

Introduction to Incident Response and Disaster Recovery

Introduction to Incident Response (IR) & Disaster Recovery (DR)

Purpose: Provide a concise, easy-to-read reference for students, new team members, or anyone needing a quick overview of the core concepts, phases, and best practices.

1. Key Definitions

Term	Meaning
Incident	Any event that compromises the confidentiality, integrity, or availability of information assets (e.g., malware infection, data breach, insider misuse).
Incident Response (IR)	A coordinated set of processes for detecting, analyzing, containing, eradicating, and recovering from security incidents.
Disaster	A large-scale event that disrupts normal business operations and may affect multiple systems or locations (e.g., natural disaster, major power outage, ransomware attack).
Disaster Recovery (DR)	The set of strategies, policies, and technical measures used to restore IT services and data after a disaster.
Business Continuity (BC)	The broader discipline that ensures critical business functions continue during and after a disruption (BC includes DR as a technical component).

2. Why IR & DR Matter

1. **Minimize Impact** – Faster detection & containment reduces financial loss, reputational damage, and regulatory penalties.
 2. **Regulatory Compliance** – Many standards (e.g., NIST, ISO 27001, PCI DSS, GDPR) require documented IR and DR capabilities.
 3. **Operational Resilience** – Enables organizations to maintain or quickly resume critical services.
 4. **Learning & Improvement** – Post-incident analysis drives security hardening and process refinement.
-

3. Incident Response Lifecycle

Introduction to Incident Response and Disaster Recovery

Phase	Primary Goals	Typical Activities	Key Outputs
1. Preparation			
	Build the foundation for effective response.	• Assemble IR team & define roles (e.g., Incident Commander, Analyst, Forensic Lead) • Deploy detection tools (SIEM, IDS/IPS, EDR) • Conduct training & tabletop exercises • Monitor alerts & logs	IR policy, runbooks, contact lists, tool configurations
2. Identification			
	Detect and verify that an incident has occurred.	• Correlate events • Perform initial triage (severity, scope) • Notify the IR team • Short-term: isolate affected host, block malicious IPs	Incident ticket, initial classification (e.g., "Potential Phishing")
3. Containment			
	Limit the spread and prevent further damage.	• Long-term: apply firewall rule changes, patch vulnerable services • Preserve evidence (snapshot, memory dump) • Delete malware, malicious accounts	Containment actions log, evidence preservation checklist
4. Eradication			
	Remove the root cause and any artifacts.	• Apply patches, harden configurations • Verify that no backdoors remain • Restore from trusted backups	Clean-system verification report
5. Recovery			
	Restore systems to normal operation safely.	• Reconnect to network after validation • Monitor for signs of re-infection	System-up-and-running confirmation, post-recovery monitoring plan

Introduction to Incident Response and Disaster Recovery

Phase	Primary Goals	Typical Activities	Key Outputs
6. Lessons Learned	Capture insights to improve future response.	meeting • Update playbooks, policies, and controls • Report to stakeholders &, if required, regulators	After-action report, updated documentation, training updates

Tip: Keep the “**5?Whys**” technique handy during the Lessons Learned phase to drill down to