BACHELOR OF INFORMATION TECHNOLOGY

SEMESTER 1, 2020

FINAL EXAMINATION (ON-LINE)

Subject Code : BIT 303

Subject Name : IT MANAGEMENT, ETHICS AND SECURITY

This examination carries 50% of the total assessment for this subject.

Examiner(s)	Moderator(s)
MS ANITHA VELAYUTHAM	Internal : DR TAN CHOON LING
Day : MONDAY Date : 4 MAY 2020	Time : 2.00PM – 6.00PM

Time allowed : 4 HOURS -WRITTEN PAPER

INSTRUCTION(S):

1. This examination is worth fifty percent (50%) of the total marks for the subject. The total marks to be awarded is 100 marks.

2. Answer the questions based on marks allocation.

3. Questions are to be answered in **Microsoft Word Document with Font Size 12 & Font Style Times New Roman.**

4. One completed name your Word document with your StudentID followed by subject code (e.g.B1223432BIT303.doc)

5. Submit your final written word document to **TURN-IT IN by end of exam (6.00pm).**

6. Please make sure that you carefully number the questions that you choose to answer, exactly the same as they appear in this examination paper.

ANSWER ALL THE QUESTIONS.

Question 1 **(10 marks)**

The National University of Texas (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's IT department is implementing. Identify and explain what are the security attributes that need to be considered for the e-voting system.

Question 2 **(15 marks)**

Consider a program that allows a surgeon in one city to assist with an operation in another city, either by manipulating the actual instruments remotely, or just by observing the operation and offering suggestions to the onsite surgical team.

Attempt the following questions.

a) Who might want to attack such a program and why? (5 marks)
b) What nature of attack might be attempted? (5 marks)
c) Explain how such attacks could be prevented. (5 marks)

Discuss your answer in detail with justification by providing examples.

Question 3 **(10 MARKS)**

Customer information is a valuable asset. People trust banks to keep their personal financial information confidential. Banks are required by law to have policies and procedures that protect against accidental, or intentional, misuse of the information.

The board of directors at Barnett's Independent Bank & Trust, Blue Water, Texas (BIBT) is committed to preserving and protecting customers' information. To that end the directorate developed this Information Security Policy.

The Security Objectives of BIBT are:

The Information Security Program at BIBT is designed to ensure that the following security objectives are met:

1. Customer information will be kept secure and confidential. The bank will implement a series of controls that help safeguard information from unauthorized viewing by non-bank personnel. Also, information about our customers will not be sold, exchanged, are given away without their prior written consent.

2. Known and anticipated threats to BIBT's Security Program will be documented, along with the measures taken to minimize the likelihood of the threats occurring.

3. Management will be proactive in searching for new threats to the bank's Security Program. Specifically, it will attend seminars and training classes on how to protect customer information. The bank will also have an annual review of its information technology operations by a qualified third party.

Based on the security objectives listed above, identify and explain what are the potential **threats** and **damages** to BIBT and customers. Explanation should be given for each threats and damages it can cause. You need to identify ONE threat and the potential damage for each of the security objectives listed above.

Question 4 **(15 marks)**

A growing number of people believe that the use of biometrics is an invasion of privacy. For example, an eye scanning device records the inner structure of a person's eye and stores that image in a database. Critics worry that databases of human traits used to maintain corporate security may actually pose a privacy threat to individuals, if such data were used in other ways.

Identify and explain ***THREE*** privacy threats and the countermeasures that need to be implemented for each that you have identified.

Question 5 **(28 marks)**

CASE STUDY – THERAC 25

The Therac-25 machine was a state-of-the-art linear accelerator developed by the company Atomic Energy Canada Limited (AECL) and a French company CGR to provide radiation treatment to cancer patients. The Therac-25 was the most computerized and sophisticated radiation therapy machine of its time. With the aid of an onboard computer, the device could select multiple treatment table positions and select the type/strength of the energy selected by the operating technician. AECL sold eleven Therac-25 machines that were used in the United States and Canada beginning in 1982.

Unfortunately, six accidents involving significant overdoses of radiation to patients resulting in death occurred between 1985 and 1987 (Leveson & Turner 1993). Patients reported being "burned by the machine" which some technicians reported, but the company thought was impossible. The machine was recalled in 1987 for an extensive redesign of safety features, software, and mechanical interlocks. Reports to the manufacturer resulted in inadequate repairs to the system and assurances that the machines were safe. Lawsuits were filed, and no investigations took place. The Food and Drug Administration (FDA) later found that there was an inadequate reporting structure in the company, to follow up with reported accidents.

There were two earlier versions of the Therac-25 unit: the Therac-6 and the Therac-20, which were built from the CGR company's other radiation units–Neptune and Sagittaire. The Therac-6 and Therac-20 units were built with a microcomputer that made the patient data entry more accessible, but the units were operational without an onboard computer. These units had built-in safety interlocks and positioning guides, and mechanical features that prevented radiation exposure if there was a positioning problem with the patient or with the components of the machine. There was some "base duplication" of the software used from the Therac-20 that carried over to the Therac-25. The Therac-6 and Therac-20 were clinically tested machines with an excellent safety record. They relied primarily on hardware for safety controls, whereas the Therac-25 relied primarily on software.

On February 6, 1987, the FDA placed a shutdown on all machines until permanent repairs could be made. Although the AECL was quick to state that a "fix" was in place, and the machines were now safer, that was not the case. After this incident, Leveson and Turner (1993) compiled public information from AECL, the FDA, and various regulatory agencies and concluded that there was inadequate record keeping when the software was designed. The software was inadequately tested, and "patches" were used from earlier versions of the machine. The premature assumption that the problem(s) was detected and corrected was unproven. Furthermore, AECL had great difficulty reproducing the conditions under which the issues were experienced in the clinics. The FDA restructured its reporting requirements for radiation equipment after these incidents.

As computers become more and more ubiquitous and control increasingly significant and complex systems, people are exposed to increasing harms and risks. The issue of accountability arises when a community expects its agents to stand up for the quality of their work. Nissenbaum (1994) argues that responsibility in our computerized society is systematically undermined, and this is a disservice to the community. This concern has grown with the number of critical life services controlled by computer systems in the governmental, airline, and medical arenas.

According to Nissenbaum, there are four barriers to accountability: the problem of many hands, "bugs" in the system, the computer as a scapegoat, and ownership without liability. The problem of too many hands relates to the fact that many groups of people (programmers, engineers, etc.) at various levels of a company are typically involved in creation of a computer program and have input into the final product. When something goes wrong, there is no one individual who can be clearly held responsible. It is easy for each person involved to rationalize that he or she is not responsible for the final outcome, because of the small role played. This occurred with the Therac-25 that had two prominent software errors, a failed microswitch, and a reduced number of safety features compared to earlier versions of the device. The problem of bugs in the software system causing errors in machines under certain conditions has been used as a cover for careless programming, lack of testing, and lack of safety features built into the system in the Therac-25 accident. The fact that computers "always have problems with their programming" cannot be used as an excuse for overconfidence in a product, unclear/ambiguous error messages, or improper testing of individual components of the system. Another potential obstacle is ownership of proprietary software and an unwillingness to share "trade secrets" with investigators whose job it is to protect the public (Nissenbaum 1994).

The Therac-25 incident involved what has been called one of the worst computer bugs in history (Lynch 2017), though it was largely a matter of overall design issues rather than a specific coding error. Therac-25 is a glaring example of what can go wrong in a society that is heavily dependent on technology.

(Written by Chris Apgar and Robert Prentice, The University of Texas at Austin)

a) Who should be responsible or accountable for the software failure in Therac-25? Analyze the case study above to solve the ethical dilemma using the four-step process and make a defensible ethical decision.

(16 marks)

b) Construct an argument using important claims and identify the reasons and objections for that claim. Discuss your argument with the aid of a decision diagram.

(12 marks)

Question 6 **(12 marks)**

Based on the Therac-25 case study above, Atomic Energy Canada Limited (AECL) have breached the IEEE-CS/ACM Software Engineering Ethics and Professional Practices.

Discuss the professional issues raised by Therac-25 and identify any ***THREE(3)*** Codes that applies to a member's professional work that has been violated by Atomic Energy Canada Limited (AECL). Explain your answer with justification.

Question 7 **(10 marks)**

A multimedia production combines elements of text, images, sounds, video, and animations. The Internet provides ready access to the raw materials of a multimedia production. The digitization of media makes it easy to combine multiple forms of media into derivative but original forms of expression. If you want to build on the work of others or incorporate the work of others in your own productions, you should understand the intellectual property laws that govern creative work.

a) What are the legal and ethical issues associated with the use of online intellectual property for which you are not the original author?

(5 marks)

b) How do you protect your own work and what protections are available to you?
(Note: Need to be specific with the Legal Acts)

(5 marks)