**Introduction**

Mobile Devices: Cyber security is more vastly acknowledged than before as the numbers people who rely on mobile device to communicate and carry out duties involving their personal data and identity vulnerability is increases. On the other hand, polymorphic exists as a malware that runs the operating systems for Android, Apple, Google, tablets and smart phones against infamous cyber-attacks by criminals and terrorists around the globe. The automated system have helped in anti-virus detection for a secure security system to ensure privacy and data security. The study will deal with a thorough evaluation of mobile devices and their surfacing in society with the increasing concerns within the cell phone network. Briefly analyzing the history of mobile devices is vital in understanding the statistics proving the increase of cyber-attacks and the emergence of mobile computing to replace traditional personal computers. The articles are categorized following the discussion topics researched upon. The research on the increase of cyber-attacks in relation to mobile devices works with additional data on why such devices are more prone to security issues than other necessary technological infrastructure such as PCs (Friedman and Hoffman, 2008). This is in place of the basics that contribute to how mobile devices influence cyber security. There are factors such as malicious intents, unprotected use of mobile devices, and negligence by organizations and IT professionals. The greatest focus should be based on issues such as software and special features commonly found in PCs, but are lacking in some mobile devices. It is a general tendency for many mobile users to purchase the devices, begin to store, and use confidential information without installing the required security features. People with malicious intents easily access the stored information through hacking unsecured mobile devices. The threat to cyber security has been heightened through using mobile devices without ensuring that security protocols are accommodated.

**Literature Review**

Relationship between Mobile Devices and PCs in Terms of Cyber Security Threats

are important for the research to focus on computer viruses as a severe impact of cyber insecurity on many mobile devices. Faiz and Maqsood (2009) note that computer viruses have been identified as dangerous risks for a commercial computer setting. Malicious programs have the capacity to access user’s confidential information, in addition to crashed mail servers. Potential threats including war, Trapdoors, Password catcher, Logic Bomb, Bacteria, Trojan horses, and network worms are also harmful to the stored information in these mobile devices. Mobile device fields are impacted by cyber-attacks in that their modern designs are similar to PCs. In fact, they have systems such data processing capacities, spreadsheet editors, text editors, and operating systems Users of mobile devices also have the ability to exchange files that are regulated to execute since are capable of connecting to the internet. Modern wireless technologies have enabled thrilling opportunities such as mobile e-commerce (that is, online financial transactions). There are cases of exchanging sensitive data in the process of executing an online purchase. Thus, security emerges as the most vital issue in such forms of mobile device services.

During the research, it is important to identify the correlation between the new generation of software for mobile devices, the web, and cloud computing. Al Haddad, Reddy, Dalvi, Singh, Obeid, Al Rihawi, Abou Selo, Elgazar, and Sans (2012) clarify that the new usage of modern technologies comes with new and increased security threats, in addition to a new generation of malicious software (malware). Al Haddad et al. (2012) evaluated the challenges of exposure to malicious software in typical application ecosystems including Google Chrome, Mozilla Firefox, Google App Engine, Facebook, Google Android, and Apple iOS. The study conducted by this group of researchers was a proof of concept to how mobile phone usage has increased challenges to cyber security. For example, they developed malware applications that stole personal information of smartphone users. Hacking Gmail accounts enable a person to access credit card numbers, passwords, and other logins. All of these enhance cyber-attacks since it becomes easy to get passwords for important accounts such as online banking transaction accounts.

**Influx of Mobile Devices and Cyber Security Threats They Pose**

The emergence of different and cheap mobile devices should also be examined in the process of defining how cyber-attacks are influencing mobile devices. Lu (2013) states that unwary users of mobile devices are to blame since they are the weakest connection to the cyber-security chain. This is because they unknowingly facilitate incoming attacks, thereby thwarting the efforts to ensure secure networks and systems. To curb the problem of cyber-attacks, emphasis should be aimed at securing systems and software by eliminating or reducing occasions where mere actions of users of mobile devices unintentionally propel external attacks and exploits. Since there is a faster user growth in mobile computing through the introduction of smartphone applications, the platform of web browsing has grown rapidly. An increase of dominant attacks such as malware has also been witnessed. Infections are continuing to happen on the World Wide Web. Rogue websites and drive-by downloads have also contributed to higher levels of cyber-attacks.

The reasons for linking increased cyber security threats to the emergence of tablets and smartphones are areas that should also be analyzed in this research. Cyber threats are not similar to everyday technology challenges faced by organizations. Therefore, it is of particular importance that the risks are dealt with at the board level. CEOs believe that IT departments are not to blame regarding the threats that mobile devices pose to cyber security, and in fact, that of the business.

The ever-rising challenge of cyber security as a result of an influx of mobile devices is an issue that should not be underestimated. Therefore, it is important to define the measures that different players in the industry have initiated to help combat problems of cyber security. CTIA (nd) observes that the rise in demand for mobile devices is accelerating at an alarming rate. In the previous year, industry analysis showed smartphone purchases outweighed tablets, laptops, and desktops for the first time in history. The issue of cyber security is in everyone’s best interests. When it comes to tackling current challenges to cyber threats, the solution should incorporate everyone.

**Contribution of Mobile Device Users to Cyber Security Threats**

There is a need to review the emergence of a new generation of employees in different organizations all over the globe. Ruggiero and Foote (2011) affirm that the millennia and the Y-generation have come of age and are securing employments in various corporate environments. Currently, organizations have also embraced the application of mobile devices for their daily operations. Employees are provided with tablets, smartphones, and other related mobile devices to enhance communication and flow of information within different branches of the company or business. During the research, the focus will be based on reasons why companies are replacing traditional technologies with smart mobile applications and devices. Factors including cost saving could be looked at since businesses seek new ways of cutting their expenses.

The research will evaluate the individual and organizational motivations for using personally owned mobile devices such as smartphones in the workplace in addition to challenges experienced from use of data security and privacy concerns of every stakeholder in the organizations. Chigona, Robertson, and Mimbi (2012) clarify that convenience, access to emails, and ease of use are the primary motives behind individuals’ use of personal mobile devices in the workplace. Additionally, employees expect heightened privacy expectations. Mobile devices such as smartphones are creating challenges to companies’ and organizational information security. The right of employees to privacy for the information they store on their mobile devices is considered infringed. Chigona et al. (2012) suggest that organizations need to engage in reconsidering employee privacy and data security policies to tackle possible disagreements between employees’ privacy and data security.

**Contribution of Hackers to Problems of Cyber Security Due to Use of Mobile Devices**

A different perception to handling the impacts of mobile phones on cyber security is essential for the research. It has been identified that the consequence of the increasing popularity of mobile devices is the rise of mobile malware. Attackers target useful user data and exploit the weaknesses of these mobile ecosystems. However, with the increasing development of malware, developers of mobile apps have taken a step in creating secure mobile systems that are not a threat to cyber security. In their study, Gelenbe, Gorbil, Tzovaras, Liebergeld, Garcia, Baltatu, and Lyberopoulos (2013) identified a project that develops novel security technologies for endless service provision in the smartphone ecosystem. These systems, popularly referred to as NEMESIS, helps in improving the safety of the mobile network through increased understanding of the landscape of cyber security and attacks. Gelenbe et al. (2012) confirm that the application is capable of handling cyber security threats since it gathers and analyzes information related to the characteristic of cyber-attacks targeted to the mobile network and mobile users.

The cause of easy access to mobile devices by cyber criminals is an issue that should be reviewed in this research. Wharton University of Pennsylvania (2013) notes that as wireless gadgets become increasingly incorporated into the lives of Americans, they increase freeways to a rising security risk. Such devices are the point of access for attackers. Barely one-third of mobile device interested in online transactions or banking has antivirus software installed on their mobile gadgets as compared to 91% of laptop owners who ensure antivirus and automatic updates are available on their devices. The techniques applied from attackers can easily access mobile device systems are another area that requires thorough analysis. Several reports indicate that cyber insecurity caused by attackers who employ old techniques alongside new ones to access information in the device of unsuspecting users. As a frontier of the new generation of cyber security, smartphones can be easily hacked several meters without having to see the actual device. Yadron (2014) wrote an article in the Wall Street Journal there is a malicious individual (name withheld) who is capable of taking over a smartphone mobile device that consists of a 30 foot afar without necessarily having to alert the phone company or user. The reason for this claim is very clear; personal digital assistants and smartphone security have not been at par with traditional systems of computer security. Measures of high technicalities such as an application of encryption, antivirus, and firewalls, are not standard on a mobile device operating systems and the cell phones themselves. Also, the operating systems lack frequent updates typical to everyday personal computers people use at homes and offices.

**Conclusion**

In conclusion, the literature review analyzed different articles concerned with the evaluation of how of mobile devices influence cyber security. The literature review filters the topic to lay emphasis on in general cyber insecurities on mobile devices. To avoid broadening the topic, parameters such as analyzing different mobile device operating systems have been avoided. However, the literature review fails to outline a permanent way to prevent the increasing rates of cyber-attacks concerning mobile devices. The explanation is that the IT industry has not yet invented an ongoing way of averting attacks arising because of the use of mobile devices. Unfortunately, the attackers are evolving with the reality that they are competent, but malicious engineers of software applications. Also, the research does not explicitly address particular operating systems found on smartphones and other mobile devices that pose the greatest threat to cyber security. Thus, the overall goal of the paper is to illustrate the impact of cell phones as the biggest threat to cyber security. The paper targets to enable readers to familiarize with threats of mobile devices from privacy to safety and the fundamentally preventable measures users can adopt to combat risks related to the attacks.

**References**

Al Haddad, T., Reddy, M., Dalvi, F., Singh, B., Obeid, O., Al Rihawi, R., & Sans, T. (2012, October). Malware. inc: analyzing the security of popular web/mobile frameworks. In *Qatar Foundation Annual Research Forum* (No. 2012).

Chigona, W., Robertson, B., & Mimbi, L. (2012). Synchronised smartphones: The collision of personal privacy and organisational data security. *South African Journal of Business Management*, *43*(2), 31-40.

CTIA. (nd). Cyber security white paper. Retrieved October 29, 2014, from, http://www.ctia.org/docs/default-source/default-document-library/cybersecurity\_white\_paper.pdf?sfvrsn=2

Faiz, A., & Maqsood, M. (2009). Information Security Threats Against Mobile Phone Services (Developers Perspective).

Friedman, J. & Hoffman, D. (2008). Protecting data on mobile devices. Information knowledge systems management. Vol. 7; 159-180

Gelenbe, E., Görbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., & Lyberopoulos, G. (2013). NEMESYS: Enhanced network security for seamless service provisioning in the smart mobile ecosystem. In *Information Sciences and Systems 2013* (pp. 369-378). Springer International Publishing.

Lu, L. (2013). Reinforcing the weakest link in cyber security: securing systems and software against attacks targeting unwary users.

Palmer, D. (2014). Mobile devices significant risk to cyber security BAE systems. Retrieved October 29, 2014, from, http://www.computing.co.uk/ctg/news/2330773/mobile-devices-significant-risk-to-cyber-security-bae-systems

Ruggiero, P. & Foote, J. (2011). Cyber Threats to Mobile Phones. United States Computer Emergency readiness team

Wharton University of Pennsylvania. (2013). Mobile devices and cybercrime: is your phone the weakest link? Retrieved October 29, 2014, from http://knowledge.wharton.upenn.edu/article/mobile-devices-and-cybercrime-is-your-phone-the-weakest-link/

Yadron, D. (2014). Smartphones become next frontier in cyber security. Retrieved October 29, 2014, from, http://online.wsj.com/articles/smartphones-become-next-frontier-in-cybersecurity-1406808182