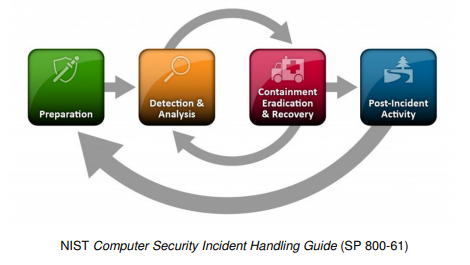
**Module 5 Risk Management**

**5.4 Incident Response**

**NIST Incident Response Process**



**Incident Response Plan**

* Incident Definition

1. NIST – occurrence that actually/potentially jeopardises the confidentiality/integrity/availability of an information system/information the system processes/stores/transmits/constitutes a violation/imminent threat of violation of security policies/procedures/acceptable use policies
2. Cybrary – unplanned disruption/degradation of network/system service & needs to be resolved immediately

* NIST Definition of Incident Response Plan – documentation of predetermined set of instructions/procedures to detect, respond to & limit consequences of malicious cyber attacks against organisation’s information system(s)
* NIST Computer Security Incident Handling Guide (SP 800-61) provides guidance on exact elements to include

1. Mission, strategies & goals of incident response
2. Senior management approval
3. Approach to incident response
4. Response team communications
5. Metrics for measuring response capabilities & effectiveness
6. Roadmap for maturing response capability
7. How incident response program fits into organisation

**Incident Response Plan (IRP)**

* Documented incident types/category definitions
* Roles & responsibilities
* Cyber-incident response teams
* Reporting requirements/escalation
* Exercise

**Documented Incident Types/Category Definitions**

* Natural
* Mechanical
* Accidental/human error
* Malicious/compromise C-I-A
* Policy violation

**Roles & Responsibilities**

* Granting clear authority for actions to be taken during incident
* Who can/does perform IRP activities

1. Incident alerting
2. Identification/triage
3. Decision making – must be organisational executive
4. Equipment collection/confiscation
5. Forensics – independence/segregation of duties
6. Repair/recovery
7. Reporting
8. Communicating – talking outside organisation

**Cyber-Incident Response Teams**

* Computer Emergency Response Team (CERT)
* Cyber Incident Response Team (CIRT)
* Computer Security Incident Response Team (CSIRT)
* Formalised, standing or ad-hoc
* Internal or external
* Central, distributed or coordinating
* Includes

1. Systems, network, database administrators
2. Legal
3. Human Resources (HR)
4. Management

**Reporting Requirements/Escalation**

* Document, document, document
* Included in many help desk systems
* Collecting evidence (physical, virtual etc.)
* Reporting/disclosing to

1. Internal management (legal, human resources, CEO, CFO)
2. Legal authorities/law enforcement (local, FBI)
3. Affected organisations/clients/customers
4. CERT ([www.cert.org](http://www.cert.org))
5. Internet Crime Complaint Centre (IC3) – [www.ic3.org](http://www.ic3.org)
6. Insurance (Cyber)

**Testing, Exercises & Training**

* Be prepared
* Prepare each role with training
* Practice using real world scenarios
* Test systems & processes to find issues
* Exercises – practice using real world scenarios

1. Table-top exercises
2. Functional

**Incident Preparation**

* Creating Incident Response Plan
* Hardware/software/communications – jump kit
* Testing & exercises
* Creating checklists – technical, procedures, contacts

**Incident Detection/Identification/Analysis**

* Alerting

1. Logs – IDS, SIEM, Antivirus
2. Humans

* Incident triage/validation
* Determine incident scope

1. What & who affected
2. # of systems
3. Identification of type (system, data, personnel etc.)
4. Analysis – impact & recoverability effort
5. Escalation
6. Documentation & notification

**Incident Containment**

* Ensuring incident doesn’t continue/spread
* Securing scene/limiting access/isolating systems (quarantine)

1. Physical
2. Network
3. Logical

* Gathering evidence

**Eradication**

* Find & eliminate root cause
* Removing elements of incident (Eg. Malware)
* Actions

1. Antivirus clean-up
2. Patching/updating software
3. Re-imaging systems
4. Restoring from backup

**Incident Recovery**

* Process of restoring & returning affected systems & devices back into your business environment
* Repair

1. Restoring from backup
2. Patching
3. Hardening systems (using known baseline)
4. Access control (network/systems)
5. Authentication (change passwords)

* Procedural changes
* Documentation

**Post Incident**

* Lessons learnt
* After-action meeting with all Incident Response Team members
* Capture actions such as cause, cost, recommendations for preventing future incidents
* Discuss what you’ve learnt from data breach
* Regulatory/legal requirements
* Update IRP