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

# Question Pool 1

***Preliminaries & InfoSec Governance and the Law***

**Objective:** This set of questions explore the preliminary concepts pertaining information/cyber security, and also the law and regularatory aspects of the same.

**Question 1**

The National University of Timbuktu (NUT) is implementing an electronic voting (e-voting) system to elect their chancellor. Only the faculty of NUT are allowed to vote online at a voting website that the university IT department is implementing.
What are the security attributes that need to be considered for the e-voting system? Be specific. For instance, do not just say 'confidentiality', but enumerate which (all) kinds of information need to be kept confidential. Note that the security attributes could go beyond the classical three used in CIA-triad.

**Solution:**

This is an open-ended questions with no unique or ideal answer.

Some example security attributes include: Confidentiality/anonymity (of who someone voted, partial results while voting is still on going not being revealed), Integrity (all votes are counted, no one can vote multiple times, no votes are tampered), access control (only members of the faculty cast their vote), Accountability/transparency (the possibility to determine where the count results are correct or not, if all casted votes are registered or not), availability (the registered vote data remains available, the system can be used to cast votes for whatever period it is supposed to be operable), etc. Note that violating some of the security goals can lead to violation of other goals simultaneously, or consequently.

**Question 2**

Provide examples showing why layered defense is not sufficient for defense in depth.

**Solution:**

Defense in depth ensures controls are applied at multiple places, and in layers. In that sense, layered security is subsumed by (is an ingredient of) defense in depth. For instance, intrusion detection systems + firewall provide layered defense against malicious traffic in a network, however, if a legitimate user's login/password has been compromised, for instance, using a phishing attack, then the hacker may still gain access to vital resources in the network.

**Question 3**

Provide an example each for preventive, detective and corrective controls, for each category — people, technology and operations.

**Solution:**

This is just one possible sample solution, many other correct ones are possible:

| | preventive | detective | corrective |
|---|---|---|---|
| people | training | tests/monitoring | (re-)training/replacement |
| technology | firewall | malware/intrusion detection | apply update patches |
| operations | set up procedures | audit/tests/monitoring | disaster recovery |

**Question 4**

Provide some example aspects of the Banking Act of Singapore that have information security implications, and explain what the corresponding information security implications are.

**Solution:**

Financial audit is carried out based on the data in the information system. Hence, it is vital that there is proper log of who all has access to the data, when this data was manipulated (provenance/integrity), etc. Likewise, the data needs to be reliably stored (persistence). These are some examples. (Refer also to the lectures for more elaboration).

**Question 5**

Provide arguments in favour or against the following statement, support with necessary example(s): Achieving the security goals of the Parkerian Hexad, namely, confidentiality, integrity, availability, possession (control), utility and authenticity is adequate when designing an information system.

**Solution:**

False. Many counter-examples can be provided. Non-repudiation is such an example of security goal which is not explicitly covered by the hexad (though one may imagine integrity or authenticity to be closely related for this specific example choice).

**Question 6**

Information Security Officers may welcome regulatory bodies establishing policy, such as certain countries' Privacy Acts that mandate the protection of personal data, and which makes security investments compulsory in related areas. Why may such an approach be ineffective in the long run?

**Solution:**

Internal controls and security practices mandated by regulatory policy will often result in company spending money to improve security and data protection to the point of compliance to the statements of the regulatory policy, protecting them against bad public relations, not security designed to protect customer privacy.

**Question 7**

The principle of 'need to know' in information security advocates that each user should have access to only as much information as needed to carry out the tasks they are assigned, and no more (least privilege access). What are potential shortcomings of such an approach to security?

**Solution:**

Implementing a need to know access paradigm may be wrought with problems of practicality — it is not always obvious what might adequate information to carry out a task, and if and when more information is sought, it may be difficult to assess and grant access in a timely manner not to disrupt functionality. In the best case situation, it may render the system inefficient, while it the worst, it may compromise functionality altogether.

**Question 8**

In the context of information security, what are some advantages for an organization to adhere to the requirements of a specific standard? What are some possible shortcomings of standards in the context of information security?

**Solution:**

Advantages: Actionable guideline on what to do, certification provides a basic level of assurance and acceptability in the global market.
Disadvantages: Similar to question 6, internal controls and security practices mandated by standards will also often result in company spending money to improve security and data protection to the point of compliance to the standards, protecting them against bad public relations, rather than putting best effort for security (and instead meeting a minimum common denominator). Furthermore, standards take a while to develop and ratify, by when the security landscape may have changed significantly, and not adequately captured in the standard, and yet giving a false sense of safety (complacency) to an organization.

**Question 9**

When an organization operates internationally, it may be faced with conflicting legal obligations across the different countries they operate in. Provide some anecdotal examples for such incidents relevant to information security.

**Solution:**

The case (discussed in lectures) of Microsoft Ireland being ordered to handover customer data by US court, which would be in violation of EU laws.

**Question 10**

Which of the following is/are not directly relevant with respect to the defence in depth doctrine for information security.

(a) Three mandatory activities of prevention, detection, and response should be present in a security system.

(b) Defense in depth should encompass people, technology and operations.

(c) The aspects of whether information is being stored, communicated or processed should be discerned when designing security.

(d) Information access should be based on least privilege, and thus compartmentalization and need to know should be implemented.

(e) Security system design should embrace ease of usage as the most important criterion.

**Solution:**

The following are NOT directly relevant:

- The aspects of whether information is being stored, communicated or processed should be discerned when designing security.
- Information access should be based on least privilege, and thus compartmentalization and need to know should be implemented.
- Security system design should embrace ease of usage as the most important criterion.

**Question 11**

Which of the following represents attributes/goals of information security?

(a) Prevention, detection, and response
(b) People controls, process controls, and technology controls
(c) Network security, system security, and application security
(d) Availability, Integrity, Authenticity

**Solution:**

Availability, Integrity, Authenticity

**Question 12**

Which of the following terms best describes the assurance that data has not been changed unintentionally due to an accident or malice?

(a) Utility
(b) Availability
(c) Integrity
(d) Possession/control

**Solution:**

Integrity

**Question 13**

Which of the following best represents the two types of IT security requirements?

(a) Functional and logical
(b) Functional and assurance
(c) Functional and physical
(d) Logical and physical

**Solution:**

Functional (what we want to have?) and assurance (how do we validate that we indeed have what was intended?).

**Question 14**

Security functional requirements describe which of the following?

(a) How to implement the system

(b) What controls a security system must implement

(c) What a security system should do by design

(d) How to test the system

**Solution:**

What a security system should do by design

**Question 15**

Which of the following terms best describes the chances that a threat to an information system will materialize?

(a) Threat

(b) Vulnerability

(c) Weakest link

(d) Risk

**Solution:**

Risk

**Question 16**

Which of the following terms best describes the weakness in a system that may possibly be exploited?

(a) Threat

(b) Vulnerability

(c) Weakest link

(d) Risk

**Solution:**

Vulnerability

**Question 17**

Which of the following best describe the term 'asset' in the context of information security.

(a) Anything that an organization buys

(b) Anything that an organization sells

(c) Anything that has a value to the organization

(d) Anything that is situated within an organization's premises

**Solution:**

Anything that has a value to the organization — this could include physical objects, software or IP (intellectual property) that the organization owns, people and skills/experience, as well as intangibles such as reputation and brand image.

---