Discussion 1

Technology, Information Technology

Discussion Security Breaches: Discuss the implications of security breaches on technology adoption. Are people hesitant to use the Internet or wireless technology for purchases due to security concerns? Are people hesitant to use technology because of privacy concerns? Are these concerns warranted and are they influenced by age, race, or gender? Security breaches diminish the public's confidence to reliance on using technological applications as these violate privacy and confidentiality. Further, organizations who were victimized by security breach incidents have reported to generate significant financial losses (Ko & Dorantes, 2006, p. 14). People opting to make purchases are hesitant to use the Internet or wireless technology due to security concerns since some electronic sites do not provide appropriate security and protection for shoppers and compromise details of personal information, especially those that necessiate divulging bank account numbers or credit card details. These concerns are warranted, since according to the information provided by Buenaventura (2011), " 130, 000, 000 credit card numbers was compromised 2 years ago, which still holds the record for the largest security breach on the Internet" (par. 11). These are potentially influenced by age, educational background and profession since those who are prolific users of the internet are mostly the young generation and those who unsuspectively divulge personal information.

Discussion 2: Potential Consequences: Discuss what the consequences should be for not adhering to security policy guidelines. Where or how should these consequences be communicated to employees? Do you think there should be stronger and better-defined government-specified policies/laws for the general public? Organizations that define security policy guidelines

should clearly indicate infractions and penalties for violations. These should be communicated to the employees through their policy manuals and code of discipline. One strongly believes that stronger and better-defined government-specified policies and regulations; as well as stiffer penalties for those found to be violating security protocols and standards on privacy and confidentiality should be imposed to minimize and ultimately eliminate security breaches.

Discussion 3: Tell me what is on your mind about Information Systems and operating systems? What good articles have you read lately? Tell me what you think about this discussion question. Information systems (IS) are " used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system" (Information System Security, n. d., par. 1). Operating systems (OS_, on the other hand, is a program that manages the data and resources of the computer system. Articles on IS and OS can be accessed from various computer journals and publications which are also available online such as the InformIT site. One could gain from being exposed to updated information from both IT and OS regarding security breaches and intensifying protection of private and personal information by reading articles from identified sites.

References

Buenaventura, D. (2011, March 31). Some Interesting Statistics on Security Breaches on the Internet. Retrieved February 20, 2012, from Bright Hub: http://www. brighthub. com/internet/security-privacy/articles/112421. aspx

Ko, M., & Dorantes, C. (2006). The Impact of Information Security Breaches

on Financial Performance of the Breached Firms: An Empirical Investigation. Retrieved February 20, 2012, from Journal of Information Technology Management: http://jitm. ubalt. edu/XVII-2/article2. pdf

Information System Security. (n. d.). Retrieved February 20, 2012, from http://www. fas. org/sgp/library/nispom/change_ch8. htm