Incident Scene

Assign ID to the scene • Incident environment protection • ID and possible sources of evidence • Collect evidence • Avoid or minimize evidence contamination

Locard's Exchange Principle	In a crime the suspected person leaves something and takes something. The leftovers can be used to identify the suspect.

Live Evidence

Primary Evidence	• Most reliable and used by trial • Original documents–Eg. Legal contracts • No copies or duplicates
Secondary Evidence	• Less powerful and reliable than primary evidence. • Eg. Copies of originals, witness oral evidence. • If primary evidence is available secondary of the same content is not valid.
Direct Evidence	Can prove without a backup support. • Eg. witness testimony by his/her own 5 senses.
Conclusive Evidence	• Cannot contradict, conditional evidence, no other supportive evidence requires • Cannot be used to directly prove a fact
Corroborative Evidence	• Use as substantiate for other evidence
Hearsay Evidence	• Something heard by the witness where another person told

Asset Management

Preserve Availability • Authorization and Integrity • Redundancy and Fault Tolerance • Backup and Recovery Systems • Identity and Access Management

Storage Management Issues	• Hierarchical Storage Management (HSM): continuous online backup system Using optical storage. • Media History: Media usage log • Media Labeling and Storage: safe store of media after labeling sequentially • Environment: Temperature and heat Eg. Magnetic media
Sanitizing and Disposing of Data	• Data Purging: degaussing Archived data not usable for forensics • Data Clearing: Cannot recover using keyboard • Remanence: Data left in media deleted
Network and Resource Management	• Redundant hardware • Fault-tolerant technologies • Service Level Agreements (SLA's) • MTBF and MTTR • Single Point of Failure (SPOF)
Incident Response - steps	1. Detect • 2. Respond • 3. Report • 4. Recover • 5. Remediate • 6. Review
Change Management	• Changes should be formally requested • Analyze requests against goals to ensure validity • Cost and effort estimation before approval • Identify the change steps after approval • Incremental testing during implementation • Complete documentation
Threats and Preventative Measures	• Clipping levels: Define a baseline for normal user errors, • Modification from Standards Eg. DDOS • Unusual patterns or events • Unscheduled reboots: Eg. Hardware or operating system issue • Input/output Controls

Intrusion Detection & Prevention Systems (IDS & IPS)

IDS (Intrusion Detection System)	Automated inspection of logs and real-time system events to detect intrusion attempts and system failures. IDSs are an effective method of detecting many DoS and DDoS attacks.
IPS (Intrusion Prevention System)	A IDS with additional caabilities to stop intrusions.

Firewalls

HIDS (Host-based IDS)	Monitor and analyze the internals of a computing system, including its network connection points. Eg. Mainframe computer
NIDS (Network-based IDS)	Hardware based device or software applications used to monitor and analyse network activity, specifically scanning for malicious activities and policy violations.

Hierarchical Recovery Types

1. Manual
2. Automatic Recovery

Types of System Failure

• System reboot
• Emergency restart
• System cold start

Data Destruction and Reuse

Object reuse	Use after initial use
Data remanence	Remaining data after erasure Format magnetic media 7 times (orange book
Clearing	Overwriting media to be reused
Purging	Degaussing or overwriting to be removed
Destruction	Complete destruction, preferably by burning

Disaster Recovery Planning

Disaster recovery process	Teams responsible for DR implementation - Salvage team - Work on normal /primary site to make suitable for normal operations
Other recovery issues	• Interfacing with other groups • Fraud and Crime: Eg. vandalism, looting • Financial disbursement • Documenting the Plan - Required documentation • Activation and recovery procedures • Plan management • HR involvement • Costs • Internal /external communications • Detailed plans by team members

Characteristics of Evidence

Sufficient	Validity can be acceptable.
Reliable	Consistent facts. Evidence not tampered or modified.
Relevant	Reasonable facts, with proof of crimes, acts and methods used, event documentation
Permissible	Evidence obtained lawfully

Interviewing and Interrogation

Interviewing	Collect facts to determine matters of the incident.
Interrogation	Obtain a confession by evidence retrieval method. • The Process: Prepare questions and topics, summarize information
Opinion Rule	Witnesses test only the facts of the case, not used as evidence.
Expert Witnesses	Can be used as evidence.

Network Analysis

Use of existing controls to inspect a security breach incident. Eg. IDS/IPS, firewall logs
• **Software Analysis:** Forensic investigation of applications which was running while the incident happened.
• **Hardware/ Embedded Device Analysis:** Eg. review of Personal computers & Smartphones

Governing Laws

• Common law - USA, UK Australia, Canada
• Civil law - Europe, South America
• Islamic and other Religious laws – Middle East, Africa, Indonesia, USA

The 3 Branches of Law	• Legislative: Statutory law - Make the laws • Executive: Administrative law - Enforce the laws • Juridical: Interpret the laws
Categories of law	• Criminal law –violate government laws result in commonly imprisonment • Civil law – Wrong act against individual or organization which results in a damage or loss. Result in financial penalties. • Administrative/Regulatory law – how the industries, organizations and officers should act. Punishments can be imprisonment or financial penalties
Uniform Computer Information Transactions Act (UCITA)	Common framework for the conduct of computer-related business transactions. A federal law Eg. Use of software licensing
Computer Crime Laws 3 types of harm	• Unauthorized intrusion • Unauthorized alteration or destruction • Malicious code
Admissible evidence	• Relevant, sufficient, reliable, does not have to be tangible
Hearsay	• Second hand data not admissible in court
Enticement	• Is the legal action of luring an intruder, like in a honeypot
Entrapment	• Is the illegal act of inducing a crime, the individual had no intent of committing the crime at first

Data Loss Prevention (DLP)

Scans data for keywords and data patterns. Protects before an incident occurs.

Network-based DLP	Data in motion. Scans all outbound data looking for anomalies. Place in edge of the network to scan all outgoing data.
Endpoint-based DLP	Data in use. Scans all internal end-user workstations, servers and devices.

Digital Data States

Data at Rest	Data that is stored on a device or a backup medium.
Data in Motion	Data that is currently travelling across a network or on a device's RAM ready to be read, updated, or processed.
Data in Use	Data that is being inputted, processed, used or altered.

Backup Types

Full	All files backed up, archive bit and modify bit will be deleted
Incremental	Backup files changed after last full backup, archive bit deleted.
Differential	Only modified files are backed up, do not delete archive bit. Need last full backup and last incremental backup for a full restore.
Redundant servers	Eg. RAID, adding disks for increased fault tolerance.
Server clustering	Set of servers that process traffic simultaneously.

Disaster Recovery Test

Desk Check	Review contents of the plan
Table-top exercise	Disaster recovery team members gather and roleplay a disaster scenario
Simulation test	More intense than a roleplay, all support and tech staff meet and practice against disaster simulations
Parallel tests	Personnel are taken to an alternative site and commence operations of critical systems, while original site continues operating
Full-implementation tests	Personnel are taken to an alternative site and commence operations of all systems, main site is shut down

BCP Plan Development

Define the continuity strategy	• Computing: strategy to protect - hardware, software, communication links, applications, data • Facilities: use of primary or alternate/remote site buildings • People: operational and management • Supplies and equipment
Roles and responsibilities	• BCP committee: senior staff, business units, information systems, security administrator, officials from all departments
Physical security	• CCTV • Fences-Small mesh and high gauge • Alarms • Intrusion detection: electromechanical, photoelectric, passive infrared, acoustical detection • Motion: wave pattern motion detectors, proximity detector • Locks: warded lock, combination lock, cipher lock, device lock, preset / ordinary door lock, programmable locks, raking lock • Audit trails: date and time stamps, successful/unsuccessful attempts, who attempted, who granted/modified access controls • Security access cards: Photo ID card, swipe cards, smartcards • Wireless proximity cards: user activated or system sensing field powered device

Evidence Lifecycle

1. Discovery
2. Protection
3. Recording
4. Collection and identification
5. Analysis
6. Storage, preservation, transportation
7. Present in court
8. Return to owner

Digital Evidence

Six principles to guide digital evidence technicians

• All general forensic and procedural principles apply.

• Upon seizure, all actions should not change the data.

• All people accessing the data should be trained

• All actions performed on the data should be fully documented and accessible.

• Anyone that possesses evidence is responsible for all actions taken with it while in their possession.

• Any agency that possesses evidence is is responsible for compliance with these principles.

Media Analysis

Part of computer forensic analysis used for identification and extraction of information from storage media. Eg. Magnetic media, Optical media, Memory (e.g., RAM)

Admissible Evidence

Relevant to the incident. The evidence must be obtained legally.

Digital Forensics

Five rules of evidence:
Be authentic • Be accurate • Be complete • Be convincing • Admissible

Investigation - To Determine Suspects

Types:
Operational • Criminal • Civil • eDiscovery

Security Incident and Event Management (SIEM)

Log review automating
Real-time analysis of events occurring on systems

Transaction Redundancy Implementations

Electronic Vaulting • Remote Journaling • Database shadowing

System Hardening

" • Uninstall unnecessary applications
• Disable unnecessary services
• Deny unwanted ports
• External storage device restriction
• Monitoring and Reporting
• Vulnerability Management System
• IDP/IPS: Attack signature engine should be updated regularly

System Recovery

1. Rebooting system in single user mode, recovery console
2. Recovering all file systems active before crash
3. Restore missing / damaged files
4. Recover security and access controls

Configuration Management (CM)

An ITILv2 and an ITSM process that tracks all of the individual Configuration Items (CI)

Configuration Items (CI)	Version: state of the CI, Configuration - collection of component CI's that makes another CI
Building	Assembling a component with component CI's Build list
Artifacts	Recovery procedures. Eg. system restart. Should be accessed by authorized users from authorized terminals.

Incident Response

Lifecycle	Response Capability • Incident response and handling • Recovery • Feedback
Mitigation	Limit the impact of an incident.

Root Cause Analysis (RCA)

Fault tree analysis (FTA)	Top down deductive failure analysis using boolean logic.
Failure mode and effects analysis (FMEA)	Review of as many components, assemblies, and subsystems as possible to identify potential failure modes.
Pareto Analysis	Looks at the predominant likely causes to deal with them first.
Cause mapping	Connects individual cause-and-effect relationships to give insights into the system of causes within an issue.

Disaster Recovery Methods

Hot Site	A real-time mirror of your system and network activity running in sync. Allows for minimum disruption and downtime.
Cold Site	An alternative workspace with power and HVAC setup, but no hardware. All recovery efforts will be technician heavy.
Warm Site	A middle-ground solution which includes skeletal hardware, software and connectivity to restore critical functionality.
Service Bureau	Contract with a service bureau to provide backup services.
Multiple centers / sites	Process between multiple data centers
Rolling / mobile sites	Mobile homes or HVAC trucks.
Recovery Time Objectives (RTOs)	• Hot site RTO: 5 minutes or hours • Warm site RTO: 1-2 days • Mobile site RTO: 3-5 days • Cold site RTO: 1 to 2 weeks

RAID, SAN, & NAS

RAID	Redundant Array of Independent / Inexpensive Disks
Disk Mirroring	Writing the same data across multiple hard disks, slower as data is written twice, doubles up on storage requirements
Disk Striping	Writes data across multiple disks simultaneously, provides higher write speed.
RAID 0	• Writes files in stripes across multiple disks without using parity information • 2 or more disks required • Fast reading and writing but no redundancy
RAID 1	• Creates identical copies of drives - has redundancy • Space is effectively utilized, since half will be given to another disk • Expensive
RAID 3	Byte level data striping across multiple
RAID 4	Block level data striping across multiple
RAID 5	Data and parity Information is striped together across all drives
RAID 0+1	Stripes data across available drives and mirrors to a seperate set of disks
RAID 1+0 (RAID 10)	Each drive in a set is mirrored to an equivalent drive in another set
Storage Area Network (SAN)	Typically use Fibre Channel and iSCSI. High speed blick level storage.
Network-Attached Storage (NAS)	Typically an NFS server, file-level computer data storage server connected to a computer network.

Disaster Recovery Terminology & Concepts

MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MTBF	Mean Time Between Failures, MTTF + MTTR
Transaction Redundancy Implementations	Electronic Vaulting • Remote Journaling • Database shadowing

Business Continuity Planning

Business Continuity Plan (BCP)	Concerns the preservation and recovery of business in the event of outages to normal business operations.
Business Impact Analysis (BIA)	The process of assessing the impact of an IT disruption. BIA is part of BCP
Disaster Recovery Plan (DRP)	A framework of steps and actions that need to be taken to achieve business continuity and disaster recovery goals. End Goal – Revert back to normal operations - planning and development must be done before the disaster - BIA should be complete
Business Continuity Steps	1. Scope and plan initiation 2. BIA - assess impact of disruptive processes 3. Business Continuity Plan development - Use BIA to develop BCP - Testing 4. Plan approval and implementation - management approval

Trusted Recovery

Breach Confirmation	Confirm security breach not happen during system failure.
Failure Preparation	Backup critical information to enable recovery
System Recovery	After a failure of operating system or application, the system should work enough to have the system in a secure state