**CE/CZ 4064: Security Management**
School of Computer Engineering, NTU Singapore

# Question Pool 2

***Risk Analysis and Assessments & Contingency Planning and Management***

**Objective:** This set of questions explore the concepts pertaining Risk Analysis and Assessments & Contingency Planning and Management.

**Question 1**

What are the key/distinguishing characteristics and objectives of Emergency Management, Crisis Management, Disaster Recovery Planning and Business Continuity Management? Provide brief examples of relevant past real world incidents requiring initiation of each of these activities.

**Solution:**

Emergency and Crisis are specific categories of contingency that are normally time critical, with significant impact on personal life and/or business survivability.
Emergency is about time criticality, need to respond quickly to reduce damage/losses of people's life, physical or information assets. (E.g., 9/11, SARS)
Crisis is about a highly impactful (normally negative) incident, it may include reputation issues; Brand at risk; Perception problem (e.g., Target data breach, Ashley-Madison data breach, NSA PRISM scandal).

DRP and BCM are focused on preparation to deal with contingency situations.

A disaster may be natural (SARS, Tsunami) or human-made (DDoS attack on Sony Playstation network, cyber-attack on Estonia), and normally Involves loss of physical assets and/or people?s life/health, and/or denial of services/access to critical IT systems.

Business Continuity Management (BCM) is broadly defined as a business process that seeks to ensure organizations are able to withstand any disruption to normal functioning.

**Question 2**

The IT department of an organization is planning to migrate the company's email and document management services to a third party cloud based service provider;s SaaS solution. The head of IT audit expressed concern about the availability and auditability of data and related application services, as the cloud service provider's infrastructure and applications are not covered by the organization's own contingency plan.

(i) What measures may have to be adopted to address this concern?
(ii) What other security risks ought to be considered, and how can they be addressed so that the systems can be migrated without compromising the organization's overall security plan?

**Solution:**

As part of the contractual agreement, ensure that the CSP has adequate redundancy and backup systems that commensurate with existing internal practices. As part of the Service Level Agreement (SLA), ensure that the time to recovery meets the organization?s requirements (at least on par with existing level of availability). In addition, should also advice IT to ensure scalability of the availability solutions (backup and recovery provisions) that may be required as the business grows or shrinks.

On auditability, as part of the contractual agreement, ensure that the CSP systems involved in handling the data and providing the related services shall allow for a third party audit to be conducted annually or periodically appointed by the organization, or allowing the organization to conduct the audit using its own audit team.

**Solution:**

List of common cloud related security risks considerations such as unauthorized access by administrators, systems/network intrusion protect, etc., requiring controls such as administrative access controls, data encryption provision, key management, application compartmentalization, data compartmentalization, law enforcement request/access disclosure, legal/regulatory compliance provisions, network security architecture, security monitoring provision, incident handling and response management, availability of access logs for security analysis.

**Question 3**

For the purpose of network management, network sniffer need to be used by support engineers, who are at times externally hired contractors, to perform network analysis tasks to fine tune or improve the performance of the network.

(i) What are the security risks associated with such network management needs? Give examples.
(ii) What policies and/or operations security controls may be used to address these security risks?

**Solution:**

Network sniffing could result in compromising the confidentiality of sensitive data, such as passwords and business critical data that are not encrypted by the applications. Network traffic analysis may reveal the critical nodes and traffics patterns of the network that knowledge of them are critical for redundancy/contingency planning. From attacker point of views, they would be important targets to cause serious disruption to the organization. [This is not an exhaustive or unique answer, and other examples could also be provided as valid response.]

**Solution:**

Addressing contractors' confidentiality protection of data will be an important policy consideration, for example, requiring contractor to sign a non-disclosure and confidentiality protection agreement, and if necessarily (for critical organizations), requiring a background check to be conducted periodically.
In terms of operations security, such activities may be permitted only with proper authorization, and for only limited period of time. Additional monitoring, such as logging of the

engineer's access, should also be used to allow validation of the tasks performed by the engineer.
In addition, applications should be designed to use secure passwords (that are encrypted), or use of two-factor authentication. Critical business data should also be encrypted at the application layer.

**Question 4**

Give some benefits and some shortcomings of using the metric of Annualized Loss Expectancy (ALE) for risk assessment.

**Solution:**

Benefit: ALE provides a mechanism to quantify the implications of a security risk by facilitating in putting monetary loss expected in one year due to a risk, and thus also allows to compare the cost-benefit of different controls.

Shortcomings: (i) Combines the two risk components - asset value and the probability of loss together simplifies things (which is sometimes good), but this simplification also means distinguishing high-frequency, low-impact events from low frequency, high-impact events based on a single number is no longer possible. (ii) Does not in itself provide any clear means to quantify the value of an asset or an exposure factor.

**Question 5**

What is the scope of penetration testing, and what is the limitation of the scope with respect to vulnerability assessment? What is the advantage of penetration testing with respect to vulnerability assessment?

**Solution:**

Penetration testing is goal oriented, and the purpose is to determine if a specific (target) security attribute can be violated. If any mechanism to violate the security attribute is found, one can stop penetration testing and report the experience with recommendations to prevent the same. The advantage is this goal oriented purpose of a pentest exercise. The disadvantages however are that because of the specific goal in mind, vulnerabilities are not necessarily explored exhaustively, be it with respect to violating other security attributes, or even the specific attribute in question.

**Question 6**

Which tier(s) of Information security continuous monitoring (ISCM) activity should the CISO of a company be directly involved in.

(a) Tier-1

(b) Tier-2

(c) Tier-3

(d) Tier-4

(e) Tier-1 & Tier-2

(f) Tier-2 & Tier-3

(g) Tier-3 & Tier-4

(h) All the tiers

**Solution:**

(e) Tier-1 (Tier 1 risk management activities address high- level information security governance policy as it relates to risk to the organization as a whole, to its core missions, and to its business functions) & Tier-2 (Tier 2 criteria for continuous monitoring of information security are defined by how core mission/business processes are prioritized with respect to the overall goals and objectives of the organization, the types of information needed to successfully execute the stated mission/business processes, and the organization-wide information security program strategy.)
Note also that there is in fact no Tier-4.

**Question 7**

Why is fault tree analysis (FTA) called top down, while event tree analysis (ETA) is called bottom up?

**Solution:**

The root of the FTA tree is an undesirable state of the system (end-result), from which one explores the different pathways through which this end result may happen, and hence, since the analysis starts from the root, it is called top down (note the irony: the trees are up-side down, and the root is at the top!).

ETA in contrast starts with an initiating event, and explores the different states (undesirarable or otherwise) the system may result in. Hence it is bottom-up - since the system state(s) are the top of the tree.

---