Cyber security, network and computer systems administrators, and computer program...

Technology, Information Technology

The paper " Cyber Security, Network and Computer Systems Administrators, and Computer Programmer" is an excellent example of an annotated bibliography on the information technology. This annotated bibliography reviews five sources for the following three occupations: Cyber Security, Network and Computer Systems Administrators, and Computer Programmer. Careers in the growing field of information technology services: Beyond the Numbers: U. S. Bureau of Labor Statistics. (2013). Retrieved October 25, 2018. This article describes the trends in the field of information technology as well as the reasoning for the current increase in the cyber-security field. The dramatic growth in cyber-attacks such as ransomware, worms, Tranjon horse, viruses, zombie, and adware threats have taken a great toll among various businesses enterprises leading to a greater demand in the cyber security profession. The computer system organizations are expected to develop and grow rapidly as the amounts of cyber-security attacks increase and innovation as well as technology advances. This article is important for my report because it provides statistical data which is done on the increase as well as the progression of demand in the cybersecurity field and information technology. The weakness of this article is that it does not contain the statistical data obtained from the most recent sources because it reflects the information collected in 2013. The articles outline the need for powerful security in the various companies' cyberinfrastructure because it will provide an impetus for website developers to create and design new as well as upgraded software to prevent, detect, and contain the present and emerging cyber-security threats. Contreras-Sweet, M. (2015, February 13). White House Summit on Cybersecurity and Consumer Protection | The U. S.

Small Business Administration | SBA. gov. Retrieved January 15, 2016. The author of this article describes various threats of cyber-security as well, detection and prevention against malware attacks. One of the largest cyber-security attacks which continuously expand and develop seems to be cardholding protection and payment security. The primary goals of this article are to empower cybersecurity professionals and analysts to manage and control threats as well as enforce the significance of protecting financial data, and personal information within the business organization. Specifically for small and medium-sized enterprises, there is always a lot struggle with various cyber threats such as ransomware that attacks the computer systems by using strong encryption algorithms because of the small budget they set aside in to cater for top cybersecurity experts. This article is important for my report because it provides crucial information that would greatly assist the cyber-security professional how to protect their businesses from various cybersecurity-related threats as well as affordable methods and strategies they can use to detect, protect, and prevent themselves from cyber threats. The author describes several strategies for the cyber-security experts can use to protect and prevent their business entities against such cyber-attack including hiding their Wi-Fi networks, establish strong and powerful passwords, buying an updated anti-malware software, and using firewalls. Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2), 143-154. This article outlines the human errors as well as various network violations of network administrators in computer systems, end users, and information security

specialists. The authors examine the organizational and human factors leading to information and computer security. The authors use error taxonomies to explain the conditions of work that contribute extremely to information and computer security in business organizations across the world such as data breaches and security vulnerabilities. The authors explored the vulnerability and information security issues by interviewing information technology professionals such as network and computer administrators, and data security professionals. They used the audiotaped interviews, which were analyzed, and transcribed by coding various themes and presenting them in the node structures. This article is crucial for my report because it uses primary data collected through interviews and analyzed scientifically. The network and computer administrator show the errors created by different computer users as intentional while those caused by the company's network and computer administrators as unintentional. The businesses organizational factor, like organizational structure, policy, security culture, and communication were cited by the authors as the main causes of information and computer insecurity in various business enterprises. Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? Information & Management, 42(1), 143-158. The article describes the role of computer programmers as well as the information technology ethics by using the information technology behavioral model which includes individual traits, situational factors, subjective norms, perceived importance, and attitude of computer programmers and other information technology professionals. This article is

important for my report because it outlines the ethical values the should adhere by the computer programmers and other information technology experts. Sekgwathe, V., & Talib, M. (2012). Cyber forensics: computer security and incident response. International Journal Of New Computer Architectures And Their Applications, (1), 127. The authors this paper focuses on the role of cybersecurity professional in mitigating against cyber threats such as viruses, ransomware, adware, and Tranjon horses facing computer systems users. The article describes all types of cyber- crimes, cybersecurity regulations and policies, as well as incident and strategic responses. The primary purpose of this article is to provide relevant and appropriate information required to contribute toward the advancements and development of the field of cyber forensics. The authors also outline various risks that are related to the cyber-security problems to help small and large scale business organization to formulate effective policies and establish strong and powerful protection against cyber attackers. As cybersecurity problems are usually self-evident to show the fragility of electronic evidence since they can easily be manipulated and modified. The article is significant for my project report since it provides information which is necessary because of the semantic analysis of cyber forensic is being utilized to review and discover various information security policy and regulation requirements and the organization’s internal and external structures, institutionalizations and schemes.