**Essay**

**Protection and security of informational systems**

Student: Vechiu Stefan, DS 1st Year

Information systems are becoming a major business driver and organizational tools that are gaining universal acceptance in all sectors of the economy. Basically, information systems are classified as hardware, software and data that facilitate communication. Protection of these systems at the physical, personal and organizational level is essential to the continuity of other operations. Through seamless exchange of information in an organizational network and over the internet, security concerns have been raised. The three major information security areas concerning authentication, authorization and confidentiality has been compromised physically or via the internet through hacking, malware and spyware programs.

Given the paradigm change associated with the internet of things, security has been the main focus. Almost all the daily activities and operations are now dependent on a safe, stable and resilient cyberspace. The military and civilian communication channels and traveling, power control systems, business operations and government services are dependent on a vast array of networks through computer networks and the internet. Cyber security for instance, is a mechanism of defined standards used by organizations and governments to practice safe security techniques and reduce the number of successful cyber security attacks. Information revolution has enabled attackers to launch their attacks miles away using malicious software’s and cause considerable damage. The same applies with terrorists. Therefore cyber security affects all other security apparatus of a country and because of the nature of attacks, it is always almost impossible to know the source of the attack. Governments and organizations are investing much in the development of comprehensive cyber security plans that provide sufficient security.

According to the Journal of Economic Management, and Financial Markets, the uses of enterprise information systems have enabled companies to assimilate various business functions and information systems into one warehouse. The data in an organization is integrated into one package that can be accessed by various departments and sections. This includes, finance, human resource department, sales and marketing, and administration. This in effect has made business operations easy and arguably efficient to execute. The centralization of all business operations, information and data at one location makes it more vulnerable to external and internal attacks. The company’s intellectual property, business data, backup information and other essentials such as employee data are susceptible to compromise if inefficient security protocols and measures are not developed and implemented. Malicious or unintentional security breaches and attacks results in business discontinuity, disruption, unreliability, inefficiency as well as eventual company and client losses. An example of such an incident is the NASDAQ malware attacks directed at the Directors Desk to cause security violations in 2011.

Most of the companies agree that employee training and awareness of security protocols and procedures is fundamental to the safety of the organizations data. Safe usage of passwords, accounts, authentication procedures and transfer of sensitive information between departments is crucial to the management of personal security. According to the paradigm shift towards cloud computing is fronting a dynamic area of information security. Until recently, information security has been revolving around technical aspects such as viruses, worms and Trojans. However, according to the Journal of Universal Computer Science, the cloud shift is necessitating more research in the fields of cloud security especially human interaction with the systems. As noted, the biggest problem arises when technology interacts with the people and this concerns the administration, management and use of information technology functionalities.

As a result, organizations have come up with different models of developing security of its systems and information. The frameworks include development of information security policies, developing employee awareness and training and governing access controls.

Information Systems security is a combination of information assets and controls intended to protect businesses and entities from emerging threats and vulnerabilities. As Spears notes, any company’s information is secure as much as the security protocols implemented to safeguard it. Untrusted information originating from wrong security policies leads to mistrust and uncertainty which impacts negatively on the continuity of a business entity.

As discussed above, the role of information security is the establishment of policies that initiate healthy working environment and controls the process of information exchange with the ultimate aim of guaranteeing confidentiality, availability and integrity. The security challenges that are mostly evident are grouped in the cryptographic, SMEs, privacy in the clouds, Internet security, forensics and security metrics among others. The fundamental aim of information security is the protection of information and data contained in the systems from disruption, destruction, modification, unauthorized access and use, and disclosure. The data protected takes the form of electronic, print, among others contained inside or outside of a computer system. Business enterprises, government entities, financial institutions among other sectors of the economy generate and store numerous files of information about their products, customer’s financials standings and employees. A large portion of this information is currently processed using computers and transmitted via computer networks or internet across the world. Comprise of the networks or information regarding such companies is unacceptable since it is attached with severe business, legal, societal and ethical implications. Privacy is also a major concern and is particularly defined differently in diverse cultures.

In the International Journal of Multimedia and Ubiquitous Engineering, Sattarova et al notes that the ultimate goal of information security is to achieve ultimate defense of information throughout its life span by preserving the CIA. This starts from creation of information, processing across the various information systems, passage and finally through to the final disposal. In order for the information to be fully protected, each component of the processing information system must possess some security controls. The layering on and overlapping of security controls gives rise to a process known as defense in depth. The defense in depth strategy outlines the protective measures put in place to guard the system against threats and vulnerabilities. It defines the strength of a information system security in reference to the weakest point of vulnerability. Controls can be used to define the mechanism of building a defense in depth strategy. The type of controls in use include administrative, logical and physical.

The protection of information in an organization is the topmost priority that should be implemented in any organization. Safeguarding data and information prevents ethical, legal and financial implications. The paper has reviewed the various security elements discussed in different journals and issues. In all, it is evident that confidentiality, integrity, and availability of information have been prioritized in the covering of their respective methods.