Department of Higher Education
University of Computer Studies, Yangon
Fourth Year (B.C.Sc.)
Final Examination
Management Information System + Information Assurance and Security (CS-404)
September, 2018

Answer all Questions **Time allowed: 3 hours**

Management Information System

I. Write short notes **ANY FOUR** of the following. (20 marks)

(a) Major Business Function of Business Organization
(b) Sociotechnical Systems
(c) Value Chain and Value Web
(d) List the major behavioral impacts of organization that applied information system.
(e) Key Technological Trends that heighten ethical concerns
(f) Differentiate between Responsibility and Accountability

II. Answer the following. (30 marks)

(a) What is an Information System? What is the different between data and information? Describe the activities of information system.
(b) Identify and Describe the Features of Organizations that help explain differences in organization's use of information system.

(or)

List and Describe Four Competitive Strategies enabled by information system that firms can purse.

(c) Identify and describes the Five Step Process for analyzing an ethical issue.

Information Assurance and Security

III. Choose a correct answer from the following: (12 marks)

1. Information security professional report spending a lot of time on
   a) Researching new technologies
   b) Political issues
   c) Developing internal security policies, standards and procedures
   d) Fixing software bugs

2. The Internet is relevant for information security because
   a) It exposed computers to attacks from around the world
   b) It caused one of the most significant Internet outages ever
   c) It led to exploits from weakness is wireless networks
   d) It caused falsification of financial records at publicly traded companies

3. The gang of 414 is famous in the information security literature for
   a) Causing one of the most significant Internet outages ever
   b) Intruding into a number of high profile computer installations
   c) Stealing commercial information by exploiting weakness is wireless networks
   d) Falsification of financial records at publicly traded companies

4. Models are useful because
   a) They highlight resource or information that is to be protected
   b) They highlight weaknesses in information systems that can be compromised
   c) They draw attention to the essential details of a problem
   d) They describe safeguards used to minimize the impact of threats

5. The CVE list is
   a) A list of all likely impacts of vulnerabilities
   b) A list of all known viruses
   c) A list of all known information security firms
   d) An inventory of known software vulnerabilities

6. The NVD database
   a) Describes likely impacts and measures to remove vulnerabilities
   b) A list of all known viruses
   c) A list of all known information security firms
   d) An inventory of known software vulnerabilities

7. Personnel assets are
   a) Software tools needed to accomplish the organization’s mission
   b) Digitally stored content owned by an individual or organization
   c) Employees whose departure could adversely affect the organization
   d) Machinery involved in supporting the business

8. Hardware assets are
   a) Software tools needed to accomplish the organization’s mission
   b) Digitally stored content owned by an individual or organization
   c) Employees whose departure could adversely affect the organization
   d) Machinery involved in supporting the business

9. Software assets are
   a) Software tools needed to accomplish the organization's mission
   b) Digitally stored content owned by an individual or organization
   c) Employees whose departure could adversely affect the organization
   d) Machinery involved in supporting the business

10. The goal of agents running a 419 Nigerian scam is to
   a) Damage the reputations of end users
   b) Damage end user computers
   c) Steal money
   d) Steal intellectual property

11. The 419 Nigerian scam is an example of a(n)
   a) Partner
   b) Activist group
   c) Natural cause
   d) Cybercrime

12. Natural causes include all of the following except
   a) Arson
   b) Earthquake
   c) Tornadoes
   d) Hurricanes

IV. Match the relevant information. (10 marks)

1) ILOVEYOU virus	a. use to proof that a user is the owner of the identity being used
2) NVD	b. compelling investments in information security procedures
3) Stuxnet	c. an inventory of known software vulnerabilities
4) APT1	d. idiosyncratic information asset
5) Steganography	e. organization attempting to make web applications more secure
6) Hardware tokens	f. deleted images on infected computers and automatically sent itself as an email attachment
7) Sarbanes-Oxley act	g. describes likely impacts and measures to remove vulnerabilities
8) CVE list	h. world's first "weaponized" computer worm
9) Intellectual Property	i. steals large valuable intellectual property from the companies several years
10) OWASP	j. the art of hidden writing

V. Answer ***<u>any six</u>*** of the following. (12 marks)

(a) What is Confidentiality?
(b) What does CIA stand for?
(c) State two important differences between conventional assets and information assets.
(d) Define vulnerability.
(e) How many asset types in the organization? List them.
(f) Define restricted assets.
(g) What is threat agent?
(h) What are external threat agents?

VI. Read the given information and answer the critical thinking questions. (16 marks)

SINGAPORE HEALTH RECORDS: HACKED

Around 1.5 million people have had their personal details stolen in a cyberattack on the Singapore government's health database, it has emerged. Reuters reported that prime minister Lee Hsien Loong, was among those who had their details stolen. The government has called the attack "the most serious breach of personal data" the country has experienced. Singapore has ironically made cyber security a top priority this year, while it acts as chair of the 10-member Association of Southeast Asian Nations (ASEAN) group. There is no word as to whom has stolen the information, but a government statement cited by Reuters said the attack between May 2015 and July 4 was "not the work of casual hackers or criminal gangs."

The Cyber Security Agency of Singapore and the Integrated Health Information System confirmed it was a "deliberate, targeted and well-planned cyberattack". Attackers repeatedly targeted the prime minister's personal details and information on medicines he was prescribed. A further 1.5 million patients who visited clinics have had their non-medical personal information illegally accessed and copied, according to the government.

Commenting on the events, Olli Jarva, Managing Consultant at Synopsys' Software Integrity Group, said: "We are beginning to see a new and scary fact – healthcare data has grown its value such that hackers are now willing to go the extra mile to obtain it. This has been a growing trend over the past few years, such that healthcare data has outgrown the value of credit card or social security numbers." Jarva said that security must be integrated into programming of health databases from the outset, with bugs and flaws identified early to prevent them being exploited. "If we leave these problems for later, the cost of fixing and reacting to breaches would be extremely costly and the effects may be devastating," Jarva added.

i. Design this case with thread model: agent, action, assets.
ii. Classify attackers according to categories of threat agents: whether external agent or internal agent.
iii. In this case, what kind of asset did the Singapore government possess?
iv. What issues led to the security breach at Singapore government health database?
v. What is the possible business impact of this security breach for both Singapore government and its people who included in health databases?