Essay summary of information and communication technology

Sociology, Communication

One of the biggest problems faced by the Information andCommunicationTechnology(ICT) industry is the threat of hackers and their destructive operations. Many individuals, businesses and government organizations have lost billions of dollars to the activities of hackers.

Hackers have different strategies of operating which keeps changing with the emergence of new technologies. Some hackers dispatch viruses to attack organization servers and personal systems. Such attacks, if successful, could result in the complete collapse of operations and activities of the targeted organizations and individuals.

Other hackers cultivate expertise in forcing unauthorized access into systems. They find their way into sensitive information such as personal bank accounts and corporate financial statements strategic plans. These hackers then either destroy the information or use it for unlawful gains at the cost of the rightful owners.

These nefarious activities of hackers have assumed such as menacing proportions that they have led to the growth of an entire industry dedicated to the protection of systems, networks and data from the threat of hackers.

The field of network, systems and data security is interesting as the challenge is to anticipate every move of the hackers and putting up adequate defenses against them. It involves reading into the perverted and sometimes brilliant minds of individuals who are the criminals of the new digital era. The topic is of concern to everyone who has digital data stored on the World Wide Web or the Internet in one way or the other.

Gamertsfelder., L., 2002, E-commerce: The Implications for the Law, e-Security. Available [Online] http://svc003. bne101v. server-web. com/Upload/PublicationUploads/publication106. pdf. (January 27, 2008)

Gamertsfelder's thesis statement for this article states that development of network security awareness in an organization works as an effective tool for combating risks against hacker activities.

He argues that all organizations need to be familiar with the consequences of the weaknesses of the securityenvironmentin which they operate. This brings about a sense of security consciousness, and a better understanding of how to manage and safeguard networks against hacker attacks. It also leads to better appreciation of the problems faced by the network administrator.

The article assesses the understanding of hackers' activities both from the insider's and outsider's views. Several scenarios depicting the operations of real-life organizations are used to show how awareness of data security risk can aid an organization in strengthening its security shield. Different types of hacker attacks against data, both from the internal and external perspective, are elaborately used by Gamertsfelder to illustrate his argument about advantages of awareness of security lapses.

This article is important as it shows how organizations can take stock of the lapses and breaches in their data security in devising ways to fight hackers.

McGuire, B., L., & Roser, S., N., 2001, What Your business Should Know About Internet Security Akauntan Nasional, April edition, Available [Online]

http://domino. mia. org. my/mia/miaWeb. nsf/0/cedaa19385281c1b48256b830029c70b/$FILE/05Apr01(tech). pdf. (February 27, 2008)

McGuire & Roser's thesis states that a company with a high level of information on how to make use of its internet security stands a lesser risk of website attack than an organization with lesser information.

The article shows how organizations can utilize their websites effectively to curtail the activities of hackers. It also shows how companies who operate websites can identify possible threats and take adequate safeguards to effectively secure their sites. McGuire & Roser gives step-by-step recommendations on how a company can secure its websites against attack.

The article is concise and expresses its points in clear and applicable terms. The article contains significant material for those organizations that seek effective ways of securing their websites and internet operations information from hackers.

Wong, S., 2003, The Evolution of wireless Security in 802. 11 networks: WEP, WPA and 802. 11 Standards, SANS Institute, Available [Online] http://cnscenter. future. co. kr/resource/hot-topic/wlan/1109. pdf. (February 27, 2008)

In the article Wong argues that the constant evolution of wireless security has ultimately led to the solution of providing security to network connections in the form of the 802. 11i wireless security standards.

The article takes a product-based approach in showing the efficacy and solution provided by wireless security to network connections. Wong discusses the insecurity associated with Wired Equivalent Privacy (WEP) which is an interim solution, and how WiFi Protected Access (WAP) provides alasting solutionthrough the 802. 11i standards. The paper shows that an organization can configure its network to provide customized solutions for its network's privacy and security.

The paper presents a wide range of ICT tools and technologies. It requires a person coached in and ICT operations and with a vast repertoire of ICT terminologies to fully understand and appreciate the significance of the paper. It is a significant work on solutions for network security.

Scheraga, D., 2005, Hackers: Keep Out Chain Store Age, Volume 81, Issue 10, October, pp. 51

The main contention of Scheraga's article is that the more a retailer relies on ICT for its daily operations, the more exposed its data is to theft.

The article provides solution-based steps for securing the data of retailers. It also examines the way retailers can manage the challenges in securing data from internal stakeholders to the organization.

The role of the US government legislation on providing insurance to retailers against the activities of hackers activities is emphasized by the article. Scheraga further presents strategic tactics that could be utilized by retailers in ensuring data integrity and minimizing loss and curbing liability. Steps on

how to design questions in implementing this strategy are listed in the article.

The article is concise and has a restricted scope in that it renders solutions only to retail operators in IT. The content of the paper is solution-based, and offers significant step-by-step guide for small operators on how to ensure data security.