Security Incident Management

A newsletter for IT Professionals

Issue 12

I. Background of Security Incident Management

What is a Security Incident?

An information security incident can be defined as an attempted or successful unauthorised access, use, disclosure, modification or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy.

It poses a threat to the computer or network security in a University in respect of availability, integrity or confidentiality. A common example is leakage of sensitive information which adversely influences the interests of a University.

Security Incident Management Process

A security incident management process involves five phases including Incident Reporting, Impact Assessment, Incident Escalation and Resolution, Incident Monitoring, and Post Incident Review.

Each of the above phases helps the University to contain the impact of information security incidents and to drive the handling process as efficiently as possible.

A properly designed and implemented security incident management should also help the University to prevent future security incidents.

Reference:
http://www.ogcio.gov.hk/eng/prodev/download/g54_pub.pdf
JUCC - Information Security Incident Handling and Reporting Mechanisms

I. Background of Security Incident Management (cont'd)

1. Incident Reporting

Incident reporting phase aims at establishing an effective and efficient mechanism to detect and report security incidents. The mechanism includes utilising human resources, such as setting up a security incident response team led by an information security officer, and receiving queries and reports from users' awareness of possible security incidents in the University's systems.

2. Impact Assessment

An assessment should be carried out for each reported incident to determine the scope and impact to the University. For example, an incident can be assessed to have high, medium or low impact to the University according the amount of monetary loss, duration of service interruption or scale of reputation damage. A brief investigation of the root cause should also be performed to enable effective planning of incident resolution.

The purpose of performing impact assessment is to maximise the processing efficiency and effectiveness, at the same time minimise the incremental resources invested in dealing with the information security incidents.

3. Incident Escalation and Resolution

Significant security incidents identified during the impact assessment require to be escalated to the senior management for their knowledge or their participation to resolve the security problems caused by the incident.

The incidents resolution involves allocating work to security incident response team members and other relevant users or departments, managing the communication between different parties and the executing the resolution plan.

4. Incident Monitoring

Security incidents with different natures indicate different timelines, resources needs and resolutions. Therefore, the status of the handling process of each incident should be closely monitored to ensure that tailor made resolution is delivered within reasonable timeline and resource constraints.

5. Post Incident Review

In a sophisticated security incident management process, the security incident response team should exercise due diligence to investigate the root cause of each security incident, and learn from these experiences to avoid recurring incidents in the future through implementing necessary mitigating controls.

Reference:
http://www.ogcio.gov.hk/eng/prodev/download/g54_pub.pdf
JUCC Newsletter - Security Incident Management

II. Risks of Security Incident Management in Universities

- **Inappropriate Impact Assessment / Resolution Timeliness**

  The assessment of security incidents in terms of urgency and severity is essential for the efficient and effective use of University's resources to address the right issues at the right time.

  The impact of a security incident might be over-estimated or under-estimated, which can lead to excessive or insufficient resources allocated for incident handling. In additioin, exposure to security risk is likely to be increased if the incidents are overlooked.

- **Insufficient Level of Escalation**

  Proper escalation of security incidents is important in the security incident management process. However, the escalation plan can be complicated and the buy-in of different levels of management is not easily achievable in a University due to its complex structure (e.g. multiple administrative or academic divisions with many levels of senior management).

  If significant security incidents are not timely escalated to an appropriate level of management for support or decision-making, it may increase the scale and depth of the impact on the University.

- **Lack of Monitoring**

  Some security incidents require longer period of attention, some needs more resources and the others demands supporting from the senior management.

  Without regular tracking of the incident status, there is a risk that adverse situations like delay in incident resolution or resource shortage may occur. In addition, the University may not be able to adapt its handling methods for incidents with volatile nature in a quickly manner.

- **Lack of Post Incident Review**

  Finding out the root cause of a security incident is very important as it can effectively prevent the recurrence of similar problems in the future.

  However, the security incident response team usually spends most of the time in impact assessment, incident escalation, resolution and monitoring. Post incident review of security incidents is likely to be overlooked and the real root causes may go undetected.

Reference:
JUCC - Information Security Incident Management Standard
JUCC - Information Security Incident Handling and Reporting Mechanisms
JUCC Newsletter - Security Incident Management

III. Vulnerabilities of Security Incident Management

- **Insecure Incident Log**

  Security incident management may require the use of in-house developed systems or vendor software for log management or tracking. Popluar incident log management tools available on the market today include D3 Security Management System and Symantec Incident Manager.

  The incident log or incident status contains a lot of sensitive information about the daily operations and security problems of the systems in the University. If this information is not well protected, the University's systems may be easily vulnerable to malicious activities.

- **Ineffective Security Incident Identification and Reporting**

  Security incident identification and reporting procedures should be probably established. Detailed instructions and accurate criteria on reporting channels and incident classifications should be in place.

  Users will be confused if the instructions / criteria on what constitutes a security incident and how to report it to the right party are not clearly documented or communicated by the University.

- **Inappropriate Impact Assessment**

  Impact assessment is important for the planning of appropriate resource allocation and timely incident resolution.

  Without thorough review and assessment of security incidents, the security incident response team may not be able to understand the severity of the incidents and develop the most appropriate resolution for them. Under-estimation of the impact of security incidents can even make the University suffer from more serious damage / loss.

- **Lack of User Awareness or Qualified Incident Response Team**

  Professional knowledge, experience and judgments of the incident response team members are very critical to a successful incident management process. In addition, as security incidents can occur anywhere in the University's network (e.g. a workstation in the library or a ledger system used by the finance department), timely identification and reporting of security incidents also requires the awareness of general users including students, faculties and other members as well.

  Unqualified security incident response team members may handle the incidents incorrectly, causing delay in handling process, excessive resources consumption or even more serious damage or loss to the University. Insufficient user awareness towards incident identification and reporting can lead to security incidents go undetected or not reported timely.

Reference:
JUCC - Information Security Incident Management Standard
JUCC - Information Security Incident Handling and Reporting Mechanisms
JUCC Newsletter - Security Incident Management

III. Exploitations of Security Incident Management

- **Information Gathering of Critical University Systems**

  Users may report a security incident when they encounter program bugs when using University's systems, or an IT staff may report that a security patch of the windows operating system cannot be correctly deployed in multiple servers within the University. Such information is considered sensitive since it may give a lot of hints to the malicious hackers regarding the vulnerabilities of the University's information systems, which may subsequently become the target of exploitations by hackers.

  If the system maintaining security logs or the security incident database is not secured, the hackers can target on University's systems using the sensitive information obtained above.

- **Decentralised Security Incident Management Structure**

  A University may have multiple separate security incident response teams established for each academic or administrative division. A potential issue of this decentralised structure is the inefficient communication among different incident response teams. Security incidents spotted by one team may not be timely communicated to the others for precaution or appropriate incident handling.

  By leveraging the time lag in communicating security incidents among the University's incident response teams, vulnerabilities exposed by the reported security incidents in one place may be used by hackers to launch malicious attacks elsewhere.

- **Social Engineering**

  Another form of exploitation with regard to the security incident management process is social engineering. Hackers may disguise themselves as members of the security incident response team and contact the users to conduct routine security check. Or they can approach users and pretend to follow up on the security incidents raised previously. The objective of the social engineering is usually to get sensitive information such as account login password and personal data for committing further attack on the University's information systems. A common example is asking the user for the password to reset his or her account due to suspicious security breaches.

  Users with privileged access to sensitive information or critical IT systems have higher possibilities to become the target of social engineering. Any sensitive information leakage from them can be utilised by hackers for more effective or deadly attacks.

Reference:
JUCC - Information Security Incident Management Standard
JUCC - Information Security Incident Handling and Reporting Mechanisms
JUCC Newsletter - Security Incident Management

IV. Hardening Steps for Security Incident Management

- **Staff Authentication Mechanism**

  Prior to the security incident response team interacting with the users for handling incidents, both the team members and the users should be familiar with the authentication mechanism to prove their identities. The purpose is to prevent any sensitive data leakage to unauthorised parties or even malicious hackers through social engineering.

  One method is to send an email notification to the user before direct telephone contact by the security incident response team. The email notification should include an incident number or authentication number, which can be used to authenticate both parties at the beginning of the call.

- **Clear Definition of Roles and Responsibilities**

  Personnel from various parties in the University are involved in the security incident management process, such as the Information Security Officer, the security incident response team, the general users, the senior management and so on. Representatives from each academic and administrative division of the University, such as Human Resources, Finance Department, Operations and Public Relations, may also be involved in the security incidents handling process.

  An effective security incident handling process depends on the co-operation and interaction of all the relevant parties, with each of them contributing their knowledge and performing assigned tasks (e.g. escalation, resolution, monitoring, etc). Hence, a clear and precise definition of the roles and responsibilities of each party is necessary and should be well acknowledged by all incident response team members.

- **Integrated Security Incident Handling Mechanism**

  In order prevent hackers from taking advantage of decentralised security incident management structure, an integrated communication mechanism between the security incident response teams within the University or even among multiple universities (that share some common IT infrastructures) is highly recommended. Some major functions of this integrated mechanism include:

  - Consider impact on other divisions or other Universities during the impact assessment phase;

  - Broadcast security incidents with impact on other divisions or other Universities through multiple channels / tools, such as e-mail, SMS, etc; and

  - Coordinate the incident handling processes among different divisions or Universities.

Reference:
http://technet.microsoft.com/en-us/library/cc700825.aspx
JUCC - Information Security Incident Management Standard
JUCC - Information Security Incident Handling and Reporting Mechanisms
JUCC Newsletter - Security Incident Management

IV. Hardening Steps for Security Incident Management (cont'd)

- **User Awareness and Staff Qualification**

  The identification and reporting of the security incidents is closely related to the user awareness of the information security concepts and understanding security incidents in terms of characteristics and consequences.

  An appropriate level of training on information security awareness should be organised by the University for its users. For members with access to sensitive information, specific trainings on security incident management should be delivered to them.

  More advanced trainings should be arranged for incident response team members so that they are equipped with right level of skills and knowledge to conduct their assigned tasks during the incidence handling process.

- **Management Support for Incident Handling**

  Some security incidents impose significant impacts on the University, such as substantial financial loss, litigations, propagation beyond University's networks, or long term service delivery disruption. These severe consequences may go beyond the control of the security incident response team.

  In this case, the attention and support from the senior management, such as the division head, president or University committee, should be sought by the security incident response team. The University should utilise the results of impact assessment to establish the criteria for escalating security incidents to the corresponding level of management.

- **Third Party Involvement**

  A large portion of the infrastructure devices or the information systems is developed and produced by the vendors. When security incidents occur in these devices or systems, certain level of third party involvement should be required to analyse the root cause of the incident and also to provide solution for the incidents, like firmware update and software patches.

  Additionally, when a security incident causes litigations, the University's legal department, external legal professionals or computer foresensic investigators should be involved to determine the right action plan and incident resolutions.

  Specific security incident response team members should be assigned to coordinate with the third parties when their involvement is required.

Reference:
http://technet.microsoft.com/en-us/library/cc700825.aspx
JUCC - Information Security Incident Management Standard
JUCC - Information Security Incident Handling and Reporting Mechanisms
JUCC Newsletter - Security Incident Management

V. Summary

As one of the most important preventive controls in a University's information security framework, security incident management is an integrated process to identify, report, escalate and resolve security incidents occured. This process also continuously refines itself based on the results of post incident reviews so that any new forms of security incidents can be timely dealt with.

Committed management, qualified incident response team and good user awareness are key factors to build a successful security incident management process. Depends on the natures of various security incidents, additional resources to engagement third parties (e.g. vendors, external professionals) should also be consdiered.

Nevertheless, cautions should be taken by the University when its security incident management process has vulnerabilities that could open the shortcuts for malicious attacks. Adequate hardening procedures should be followed to eliminate those flaws.