Top three trends in your profession essay sample

Law, Security

The top three trends in the Cyber Security field are salary, career advancement, and the need for predictions of the future in how information is exchanged.

Cyber-crimes are becoming more popular and because of the many attacks that are happening much more frequently it has caused for a higher demand in cyber security professionals. Companies spend millions of dollars to correct security breaches within their organization. Back in 2008 the salary range for IT security professionals were in the $80, 000 to $90, 000 pay range per year, whereas in surveys from 2014 it shows these professionals earning $100, 000 or more a year for manager positions. Of course this differs based on experience, education, and certifications that individuals obtain but research shows that the demand and salaries for cyber security professions are only increasing.

The advancement of careers for Cyber Security professionals are also on the uprising. Cyber Security is a constantly evolving career that you have to stay abreast on. As long as you are well informed and up to date on the latest security breaches and the latest security controls you have a cutting edge and can provide the latest updates to a company. With this cutting edge you have the opportunity to advance in this fast growing career field. After I have studied a great amount into the Cyber Security field I plan to take my career farther and get some certifications under my belt for career advancement.

Another trend in the Cyber Security is how you can predict the future in how information is received. With the enormous amount of security breaches that have taken place and are only increasing a new form of password security

has to be in place. Passwords will no longer be able to protect accounts in 2015 and a new trend in adopting different approaches to authentication must be presented.

1. Identify the NAICS code of your industry or the SOC code

http://www. onetonline. org/link/summary/15-1122. 00

Summary Report for: 15-1122. 00 – Information Security Analysts Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses. Sample of reported job titles: Computer Security Specialist, Computer Specialist, Data Security Administrator, Information Security Analyst, Information Security Manager, Information Security Officer, Information Security Specialist, Information Systems Security Analyst, Information Technology Security Analyst, Information Technology Specialist

2. Identify and list the key concepts and terms related to researching, describing and discussing the top three trends in your industry/profession. Key concepts in researching, describing, and discussing cyber security:

New technology development

Security breaches

Cyber attacks

Cyber security

3. Identify the Library References you will use in developing the annotated bibliography UMUC Library Research

Web Searches – Government websites, references resources, search engines Books

4. Create a short informative annotated reference list of at least 6 references.

Cyber Security – Emerging Trends and Investment Outlook. (n. d.). Retrieved February 19, 2015, from http://www. researchandmarkets. com/research/m4f6wf/cyber_security

This article focuses on the analysis of the cyber security environment, potential sources of cyber-attacks, preferred strategies deployed to counter cyber attacks, and planned investment on cyber security products and services over the next two years. It also analyzes key barriers to cyber security, identifies prominent markets for cyber security products and, projects demand for cyber security products and services over the next two years. Executives expect cyber-attacks to result in security lapses, data leaks, and miscommunication within the organization. Email propagation of malicious code is the most frequently used technique by cyber-attackers. Executives state that the majority of cyber threats originate from China and that organizations are conducting periodic review of systems and administrative logs, and adopted computer security policies, to counter cyber-attacks over the next two years. This article supports my third trend on predictions of the future in how information is exchanged.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61.

This study investigates how knowledge in network operations and information security influence the detection of intrusions in a simple network. A Intrusion Detection System (IDS) was developed to examine how individuals detect malicious events and declare an attack based on a sequence of network events. The results indicate that more knowledge in cyber security facilitated the correct detection of malicious events and decreased the false classification of benign events as malicious. While knowledge of cyber security helps in the detection of malicious events, situated knowledge regarding a specific network at hand is needed to make accurate detection decisions. Responses from participants that have knowledge in cyber security indicated that they were able to distinguish between different types of cyber-attacks, whereas novice participants were not sensitive to the attack types. It is explained how these findings relate to cognitive processes and their implications for improving cyber security.

Trautman, L. J. (2015). Cybersecurity: What About US Policy?. Available at SSRN 2548561.

This is a scholarly article talks about how the U. S. Congress passed five major legislative proposals designed to enhance U. S. cybersecurity. Following signature by the President, these became the first cybersecurity laws to be enacted in over a decade, since passage of the Federal Information Security Management Act of 2002. An analogy with the recent deadly and global Ebola epidemic is used to illustrate policy challenges, and

assists in transforming the technological language of cybersecurity into a more easily understandable story. Much like Ebola, cyberthreat has the ability to bring our cities to a standstill. Many cybersecurity policy implications are strikingly similar to those necessitated by Ebola. The characteristics of selected competing cybersecurity constituency groups are discussed: consumers; investors; law enforcement; business; federal, state and local government; and national security interests. It focuses on the progress toward dealing with the new pandemic of technological virus. The critical need for an immediate and effective coordinated approach to cybersecurity, and crafting policy goals and strategies are offered.

Corbin, K. (2013, August 8). Cybersecurity Pros in High Demand, Highly Paid and Highly Selective.

A survey of cyber security workers reveals a profile of a highly compensated profession whose members say the integrity of their employer matters most. It explains how experts in cybersecurity are among the most sought-after professionals in the tech sector, with demand for workers in that field outpacing other IT jobs by a wide margin. Cybersecurity professionals report an average salary of $116, 000, or approximately $55. 77 per hour. That’s nearly three times the national median income for full-time wage and salary workers, according to the Bureau of Labor Statistics. The survey shed some light on the educational profile of the cybersecurity workforce. Eight-five percent of respondents said that they hold a professional certification, naming the Certified Information Systems Security Professional

(CISSP), Cisco Certified Network Professional Security (CCNIP), and Certified Ethical Hacker (CEH) as the most popular credentials.

Career Advancement Opportunities for Cybersecurity Professionals. (2013, January 1). Retrieved January 1, 2015, from https://missioncriticalinstitute. org/cybersecurity-professionals/

This article supports my trend on career advancements. Over 150, 000 New U. S. Cybersecurity Jobs/Year through 2017 and over 400, 000 New Global Cybersecurity Jobs/Year through 2017. The daunting cybersecurity staffing shortages confronting public and private sector employers enable qualified cybersecurity professionals to advance rapidly. The National Intelligence Estimate describes cyber threats as #1 of all U. S. national security challenges. Cyber-attacks, security breaches, compliance challenges and new technologies (e. g., BYOD, social media, mobile security, and cloud security) continually fuel the demand for qualified cybersecurity professionals. Thus, for experienced cybersecurity professionals, especially those who hold a security clearance and DoD- 8570 compliant certification, the opportunities for career advancement are extraordinary.

Lowe, J. (n. d.). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. Retrieved February 15, 2015, from http://3to1z93m5aspz1tlz1zcsjta2m. wpengine. netdna-cdn. com/keckjw/wp-content/uploads/sites/2169/2014/11/Myths-and-Facts-for-Control-System-Cyber-security. pdf

This article relates to my third trend on predictions of the future of cyber security and how information will be exchanged. The British Columbia Institute of Technology (BCIT) maintains an industrial cyber security incident data- base, designed to track incidents of a cyber security nature that directly affect industrial control systems and processes. This includes events such as accidental cyber-related incidents, as well deliberate events such as external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations. Incidents were almost evenly split between ac- cidental, internal and external sources, with only 31% of the events being generated from outside the company. Accidents, inappropriate employee activity and disgruntled employees accounted for most of the problems. This information is used to determine the step that need to be taken in order get a hold on security breaches and how information can be safely exchanged.