# Wk12 revision questions essay example

ASSIGN BUSTER

## Wk12 revision questions

The following paper is aimed at providing a comprehensive look into the ethics and security concerns in the IT industry and how these principles are also applicable in the cross section of general industries.

## Section 1

Module 1 – Ethics

Question 1 – What is privacy? Provide some reasons why it is important.

Answer:

Privacy is the basic right of every individual whether it is in the physical form or in the cyberspace. Privacy is the ability to keep personal information intact, without disclosing it to others. It is the desire to stay anonymous, whenever required. The cyber world is plagued hijackers and attackers, in such a case with-holding personal information is the right of every individual. Many decision taking tasks can also be termed private wherein the power of the decision lies with the person affected by the condition.

## Some of the important reasons for privacy include;

In absence of privacy, building relationships would be difficult

Privacy helps to stay secure. Security is the basic need of every individual

Privacy helps to protect people from those in power positions

Question 2 – What makes an IT expert a professional? Discuss the relationship between what is considered professional behaviour and professional ethics. Make sure you give practical examples.

## Answer:

A professional is a person who has been well trained in his area of expertise and is paid to perform his job, for example a doctor or a teacher. After studying and undergoing thorough training a person becomes a professional in his respective field. Similarly in case of an IT expert, he undergoes training and learns the various aspects of Technology, security, networking etc. and upon his successful completion, is hired by companies for his specialized services, thus this makes him a professional.

Professionals once equipped with the right knowledge and the right tools, need to employ them correctly. Exploitation or abuse of power is unethical, thus professional ethics encompasses the rightful employment of specialized knowledge. Most organizations have implemented codes of ethics, which every professional of the organization is required to follow. For example, while a professional hijacker might be useful for governmental organizations, but he needs to exercise his powers correctly and thus ensure professional ethics.

Similarly a professional behaviour includes the way a person conducts himself, his integrity towards his work and quality commitment. A professional is well aware of his responsibilities and thus works towards achieving the target goals. Professional behaviour when equipped with adherence to the professional ethics laid down by the organization ensures both, personal as well as company growth. One must realize the importance of dispatching ones duties professionally, as it not only aides in better growth but also helps to achieve set goals.

Question 3 – What is intellectual property (IP) and what can be considered to be IP? Are there any special problems with the ownership of computer programs?

Intellectual property (IP) relates to the efforts of the mind: innovations, fictional and creative performs, and signs, names, images, and styles used in industry.

IP is separated into two classes: Business real estate asset, such as innovations (patents), images, business styles, and geographic indications of source; and Copyright, such as fiction and creative performs such as books, poetry and plays, films, musical performs, creative performs such as drawings, artwork, photographs and sculptures, and architectural styles.

Computer programs are never a completely new invention but are evolved from present programs and codes. Being a tangible property, many various aspects add to the development of a computer program. Thus it can be said that a computer program is not 100% original, but is instead influenced by many other programs. This clearly states that a computer program cannot be exclusively owned by a single entity, but is the partnership of many others.

## Section 2

Module 2 – Security

Question 1 – Describe how security architecture principles fit within the security planning? Provide 3 examples of how in the industry the general principles are implemented.

## Answer:

In order to create a secure environment for computing, extensive planning is undertaken. Security models are implemented on a large scale in order to avoid any malpractice, and offer completely private and secure environment. Security architecture principles consists of security services that are applied to a computer in order to provide maximum security to its users, the performance levels necessary in order to fight the threat and the system elements in order to successfully implement the services. Thus while undergoing security planning; these security architecture principles play an integral part in order to ensure a secure and private environment.

## These general principles are implemented throughout the industry such as in-

Defense in depth which is an IA concept and which provides several layers of defense throughout the IT system. This includes biometrics, authentication or password process etc.

Diversity of Vendor: when corporations acquire computer systems from a single vendor. The entire lot is under threat as a single bug affecting one computer, can affect the entire corporation systems. In order to avoid this issue, it is better to practice diversity of vendor and thus acquire various systems from various vendors in order to avoid complete system failure and other vulnerabilities.

Firewalls are nothing but a barrier constructed in order to avoid the spread of malicious content, bugs, malware etc.

Question 2 – What makes a network vulnerable? List 4 precursors to an impending attack.

Some of the factors that make a network vulnerable include;

Anonymity

Many points of attack-both targets and origins

Sharing

Complexity of systems

Unknown perimeter

Unknown path

The 4 precursors to an impending attack include

Port Scan

Social Engineering

Reconnaissance

OS and Application Fingerprinting

Question 3 – What is the difference between Policy, Standards, and Practices? What rules must be followed when shaping a policy?

Policy: A plan or plan of action, as of a government or business, designed to effect and figure out the choices and which influence the decisions.

Standard: It is a released paper that contains a specialized requirements or other accurate requirements designed to be used continuously as a guideline, guide, or description. Requirements help to make life easier and to increase the stability and the potency of many products or services we use.

Practice: It is the methodology used through research and which has over

the years proven to be reliable in achieving the desired results. They are a set of procedures and guidelines which have been formulated for the employees to follow in order to ensure proper functioning of the company.

Some of the rules that must be followed while shaping a policy include;

Formulate a policy that adheres to the law and the rules and regulation set forth by the law.

The policy must be backed by proper reasons that support and justify the policy.

The policy formulated should be in the interest of the organization and result in its growth

The policy should incorporate the end user of the Information Systems

Issue specific policies should guide the employees towards proper usage of technology for configuring/maintaining systems.

## References:

1. Oppenheimer B. (2012). How legislatures shape policy and budgets. 5 June 2012. Retrieved from web. http://www. jstor. org/discover/10. 2307/439702? uid= 3738256&uid= 2129&uid= 2&uid= 70&uid= 4&sid= 47699067345027

2. W. Gates G. (2011). How uncertainty about privacy and confidentiality is hampering efforts to more effectively use administrative records in producing U. S. National Statistics. 5 June 2012. Retrieved from web. http://repository. cmu. edu/cgi/viewcontent. cgi? article= 1072&context= jpc

3. Meunier P. (2012). Class of Vulnerabilities and attacks. 5 June 2012. Retrieved from web. http://homes. cerias. purdue.

edu/~pmeunier/aboutme/classes_vulnerabilities. pdf

4. Trusted Information sharing network for critical infrastructure protection. 5 June 2007. Retrieved from web. http://www. dbcde. gov. au/__data/assets/pdf_file/0016/70621/SIFT_Full_Report_020707. pdf

5. Strahlendorf P. (2012). Professional Ethics. 5 June 2007. Retrieved from http://www. bcsp. org/pdf/PresentationsArticles/714_1. pdf

6. " Security Policy." (2008). 22 February, 2009 Retrieved from web. http://searchsecurity. techtarget. com/dictionary/definition/what-is-security-policy. html

7. Security Architecture. 9 June 2012. Retrieved from web. http://www. checkpoint. com/services/education/training/courses/samples/PoNS_C09_Security_Architecture. pdf