Wa#2

Linguistics, English

1. Access security refers to ensuring the security of data by limiting access to those who only have the permissions to access them. Access security allows people to access data that they need to do their jobs, and nothing more than that. It also includes access to security reporting systems. Semantic security pertains to preventing the release of unprotected information that happens when the organization releases several documents that do not have individual protections. A breach of semantic security happens when people infer information that they do not have permission to know through data triangulation. An example is an employee who gets access to several reports on salaries and decides to compute the individual salaries of some employees. She is allowed to access each report individually, but she does not have permission to know individual salaries. In other words, not properly understanding the implications of access to several data all at once can lead to semantic security breaches.

2. Reporting systems increase the risks of semantic security breaches because they give access to several reports simultaneously for reporting needs. Reporting systems do not realize that giving a bulk of information to one employee can result to the latter using them to deduce certain information that they are not allowed to know or access. These systems are important to getting work done, but they can offer access to too much information that can result to semantic security breaches. These systems unintentionally offer information that one person should not have, provided that the person does some deduction that can result to logical assumptions.

3. An organization can protect itself from accidental losses due to semantic security problems by ensuring that no one person can get access to several

data systems or data that can result to semantic security breaches. At the same time, it can hire one people to do one part of the job and not all of the activities of the job, so each person can have limited permissions to access data. Furthermore, it can create clear policies about permissions and data restrictions and penalties for transgressions. These transgressions can prevent employees from conducting data triangulation. Moreover, it can also ensure that the organization has records of the data access it gives to different employees, so that if semantic security breaches happen, they can determine who accessed what. At the same time, the organization can purchase insurance on its semantic security, so that it can have access to financial resources, if breaches occur.

4. An organization has a legal responsibility to protect the company from potential losses due to semantic security problems because the latter can seriously negatively affect shareholders, employees, and consumers. Having access to different kinds of information can pose financial and/or security risks to these stakeholders, such as identity theft and physical theft from knowing how much they are making and where they live. As a result, the organization must ensure that it is not being irresponsible in collecting and protecting data. Otherwise, if problems happen to these stakeholders, they can charge the organization for not protecting the privacy and confidentiality of their data. The organization will then face lawsuits that could have been prevented if it invested time, money, and effort on its semantic security.

5. I think that some semantic security problems are inevitable because not every IT or manager can determine risks and respond to them swiftly and effectively. I see an opportunity for new products for insurance companies if

they can give some form of insurance, in case semantic security problems result to losses to the company. In addition, it can offer security measures, such as building relationships to prevent potential semantic security issues. This means that the insurance company knows how to develop and maintain an emotional connection with users that it can prevent them from thinking about using their data access to know more than they should know and use that for illegal or unethical self-gain actions.