptance and Risk Appetite

- Risk is assessed and monitored

- Willingness to tolerate a certain level of risk

Risk Awareness

- Communicate risk factors to stakeholders
- Risk registers
  - Risk matrix
  - Graphs

Business Impact Analysis

- Business impact analysis (BIA) reports for threat scenarios

Mission Essential Functions

- **Maximum tolerable downtime (MTD)**

- Identification of Critical Systems
- Single Points of Failure
- Disasters
- Disaster Recovery Plans
- Functional Recovery Plans

Physical Security Controls

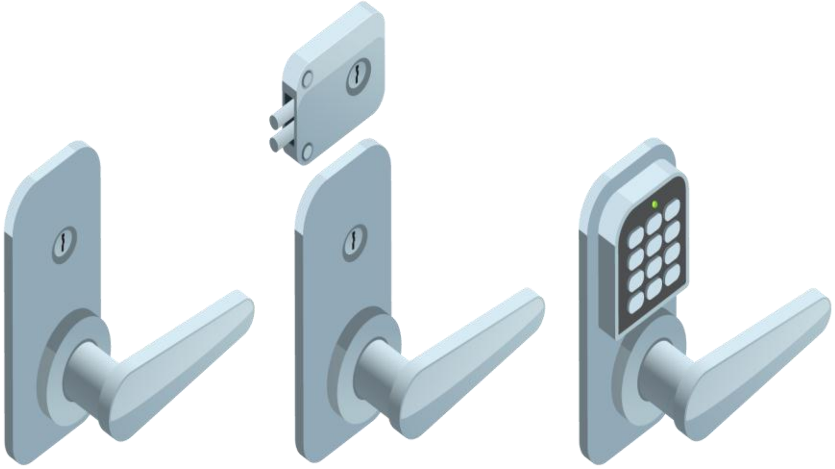
- Authentication
  - Create access lists and identification mechanisms to allow approved persons through barriers
- Authorization
  - Create barriers around a resource so that access can be controlled through defined entry and exit points
- Accounting
  - Keep a record of when entry/exit points are used and detect security breaches

Site Layout, Fencing, and Lighting

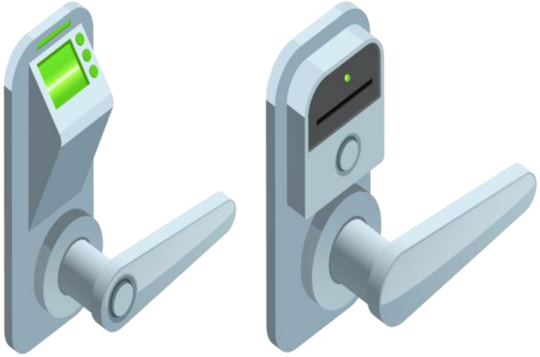
- Site layout
  - Zone-based design to accommodate traffic flows and surveillance
  - Signage
  - Industrial camouflage
- Barricades and entry/exit points
  - Bollards
- Fencing
- Lighting
  - Make staff feel secure
  - Assist surveillance

Gateways and Locks

- Lock types
  - Physical (conventional/deadbolt)
  - Electronic
    - Cipher/combination
    - Magnetic swipe card
    - Smart card/proximity reader
  - Biometric
- Access control vestibules/mantraps and turnstiles
- Cable locks



Images from user macrovector © 123RF.com.



Images from user macrovector © 123RF.com.

Physical Attacks Against Smart Cards and USB

- Smart card attacks
  - Cloning
  - Skimming
  - Card types and vulnerability level

Alarm and Sensor Systems

- Circuit
  - Open or closed
  - Detect intrusion through a barrier
- Motion detection
  - Radar or infrared
  - Detect intrusion in a space
- Noise detection
- Proximity readers

Security Guards and Cameras

Image by Dario Lo Presti © 123RF.com.

- Security guards
  - Police entry points
  - Operate surveillance mechanisms
  - Respond to alarms
- Remote surveillance and monitoring
  - Video/CCTV
  - Motion recognition
  - Object detection
  - Robot sentries
  - Drones/UAV

Reception Personnel and ID Badges

- Challenge policy
- Reception personnel and visitor logs
  - Sign-in/sign-out
  - Visitor information
- ID badges

Secure Areas

- Server rooms and data centers
- Lockable cabinets
- Colocation cages
- Safes
- Vaults

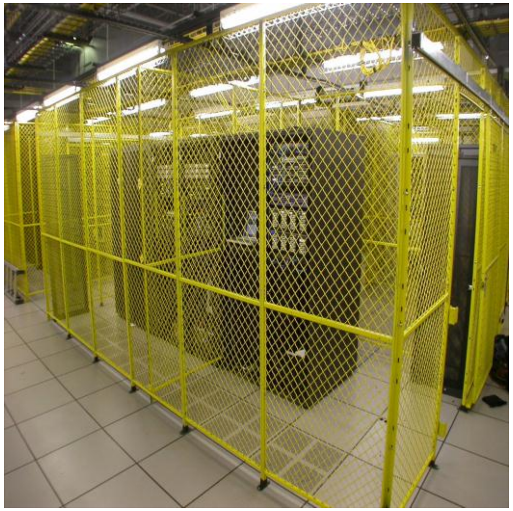


Image © 123RF.com.

Image © Chris Dag and shared with CC BY 2.0 flickr.com/photos/chrisdag/865711871.

Heating, Ventilation, Air Conditioning

- Cooling/warming, humidity, dust control
- Optimum temperature and humidity levels
  - Moisture detection sensors
  - Temperature detection sensors

Hot and Cold Aisles

- Optimize air flow
- Place servers back-to-back
- Hot aisle/cold aisle
- Do not allow contamination of cooled air by warmed air

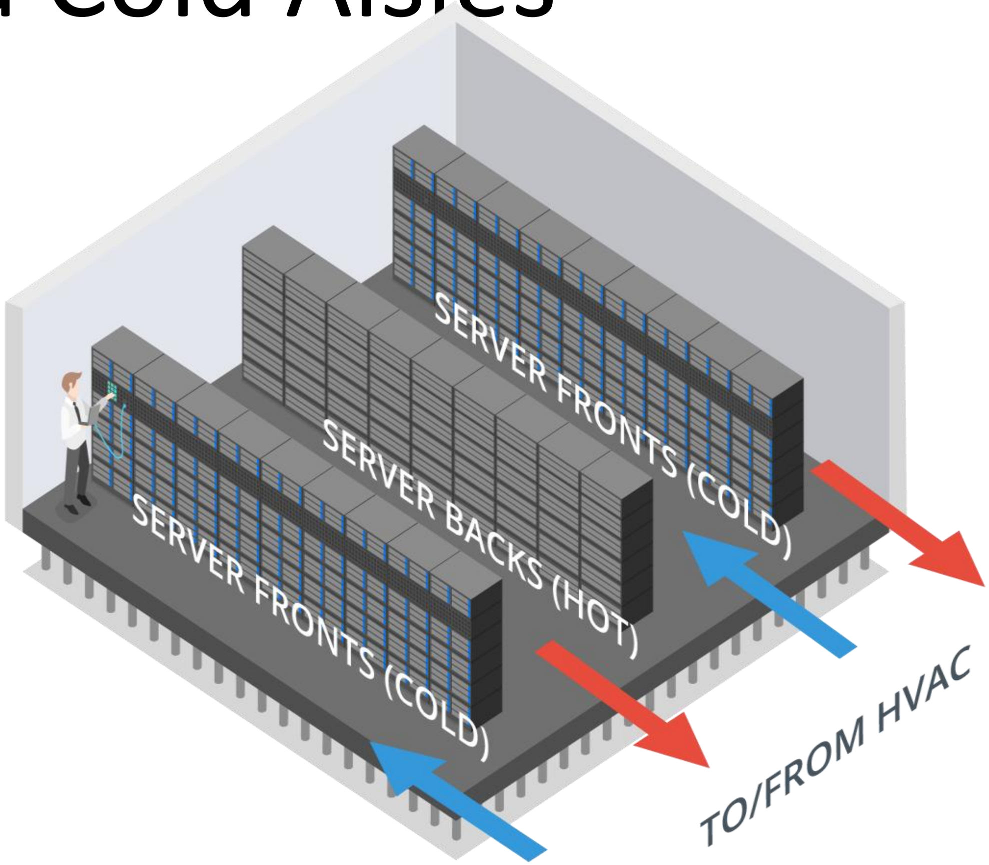


Image © 123RF.com.

Fire Detection and Suppression

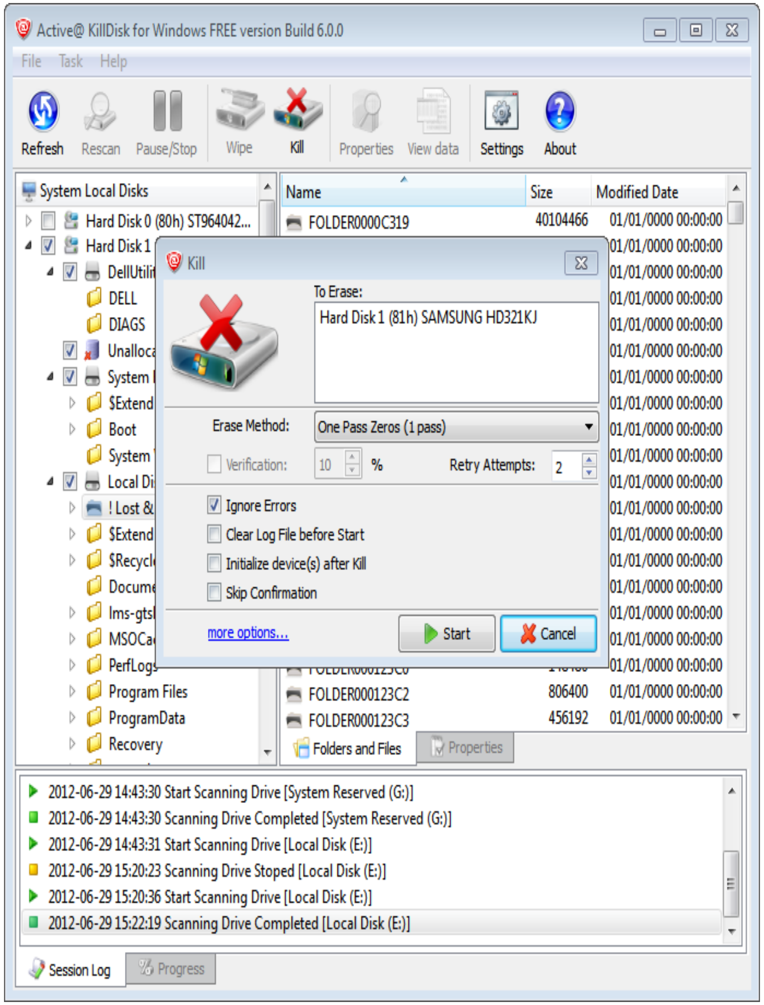
- Fire safety
  - – Fire exits and evacuation procedures
  - – Fire-resistant building design
  - – Smoke/flame detectors/alarms
- Personal fire extinguishers
  - – Class C for use around electrical hazard

Secure Data Destruction

Photo by monsterkoi on Pixabay.

- Media sanitization/remnant removal
- Physical destruction
  - Burning/incineration
  - Shredding/pulping
  - Pulverizing
  - Degaussing
- Use of third-parties and certificates of destruction

Data Sanitization Tools



Name	Size	Modified Date
FOLDER0000C319	40104466	01/01/0000 00:00:00
FOLDER000123C2	806400	01/01/0000 00:00:00
FOLDER000123C3	456192	01/01/0000 00:00:00

Kill

To Erase: Hard Disk 1 (81h) SAMSUNG HD321KJ

Erase Method: One Pass Zeros (1 pass)

□ Verification: 10 %　Retry Attempts: 2

☑ Ignore Errors
□ Clear Log File before Start
□ Initialize device(s) after Kill
□ Skip Confirmation

more options...　Start　Cancel

```
2012-06-29 14:43:30 Start Scanning Drive [System Reserved (G:)]
2012-06-29 14:43:30 Scanning Drive Completed [System Reserved (G:)]
2012-06-29 14:43:31 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:20:23 Scanning Drive Stoped [Local Disk (E:)]
2012-06-29 15:20:36 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:22:19 Scanning Drive Completed [Local Disk (E:)]
```

Screenshot used with permission from LSoft Technologies, Inc.

- Secure disposal of electronic data remnants
- Overwriting/disk wiping
  - Zero filling
  - Multiple passes
- Secure Erase (SE)
  - Hard disk drives (HDD)
  - Solid state drives (SSD)/flash media
- Instant Secure Erase (ISE)/crypto erase
  - Self-encrypting drives (SED)
  - Delete media encryption key