Joint Universities Computer Centre Limited
(“JUCC”)

Information Security Awareness Training- Session Four

Information Security Incident Management

Agenda

- Overview of Information Security Incident Management
- Roles and Responsibilities in Information Security Incident Management
- Information Security Incident Classification and Incident Handling Procedure
- Forensic Investigation
- Information Security Incident Management Guidelines

Definition of Information Security Incident Management

Wikipedia:

Information Security Incident Management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events.

ISACA (CISM Review Manual):

Information Security Incident Management is the operational part of risk management. It is the activities that take place as a result of unanticipated attacks, losses, theft, accidents, or any other unexpected adverse events that occur as a result of the failure or lack of controls.

OGCIO:

Information Security Incident Management is a set of continuous processes governing the activities before, during and after a Information Security Incident occurs

Importance of Information Security Incident Management to Education Institutions

Examples of Information Security Incidents in Campus:

- Web defacement
- Phishing email / phishing web site
- Data theft / Identity theft
- Loss of unencrypted portable media / Data leakage
- Improper use of campus IT resources (e.g. Bittorrent)
- Computer virus / worm / trojan horse

Benefits of Information Security Incident Management to Education Institutions:

Campus Perspective

- Protect the institutions' reputation
- Reduce business impact (e.g. financial loss) of incidents by timely resolution
- Reduce the risk of legal infringement (e.g. copyright law and Personal Data (Privacy) Ordinance ("PDPO"))

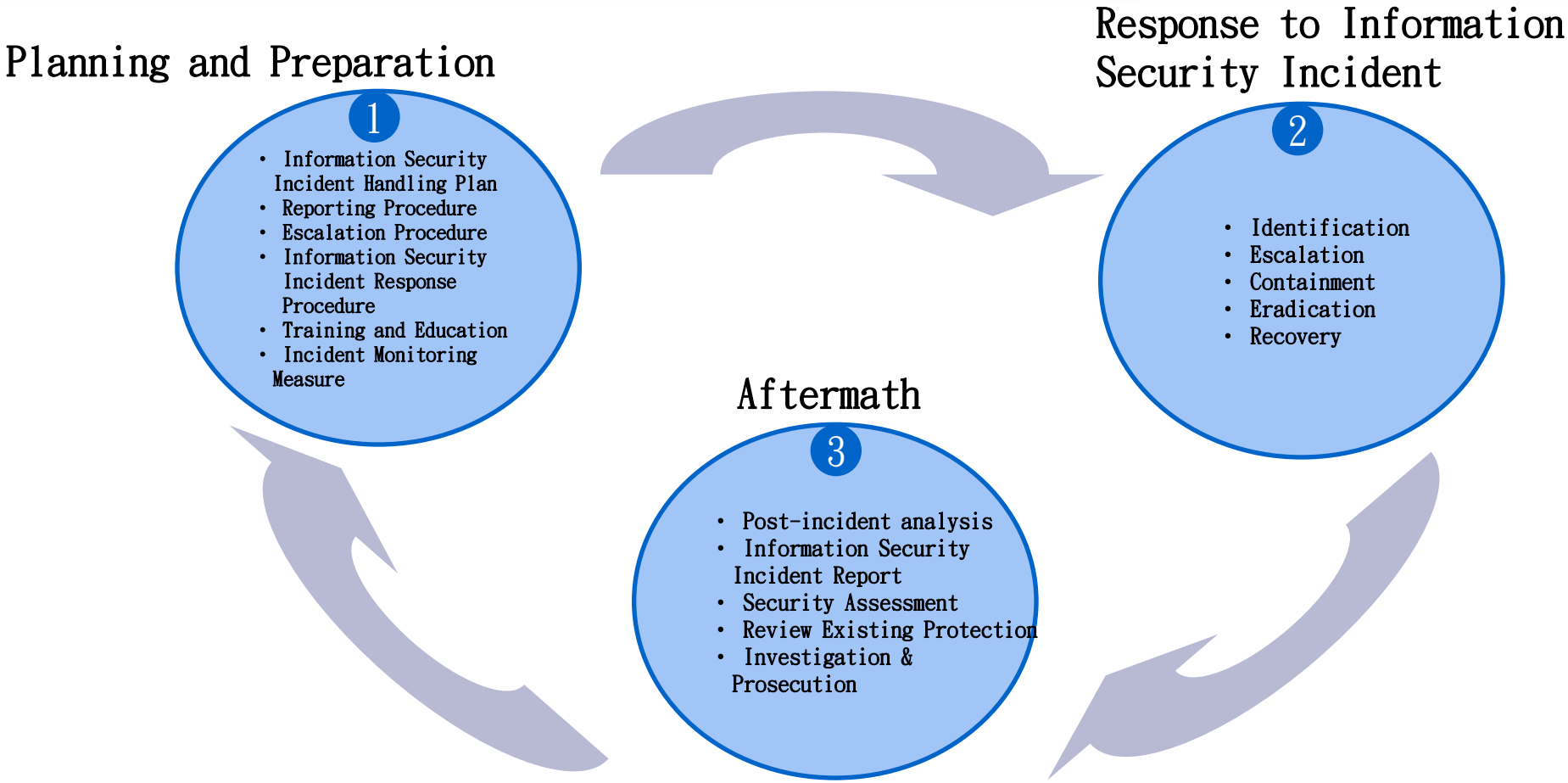
IT Perspective

- Improve monitoring, system availability as well as service quality
- Proactive identification of system, process and control improvement
- Enhanced Management Information regarding service quality

Essence of Information Security Incident Handling:

- Ensure that resources are available to handle the incidents, e.g. manpower, technology, etc
- Ensure that all the responsible parties have clear understanding about the tasks required
- Ensure that the incident response is efficient
- Ensure that the response activities are recognised and coordinated
- Minimise the possible impact of the incident
- Share experience in incident response within and among team members
- Prevent further attacks and damages
- Deal with related legal issues

Information Security Incident Handling Cycle



Information Security Incident Handling Cycle

Roles and Responsibilities in Information Security Incident Management

Institution's Management

- Buy-in and support of the development and execution of Information Security Incident Management
- Key decision maker
- Raise the awareness in the campus

Information Technology Professional

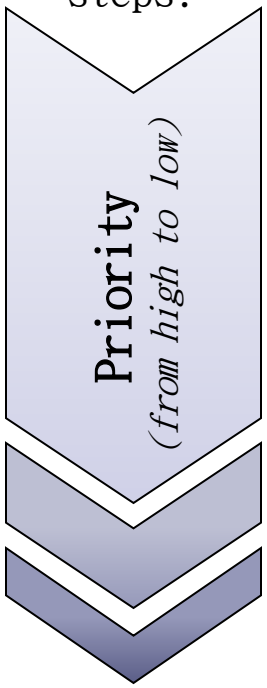
- Overall management and supervision of Information Security Incident handling within the institution
- Perform incident evaluation and decide on incident response procedures
- Alert the management upon receipt of report on Information Security Incident
- Reporting progress to management
- Coordinating various external parties, such as Police, HKCERT, service contractors, support vendors, and security consultants etc. in handling the incident
- Seeking necessary resources and support from the senior management

Everyone in the Institution

- Proper use and protect the institution's information asset
- Do not commit any hacking activities in the institution
- Keep an eye on information Security Incidents, e.g. data leakage, computer crime, etc
- Report any suspicious cases to your IT department

Prioritisation of Incidents

The IT Professional should start to identify the incident, which involves the following steps:



1. Determine if an incident occurs

- Determine the validity of a reported incident

2. Perform preliminary assessment

- Determine the type of the incident, and assess the scope, damage
- Precautions or defensive measures can be taken promptly to reduce impact

3. Log the incident

- Record all Information Security Incidents, actions taken and the corresponding results

Types of Information Security Incident Handling

Below are some examples of types of Information Security Incidents:

Type	Example(s)	Treatment
Human Error	• Accidental deletion of data	• Restore backed up data
	• Misplaced passwords	• Change passwords and inspect audit logs for any access to sensitive information during the period when the passwords were misplaced
Machine Failure	• Web server crashes	• Start up backup server • If no backup server, restore last restored image of the Web server
Malicious Terror	• Viruses, Worms, Mal-ware	• Isolate the affected system/ servers • Quarantine and remove the virus • Post-impact analysis (e.g. Check if any sensitive information was affected, review firewall configuration and determine whether anti-virus software is up-to-date)

Information Security Incident Classification and Incident Handling Procedure

Incident Escalation

Escalate the incident to management following the predefined escalation procedure

General User

A member of the university community who becomes aware of the information Information Security Incident should immediately:

- Disconnect the compromised system and equipment from the network
- Avoid making any updates or other modifications to software, data or equipment involved or suspected of involvement with an information Information Security Incident until management has completed their investigation
- Contact management

IT Professional

The IT professional performs the investigation and remediates the problem as instructed by management

Management

Management to make key decisions, e.g:

- Contact the Technology Crime Division of the Hong Kong Police Force Commercial Crime Bureau if the institution suspects a computer crime has been committed
- Report to the Office of the Privacy Commissioner for Personal Data (PCPD) if personal data is involved in a Information Security Incident

Incident handling and investigation

Incident handling and investigation

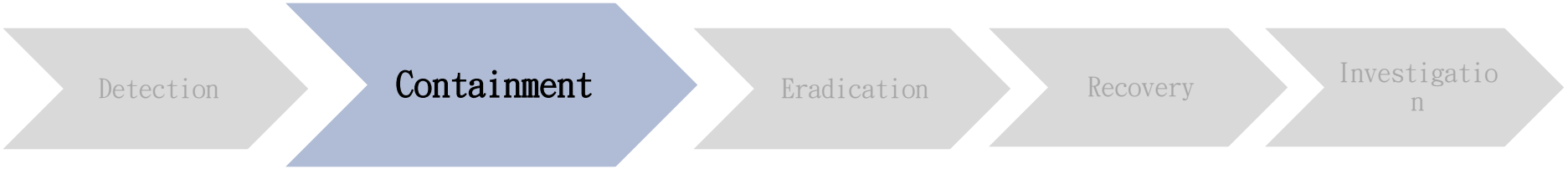
Detection | Containment | Eradication | Recovery | Investigation

Objective: Determine whether an incident has occurred and, if so, the type, extent and magnitude of the problem

- Signs of an incident may include:

1. Antivirus software alerts when it has detected a virus or worm
2. Web server crashes
3. Slow access to hosts on the Internet / Intranet
4. Suspicious person or party requests for personal information
5. Unusual deviation in network traffic flow

Incident handling and investigation



Objective: Limit the scope, magnitude and impact of an incident before it causes further damages

- Activities may include:

1. Conducting impact assessment
2. Protecting sensitive or critical information and system
3. Decide whether to continue or suspend the operation and service of the compromised system
4. Building an image of the compromised system for investigation purpose
5. Checking any systems associated with the compromised system
6. Unplug network cable
7. Shutting down or isolating the compromised host or system temporarily
8. Stopping operation of the compromised server
9. Disabling some of the system's functions
10. Removing user access or login to the system
11. Keeping a record of all actions taken during this stage

Incident handling and investigation

Objective: Remove the cause of the incident from the system

- Activities may include:
  1. Stop or kill all active processes of the hacker to force the hacker out
  2. Delete all the files created by the hacker (e.g. web defacement)
  3. Eliminate all the backdoors and malicious programs installed by the hacker
  4. Apply patches and fixes to vulnerabilities
  5. Correct any improper settings in the system and network
  6. Remove computer virus, if any
  7. Change all system passwords
  8. Keep a record of all actions performed.

Incident handling and investigation

Objective: Restore the system to its normal operation

- Activities may include:
  1. Re-install the deleted/damaged files or the whole system from the trusted source (e.g. system backup / installation media)
  2. Perform system functional test
  3. Harden the system
  4. Disable unnecessary services
  5. Conduct a pre-production security assessment
  6. Keep a record of all actions performed

Incident handling and investigation

Investigation

Objective: Conduct analysis on the incident and response actions for future reference

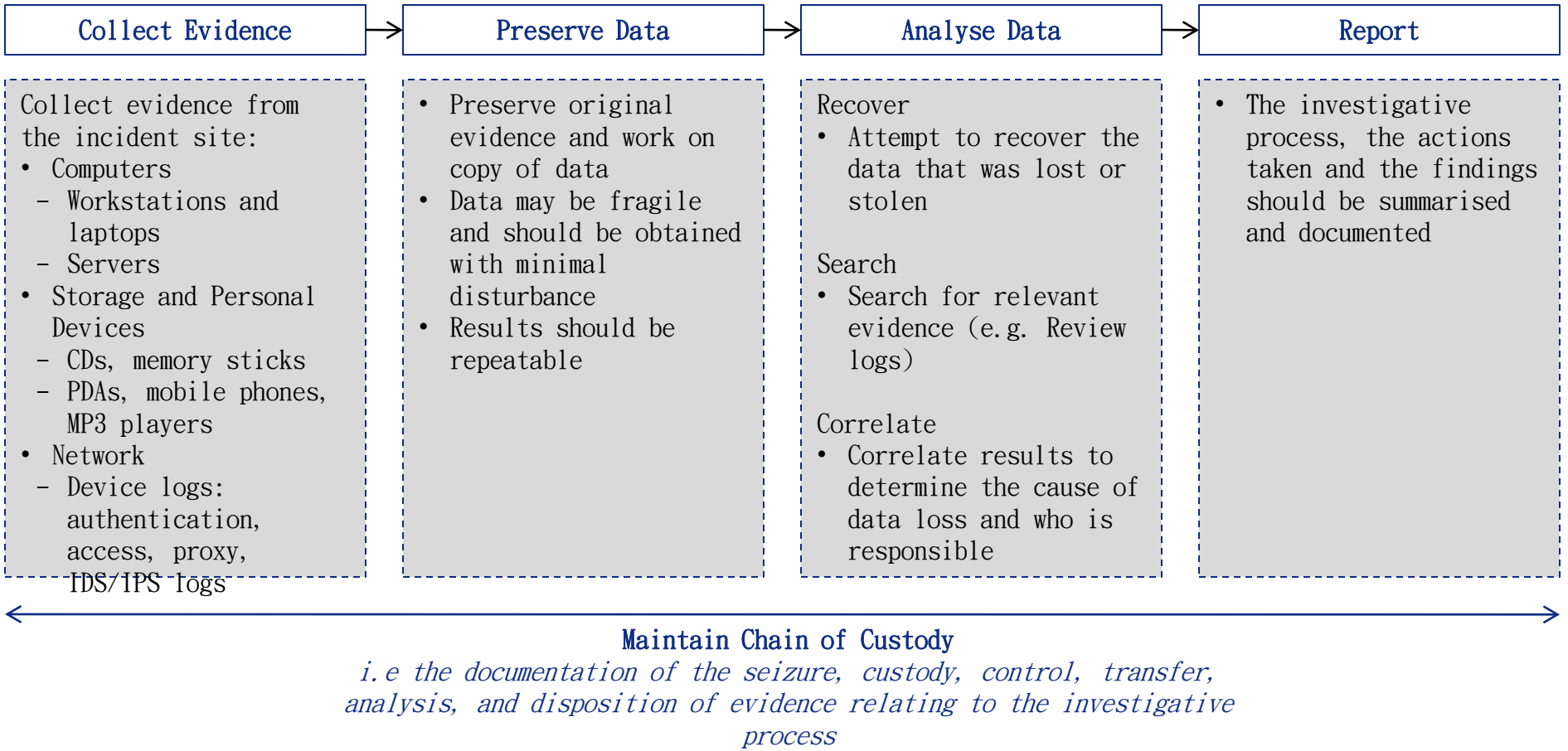
- Examples of analysis include:
  - Firewall log and system log analysis
  - File integrity assessment
  - Vulnerability assessment
  - System image assessment
  - Assess damage of incident, which may include manpower, monetary cost, cost of disruption, legal liability and loss of reputation
  - Recommended actions to prevent further attack
  - Additional tools used or needed to aid in the detection and eradication process
  - Forensic investigation

Forensic Investigation

Definition:

- Forensics is the use of scientific techniques to solve crimes
- Usually applies to examination of evidence
- Forensics seeks to provide an accurate representation of extracted data
- Forensics can be a tool to aid incident management by identifying what data was lost and how data was lost

Forensic Investigative Process



Information Security Incident Management Guidelines

- INFORMATION SECURITY INCIDENT HANDLING GUIDELINE
  [http://www.ogcio.gov.hk/eng/prodev/download/g54_pub.pdf]
- Computer Information Security Incident Handling Guide
  [http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf]

Summary

- Information Security Incident Management
  - Definition & Examples of Information Security Incident
  - Importance of Information Security Incident Management
  - Roles and Responsibilities
  - Information Security Incident Handling Procedures
    - Detect
    - Contain
    - Eradicate
    - Recover
    - Investigate

Q&A

?