**Social Security Practice ITSC311**

**Introduction to Information Security, The Need for Security and Legal Ethical in Info Security**

**Question 1**

Using technical language in information security define the following terms:

* 1. **Exploit** to compromise an information system thus taking advantage of a vulnerability or exposure in software (2 marks)
  2. **Risk** the probability of an unwanted occurrence such as adverse event or loss (2 marks)
  3. **Vulnerability** a potential weakness in an asset or its defensive control system (2 marks)
  4. **Threat** any event or circumstance that has the potential to adversely affect an asset (2 marks)
  5. **Ethics** codes or principals of an individual or group that that regulates and define acceptable behaviour (2 marks)

**Question 2**

Securing information assets is an incremental process that requires coordination, time and patience. Briefly describe the two main approaches to information security implementation in any organization. (8 marks)

**Top-Down Approach**, in which the project is initiated by upper-level managers who issue policy, procedures and processes, dictate the goals and expected outcomes, and determine accountability for each required action, has a higher probability of success. This approach has strong upper-management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture.The most successful kind of top-down approach also involves a formal development strategy referred to as a systems development life cycle. For any organization-wide effort to succeed, however, management must buy into and fully support it. The role played in this effort by the champion cannot be overstated.

**Bottom-up approach** is the technical expertise of the individual administrators. Working with information systems on a day-to-day basis, these administrators possess in-depth knowledge that can greatly enhance the development of an information security system. They know and understand the threats to their systems and the mechanisms needed to protect them successfully. Unfortunately, this approach seldom works, as it lacks a number of critical features, such as participant support and organizational staying power.

**Question 3**

Briefly explain any five critical characteristics of information security (10 marks) **Availability** enables authorized users—people or computer systems—to access information without interference or obstruction and to receive it in the required format. Consider, for example, research libraries that require identification before entrance. Librarians protect the contents of the library so that they are available only to authorized patrons. The librarian must accept a patron’s identification before the patron has free access to the book stacks. Once authorized patrons have access to the stacks, they expect to find the information they need in a usable format and familiar language. In this case, the information is bound in a book that is written in English.

**Accuracy** Information has accuracy when it is free from mistakes or errors and has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider a checking account, for example. You assume that the information in your account is an accurate representation of your finances. Incorrect information in the account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much money from your account, the value of the information is changed. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make other mistakes, such as bouncing a check.

**Authenticity** Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, you assume that a specific individual or group created and transmitted the e-mail—you assume you know its origin. This is not always the case. E-mail spoofing, the act of sending an e-mail message with a modified field, is a problem for many people today because the modified field often is the address of the originator. Spoofing the sender’s address can fool e-mail recipients into thinking that the messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have.

**Confidentiality** Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that only users with the rights, privileges, and need to access information are able to do so. When unauthorized individuals or systems view information, its confidentiality is breached. To protect the confidentiality of information, you can use several measures,

The value of confidentiality is especially high for personal information about employees, customers, or patients. People who transact with an organization expect that their personal information will remain confidential, whether the organization is a federal agency, such as the Internal Revenue Service, a healthcare facility, or a business

**Integrity** Information has integrity when it is whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. For this reason, a key method for detecting a virus or worm is to look for changes in file integrity, as shown by the file size. Another key method of assuring information integrity is file hashing, in which a file is read by a special algorithm that uses the bit values in the file to compute a single large number called a hash value. The hash value for any combination of bits is unique.

**Utility** The utility of information is the quality or state of having value for some purpose or end. In other words, information has value when it can serve a purpose. If information is available but is not in a meaningful format to the end user, it is not useful. For example, U.S. Census data can quickly become overwhelming and difficult for a private citizen to interpret; however, for a politician, the same data reveals information about residents in a district, such as their race, gender, and age. This information can help form a politician’s next campaign strategy. Possession The possession of information is the quality or state of ownership or control. Information is said to be in one’s possession if one obtains it, independent of format

or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always lead to a breach of confidentiality. For example, assume a company stores its critical customer data using an encrypted file system. An employee who has quit decides to take a copy of the tape backups and sell the customer records to the competition. The removal of the tapes from their secure environment is a breach of possession. But, because the data is encrypted, neither the former employee nor anyone else can read it without the proper decryption methods; therefore, there is no breach

of confidentiality.

**Question 4**

Briefly explain the **five** types of law as identified by Whitman and Mattord (2015). (10 marks)

Constitutional Law: Originates with the U.S. Constitution, a state constitution, or local constitution, bylaws, or charter.

• Statutory Law: Originates from a legislative branch specifically tasked with the creation and publication of laws and statutes.

Statutory law, one can further divide laws into their association with individuals, groups, and the “state”:

• Civil law embodies a wide variety of laws pertaining to relationships between and among individuals and organizations. Civil law includes contract law, employment law, family law, and tort law. Tort law is the subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial injury. Perceived damages within civil law are pursued in civil court and are not prosecuted by the state.

• Criminal law addresses violations harmful to society and is actively enforced and prosecuted

by the state. Criminal law addresses statutes associated with traffic law, public order, property damage, and personal damage, where the state takes on the responsibility of seeking retribution on behalf of the plaintiff, or injured party.

• Regulatory or Administrative Law: Originates from an executive branch or authorized regulatory agency, and includes executive orders and regulations.

• Common Law, Case Law, and Precedent: Originates from a judicial branch or oversight board and involves the interpretation of law based on the actions of a previous and/or higher court or board.

**Question 4**

Briefly explain the components of any Information System that enables it to deliver an information resources within an organization? (12 marks)

**Software**

The software component of an IS includes applications (programs), operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure. The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. The information technology (IT) industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software. In fact, many facets of daily life are affected by buggy software, from smartphones that crash to flawed automotive control computers that lead to recalls.

Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, costs, and manpower. Information security is all too often implemented as an afterthought rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

**Hardware**

Hardware is the physical technology that houses and executes the software, stores and transports the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted hardware access is possible. Before September 11, 2001, laptop thefts in airports were common. A two-person team worked to steal a computer as its owner passed it through the conveyor scanning devices. The first perpetrator entered the security area ahead of an unsuspecting target and quickly went through. Then, the second perpetrator waited behind until the target placed the computer on the baggage scanner. As the computer was whisked through, the second perpetrator slipped ahead of the victim and entered the metal detector with a substantial collection of keys, coins, and the like, slowing the detection process and allowing the first perpetrator to grab the computer and disappear in a crowded walkway.

**Data**

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset of an organization and therefore is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When used properly, they should improve the security of the data and the applications that rely on the data. Unfortunately, many system development projects do not make full use of the database management system’s security capabilities, and in some cases the database is implemented in ways that make them less secure than traditional file systems. Because data and information exist in physical form in many organizations as paper reports, handwritten notes, and computer printouts, the protection of physical information is as important as the protection of electronic, computer-based information.

1

**People**

Though often overlooked in computer security considerations, people have always been a threat to information security. Legend has it that around 200 B.C., a great army threatened the security and stability of the Chinese empire. So ferocious were the Hun invaders that the Chinese emperor commanded the construction of a great wall that would defend against them. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for more than a thousand years. Initially, the Khan’s army tried to climb over, dig under, and break through the wall. In the end, the Khan simply bribed the gatekeeper—and the rest is history. Whether this event actually occurred or not, the moral of the story is that people can be the weakest link in an organization’s information security program. Unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate people to obtain access information about a system.

**Procedures**

Procedures are another frequently overlooked component of an IS. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization’s procedures, it poses a threat to the integrity of the information. For example, a consultant to a bank learned how to wire funds by using the computer center’s procedures, which were readily available. By taking advantage of a security weakness (lack of authentication), the bank consultant ordered millions of dollars to be transferred by wire

to his own account. Lax security procedures caused the loss of more than $10 million before the situation was corrected. Most organizations distribute procedures to employees so they can access the information system, but many of these companies often fail to provide proper education for using the procedures safely. Educating employees about safeguarding procedures is as important as physically securing the information system. After all, procedures are information in their own right. Therefore, knowledge of procedures,

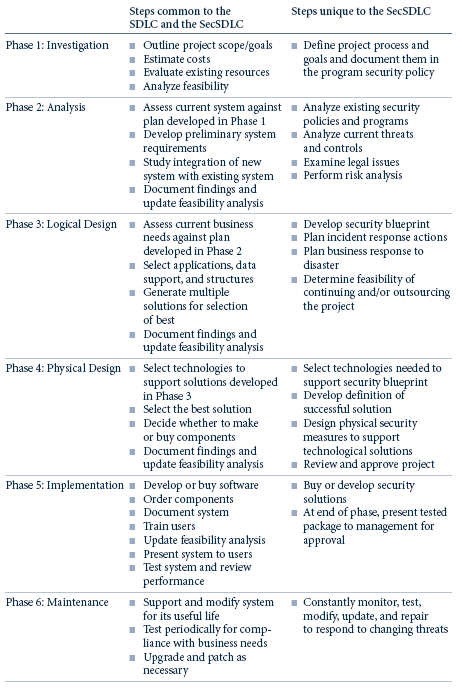
as with all critical information, should be disseminated among members of an organization on a need-to-know basis.

**Networks**

Networking is the IS component that created much of the need for increased computer and information security. When information systems are connected to each other to form LANs, and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge. The physical technology that enables network functions is becoming more accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to the system’s hardware components is still important. However, when computer systems are networked, this approach is no longer enough. Steps to provide network security such as installing and configuring firewalls

**Question 5**

With the increase in security breaches most organization have to incorporate security in to the Systems Development Life Cycle when developing new systems. Identify and explain the six phases which are part of the SecSDLC. (12 marks)



V6