International Journal
of Online Graduate Education

The Cyberthreat in IoT, Mobile Learning, and Wearable Devices in Education

Willy Ochaya
Northcentral University

Cyberattacks have a similar global economic impact of a natural disaster such as Hurricane Katrina, according to Lloyds, the world's specialist insurance market of London report. According to Lloyd’s of London, global cyberattacks pose a considerable risk to businesses, health service, and education, resulting in average economic losses of between $4.6bn and $53bn a year. This research was prompted by a concern about the growing threat, stemming from the upsurge in cyberattacks on the significant business, health, education and government infrastructures on a global scale. Practitioner responsibilities should include searching for any innovation, threat, and a pedagogical trend that can impact education and share it via peer journals, advocating for the danger or adoption of technologies within the educational system. This is a considerable problem facing educational institutions, according to the Center for Digital Education (CDE, 2017) report, which confirms that most institutions of higher learning still use outdated network infrastructures. Accepted Use Policy (AUP) and un-automated services allow major, unabated security breaches because they use outdated network equipment and AUP is not recommended for use beyond the end of its life cycle. This research intends to raise awareness among policymakers, academics, students, and faculty members about the cyber threat in Internet of Things (IoT), Mobile Learning Devices (MLD), and wearable technology. These are new concepts and, consequently, there is little available research on the topic.

Introduction

The end of the 20th Century and the beginning of the twenty-first century saw higher education institutions embracing the use of Internet of Things (IoT), bring your own device (BOYD), and wearable and mobile learning device (MLD) as a new paradigm shift in education (Dlodlo, 2012; Rajasingham, 2010; Tsinakos, 2013). In this period, institutions, scholars, and governments joined in implementing the concepts as the tool for implementing pedagogical strategies, particularly eLearning, using a learning management system (LMS), which is commonly used in distance learning (Alkhalaf, Amasha, & Al-Jarallah, 2017; Moreira, Ferreira, Rajasingham, 2010; Santos & Durão, 2016; Tsinakos, 2013). However, the well-established presence of cyberthreats presents the need for foundational training for new hires in AUP awareness, and the same for students and staff members using the institution’s network (Tsinakos, 2013).

Unfortunately, the acquisition of the IoT and wearable devices among students attending online colleges and universities has made Internet traffic flow to and from educational networks vulnerable to cyberthreats. According to Dlodlo (2012), IoT, BOYD, MLD, and wearable devices form part of information and communication technology in education, and they use Wi-Fi, Bluetooth, or Ethernet via sensors for interconnection with other devices or things (Bernsteiner, Kilian & Ebersberger, 2016; Brown & Mbati, 2015; Behera, 2013; Chitanana, 2012; Chitanana, 2015; Lee & Lee, 2015; Ziegeldorf, Morchon, & Wehrle, 2014). According to Bulgurcu, Cavusoglu, and Benbasat (2010) and Jacobsen (2013), the introduction of Internet Protocol version 6 (IPv6) brought about the growth of the IoT and wearable technology in the education and health sectors (Federal Bureau of Investigation Cyber Division, 2014). Utilizing MLD, BOYD, and IoTs while accessing the application puts data resources at risk. They are vulnerable to hacking because the hackers prey on their failure to follow AUP guideline protocols, and other weaknesses (Bitsight Technology, 2015; Creeger, 2010; Custer, 2010).

According to Creeger (2010), students, faculty, and staff are the most vulnerable population to cybersecurity defenses in the educational network, due to human behavior and error in distributing bots. According to Custer (2010) and Kerravala (2016), human error accounts for more than 90% of cybersecurity attacks. These are often due to lack of user awareness of AUP and functionality of some feature of the IoT and wearable devices. Additionally, users often do not understand the meaning of notifications that require their attention.

Statement of the Problem

A problem exists related to the lack of user awareness of AUP in the use of IoT and wearable devices protocol for the institutional network. Numerous IoT devices, with or without access permission, all seeking constant attention from the users, leaves users overwhelmed by interaction requests from such devices. According to Anderson and Rainie (2014) and Halpern (2014), more than 50 billion devices will be interconnected in healthcare, customer services, education, and homes by 2025. Additionally, Halpern (2014) noted that between 2018 and 2025 cybercrime would increase within educational institution networks, supporting their prediction (Custer, 2010 and Dodge, 2009). Many schools are slow in recognizing the cybercrimes, security risks and human error associated with BOYD, MLD, IoT and wearable technologies (Thierer, 2015; 2013; McGuire & Dowling, 2013; Won, Ok-Ran, Chulyun, & Jungmin, 2011). This is especially true where there is a flaw in policy, AUP or old AUP to guide, manage, or control, the influx of mobile technologies (Anderson & Rainie, 2014; Halpern, 2014).

Furthermore, problems occur when there is a lack of AUP regulation and policy-based management guidelines and protocol, enabling human errors caused by students, faculty, and staff while accessing institutional networks (Bernsteiner et al., 2016; Chitanana, 2012; Chitanana, 2015). Many institutions are overwhelmed with the new technologies due to lack of funding or qualified security personnel to monitor cyberthreats or to update their policy and software (Thierer, 2015; 2013; McGuire & Dowling, 2013; Won et al., 2011). Knowledge gained about these problems is shared through publication to give other educational institution administration and staff the ability to understand the danger of cyberthreats. Further, recommendations concerning the necessary steps to reduce cybercrimes and cybersecurity threats within institutions of higher learning and organizations were examined (Chitanana, 2012; Chitanana, 2015; Coleman, 2015).

Purpose of the Review

This literature review explored AUPs, and scrutinized IoT and wearable devices protocol within institutional networks by building upon theory outlined in referenced works. By extending this approach to education, the sutdy included the policy challenges each institution faces when students, faculty, or staff lack awareness of AUP for the new devices, and to enlighten educators of the risk of using IoT devices without policy guidelines for the new devices. The intention of using this method is to integrate and guide the author in collecting literature for analysis more synergistically by utilizing data as a whole. Further, this study examined the Protection Motivation Theory (PMT) against ransomware as opposed to rampant virus threats. Findings indicate the need for training awareness of AUP, as it relates to IoT and wearable devices, is more appropriate for this study (Creswell & Plano Clark, 2011; Liang and Xue, 2010; Thierer, 2015; Doanea, Boothe, Pearson, & Kelle, 2016).

Description of the Project

Universities and colleges have become the most targeted institutions by hackers (Harris & Hammargren, 2016). According to Perera, Zaslavsky, Christen, and Georgakopoulos (2014). According to Perera et al., (2014) the evolution of the IPv6 gave rise to various and complex types of theIoT, beginning with a desktop application, web application, and mobile computing to the IoT (e.g. smartphones, smart cars, smart homes, etc.). The authors went on to add that the evolution of the internet began with the necessary communication link between two computers using a computer network in the 1960s. Later, in the 1980s TCP/IP was introduced, which subsequently gave rise to the worldwide web. This made it possible for the mobile device to connect to the internet, and precipitated the social network where users get connected to multiple IoT. Today, web connectivity is not coordinated, and lacks connectivity protocol standards. According to Vermesan et al. (2013), IoT is a new paradigm that covers a variety of things/objects that, through wireless and wired connections, work together to reach common goals – while simultaneously making them difficult to monitor.

This literature review used institutional publications to examine the problems relating to lack of awareness of AUP, hacking, and other security breaches (e.g. Distributed Denial of Service [DDOS] attacks, ransomware, and malicious code techniques used by cybercriminals online andElliott, 2010; Liang & Xue, 2010; Thierer, 2015). The goal of the review is to create awareness of the dangers to education, and to offer potential solutions to such problems. The data collected explored documented characteristics to identify divergent and convergent themes associated with these phenomena (Creswell, & Plano Clark, 2011). This study also examined how the AUP can guide users to comply with regulation sets for using their computers, MLDs, IoTs, and wearable devices when accessing the network resources, storage, and services (Anderson & Agarwal, 2010, Crossler et al., 2014; Liang & Xue 2010; Thierer, 2015). Pearson (2015), supported this strategy of training and creating awareness of the AUP, and pointed out that the twentieth century is the era of digital transformation which compels educational institutions to embrace IoT devices to track students' ongoing activities with the school. The inclusion of wireless mobile devices in the network added pressure on IT personnel to manage and control these devices as they now combine both traditional networking and digital networking in their information, as well as instructional technology systems.

Literature Review

Cyberthreats in IoT, Mobile Learning, and wearable devices in Education are the areas of concern related to AUP because they relate to internet connectivity and utilization (Elliott, 2010). Many IoT, mobile learning (ML), and wearable devices are embraced within the institution of higher education - especially distance education or e-learning (Garrison, 2011). IoT entails accessing the internet with multiple devices any time and in any place (Halpern, 2014; Lee, & Lee, 2015; Mock & Paden, 2015). According to Won, Ok-Ran, Chulyun, and Jungmin (2011), cybercriminals are currently targeting institutions and users who use a university network, and are leveraging security flaws that could be attacked using ransomware and other malicious software. Most educational institutions are vulnerable, particularly those that provide services via eLearning and distance learning, due to human errors. These problems are overshadowed by the growth of the large numbers of multiple IoT, ML, and wearable devices as they access the educational intuitions' servers without proper protocol. Headlines about the cyberattacks involving businesses and other industries seem to overlook educational institutions and health services (Ciampa, 2014). Cyberthreats pose problems in education and other institutions because they threaten the integrity of large amounts of intellectual property and student and patient records. Additionally, these institutions serve as the weakest link for hacking financial information, personal identification, social security numbers, and intellectual property. Quirolgico, Voas, Karygiannis, Michael, and Scarfone (2015), also warned that the use of mobile apps could potentially lead to serious security issues because they may contain software vulnerabilities that are susceptible to attack by hackers.

Cyberthreats come in many forms. Some are malicious software designed to disrupt or steal users' identities or intellectual property. (Chiampa & Blankenship, 2012; Elhai & Hall, 2016; McGuire & Dowling, 2013; Thierer, 2013; Won et al., 2011). Websites can monitor highly personal communication and can capture data such as passwords for mobile banking apps where there is a vulnerability in a network with no AUP, or an outdated AUP (Doherty et al., 2011). How big will a problem of lack of security on IoT, ML, and wearable devices have in education? Liang and Xue, (2009; 2010) provided the only theoretical lens in this area, which could be useful in determining the extent of the problem, and could be adapted and used for future related studies in education.

Significance of the Study in Education (eLearning)

The current state of cyberthreats to IoT, ML, and wearable devices is still limited, and rarely reported to police if the incident occurs. However, the incidents are not well documented within the literature, especially regarding AUP awareness in the educational cyberthreat landscape (Liang, & Xue, 2009; 2010). At least one study highlighted the need to enhance the knowledge of AUP and cybersecurity threat in education, as more threats are becoming increasingly sophisticated, especially in e-learning devices. The limited attention on e-learning calls for further exploration about the appropriateness of AUP in mitigating cyberthreats (Jones & Heinrichs, 2010).

According to Sharpel (2011), IoT and wearable technology as a personal ecosystem have more potential for education and training among educators. They are all-purpose computing devices, with multi-core processors, cameras, sensors, audio recorders, and touchscreen capability, with various form factor sizes with embedded Wi-Fi and Bluetooth connectivity, making them all prone to security threats (Johnson, Smith, Willis, Levine, & Haywood, 2011). The recent spike in cyberattacks has prompted the Department of Homeland Security's National Cyber Security Division (NCSD) to issue a warning of the looming threat to the institution of higher learning and the public at large (Rajewski, 2013). Unfortunately, most of the current scholars centered their works on the technological benefits, use for learning and teaching, and praising their potential as tools in education (Behera, 2013; Brown & Mbati, 2015; Martin, McGill & Sudweeks, 2013; Mueller, Wood, & De Pasquale, 2012; Pereira & Rodrigues, 2013; Tsinakos, 2013). Little consideration has been given to their risk, as they are linked to pedagogy and instructional design (Rajasingham, 2010). In contrast to other studies, IoT and wearable technology have more potential for education and training among educators, and need to abide by the institutional AUP. One study noted that educators like Rajasingham (2010) still centered their work on technology use for learning and teaching in their published materials, praising the potential of this technology rather than featuring the threat facing more devices in education. They show little consideration of their risk as they are linked to pedagogy and instructional design to users' interaction (Behera, 2013).

Evaluation

Creeger (2010) and the Cyber Threat Alliance (CTA) (2015) both agree that one example of a security breach is when malware like ransomware encrypts user computer files and demands a ransom payment for the key to unlocking the equipment file. Elhai and Hall (2016) also provided additional examples of these problems and described it as flaws, which can result in electronic data breach problems caused by lack of AUP awareness. Lacking knowledge of electronic data breaches is a problem because a hacker uses the back door of the user's devices, or IoT, to secretly gain entry into a device and a computer system, and spread malicious codes to users' devices or equipment and disrupt institutional services (Elhai & Hall, 2016). According to Doherty et al. (2011) and Elhai and Hall, (2016), this flaw enables cybercriminals to enter institutional servers and demand ransom from the institution, demanding payment before they release the service.

Cybercriminals use malicious software to steal user data and intellectual property (Chiampa & Blankenship, 2012; Elhai & Hall, 2016; Thierer, 2013; McGuire & Dowling, 2013; Won et al., 2011). Additionally, Loraas, Crossler, Long, and Trinkle (2014) acknowledge that training employees on the danger of cybercrime can be a useful asset in the effort to reduce the risk of threats to information security, privacy law, and violation of the Family Educational Rights and Privacy Act (FERPA). Studies have outlined procedures for cybersecurity awareness and why higher Educational institutions need to address cyber threat (Rajewski, 2013). Cybersecurity Awareness Month initiative, first created in October 2004 by NCSD due to the increasing threat of domestic and international cyber-attacks, was created to promote cybersecurity awareness for educational institutions (Rajewski, 2013). For example, the NCSD, in collaboration with National Cyber Security Alliance, uses Cyber Security Awareness Month to promote Security awareness among institutions. The department pointed out that educational institutions are at high risk of cyber threat and attack due to the level and the knowledge of the users they have (Rajewski, 2013). The department also noted that the rate of cyber hacking and attack has soared among institutions of higher learning (Rajewski, 2013). Additionally, they warned that higher educational institutions are vulnerable to losing intellectual property as well as personal information of students, faculty, and staff due to insider or outsider threat actors (Rajewski, 2013). Most universities and colleges need to be aware of the significance of intellectual property as well as student data (Behera, 2013; Chang, 2012; Martin et al., 2013; Thierer, 2013; Quirolgico et al., 2015).

On February 12, 2013, President Obama issued Executive Order (EO) number 13636, "Improving Critical Infrastructure in Cybersecurity." The Executive Order was designed to encourage the development of cybersecurity, and provided a useful and cost-effective approach to managing cybersecurity risk for the following of information and systems which involved the delivery of critical infrastructure and services. The policy was written in collaboration with the Information Technology (IT) industry to guide organizations on managing cybersecurity risk. The policy was adopted by the United States Cybersecurity guide to enhance the cybersecurity landscape and economic prosperity by promoting safety, security, business confidentiality, privacy, and civil liberties. The the policy also supported creation of a voluntary risk-based cybersecurity framework as a set of industry standards and best practices to help organizations, regardless of their size, to manage cybersecurity risks which may occur due to human errors (Executive Order 13636, 2013).

A portion of the literature revealed that there is limited research on theoretical perspectives involving the threat related to MLD, IoT, and wearable devices in education,where students are more interconnected than ever with their devices. This interconnectivity brings with it increasing risk of threat, fraud, and abuse with the new technology landscape, as more institutions are embracing these technologies (Baran, 2014; Thierer, 2015). For example, Bitsight Technology conducted research in 2015 that found that in the education industry, 58 percent of shared network files contain social security numbers, medical records, intellectual property, and financial data of staff, faculty, and students, making them particularly vulnerable to cyberattacks. Additionally, Custer (2010), noted that human behavior also contributes to security vulnerability due to lack of AUP awareness. The AUP awareness guideline is useful for safe use of the internet (Custer, 2010). The aim and objective of the IoT is to connect with anything, anytime, anywhere, with other IoT. However, some use it with the intent of stealing cash, compromising intellectual property, or defacing the network, thus blurring the line between the malicious users trying to get in and legitimate users exercising honest behavior Veresan et al. (2013).

Exigent research has focused primarily on the value of mobile learning for students in eLearning, distance learning, and teacher education development Baran (2014). Researchers have only just started exploring the potential of MLD within education and teacher development. Yet gaps in the literature still exist in the integration of mobile learning into education and teacher training, and few studies explored the threat and risk they posed to educational institutions (Baran, 2014). According to the U.S. Department of Education Safeguarding Student Privacy (n.d.), all schools must act responsibly to safeguard students' personally identifiable information - from practitioners of early learning to those developing systems across the education continuum.

Additional research identified the problem of information security threats in MLD, and why the issue is critical in analyzing the cyberthreat in IoT, mobile learning, and wearable devices (Liang, & Xue, 2009, 2010). Since the topic is so new, it is important to create awareness of safe AUP use, to outline how cyberthreat in IoT, mobile learning, and wearable devices occurs by pointing out the problem and why it is worth exploring (Beyer, 2014). A portion of the literature still revealed that there are few reports on theoretical perspectives and models involving cyberthreats in mobile learning research in education Baran (2014), and they are often limited to internal documents and whitepapers. Furthermore, the literature indicated that further inquiry is needed to add to the body of knowledge within education related to the doctoral learner's field of specialization in eLearning (APA 2010; Beyer, 2014). In the online learning environment, malware creators can reach students or instructors by email, social media, SMS and websites that can monitor highly personal communication and capture vital data such as password and mobile banking application.

Furthermore, Mock and Paden (2015) warned that the IoT as a platform for objects and devices connected to the internet add to the connectivity problem facing mobile devices. They can pose some serious risks for educational institutions and their networks. They can also include external organizations like device manufacturers and software developers by the threats involving their hardware and software products (Mock & Paden, 2015). This study used the auto industry, whose products interact with mobile devices and the IoT, and how they affect users, especially college level drivers, for example (Bulgurcu, Cavusoglu & Benbasat, 2010; Mock & Paden, 2015). The authors noted that in the auto industry, where many new vehicles have computer systems that interact with mobile devices, hackers could compromise them like any other computer or mobile device. Today, many educational institutions own sensors, printers, cameras, and other campus-installed devices that can easily be hacked and compromised (Mock & Paden, 2015).

According to the Ponemon Institute (2013), employees are moving intellectual property (IP) outside the company in all directions without control. They also pointed out that 41 percent of employees downloaded IP onto their tablets or smartphones – making this confidential information more vulnerable as it leaves corporate-owned devices. Thirty-seven percent use file-sharing apps (such as Dropbox or Google Docs) without permission from their employer. According to Beyer (2014), sensitive data is rarely cleaned up; and the majority of employees put these files at further risk if they do not take steps to delete the data after transferring it.

There is an increasing trend for BYOD, and given the growing number of students using MLD, it is inevitable that an increase in vulnerability will occur. Liang and Xue’s (2009, 2010) Theory of Avoidance of IT Technology Threats (TTAT) helps explain how individual IT users behave to avoid the risk of malicious information technologies during the time of antivirus, but not ransomware. Currently, ransomware has established a new level of sophistication and attack, not on one individual, but on a large scale making the study more complicated by requiring the study of more than just individual institutions.

Mobile devices have brought a paradigm shift in education (Burden & Aubussun, 2012; El-Hussein & Cronje, 2010; Kearney, Schuck, Burden, & Aubussun, 2012; Pegrum, 2013; Taylor, 2011; Williamson, 2010). Moreover, none addressed the issue of the cyber threats facing mobile devices in education, except those in corporate entities and information systems. Taylor (2011) noted that mobile technologies had changed the way many students interacted in their activities, compared to the previous educational technology approach. In his studies, Pegrum (2013) posits that handheld mobile devices make mobile-learning (m-learning) and e-learning possible anywhere, anytime. According to Lee, Lee & Kweon (2013), mobile devices use multimedia to deliver digital audio, video, and other multimedia content to students anywhere at any time, and make them more ubiquitous for learning in education. Pegrum, Oakley, and Faulkner (2013) claimed that smartphones are now owned by many students making the BYOD concept more applicable to education (Anderson & Rainie, 2014).

Furthermore, according to various studies, the authors endorsed and predicted the importance of m-learning devices as a paradigm shift in higher education (Akella, 2012; El-Hussein & Cronje, 2010; Kearney, Schuck, Burden, & Aubussun, 2012; Rajasingham, 2010; Williamson, 2010). However, these studies failed to note that smartphones and tablets are prone to threats such as malware and data theft in higher education. Additionally, a fraction of smartphones and tablets are protected by security software from the manufacturers, despite a rise of malware targeted at mobile devices. Furthermore, most of the users are ignorant of the threat. Students are incorporating devices they already own, such as cell phones, tablets, and smartphones, into their learning activities. In college and university environments, mobile devices are becoming an essential part of students’ and faculties’ daily routines. According to a 2011 Pew report, in their Internet Project Teen Survey, 77 percent of 12- to 17-year-olds have cell phones. Technology has become synonymous with living and learning. Most recently, there has been interesting in BYOD or Bring Your Own Technology (BYOT) policies in K-12 schools (Ion, 2015).

Additionally, Microsoft recently got hit by cyberattacks in 150 countries around the world in 2018 alone, and warned that these attacks have been a wakeup call. Microsoft also blames the government for not disclosing the vulnerabilities that have caused widespread damage around the world. According to Microsoft, viruses are known to exploit the flaw in Microsoft Windows, which was first identified by US intelligence. The virus captures the user's file and demands payment. Mirai malware exploitation and WannaCry ransomware attacks were other attacks that made news this year.

According to the FBI’s 2015 public service announcement, alert Number I-091015-PSA, IoT presents opportunities for cybercrime as more businesses, educational institutions, and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences. Their connection to the internet increases the target space for malicious cyber actors. IoT and wearable devices are connecting node and hub for communication in eLearning or educational technology, incorporating all forms of online instruction using personal devices (Behera, 2013; Coleman, 2015; Souppaya & Scarfone, 2013; Tymoshy, 2016; Williamson, 2010).

A challenge in choosing interventions to avoid cyberthreats in IoT, mobile learning, and wearable devices in education is that there is no clear model to follow. The online learning environment involves using a broad range of IoT, MLD, and wearable technology from many devices, scattered worldwide, making them difficult to track (Deng, Chai, Tsai, & Lee, 2014; Jonassen, Howland, Marra, & Crismond, 2008). In the process, they can either infect another colleague, or get infected by the member, or via the educational network while accessing learning and educational resources. This susceptibility calls for intervention strategies. According to a study done by the Ponemon Institute, (2011) non-compliance of institution cybersecurity policies cost institutions more than 2.66 times that of maintaining compliance. The study recommends more peer writers from education to cover the topic and the use of training instead of following the Laing & Hue (2009, 2010) model. At this stage, students and instructors need to know the danger of using multiple technologies as they enhance their learning and teaching experiences. This can be done by organizing training to create awareness of the threat of malicious software and cybercriminals, and to encourage the students, faculties, and staff members to use software like Malwarebytes or Microsoft Defender, or alert student to install them. This will help avoid the risk of getting attacked, and enhance safety by abiding by AUP and COPPA policy set to guide and protect students while online (CDE, 2017).

Conclusion

IoT, MLD, and wearable devices are frequently misused by students, faculty, and staff members who are not fully aware of the cyber danger. These stakeholders need to be aware of the existence of cyber dangers via training, publication, and attendance of trade shows where these topics are discussed. Additionally, they need to be aware of what the market is offering to students and the potential threat these devices might be having, and how to mitigate the risk. It is clear from the available literature that the cybersecurity threat in educational institutions has been shown through numerous studies to be rapidly increasing, and that if educational institutions, students, staff, and faculty members do not institute the proper safeguards and best practices, cyberattacks will only continue to increase in education, which could have social and economic impacts.

Cybersecurity is concurrently integrated with technology in an era where public and personal devices and IoT share inter-connection. Most of the ransomware attacks and traits involve global attacks using IoT, MLD, and wearable technologies using ransomware. It is a problem that does not currently have an adequate remedy. Attacks move from country to country, and spread from institution to institution. There are no universal methods of intervention to mitigate and curb the attacks, due to the relative novelty of the phenomenon. Few science and engineering journals are just beginning to explore and document them, and for now I recommend that all educational practitioners explore more science and engineering journals and share the information with educational institutions, member of the faculties, students, and staffs and collaborate, with FBI and use services provided by regional organization like Finger Lakes Technologies, Group, Inc. There are plenty of online technical reports, and research requiring the subscription to these non-academic corporate institutions. As a recommendation, weekly training is a good start for the professional staff. Awareness of the acceptable use policy AUP would make the whole organizations safe. More examples of recommended procedure for educational institutions are provided in the appendix of this study.

It is recommended that stakeholders should monitor FBI public service announcements regularly. Currently, the FBI estimates that the costs of ransomware have reached an all-time high. They also warned that last year cybercriminals had collected over $209 million in the first three months of 2016 by threatening businesses and institutions to unlock their computer servers (Fitzpatrick & Griffin, 2016). To be safe and protected, users must obtain the latest information by subscribing to significant publications from software vendors like Symantec, IBM, Microsoft, Malwarebytes and research bodies such as Gartner, IDG, and much more for the latest global cyber landscape. Most of the information regarding cyberthreats and intervention can be obtained by subscription to the major agencies and service providers mentioned above regarding any form of anomaly worldwide. Government agency like FBI can be of help.

According to FBI 2015 the public service, announcement alert Number I-091015-PSA, for example, IoT poses more threats to businesses, educational institutions, and homeowners since most the users use web-connected devices online without knowing the threat facing them. In education students, faculties and staffs are using IoT, and wearable devices are to connect to the institution node and hub for communication in eLearning or educational technology and cloud service. New technology like Cisco Spark devices relies on IoT using cloud service (Behera, 2013; Coleman, 2015; Souppaya, & Scarfone, 2013; Tymoshy, 2016; Williamson, 2010).

For practitioners, there is a need to be aware that the world’s mobile user population has reached 1.3 billion as reported by Wire Magazine, (2012, p.93) and that they should be aware of the danger this may present to users. According to Wired Magazine, the average cost of data breaches reached $5.5 million in 2011. According to Wired Magazine (2012), in the USA, the number of corporate entities using online classes grew from 4% to 77% in 2011. Friedman, Daniel, and Hoffman, (2013), Williamson, (2010), in their studies, acknowledged that mobile devices such as laptops, tablets, and cell phones had become essential tools both for enterprise productivity, and in education.

Quirolgico et al. (2015), warned that the use of mobile apps could potentially lead to serious security issues because mobile devices and apps may contain software vulnerabilities that are susceptible to hackers. Such vulnerabilities may be exploited to gain unauthorized access to an organization's information or an individual's privacy. Training in awareness of AUP; introducing cybersecurity in the pedagogy beginning from K1-Higher education; using automation for monitoring the network analysis and reporting; collaboration with resourceful institutions; sharing knowledge base; transparencies about the threat; and ensuring the intellectual properties; students' information is the recommended approach to keeping institutions and personally identifiable information safe from ransomware.

References

Alkhalaf, S., Amasha, M., & Al-Jarallah. A. (2017). Using m-Learning as an effective device in teaching and learning in higher education in Saudi Arabia. *International Journal of Information and Education Technology, 7*(6). Doi: 10.18178/ijiet.2017.7.6.903

Akella, D. (2012). Creating a community of learners online: Connect, engage & learn. *International Journal of Technology in Teaching and Learning*, *8*(1), 63-77.

Anderson, J., & Rainie, L. (2014). The future-of-the-internet. Retrieved from http://www.pewinternet.org/topics/future-of-the-internet/.

Baran, E. (2014). A review of research on mobile learning in teacher education, *Journal of Educational Technology & Society*, *17*(4), 17–32. Retrieved from http://www.ifets.info/journals/17_4/2.pdf

Behera, S.K (2013). M-Learning: A New Learning Paradigm. *International Journal on New Trends in Education and Their Implications*, *4*(2), 24-34. Retrieved from http://www.ijonte.org/FileUpload/ks63207/File/03.behera.pdf

Bernsteiner. R, Kilian, D, Ebersberger, B (2016). Mobile cloud computing for enterprise systems: A conceptual framework for research. *International Journal of Interactive Mobile Technologies*, *10*(3), 72-76. doi: http://dx.doi.org/10.3991/ijim.v10i2.5511

Beyer, C. (2014). Mobile security: A literature review. *International Journal of Computer Applications, 97*(3). doi:10.5120/17025-7315.

Brown, T. H., & Mbati, S. (2015). Mobile learning: Moving past the myths and embracing the opportunities. *The International Review of Research in Open and Distributed Learning, 16*(2). Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/2071

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Chatterjee, S., Saker, S., & Valacich, J. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT Use. *Journal of Management Information Systems, 31*(4), 49–87. doi: 10.1080/07421222.2014.1001257.

Chang, F. (2012), The next wave, introducing the federal cybersecurity. *R&D Strategic Plan, 19*(4). Retrieved from https://www.nsa.gov/research/tnw/tnw194/articles/pdfs/tnw_19_4_web.pdf

Chen W., Lee, C., Tan, A., Wettashge, M., & Wong, P. (2012). From device centric to people centric ubiquitous computing: Pre-service teachers using technology across spaces, Asia-Pacific Society for Computers in Education. *Research and Practice in Technology Enhanced Learning, 7*(1), 45-60.

Chitanana, L. (2012). Bandwidth management in universities in Zimbabwe: Towards a responsible user base through effective policy implementation. *International Journal of Education and Development using Information and Communication Technology, 8*(2), 62-76. Retrieved from http://www.eric.ed.gov/fulltext/EJ1084130.pdf

Chitanana, L. (2015). Bandwidth Management in the era of bring your own devices (BYOD). *The Electronic Journal of Information Systems in Developing C+ –countries, EJISDC* (2015) 68, 3, 1-14, Retrieved from

Ciampa, K. (2014). Learning in a mobile age: An investigation of student motivation. *Journal of Computer Assisted Learning, 30*(1), 82–96.

Creswell. J. W., Plano Clark, V. L. (2011). *Designing and conducting mixed methods research* (2nd ed.). Thousand Oaks, CA: Sage.

Custer, W. L. (2010). Information security issues in higher education and institutional research. *New Directions for Institutional Research, 2010*(146), 23-49. doi: 10.1002/ir.341.

Deng, F., Chai, C. S., Tsai, C. C., & Lee, M. H. (2014). The relationships among Chinese practicing teachers' epistemic beliefs, pedagogical beliefs, and their beliefs about the use of ICT. *Educational Technology & Society, 17*(2), 245–256. Retrieved from http://www.ifets.info/journals/17_2/20.pdf

Dlodlo.N. (2012). The internet of things technologies in teaching, learning and basic education management. *CSIR Meraka Institute*. Retrieved from, http://researchspace.csir.co.za/dspace/bitstream/10204/6017/1/Dlodlo3_2012.pdf

Doanea, A. N, Boothe, L. G, Pearson, M. R, Kelle, M. L (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior, (60),* 508–513. doi: http://dx.doi.org.proxy1.ncu.edu/10.1016/j.chb.2016.02.010

Dodge, A. (2009). Educational Security Incidents (ESI) year in review 2008. Retrieved from http://www.adamdodge.com/esi/year_review_2008.

Educause (2005). Seven things you should know about Wikis. Retrieved from https://net.educause.edu/ir/library/pdf/ELI7004.pdf

El-Hussein, M. O., & Cronje, J. C. (2010). Defining mobile learning in the higher education landscape. *Educational Technology and Society*, *13*(3), 12-21. Retrieved from http://www.ifets.info/journals/13_3/3.pdf

Elhai. J. D., & Hall, A. B. (2016). Anxiety about internet hacking: Results from a community sample. *Computers in Human Behavior*, *54*(2016). doi: http://dx.doi.org/10.1016/j.chb.2015.07.057.

Elliott. (2010). Botnets: To what extent are they a threat to information security? *Information security technical report, 15*(2010), 79-l03. doi: 10.1016/j.istr.2010.11.003

Executive Order no. 13636, (2013). Improving critical infrastructure cybersecurity, DCPD-201300091. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Garrison, D. R. (2011). *E-learning in the 21st century: A framework for research and practice* (2nd ed.). London, UK: Routledge/Taylor and Francis.

Haag, J. (2011). *From eLearning to mLearning: The effectiveness of mobile course delivery*. Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2011. Retrieved from, http://elearningb Jason Haag rothers.com/mobile-eLearning-express/

Halpern, J. (2014). The future-of-the-internet, Pew Research Center. Retrieved from http://www.pewinternet.org/topics/future-of-the-internet/

Hassan, W. U., Nawaz, M. T., Syed, T. H., Arfeen. M. I., Naseem. A., & Noor. S. (2015). Investigating students' behavioral intention towards adoption of mobile learning in higher education. *Institutions of Pakistan, Technical Journal*, *20*(3), 34-47. Retrieved from http://web.uettaxila.edu.pk/techjournal/2015/No3/TECHNICAL_JOURNAL_VOL_20_NO_3.pdf

IDG connect (2016). How IoT companies can learn from the Mirai malware exploitation. Retrieved from http://www.idgconnect.com/blog-abstract/22940/how-iot-companies-learn-mirai-malware-exploitation

Jonassen, D., Howland, J., Marra, R., & Crismond, D. (2008). *Meaningful learning with technology* (3rd ed.). Upper Saddle River, NJ: Pearson.

Jones, B., & Heinrichs, L. (2010). Exploring mobile device security policies in higher education. *Issues in Information Systems, 11*(1), 204-210. Retrieved from http://iacis.org/iis/2010/204-210_LV2010_1470.pdf

Kearney, M., Schuck, S., Burden, K., & Aubussun, P. (2012). Viewing mobile learning from a pedagogical perspective. *Research in Learning Technology, 20*.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and Challenges for enterprises. *Horizons*, *58*, 431-440. doi: http://dx.doi.org/10.1016/j.bushor.2015.03.008Business

Lee, H., Lee, W. B., & Kweon, S. C. (2013). Conjoint analysis for mobile devices for ubiquitous learning in higher education: The Korean case. *TOJET*, *12*(1).

Liang, H., & Xue, Y. (2009). Avoidance of IT threats, a theoretical perspective. *MIS Quarterly, 33*(1), 71-90. Retrieved from http://dl.acm.org/citation.cfm?id=2017417

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413. doi: 10.1.1.170.5816&rep=rep1&type=pdf

Loraas, T. M., Crossler, R. E., Long, J. H., & Trinkle, B. S. (2014). Understanding compliance with BYOD (bring your own device) policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226. doi: 10.2308/isys-50704 Spring 2014 pp. 209– 226.

Lloyds. (2017). Cyber risk cybers secure. Retrieved from https://www.lloyds.com/

Martin, R., McGill, T., & Sudweeks, F. (2013, July). *Learning anywhere, anytime: student motivators for m-learning.* In Proceedings of the Informing Science and Information Technology Education Conference (pp. 51-67). Informing Science Institute.

McGuire. M., & Dowling, S. (2013). Cybercrime: A review of the evidence research report 75. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

Mock, T., & Paden, K. (2015). Organizational risks and the Internet of Things. Retrieved from http://er.educause.edu/blogs/2015/10/organizational-risks-and-the-internet-of-things

Moreira, F., Ferreira, M. J, Santos, C. P., & Durão, N. (2016). Evolution and use of mobile devices in higher education: A case study in Portuguese Higher Education Institutions between 2009/2010 and 2014/2015. *Telematics and Informatics, 34*(6), 838-852. http://dx.doi.org/10.1016/j.tele.2016.08.010

Mueller, J. Wood, E., & De Pasquale, D. (2012). Examining mobile technology in higher education: Handheld devices in and out of the classroom, *International Journal of Higher Education*, *1*(2). doi: http://dx.doi.org/10.5430/ijhe.v1n2p

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials, 16*(1). doi: 10.1109/SURV.2013.042313.00197

Pereira, R. E., & Rodrigues, J. P. (2013). Survey and analysis of current mobile learning applications and technologies. *ACM Computing Surveys, 46*(2). doi: 10.1145/2543581.2543594

Nahorney, B. (2015). Cyber security threat analyst for Symantec. *Symantec Intelligence Report.* Retrieved from https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_09-2015.en-us.pdf

Pearson. (2015). Student mobile device survey national report: College students. Retrieved from http://www.pearsoned.com/wp-content/uploads/2015-Pearson-Student-Mobile-Device-Survey-College.pdf

Ponemon Institute. (2013). How employees are putting your intellectual property at risk. Retrieved from https://www4.symantec.com/mktginfo/whitepaper/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf

Ponemon Institute. (2011). Smartphone security survey of U.S. consumers. Retrieved from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Pegrum, M., Oakley, G., & Faulkner, R. (2013). Schools are going mobile: A study of the adoption of mobile handheld technologies in Western Australian independent schools. *Australasian Journal of Educational Technology, 29*(1).

Rajasingham, L. (2011) Will mobile learning bring a paradigm shift in higher Education? *Education Research International, 2011.* doi: 10.1155/2011/528495

Rajewski, J. (2013). Cyber security awareness - Why higher education institutions need to address digital threats. Retrieved from http://www.huffingtonpost.com/jonathan-rajewski/cyber-security-awareness_b_4025200.html+

Rathore, S. (2015). Steganography: Basic and digital forensics. *International Journal of Science, Engineering and Technology Research, 4*(7). Retrieved from http://ijsetr.org/wp-content/uploads/2015/07/IJSETR-Vol-4-Issue-7-2589-2593.pdf

Saini, M., & Saini, G. (2014). Steganography & tools used for steganography. *International Journal of Scientific & Engineering Research, 5*(1). Retrieved from https://www.ijser.org/researchpaper/Steganography-tools-used-for-Steganography.pdf

Federal Bureau of Investigation Cyber Division. (2014). Health care systems and medical devices at risk for increased cyber intrusions for financial gain. Retrieved from https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication 800-124 Revision 1 US Department of Commerce*. doi: http://dx.doi.org/10.6028/NIST.SP.800-124rl

Taylor, C. A. (2011). *The mobile literacy practices of adolescents: an ethnographic study* (Doctoral dissertation, Monash University).

The Center for Digital Education (CDE) (2017). Preparing for the inevitable strategies to help higher education protect data. Retrieved from www.centerdigitaled.com

Thierer. A. (2015). The Internet of Things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Richmond Journal of Law and Technology, 21*(2). Retrieved from http://jolt.richmond.edu/v21i2/article6.pdf

Thierer. A. (2013). Privacy and security implications of the Internet of Things. Retrieved from http://mercatus.org/publication/privacy-and-security-implications-internet-things

Tsinakos, A. (2013). State of mobile learning around the world, China Central Radio & TV. Beijing, China: University Press.

Tymoshy, N. (2016). The most vulnerable device at risk in the industry are IoT and wearable devices. Retrieved from https://www.softserveinc.com/en-us/

Whatis (2014). Presentation software (presentation graphics). Retrieved from http://whatis.techtarget.com/definition/presentation-software-presentation-graphics

Won, K, Ok-Ran, J, Chulyun, K, & Jungmin, S. (2011). The dark side of the Internet: attacks, costs, and responses. *Special Issue on WISE* 2009 - *Web Information Systems Engineering, Information System*s, *36*(3), 675-705. doi: 10.1016/j.is.2010.11.003,

Quirolgico, S., Voas, J., Karayiannis, M., & Scarfone, K. (2015). Vetting the security of mobile applications, *NIST Special Publication 800-163, U.S. Department of Commerce, National Institute of Standards and Technology*. doi: http://dx.doi.org/10.6028/NIST.SP.800-163

Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., ... & Cousin, P. (2013). Internet of things strategic research and innovation agenda. *River Publishers Series in Communications, 7.*

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K.(2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks, 7*(12), 2728-2742. doi: http://dx.doi.org/10.1002/sec.795S

Appendix

Recommendation for Training Lesson plan for Cybersecurity

Learning Objective

-To create an understanding of AUP, cyber security, forensic investigation, preservation and analysis

-To gain knowledge of the cyber threat, attack techniques, tools, and analysis

Topic Outline

- Cyber security concept, methods, and tools

- Learn investigation, preservation, and analysis

-Types of cybersecurity threats and attack techniques

Anatomy of cybersecurity attack process

- Identify and isolate processes

- Automation and modularization

- Documentation

- Sharing a knowledge base

Instructional practice and strategies

- Presentation of information

- Active lab work and learning

- Team work

Software tool

- Stools4, File Checksum integrity verifier (FCIV) Netflow

Key Indicator of Cybersecurity process

- Recognition of cyber security principles involved

- Basic knowledge of evident preservation

- Basic knowledge of cyber analysis

- Learn about steganography (Rathore, 2015; Saini & Saini, 2014).