The University of Queensland
School of Information Technology and Electrical Engineering

Semester 2, 2017

COMS3000/7003 – Tutorial 1, Answers

Q1) What are the 3 aspects of Information Security that make up the "CIA Triad"? Give an example of how Information Security can be compromised in regards to each of these aspects. Sometimes "Authenticity" and "Non-repudiation" are listed separately to the primary aspects of the CIA Triad – give specific examples of how Information Security can be compromised in regards to Authenticity and Non-repudiation.

Confidentiality (Privacy, Secrecy)
- Confidential medical information exposed

Integrity
- Student changing his/her grades in UQ data

Availability
- Denial of Service (DoS) attack renders servers unreachable

Authenticity
- Email with false sender address (no integrity of the binding between sender and the address given)

Non-repudiation
- Someone making an online credit card purchase and later denying it (integrity of the binding between the source and the integrity of the transaction itself)

The CIA Triad consists of Confidentiality, Integrity and Availability. These are characteristics of the information itself – the others are characteristics of information processes and rely on one or more components of the CIA Triad (these last two are supported by the integrity of bindings provided by digital signatures).

Q2) Describe the difference between a threat, a vulnerability and a risk?

A **threat** is any circumstance or event with the potential to cause harm to an information system. A **vulnerability** is a weakness of the system (computer, network etc.) through which a **threat** can be realised. A Threat exists outside of the information system considered. It is something (event, circumstances, people etc.) that can potentially cause harm to an information system. Threats can be realised by exploiting existing vulnerabilities. Whereas, a **risk** is the likelihood that a particular **threat**, will exploit a particular **vulnerability** of a system resulting in a particular **impact**.

Q3) Threats can be classified in three categories:

- *Environmental threats* include natural disasters and other environmental conditions.
- *Deliberate threats* are those threats involving the intentional damage to data, software or hardware.
- *Accidental threats* relate to errors and omissions.

Give at least three examples of Threats for each category.

Environmental Threats:

- Fire
- Earthquake
- Flood
- Storm
- Extreme Temperatures and Humidity
- Vermin

Accidental Threats:

- User Errors
- Building Fire
- Technical failures
- Transmission errors

Deliberate Threats

- Sabotage
- Malicious Code (Virus, Worm etc.)
- Denial of Service Attack
- Eavesdropping
- Social Engineering
- Theft

Q4) Give at least 5 examples for vulnerabilities in the context of information security.

- Lack of user training
- Lack of Antivirus Software
- Lack of a Backup procedure
- Location where data is stored is in an area susceptible to natural disasters
- Lack of fire detector, sprinkler system
- Lack of physical access control (e.g. Door locks)
- Lack of firewalls
- Incorrectly configured software or hardware

Q5) (Quantitative Risk Analysis)
A widget manufacturer has installed new network servers, changing its network from a peer-to-peer network to a client/server-based network. The network consists of 100 users who make an average of $40 an hour for the company, working on 100 workstations. Previously, none of the workstations involved in the network had anti-virus software installed on the machines. This was because the workstations didn't have floppy disk drives or Internet connectivity, so the risk of viruses was deemed minimal.
One of the new servers provides a broadband connection to the Internet, which employees can now use to send and receive email. One of the managers read in a trade magazine that other widget companies have reported an 80 percent chance of viruses infecting their network within year after connecting it to the Internet. The magazine also mentioned that it may take upwards of three hours to restore data that's been damaged or destroyed.
A vendor will sell licensed copies of anti-virus software for all servers and the 100 workstations at a cost of $4,700 per year. The company has asked you to determine the annual loss that can be expected from viruses, and determine if it is beneficial in terms of cost to purchase licensed copies of anti-virus software.

a) What is the Annualised Rate of Occurrence (ARO) for this risk?
b) Calculate the Single Loss Expectancy (SLE) for this risk.
c) Calculate the Annualised Loss Expectancy.
d) Determine whether it is beneficial in terms of monetary value to purchase the anti-virus software by calculating how much money would be saved or lost by purchasing the software.

a.) The Annualised Rate of Occurrence (ARO) is the likelihood of a risk occurring within a year. The scenario states that trade magazines calculate an 80% risk of virus infection after connecting to the Internet, so the ARO is 80% or .8.

(To be mathematically precise, we would have to specify the probabilities for the virus infection happening once, twice, etc. within a year. The frequency would then be the weighted average of these values. Since quantitative risk analysis works on rough approximations, this is usually ignored and the probability of an event occurring is used as its frequency of occurrence.)

b.) The Single Loss Expectancy (SLE) is the dollar value of the loss that equals the total cost of the risk. In the case of this scenario, there are 100 users who make an average of $40 per hour. Multiplying the number of employees who are unable to work due to the system being down by their hourly generated revenue, this means that the company is losing $4,000 an hour (100 x $40 = $4000). Because it may take up to three hours to repair damage from a virus, this amount must be multiplied by three because employees will be unable to perform duties for approximately three hours. This makes the SLE $12,000 ($4,000 x 3 = $12,000).

c.) ALE = ARO*SLE = 0.8 * $12,000 = $9,600.

d.) Because the ALE is $9,600, and the cost of the software that will minimize this risk is $4,700 per year, this means that the company would save $4,900 per year by purchasing the software ($9,600 - $4,700 = $4900).