CultureLink

CSX – Cybersecurity Fundamentals

Section 5 : Incident response

Course Plan

Module Titles
Section 1 – Cybersecurity Introduction and Overview
Section 2 – Domain 1: Cybersecurity Concepts
Section 3 – Domain 2: Security Architecture Principles
Section 4 – Domain 3: Security of Networks, Systems, Applications and Data
Section 5 – Domain 4: Incident Response
Section 6 – Domain 5: Security Implications and Adoption of Evolving Technology
Section 7 – Course Review
Section 8 – Practice Exam

Learning Outcomes for this Module

- Knowledge of incident categories for responses
- Knowledge of business continuity/disaster recovery
- Knowledge of incident response and handling methodologies
- Knowledge of security event correlation tools
- Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)
- Knowledge of types of digital forensics data
- Knowledge of basic concepts and practices of processing digital forensic data

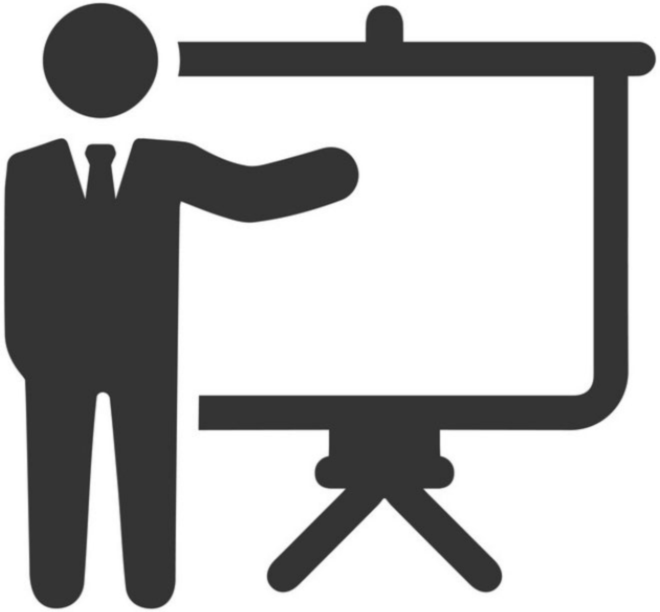
Learning Outcomes for this Module

- Knowledge of anti-forensics tactics, techniques and procedures (TTPS)
- Knowledge of common forensic tool configuration and support applications (e.g., VMware®, Wireshark®)
- Knowledge of network traffic analysis methods
- Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files

Topics for this Module

- **5.1** Event vs. Incident
- **5.2** Security incident response
- **5.3** Investigations, legal holds and preservation
- **5.4** Forensics
- **5.5** Disaster recovery and business continuity

Current Events



Section 5.1

Event vs. incident

Question – Event vs. Incident

What is the difference between these to terms?

Event: *Any change, error or interruption within the IT infrastructure*

Incident: *A violation or imminent threat of a violation of computer security policies, acceptable user policies (AUP), or standard security policies."*

Source: NIST

Types of incidents

- List (not complete) of incident types:

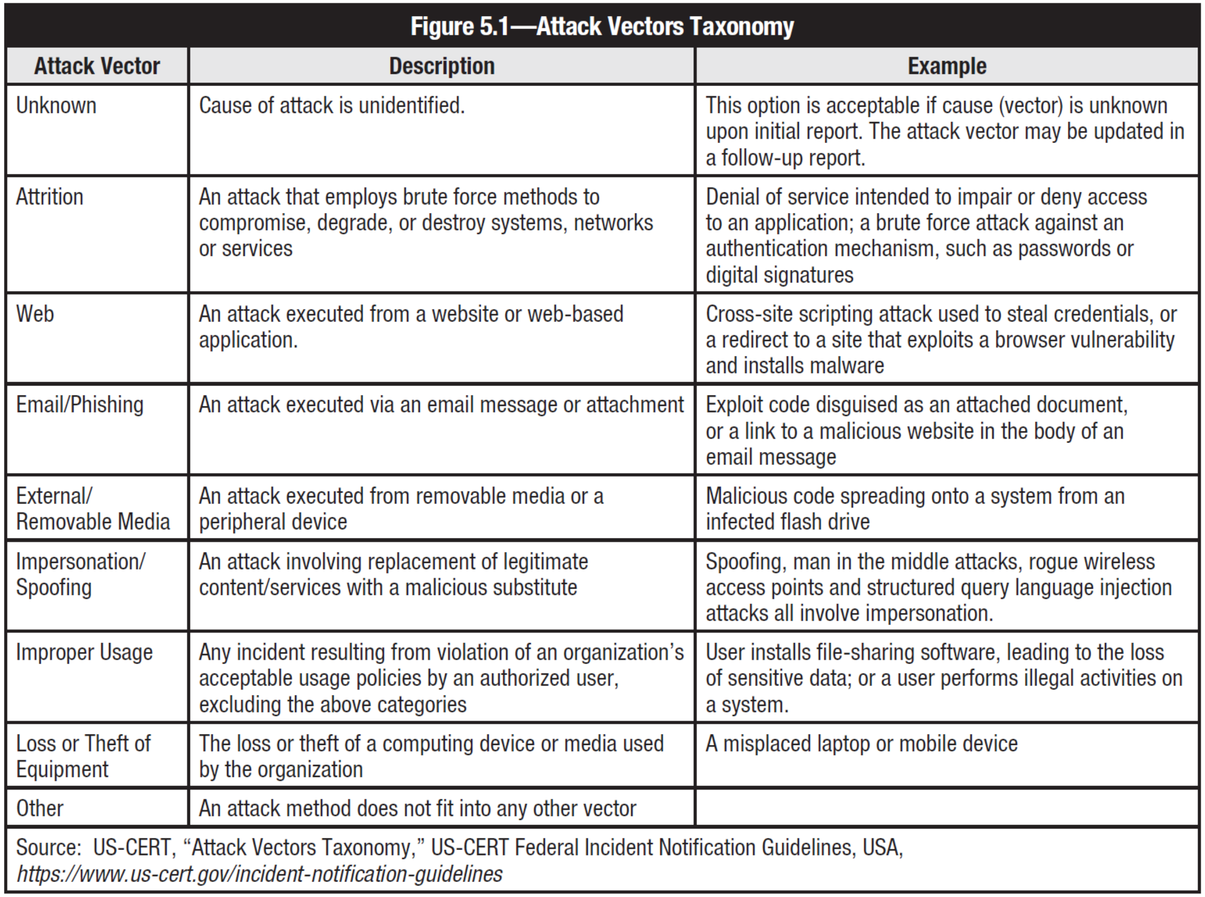


Figure 5.1—Attack Vectors Taxonomy

Attack Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks or services	Denial of service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware
Email/Phishing	An attack executed via an email message or attachment	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message
External/ Removable Media	An attack executed from removable media or a peripheral device	Malicious code spreading onto a system from an infected flash drive
Impersonation/ Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points and structured query language injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization	A misplaced laptop or mobile device
Other	An attack method does not fit into any other vector	

Source: US-CERT, "Attack Vectors Taxonomy," US-CERT Federal Incident Notification Guidelines, USA, *https://www.us-cert.gov/incident-notification-guidelines*

Source: NIST SP 800-61

Types of incidents

- European Union Agency for Network and Information Security (ENISA) provides this TAXONOMY :

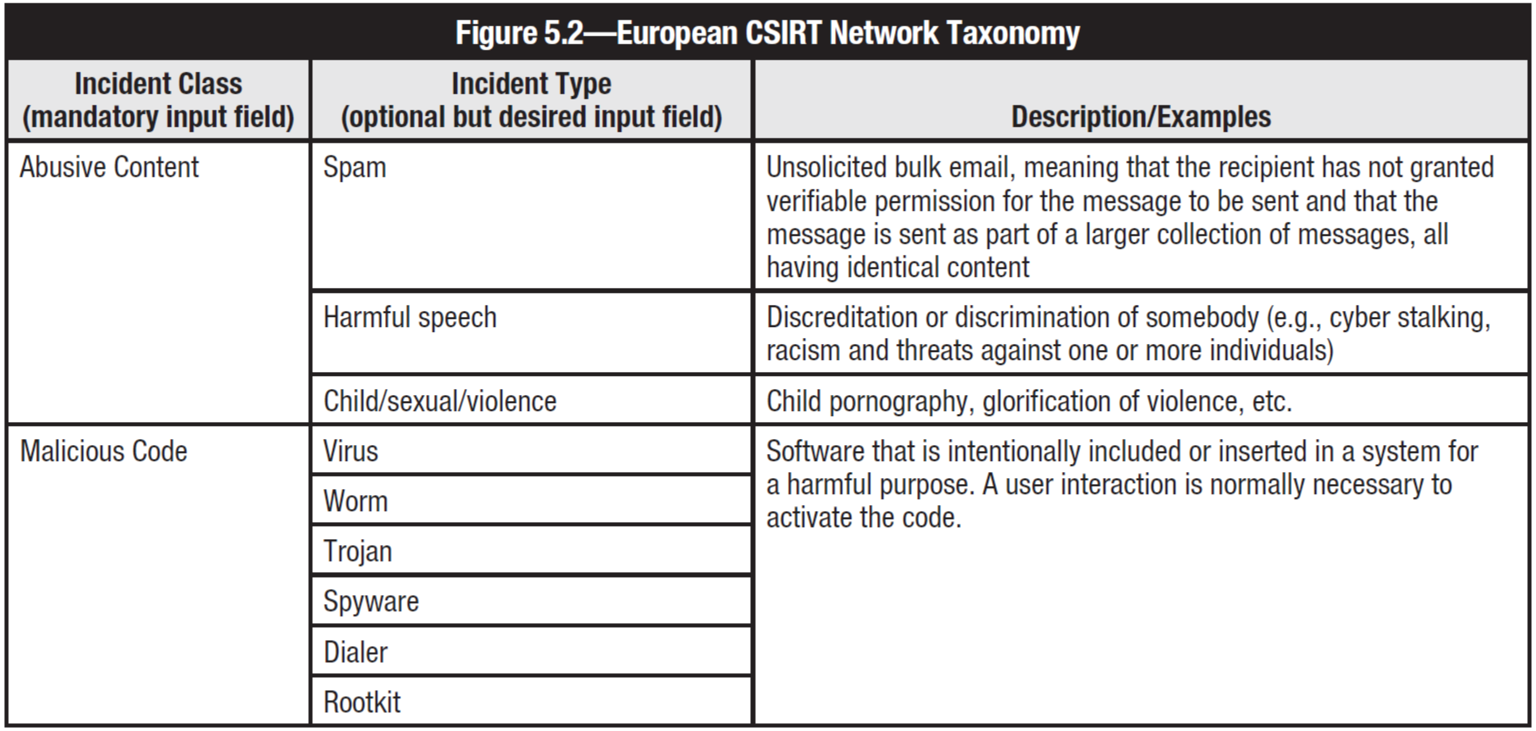


Figure 5.2—European CSIRT Network Taxonomy

Incident Class (mandatory input field)	Incident Type (optional but desired input field)	Description/Examples
Abusive Content	Spam	Unsolicited bulk email, meaning that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having identical content
	Harmful speech	Discreditation or discrimination of somebody (e.g., cyber stalking, racism and threats against one or more individuals)
	Child/sexual/violence	Child pornography, glorification of violence, etc.
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
	Rootkit	

See more on pg. 123 on study guide

Source: NIST SP 800-61

Any questions?

Section 5.2

Security incident response

Question

What is an Incident response?

"A program that prepares an entity for an incident" (*Incident:* an event or occurrence)

Security incident response plan (IRP)

What is involved?

1. **Preparation** to establish roles, responsibilities and plans for how an incident will be handled
2. **Detection and Analysis** capabilities to identify incidents as early as possible and effectively assess the nature of the incident
3. **Investigation** capability if identifying an adversary is required
4. **Mitigation and Recovery** procedures to contain the incident, reduce losses and return operations to normal
5. **Postincident Analysis** to determine corrective actions to prevent similar incidents in the future

Question

Why do we need it?

- The business needs to prepare. Not preparing is a recipe for disaster
- Organization can respond in a timely manner
- Incident are more frequent these days

Discuss components

- From the study guide (pg. 125, 126) review what each components entails

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

Any questions?

CultureLink

Section 5.3

Investigations, legal holds and preservation

Investigations, legal holds and preservation

- Cybersecurity **investigation activities (objectives)**:
  - Collection of evidence
  - Analysing evidence
  - Identifying perpetrator or unauthorized access
- Incident response activities (objectives):
  - Preparation
  - Detection and analysis
  - Containment, eradication and recovery
  - Post incident activity
- **Gotcha: Two investigations overlap, incident response activity needs to be careful not to damage evidence**

Evidence preservation

- Most organizations are weak in dealing with intrusions and electronic crimes
- Documentation is poor
- Impacts "**chain of custody**"

- **Chain of custody:**
  - **How the evidence is handled, maintained**
  - **Who owns it**
  - **How its transferred**
  - **How it is modified**

- **Chain of custody needs to be maintained chronologically or else it will be dismissed in court**

Legal requirements

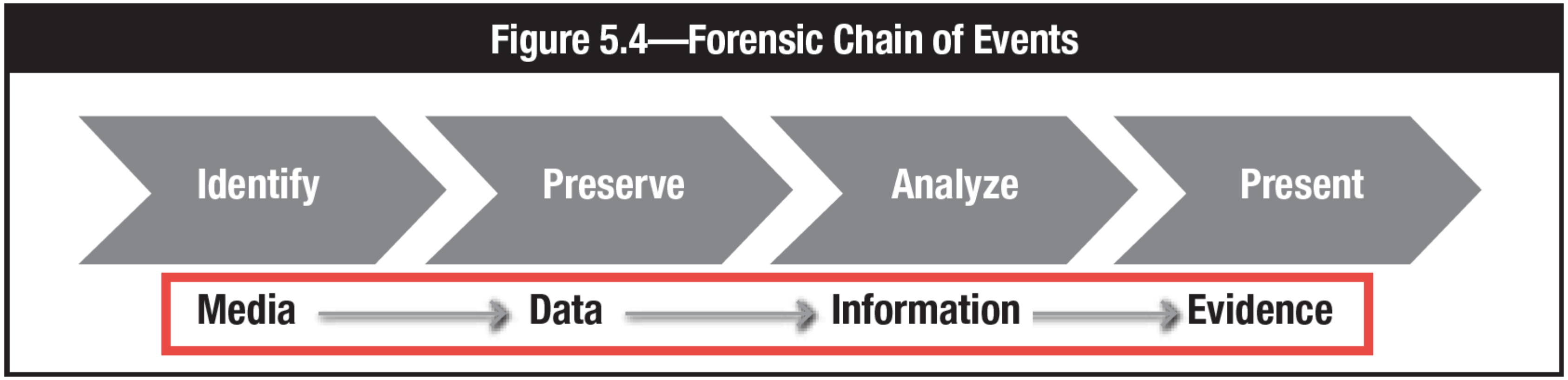
- Evidence collection and storage
- Chain of custody of evidence
- Searching or monitoring communications
- Interviews or interrogations
- Law enforcement involvement
- Labor, union and privacy regulation

Any questions?

Section 5.4

Forensics

Forensics



Identify: Identify of information that might form evidence

Preserve: Practice of preserving evidence

Analyze: Extracting, processing, interpreting data

Present: Presenting audience to various people (mgt, court, etc.)

CultureLink

Digital investigation video

- **Digital investigation:** https://www.youtube.com/watch?v=rZ63OH2TAOo

- Evidence has changed, now dealing with computers, phones, tablets, USB drives, etc.
- Digital information is fragile
- Real case examples

Digital investigation video

What did you learn?

- Data protection
- Imaging
- Extraction
- Interviews
- Ingestion / Normalization
- Reporting

Network traffic analysis

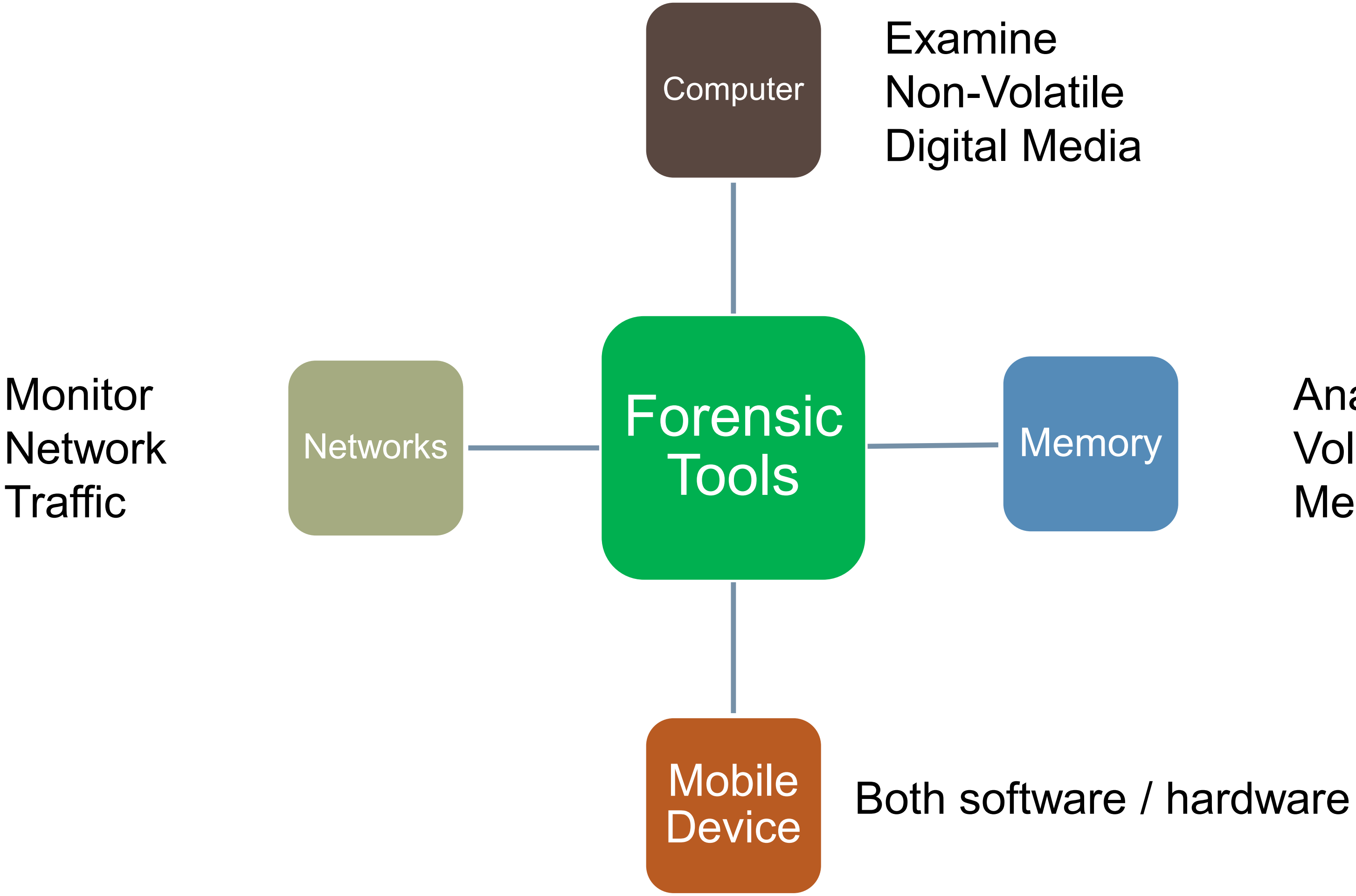
Many tools out in the industry to monitor:

- **Solarwinds**
- **Microsoft**
- **Wireshark**
- **Angry IP**

Log file analysis features of tools:

- Audit reduction tools
- Trend / Variance-detection tools
- Attack-signature-detection tools

Digital forensic tools



Examine Non-Volatile Digital Media

Monitor Network Traffic

Analyze Volatile Memory

Both software / hardware

Digital anti-forensic tools

Anti-forensic tools make it difficult/impossible for investigators to retrieve information:

Activities include:

- Securely deleting data
- Overwriting metadata
- Preventing data creation
- Encrypting data
- Encrypting network protocols
- Hiding data in slack space or other unallocated locations
- Hiding data or a file within another file (steganography)

If the anti-forensic measures taken were drastic enough, investigators may not ever crack into the computer system.

Any questions?

Section 5.5

Disaster recovery and business continuity plans

Disaster recovery and business continuity plans

Disasters cause disruptions in critical information resources:

- Natural calamities, such as earthquakes, floods, tornadoes and fire, or a disaster may be caused by events precipitated by humans such as terrorist attacks, hacker attacks, viruses or human error

A **cybersecurity-related disaster** may occur when a disruption in service is caused by:

- System malfunctions, accidental file deletions, untested application releases, loss of backup, network DoS attacks, intrusions or viruses.

Business continuity plan (BCP)

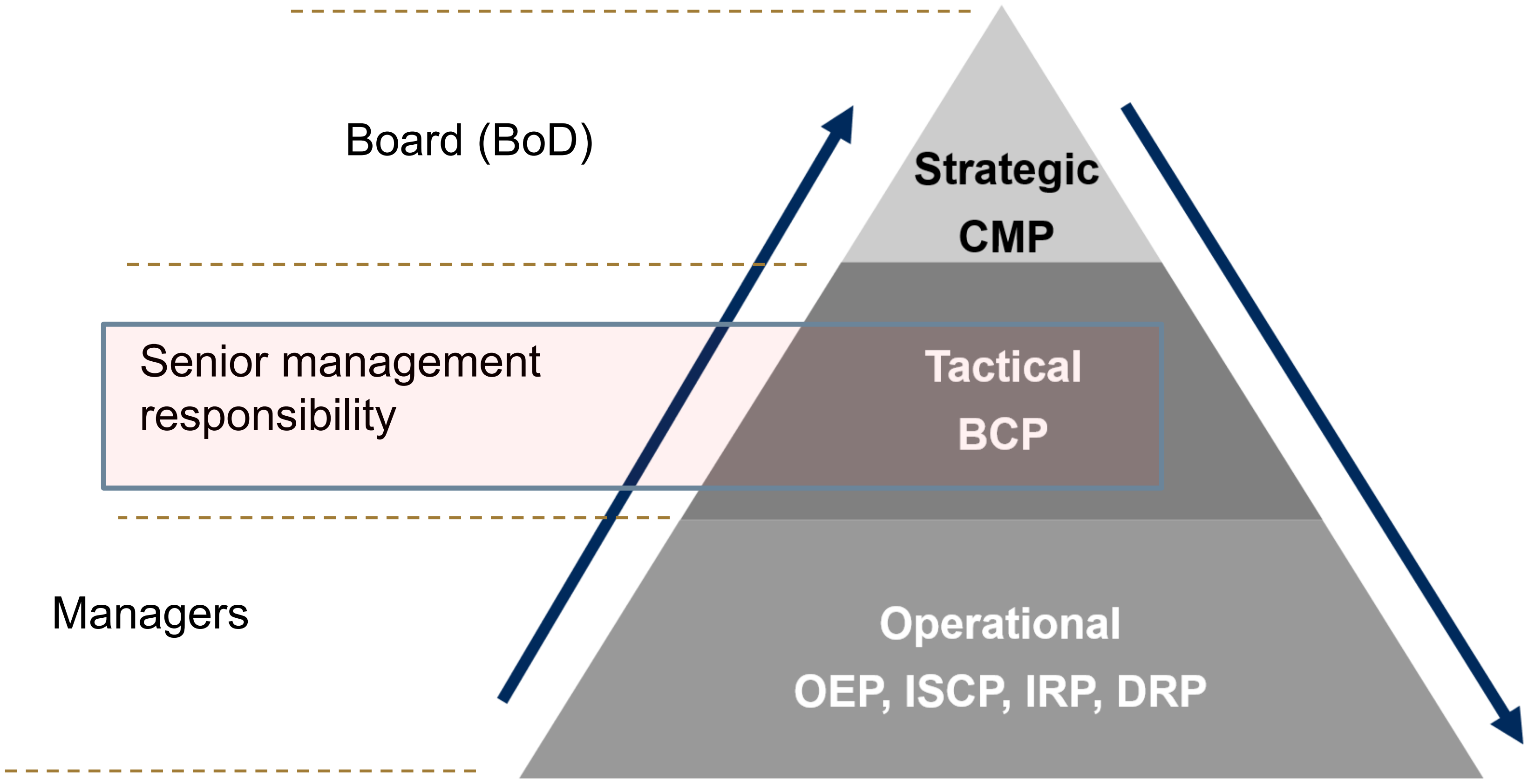
- A business continuity **plan** (**BCP**) is a **plan** to help ensure that **business processes can continue during a time of emergency or disaster.** Such emergencies or disasters might include a fire or any other case where business is not able to occur under normal conditions – *Wikipedia*

BCP takes into consideration:

- Critical operations necessary to the survival of the organization
- The human/material resources supporting these critical operations pre-disaster readiness covering incident response management to address all relevant incidents affecting business processes
- Evacuation procedures
- Procedures for declaring a disaster (escalation procedures)
- Circumstances under which a disaster should be declared

Business continuity plan (BCP)

Responsibility of senior management



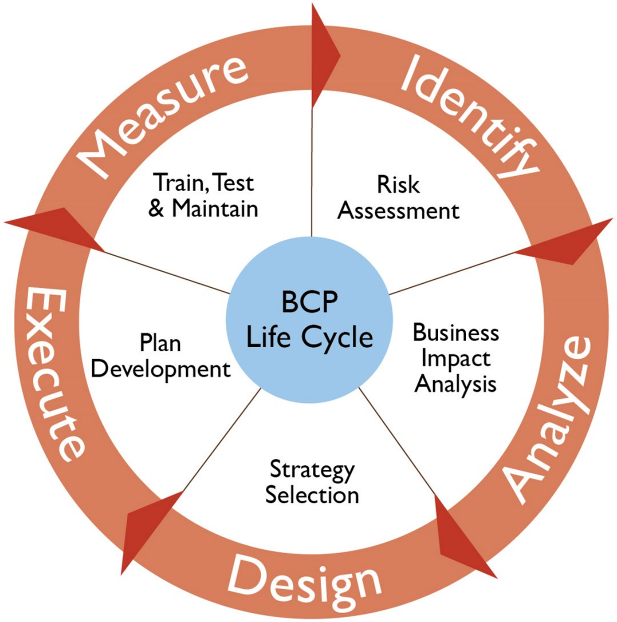
Source: Information Assurance Handbook

Business impact analysis

- To prepare BCP / DRP – first step identify business processes of strategic importance

- Analyze process through Business Impact Analysis:
  - Identify resources (physical, non-physical, 3rd party)
  - Data
  - Infrastructure
  - Potential vulnerabilities

BIA:
What are the business process?
What are the critical information
Resources related to critical business process?
What is the critical recovery time



Business impact analysis

Questions it considers:

- What are the different business processes?
- What are the critical information resources related to an organization’s critical business processes?
- What is the critical recovery time period for Information resources in which business processing must be resumed before significant or unacceptable losses are suffered?

Business impact analysis

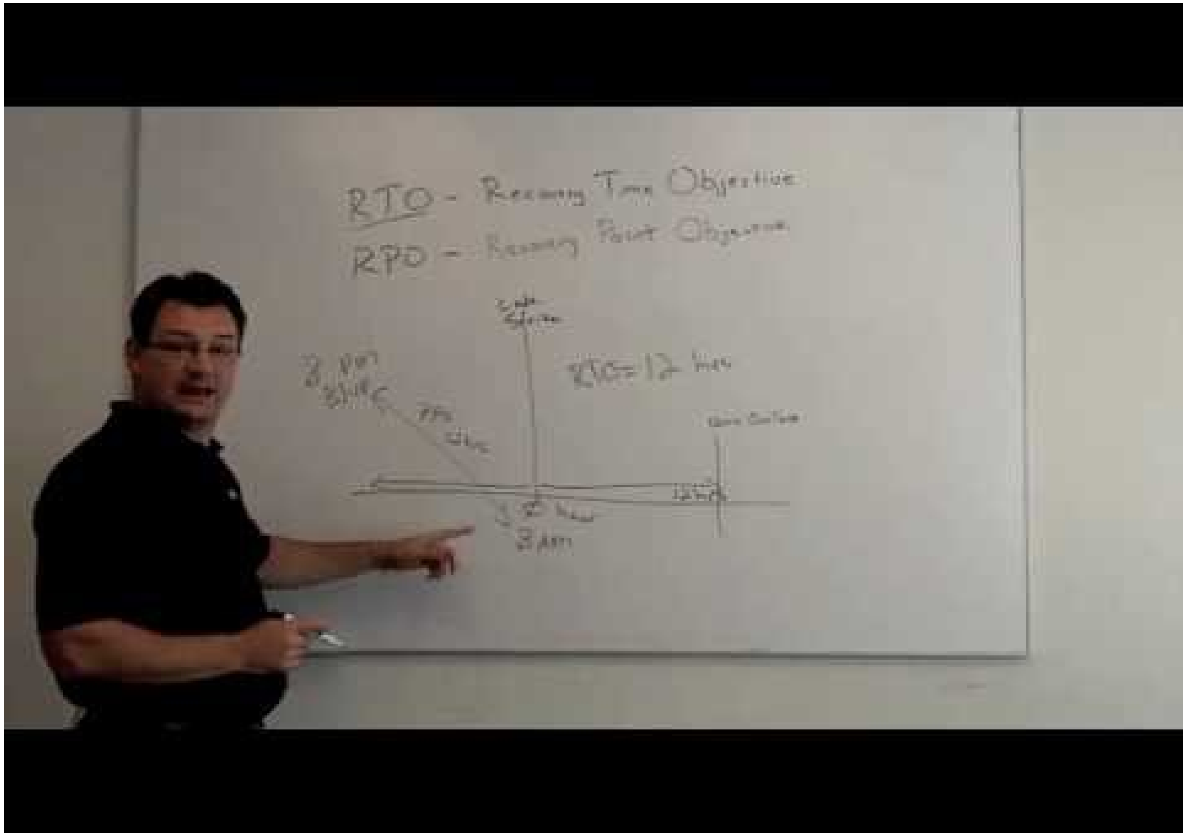
Also establishes:

- **Recovery Point Objective (RPO)**
- **Recovery Time Objective (RTO)**

Example:

- (1) RTO of 2 hours indicates that organization needs to ensure that their system downtime should not exceed 2 hours.
- (2) RPO of 2 hours indicates that organization needs to ensure that their data loss should not exceed 2 hours of data captured.
- (3)In any given scenario, for critical systems, RTO is zero or near zero. Similarly, for critical data, RPO is zero or near zero.
- (4)In any given scenario, lower the RTO/RPO, higher the cost of maintenance of environment.
- (5)In any given scenario, low RTO/RPO indicates that disaster tolerance is low. Other way round, if disaster tolerance is low, RTO/RPO should be low.

RTO / RPO video reference



https://youtu.be/SeS6ke3B4Tg

Information system BCP (IS BCP)

- Approach is the same as BCP
- Continuity of IS processing
- IS BCP should be aligned with the strategy of organization

Backups procedures

Three types of backups:

- Full backup
- Incremental
- Differential

- **Full backups** provide a complete copy of every selected file on the system, regardless of whether it was backed up recently.
- **Incremental backups** copy all files that have changed since the last backup was made, regardless of whether the last backup was a full or incremental backup.
- Differential backups copy only the files that have changed since the last full backup.

Any questions?

Thank You