JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

BSc Computer Security & Forensics
First Semester Second Semester Examination 2013/2014

IIT 3126 - Computer, Law, Ethics and Society

ANSWER ANY THREE QUESTIONS

TIME: 3 HOURS

Q1

a) What should an information security practitioner do that can minimize the organization's legal liabilities? (**2 Marks**)

b) What are the major differences between law and ethics in IT? (**2 Marks**)

c) What is the US Federal Privacy Act? Is there an equivalent Act in Kenya. (**4 Marks**)

d) Briefly explain how information security professional can deter unethical and illegal behavior of an employee? (**2 Marks**)

e) What is the most important responsibility of an information security professional? (**2 Marks**)

f) What important information does the National Security Agency's (NSA's) Information Assurance Directorate provide? Is there an equivalent office in Kenya, if so, provide its mandate. (**4 Marks**)

g) What is the organization's responsibility regarding information security? Briefly how your organization tackles information security issues. (**4 Marks**)

Q2. Integrity & Policy

a) Briefly explain why ensuring of the integrity of business information is the PRIMARY concern of the Procedural Security (2 **Marks**)

b) Briefly describe the function of a corporate information security policy? (**2 Marks**)

A. Issue corporate standard to be used when addressing specific security problems.
B. Issue guidelines in selecting equipment, configuration, design, and secure operations.
C. Define the specific assets to be protected and identify the specific tasks which must be completed to secure them.
D. Define the main security objectives which must be achieved and the security framework to meet business objectives.

c) When developing information security policy, why is it important that senior management must endorse a security policy? (**3 Marks**)

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.
D. So that they can be held legally accountable.

d) **Acceptable use policy** is the documents in which assignment of individual roles and responsibilities is defined, why is this document critical an organization? (**2 Marks**)

e) When developing an information security policy, what is the FIRST step that should be taken? (**2 Marks**)

A. Obtain copies of mandatory regulations.
B. Gain management approval.
C. Seek acceptance from other departments.
D. Ensure policy is compliant with current working practices.

f) Which one of the following is NOT a fundamental component of a Regulatory Security Policy? (**1 Marks**)

A. What is to be done.
B. When it is to be done.
C. Who is to do it.
D. Why is it to be done

Briefly explain why? (**2 Marks**)

g) Why is important that in an organization, an Information Technology security function should be lead by a Chief Security Officer and report directly to the CEO. (**2 Marks**)

h) Briefly explain why security is a process that is continuous?

A. Continuous
B. Indicative
C. Examined
D. Abnormal

i) State the three fundamental principles of security? (**1 Marks**)

A. Accountability, confidentiality, and integrity
B. Confidentiality, integrity, and availability (CIA)
C. Integrity, availability, and accountability
D. Availability, accountability, and confidentiality

Q3 Network Security

a) Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained? (**1 Marks**)

A. Communications security management and techniques
B. Networks security management and techniques
C. Clients security management and techniques
D. Servers security management and techniques

b) Which one of the fundamental principles of security ensures that the data is accessible when and where it is needed? (**1 Marks**)

A. Confidentiality
B. Integrity
C. Acceptability
D. Availability

c) Which of the following describe elements that create reliability and stability in networks and systems and which assure that connectivity is accessible when needed? (**1 Marks**)

A. Availability
B. Acceptability
C. Confidentiality
D. Integrity

d) Most computer attacks result in violation of which of the following security properties? (**4 Marks**)

A. Availability
B. Confidentiality
C. Integrity and control
D. All of the choices.

Explain why?

e) The Structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, and authentication, and confidentiality for transmissions over private and public communications networks and media includes: (**2 Marks**

A. The Telecommunications and Network Security domain
B. The Telecommunications and Netware Security domain
C. The Technical communications and Network Security domain
D. The Telnet and Security domain

Explain why?

f) Information security is the protection of data. Information will be protected mainly based on three important factors, briefly explain why? (**4 Marks**

A. Its sensitivity to the company.
B. Its confidentiality.
C. Its value.
D. All of the choices.

h) Defined what is the Maximum Tolerable Downtime (MTD) in IT: (**1 Marks**

A. Maximum elapsed time required to complete recovery of application data
B. Minimum elapsed time required to complete recovery of application data

C. Maximum elapsed time required to move back to primary site a major disruption
D. It is maximum delay businesses that can tolerate and still remain viable

i) What principle requires that a user be given no more privilege then necessary to perform a job? (**2 Marks**

A. Principle of aggregate privilege.
B. Principle of most privilege.
C. Principle of effective privilege.
D. Principle of least privilege.

j) To ensure least privilege requires that _____ is identified, explain why? (**2 Marks**

A. what the users privilege owns
B. what the users job is
C. what the users cost is
D. what the users group is

Q4 Ethics and Integrity

a) Which of the following measures would be the BEST deterrent to the theft of corporate information from a laptop which was left in a hotel room?

A. Store all data on disks and lock them in an in-room safe
B. Remove the batteries and power supply from the laptop and store them separately from the computer
C. Install a cable lock on the laptop when it is unattended
D. Encrypt the data on the hard drive

b) Which one of the following are examples of security and controls that would be found in a "trusted" application system?

A. Data validation and reliability
B. Correction routines and reliability
C. File integrity routines and audit trail
D. Reconciliation routines and data labels

c) What is disaster recovery? How can it be implemented at your school or work?

d) What business decisions will you have to make as a manager that has both an ethical and IT dimension?

e) What potential security problems do you see in the increasing use of intranets and extranets in business? What might be done to solve such problems?

f) What are your major concerns about computer crime and privacy on the Internet? What can you do about it?

g) You are a computer system manager. An employee is out sick and another employee requests that you copy all files from the sick person's computer to theirs so that they can do some work. What do you do?

h) You work for one of the large credit card companies. Someone asks you to get a copy of a person's file. He will pay you US$1000.

   i) What do you do?
   ii) Who are the stakeholders?
   iii) What alternative actions are open to you?
   iv) Which are ethically prohibited or obligatory?
   v) You know another employee sells files with people's personal information. What do you do?

   vi) You are the manager of a university computer system that provides computer accounts and email facilities to students. You discover that a handful of students have been spamming the entire class and sending junk email to all of the email aliases. You are unable to find out exactly who these students are as they are using a facility outside the university and posting anonymously. What do you do?

Q5 Ethical

a) What is privacy?

b) Why is Personal Information valued?

c) Your grandmother is quite forgetful and, as her legal guardian, you have the authority to access her bank account to pay her bills. She has quite a bit of money in her savings account. Would it be OK to deduct a small "service fee" from her account for your services? Why or why not? Discuss the ethics of this situation.

d) Using the scenario described in the previous question, you have a temporary need for $500 to pay your credit card bill. You should be able to repay the loan when you get paid next month. Would it be OK to borrow the money from your grandmother's account? Why or why not? Discuss the ethics of this situation. Since your grandmother is so forgetful, you feel that there's no point in asking her permission – you expect that she would probably say yes, anyway.

e) Suppose you have discovered the username and pin for your neighbor's bank account. Would it be OK to check the account balance? Should you tell your neighbor that he or she should change his pin? Discuss the ethics of this situation.

f) Is it an ethical countermeasure of content providers to inject poisoned files to protect their contents against illegal file sharing of P2P network users?

g) Describe a possible alternative to using copyright, such as subscription or compulsory licensing services. How do the ethics change for the stakeholders involved?

h) Is there an ethical difference between stealing a physical DVD from a brick and mortar store and downloading a digital copy of a DVD from a file sharing network?