CHAPTER 3
SECURITY INCIDENT HANDLING

3.1 What is an Information Security Incident?

3.1.1 An information security incident is an adverse event in an information system and/or a network that poses a threat to computer or network security in respect of confidentiality, integrity and availability.

3.1.2 Examples of security incidents include denial of service attack, compromise of protected information systems or data assets, leaks of classified data in electronic form, malicious destruction or modification of data, abuse of information systems, massive malware infection, website defacement, and malicious scripts affecting networked systems.

3.2 Objectives of Security Incident Handling

3.2.1 A well-defined security incident handling plan is vital to the efficient and effective handling of security incidents, minimising impact and damage, and rapidly recovering operation of an information system. Below are the major objectives of security incident handling:

(a) Minimise losses and subsequent liabilities to the school.

(b) Minimise the possible impact of the incident in terms of information leakage, corruption and system disruption, etc.

(c) Ensure that the response is systematic and efficient and that there is prompt recovery for the compromised system.

(d) Ensure that the required resources are available to deal with incidents, including manpower, technology, etc.

(e) Ensure that all responsible parties have a clear understanding regarding the tasks they need to perform during an incident by following predefined procedures.

(f) Ensure that all response activities are recognised and coordinated.

(g) Prevent further attacks and damage.

(h) Deal with related legal issues and refer to the Hong Kong Police Force (HKPF) for criminal investigation when deemed appropriate.

(i) Report to the Office of the Privacy Commissioner for Personal Data (PCPD) if personal data is involved.

(j) Preserve information for investigation as far as practicable.

3.3 Steps for Security Incident Handling

3.3.1 Security incident handling is a set of continuous processes governing the activities before, during and after a security incident occurs.

3.3.2 Proper and advanced planning ensures that all response procedures are known, coordinated and systematically carried out. It also facilitates management in making appropriate and effective decisions in tackling security incidents, and in turn minimises any possible damage. The plan includes strengthening of security protection, making an appropriate response to the incident, recovery of the system and other follow up activities. There are five major steps in security incident handling. An overview of these steps is provided below:

(a) **Planning and Preparation**: Schools should plan and prepare for the resources as well as develop proper procedures to be followed. Some suggestions to schools are as follows:

- Determine the school's policies.
- Make sure the incident response strategy is consistent with the school security policy and sufficient authority is granted to the incident response team to take specified actions, e.g. switch off school servers in the critical moment.
- Define roles and responsibilities of all parties participating in the security incident handling process.
- Establish the list of prioritised information asset / services and acceptable downtime.
- Develop Reporting Procedure, Escalation Procedure and Security Incident Response Procedure. These procedures should be communicated to all staff, including management personnel, for their reference and compliance.
- Develop and maintain good backup strategy.
- Develop and maintain the Call List.
- Provide adequate staff training to ensure all concerned staff and management are capable of handling security incidents.

- Educate users the emergency procedures and way of incident reporting.
- Set up monitoring and alerting mechanism for computer systems, such as install intrusion detection system, anti-malware and content filtering tools, enable system and network audit logging and perform periodic security checking using security scanning tools.

(b) **Detection and Reporting**: Schools should detect security events according to the established detection and monitoring mechanism. Schools should also follow the reporting procedure to bring the security events to the attention of senior management. The major activities in this step are:

- Detection Measure
  - ✧ Monitor abnormal events, e.g. error messages, suspicious events in logs, poor performance and unusual capacity growth.
  - ✧ Analysis of log information from devices, services, hosts, and various systems.
  - ✧ Reports from users or help desk.
  - ✧ External notifications coming from outsiders such as telecommunication service providers, Internet service providers (ISPs), general public, media, or external service providers.
- Reporting
  - ✧ All staff should be well aware of and have access to the report procedures for reporting different types of possible information security events.
  - ✧ Information such as date/time for detection, systems affected, observations, contact information of the reporter should be the basis of reporting an information security event.

(c) **Assessment and Decision**: After an event has been detected, schools should determine if an incident has actually occurred. If an event is identified to be an information security incident, schools should determine the type of the incident, and assess its scope, damage and impact in order to effectively deal with it. Schools should also follow the predefined escalation procedure to notify the appropriate parties and escalate the incident to the appropriate level. The major activities in this step are:

- Assessment of Incident
  - ✧ IT Head and TSS should determine whether or not an incident has actually

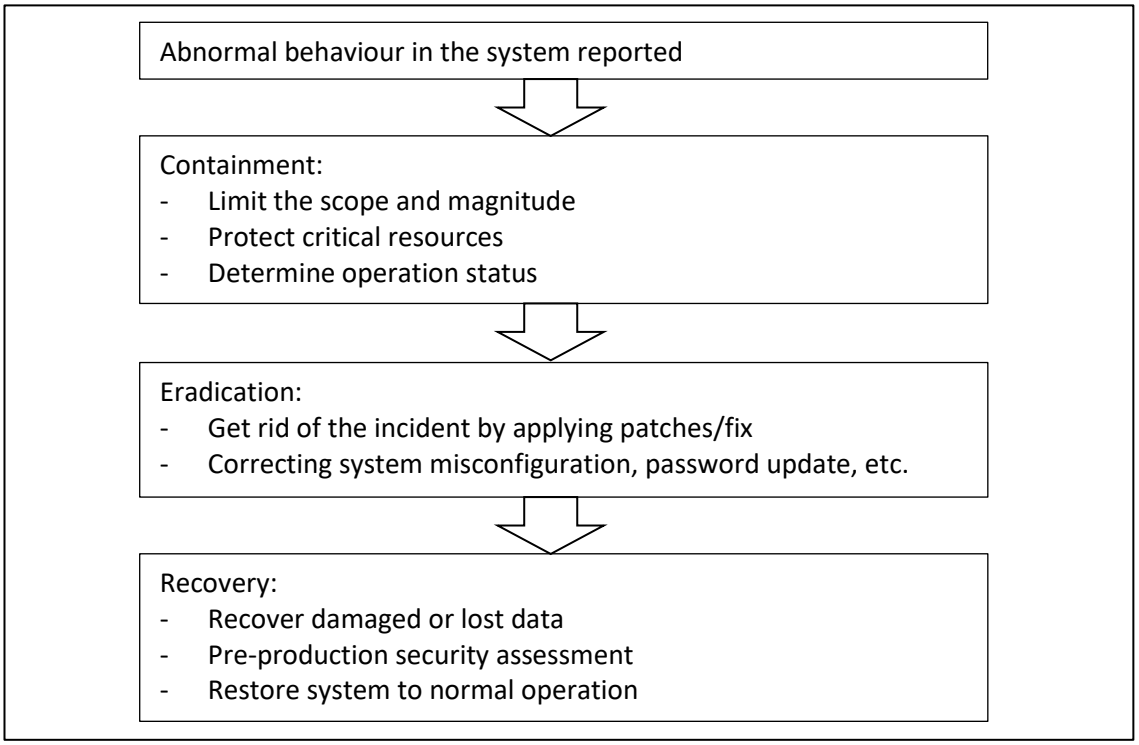
occurred. However, it is often difficult to determine whether the abnormality found is a symptom of an incident. Some evidences may reveal that the abnormality is caused by something else, for example, hardware failures or user errors.

- ✧ To determine if an abnormality is a result of system problems or actual incidents, the IT Head and TSS should collect information about the detection of an information security event and seek clarification from the person who reports the security event.

- Escalation

  - ✧ The IT Head should then determine the type of the incident, and assess its scope, damage and impact in order to effectively deal with it and report the incident to the school management.
  - ✧ Some precautions or defensive measures can be taken promptly in the light of the damage made and the impact involved.
  - ✧ Any observed or suspected security incidents or security problems in information systems or services should be reported immediately to the responsible party and handled according to the incident handling procedure.
  - ✧ If the incident is a potential multiple point attack targeting at the school, the school is recommended to notify HKCERT for information and advice.
  - ✧ If the school suspects a computer crime has been committed, the school should contact the Cyber Security and Technology Crime Bureau of HKPF.
  - ✧ All security incidents, actions taken and the corresponding results should be recorded.
  - ✧ A snapshot of the compromised system should be obtained as soon as suspicious activities are detected, and as far as technically and operationally feasible. This can prevent the attacker from destroying the evidence and support subsequent case investigation, such as forensic evidence collection.

(d) **Response to Security Incident**: When a security incident is identified, schools should follow the security incident response procedure to carry out actions to tackle the security incident and to restore the system to normal operation. The response procedure is broadly categorised into three stages: Containment, Eradication and Recovery. It should be noted that the response procedure may not strictly follow the order of the three stages, which has to be customised to meet practical needs.



(e) **Post-Incident Actions**: When the incident is over, follow-up actions should be taken to evaluate the incident and to strengthen security protection to prevent recurrence. This should start as soon as possible after the incidents. Principal, IT Head, and users should be involved.

- To carry out post-incident review and find out areas of improvement, for example:
  - ✧ Checking if the current configuration and procedure are sufficient.
  - ✧ Checking if more user education is required.
  - ✧ Determining if an external security audit is required.
  - ✧ Determining if the incident should require any legal action.
- A report summary with recommendations for improvement should be sent to the Principal.

- The principal should assess the report and select the recommendations for improvement to be implemented.

- A periodic security risk assessment and audit exercise is recommended for systems under security exposure, especially for those that have been affected by security incident. Security review and audit of a system should be an ongoing exercise to promptly identify possible security loopholes and/or areas of improvement to the system as a result of technology advancement in both security protection as well as attack/intrusion.

- Security related policies, standards, guidelines and procedures should be regularly reviewed and modified as necessary to ensure the effectiveness of the overall security protection to an information system.

3.4 Training and Education

3.4.1 Schools should ensure all staff observe the security incidents handling / reporting procedure for information systems accordingly. Staff should be familiar with the relevant procedures from incidents reporting, identification, and taking the appropriate actions to restore the system to normal operation. Drills on incident handling is recommended to be organised regularly for staff to practise the procedures.

3.4.2 In addition, sufficient training to system operation and support staff on security precaution knowledge is also important, in order to strengthen the security protection of the system or functional area, and reduce the chance that an incident may occur.