Chapter 56
Women to the Rescue in Cyber Space

Kristin Brittain
Florida Atlantic University, USA

Marianne Robin Russo
Florida Atlantic University, USA

ABSTRACT

The world is a complex array of human actions within an individual's sphere of influence and within a more global context. In either case, human actions can be susceptible to privacy and cyber security concerns. The consequences of targeted attacks on strategic cyber-systems, inclusive of nuclear power plants, electrical grids, water systems, would be quite high were they to actually materialize. Security gaps must be assessed and efficiently managed, and a viable workforce must be trained and vetted to take on this security effort. Therefore, with the intersection of human resources and women, who would be capable of training and going beyond the male cyber world realm? Women employment power may be the answer to filling the critical needs of the individual and larger entities that may be in need of cyber protection. This is explored in this chapter.

INTRODUCTION

The world is a complex array of human actions within an individual's sphere of influence and within a more global context. In either case, human actions can be susceptible to privacy and cyber security concerns. With technology as an added variable in the lifespan of many humans, cyber security issues could become a liability for the individual. For example, if an individual loses a cell phone, the individual's personal sphere of cyber safety could be temporarily eradicated. Within a societal perspective, cyber security could prove to be a grand emergency. If in fact cyber security is breached on a more holistic level, it could be argued that this kind of breach can include more intensive problems. For example, there may be environmental areas or even nuclear issues should a cyber security problem arise. In this sense, a technological glitch of this kind could have a permanent way of eradicating life on the planet. The consequence of targeted attacks on strategic cyber-systems (that is nuclear power plants, electrical

DOI: 10.4018/978-1-5225-8897-9.ch056

grids, water systems) would be quite high were they to actually materialize. The realistic security gap problem is what practitioners must take into consideration in their efforts to efficiently manage risks" (Helms, Costanza, & Johnson, 2012, p. 62). "Currently, agencies such as the USCC and the National Security Agency (NSA) maintain a commitment to addressing cyber-terror threats through investments in highly sophisticated satellite technologies that are used to monitor potential avenues of attack targeting national infrastructure" (Helms, Costanza, & Johnson, 2012, p. 62).

Security is very important in terms of Internet use in that it impacts not only the individual but affects transnational corporations when using the Internet. The idea of security on the Internet is defined as the concept of "cyber security," or safety on the Internet. It should be noted that as fast as technology is advancing, security gaps may become apparent, and which may exacerbate over time (Hoffman, Burley, & Toregas, 2012, p. 34).

Therefore, would it not be a viable investment, in terms of funding and human resources, to assure that the Internet and other Internet Communications Technology (ICT) are guarded against those who may wish to create chaos and wreak havoc in an economic, military, and social sense? It would be a logical deduction that with the increase in technology, the need to defend and protect the Internet and ICT is acute in terms of potential technological crimes. It is within the realm of ICT education, and education and training received in the workplace, that the vetting of a cyber security workforce who can manage safety initiatives as various factions traverse the vastness of the cyber highway.

A question should come to mind regarding the kind of workforce that would fulfill cyber security positions? What could be the demographics of those who would protect the cyber environment? Should the human resource effort focus on women? Is it possible for women to actually rear offspring and stay at home, could the home be made a cyber security workplace? Are women capable of training as cyber security personal? Could women be cyber security analysts using a more flexible scheduling when securing this kind of cyber security training and potential occupation? Human resource operations may have to examine this kind of gender workforce potential and decipher what the learning requirements would be in a cyber world that is in a constant state of evolution. According to Hoffman, Burley, and Toregas (2012) human resource officers may have a difficult time of vetting people in computer training due to the changing nature of IT and changing nature of the job requirements that fit these newly defined job categories. Therefore, with the intersection of human resources and women, who would be capable of training and going beyond the male cyber world realm? Women employment power may be the answer to filling the critical needs of the individual and larger entities that may be in need of cyber protection.

INTERNET SECURITY NEEDS

In the 21st century, the Internet has become an important and sometimes primary way in which individuals and groups communicate. Due to this fairly recent and robust communication application, problems with cyber attacks have ranged from viruses and hacking into corporate databases to the breaching of national defense systems. Some of this hacking has come from individuals with ties to governments, while some have not. In either case, or another iteration of intent, this type of hacking is criminal in nature. Cyber problems are explained by Singh and Siddiqui (2011) as "…theft, information sabotage, copyright infractions, breach of professional trust, digital privacy, intellectual property, distribution of illegal content, anti-competitive attacks, industrial espionage, trademark infringements, disinformation, denial of service, various forms of fraud" that can be remotely initiated and maintained (p. 1). Therefore,