The International Journal Of Engineering And Science (IJES)
|| Volume || 5 || Issue || 4 || Pages || PP -01-10|| 2016 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Overview of Cyber Security: Endangerment of Cybercrime on Vulnerable Innocent Global Citizens

Dr. Joseph O. Esin
Lead Professor of Computer Information Systems Jarvis Christian College, Hawkins, Texas USA

ABSTRACT

The global community is filled with uncertainties and constant threats of cybercrime, global economic collapse, social and economic insecurity. The evolving issue of cybersecurity will soon have far reaching economic consequences on our connected global society. Leaders of developed and developing nations must be prepared to launch protective plan of action against perpetrators of cybersecurity attacks. In the past, regular mail systems and fax machines were used for data and documents transmission and Radio network was used for local, national and international communications. Today, the culture of high definition television, broadband-direct connection, electronic mails, Internet access, and cyber technology has taken over the global transmission and communication operations. Cyber-technology is progressing at an overwhelming pace, posing an ever-present danger to all segments of innocent global populaces. Current researchers, such as Rejesh, (2013), Shinder (2008) and Enghelberg, (2003) recommends the creation of global collaborative partnership (GCP) to provide strategies and commanding directives to provide stable security for vulnerable global residents. The Paris and San Bernardino attacks on innocent citizens are a forewarning to leaders of developed and developing nations to create cyber security-savvy workforces to prevent future tragedies. As a part of GCP ground strategy, software developers must develop preemptive built-in capabilities to deter cybercriminals.Cyber-crime is affecting the physical existence of innocent citizens of the global society and it is a devastating threat. In isolation, individuals, government agencies, corporate organizations, financial institutions and higher education systems are vulnerable to cybercriminals. The most credible and reliable techniques to defeat perpetrators of cybercrime today and tomorrow, must include the implementation of a united front to work together through trust, dedication and commitment. The threats of cybersecurity are penetrating all segments of world organizations and educational settings.

The culture of the education enterprise is the exchange of ideas, values, beliefs, cultural backgrounds, instruction and learning process. Presidents, vice-chancellors, professors, instructors, allied educators are strongly encouraged to create plan of action to protect vital data, information and infrastructure of the entire educational facilities from cyber-attacks. The unforeseen incidences in Paris, France and San Bernardino, in California, United States is an enduring development and a commanding steps empowering national and higher education leaders, professors, instructors and allied educators to implement a well-structured plan of action, effective security measures and workforces to dismantle perpetrators' malicious intent to destroy the entire institutions of human civilization.

Date of Submission: 01 April 2016 Date of Accepted: 14 April 2016

I. INTRODUCTION

The world has been reduced today to a global village or community through the invention and continuous improvement in communications. This advancement in cyberspace has brought along with itself the concomitant progress in education, economic growth and political collaboration and cooperation. However, these advances have at the same time almost empowered criminals and terrorists to avail themselves of this ease of communication to create and disrupt the continuous progress of humanity. Each supplication in advancement has brought with it a similar degree, if not more of criminal growth. Cyber-criminals are becoming sophisticated and more determined on a daily basis to undermine the relative peace in which these developments can best be enjoyed and encouraged. Consequently, each thought about a new development in progress must be conceived along with a parallel development of methods to counteract and circumvent criminal attempts to undermine and turn these developments against the citizens they were supposed to serve. Mcintosh, Petries and Rejesh (2013), in their study on treasury and trade solution, noted that the implementation of tight and effective security measures is imperative to decrease cybercriminals' scheming strategies in a digital society. Digital services require commanding security measures to guarantee transmission of data, information and network system resources. The majority of cybercrimes and their associate threats, according to Mcintosh, Petries and Rejesh (2013), are intrusion activities where attackers are naturally located outside and within the outskirts of organizations. Security attacks rarely come from within the organization or from individuals who are vested and entrusted with confidential data and information, security apparatus and inclusive transactions of the system.

Current researchers on cybercrime and cyber security such as Mcintosh, Petries & Rejesh, (2013), Shinder (2008) suggested that government agencies, corporate organizations, financial institutions and higher education systems must implement operational behavior analysis tools to flag anomalies in network activities of employees and to monitor when behavior falls outside the scope of their regular duties and access rights. As a result, operational behavior analysis tools were designed to monitor internal cybercrime and abnormalities amongst current employees (Shinder, 2002).The process enables institutions to stop employees from stealing intellectual property or destroying data since the alerts are activated in real-time as the employee is engaging in unauthorized activity on the network. It is logical to conclude that operational execution and monitoring of employee's behavior analysis will definitely minimize the alarming rate of stealing intellectual property, confidential data, and classified information by current employees and perpetrators of cybercrime.

II. CYBERSECURITY OPERATIONS

Computer security is a process of preventing unauthorized computer access, including changing and destroying data and information on organization network system and security breach. A security breach involves the unauthorized computer network access such as unapproved access to individual and organization emails, financial data, and malicious shut down of organizations' network file servers. In response to this vulnerability, cybersecurity has been developed to circumvent the theft of information and harm effected on vulnerable citizens by the criminals. This cybersecurity is the collection of technologies, procedures, developments and activities designed to protect networks, computers, devices, software programs, resources, information and data from attack, damage and access by unauthorized users. It is a challenging task because it is difficult to coordinate an effective response due to the unexpected nature of cyber-attack. . Cyber security is directly related to measures used to protect and control the flow of outgoing and incoming data and information into other nations and organizations. Government agencies, military, corporations, financial institutions, healthcare industries, and educational enterprises tend to maintain and store large amounts of confidential information on computers and transmit data across networks to other computers. With the growing volume and sophistication of cyber-attacks, urgent attention is required to protect sensitive information from being uncovered or proselytized.

Long ago, the world community operated very well in peace, calm, and quiet, in a relaxed, stress-free environment using dial-up telephones for communication. Regular mail systems and fax machines were used for transmission and communication, and the radio system for local, national and international news. The culture of high definition television, broadband-direct connection, electronic mail and the Internet access, cyber technology, telemedicine, telesurgery, cyberbullying and cyberstalking has taken over the global transmission and communication operations. The exponential growth of cyber-technology has inadvertently forced inventors and citizens to concentrate on these developments at the expense of the lapses in security, posing threats to innocent residents of all segments of the global community. These lapses in security led to the perpetuation of three major disasters in this century- on September 11, 2001 attacks (code-named 9/11) in New York, Pennsylvania, the District of Columbia in United States, on November 13, 2015 in Paris, France and on December 4, 2015 in San Bernardino, California, United States.

The three incidents, in addition to other minor ones, awakened in the citizens an awareness of the reality of the evil intentions of criminals and the need to implement well-thought-out plans of action of active security measures to dismantle or prevent cybercriminals' malicious intent to destroy the entire institutions of human development. A closed reflection on the three horrified snapshots depicted below clearly confirms the possibility of the loss of many lives during unexpected cybercriminal attacks. In order to interrupt and put an end to cybercrime, the world nations, members of the legislative branch of the government and Human Intelligence, must be fully united, and resolute on a common front of confrontation against heartless cybercriminals.

The World Trade Center burns after being hit by a plane in New York in this file photo on September 11, 2001

November 13, 2015 in Paris, France

December 4, 2015 in San Bernardino Attack, California, United States

In the current technology-engendered and the internet-provoked community, threats of cybersecurity are the heart of everyday and everywhere newscast, television broadcast, news bulletin and radio talk show. Cybersecurity and associated threats are a common topic of conversation. Institutions, organizations and government agencies notify employees not to open unsure and indefinite emails and to create resilient private passwords and use other well-thought-out techniques to protect organization data and information. According to **insecpro.com,** there are approximately 556 million cyber victims per year, and an excess of 1.5 million victims on a daily basis, more than 232 million characteristics exposed, and as many as 120,000 repetitive charges of creating and sending spam and infected email messages, code-named Botnets "zombie" each day (Enghelberg, 2003).

Further exploration of **www.insecpro.com/index.php/cyber-crime-statistics** reveals the discoveries of infographic data confirming that in 2013, fifty-nine percent (59%) of ex-employees admitted to stealing organization's data and information when leaving previous jobs. The episodes in Paris and San Bernardino serve as double-crossing and disloyal point of reference against the institution of human civilization. These events have threatened the security of innocent global citizens and also placed law enforcement officers and various branches of state and federal government on ready-to-act mode. Therefore, leaders of the unified global community, legislative units, chief executive officers and decision makers of public and private organizations are strongly encouraged to acknowledge the looming cyber threats. The international environment is entrenched in uncertainties and constant threats of cybersecurity, global economic disaster and social prosperity challenges. The continuous existence of cybersecurity threats is on the brink of creating far reaching economic consequences on connected global society. Consequently, world leaders must be willing and ready to become tenacious drivers for adequate ground-breaking protective plan of action against digital invasion. The impact of the threats of cybersecurity include disruption of legitimate operations, denial of service, sabotage, direct financial loss, reputational damage, loss of attractiveness, theft of trade secrets, and the lack of trust among customers, employees, shareholders and business partners.

III. COMBATING THREATS OF CYBERCRIME

Perpetrators of cybercrimes are deep-rooted in cyber fraud, cyber sabotage, and cyber-espionage, and in asymmetric and traditional type of maximum cyber-threats against the innocent global citizens. The alarming rate of the looming cyber security threats is supported by the use of associate cyber-devices such as smartphones, Internets, emails and microcomputers. In fact, every nation has exclusive sets of rules and procedures to enhance cyber security against these threats. The established rules must be systematic to include manufacturers of computer operating systems (OS) and computer network operating systems (NOS). In a never-ending and long-lasting global confrontation with perpetrators of cyber security threats, hardware, software, emails and internet manufacturers and providers must become active members of the collaborative attempt to defeat all agents of cyber threats. The hardware, software, emails and internet manufacturers are distributing millions of technologies, such as emails, smartphone, and internet with cyber-scam capability which, unfortunately, are now used as armament by cybercriminals. The international community is going through serious stressful conditions and global leaders and their counterparts cannot ignore undisclosed variables that are playing a key role in propagating global conflict. Majority of cyber terrorist operations are now transmuting into encryption format equipped with improved cyber-technologies, code-named asymmetric, and ready to carry out unsympathetic attack on innocent citizens.

Threats to humankind, which is analogous to cybercrime, have been in existence from the beginning of our human civilization. The institution of human civilization has witnessed instability, mayhem and turbulence from creation up to the present time. The human race has lived through biblical conflict between Cain and Abel, Esau and Jacob and rebellious encounters from the era of Sparta, Alexander the Great, Pompeii, Julius Caesar, Genghis Khan, Napoleon, Wellington, Allenby, World War I, World War II, Yom Kippur, 1982-Falklands, 1990-Iraqi War, 2001-New York, 2015-Paris and 2015-San Bernardino terrorist attacks. The above-mentioned list of ill-disposed confrontations posited that cybersecurity threats are opening new outlets of conflict and war with impunity, pushing global leaders to adopt and implement collaborative data, information collection, and sharing to combat the threats against humanity. Cybercriminals are hard-hearted, outdoor-prisoners with all-out punitive intentions to carry out suicide bombings, targeting innocent residents and social gatherings. In order to interrupt and put an end to cybercrimes, leaders of the world nations are strongly urged to be fully united in all-inclusive measures to terminate perpetrators of cybersecurity. They need full collaboration, money, trained personnel and citizens who are alert to the real danger of cyber insecurity and attack. Indeed, cyber activities are borderless, for they exist and are executed across national and geopolitical borders. Hence, there is grave need to approach this crime from this perspective of “borderlessness” (Popescu, 2016).

IV. FRAMEWORK OF CYBERCRIME

The 24 hours a day, 7 days (code-named 24/7) network connections tend to provide cybercriminals contented access and adequate time to freely plan to gamblewith user name, password and figure out the type of transmission control protocol (TCP) and user datagram protocol (UDP) ports that are vulnerable to crime perpetrators. Undoubtedly, since the assigned (IP) address tends to stay the same and unchanged, it is almost stress-free for perpetrators of cybercrime to launch heartless attacks on wireless network systems. The unhindered and unlimited direct access is engrained with increased connectivity speed. The normal dial-up and analog modem is limited to 56Kbps, with a connectivity speed virtually which is seemingly inexpensive, slow and time-consuming. However, the speedy emergence of direct access communication hasempowered wired and wireless cable manufacturers to offer higher download speeds and higher upload speed operations. Mcintosh, Petries, and Rejesh, (2013) and Shinder (2008), noted that transfer rates at all phases of direct connections, regardless of carriers and manufacturers, should be limited to 128Kbps by wired cable providers and anywhere from 128Kbps to 764Kbps by direct connection providers.

The process of sharing actionable data, information and acquisition of intelligence is inevitable in attempts to bridge the gap to stop the distribution threats of cyber security to organizations and defenseless personnel and infrastructure (Kim 2004, and Chen & Whisnant 2002). This strategy calls for to the sharing of acquired data against threats of cybersecurity, tenacity to implement world-wide 24-hours monitoring systems to dismantle perpetrators of cybersecurity and pre-emptive and proactivemeasures to defeat them everywhere and to become the watch words of all leaders. All-inclusive hard work must include empowerment of law enforcement officials, intelligence collection operations and sharing of information directly related to imminent danger. Due to the consistently invisible and persistent cyber-crime, culprits of such undertakings must be detached from global organizations. The world communities must persistently be attentive, alert and ready for instantaneous response to cyber security threats. Alertness, readiness, and willingness play a key role in adopting the Executive Order (E.O) 13636 signed by the President of the United States, which lays a lot of emphasis on collaboration and quick response:

The U.S. Government has developed systems and procedures to increase the timeliness and quality of cyber threat information shared with at-risk private sector entities. We are placing great emphasis on unity of effort by agencies with a domestic response mission.”

V. CYBERCRIME IN EDUCATIONAL SETTINGS

The threats of cybercrime are penetrating all segments of the world, and education settings are no exception. The culture of the education enterprise involves the exchange of ideas, values, beliefs, cultural backgrounds, instruction and learning endeavors. Presidents, vice-chancellors, professors, instructors, school district superintendents, principals and allied educators are strongly encouraged to create measurable plans of action to protect vital data, information and infrastructure of the entire educational facilities from misuse or abuse. In the process, these administrators and associated stakeholders must be prepared, ready and willing to establish compliance and regulatory standards to effectively combat threats of cyber security.

The concept that threats of cybercrime is the responsibility of information technology (IT) unit is a myopic and inaccurate approach to the problem. It is an escapist approach to avoid confronting real issues. The credible vehicle to comprehensive cybersecurity measures is to enlist the support of every unit of the organization and engage them as allies in the process of safeguarding the organization. The consequence of doing nothing is much greater than the charge of putting adequate cyber security measures in place to combat threats of cybercrime and breach of confidentiality. The projected measures must involve various segments of the organizations, such as fiscal affairs and human resources units to help in establishing stable cyber liability insurance and benefits, and synthesized agreement with outside vendors to protect organizational financial records. The present-day display of threatening and intimidating emails of December 12, 2015 led to involuntary academic break-ins in two of the largest school districts of the U.S.A. -- Los Angeles, and New York.

The stability of the higher education institutions is being threatened by the outbreak of cybercrime threats on a frequent basis. There is great support for the expansion of computer science and computer information technology degree programs in the colleges and universities. However, the projected growth and new course offerings must include courses such as introduction to threats of cybercrime, cyber security network, computer forensics and investigations. The digital age is creating series of digital changes and data breaches for institutions of higher education across the globe. The increased sophistication of cybercrime threats is related to the emergence of new technologies affecting how data and information are backed-up, stored, retrieved and maintained.

Academic deans of computer science (CS) and computer information technology (CIT), (code-name, computer information systems (CIS)),are strongly encouraged to establish an instructional academic alliance with experienced personnel from a number of law enforcement units, including police officers, state troopers, Homeland Security, Central Intelligent Agency (CIA),and Federal Bureau of Investigation (FBI) as official guest-instructors operating at the supervision of full-time CS, CIT or CIS professors. This collaboration will provide the students and staff with the requisite information from experts who deal with these threats on a daily basis. This information sharing will be a first step toward combating cybercrime. Cyber criminologyis a fairly new development designed to provide adequate skills and expertise to investigate and prevent intrusions of security protocols in computer network systems. Upon successful completion of new cyber security studies, graduates will acquire expertise to protect institutions of higher education against threats of theft and misuse of critical information and vulnerabilities by assisting with forensic analysis of cyber incidents.

Strategies to prevent and protect against cybersecurity attacks must be supported by human and financial resources. Due to rapid growth of cyber security, the majority of organizations suffer from inadequate financial sponsorship and fragmented cadre of professional development programs. Hoffman, Burley and Toregas (2011), in their empirical research on cyber security, posited that unending professional education development must be adopted as a national security project by national and state governments, organizations and academic stakeholders. Unfortunately,there is no first-hand evidence and documentation on how to effectively respond to cyber security attacks. Hoffman, Burley and Toregas (2011) and Honig (2011) noted that the field of cybersecurity today is analogous to 19th century medicine where medical practitioners were often self-taught and, uneven in capabilities. These practitioners functioned within an emerging field directly related to a complex, dynamic and somewhat unpredictable environment with no or limited professional standards for performance.

The development and incorporation of cyber security into the higher education core curricular will help to empower the current and future generations for stronger responses to cyber security attack. The strategy calls for the development of all-inclusive coherent plan of action that involves higher education administrators, academic professors, allied educators, K-12 students, and science and non-science professionals. It is logical to conclude that the culture of cyber security has international components and requires multi-disciplinary method of approach because of the fluid nature of cybercrime. Traditional degree programs naturally take from four to eleven years of studies. Unfortunately, none of these are related to cyber security or measures to respond to cyber security threats.

Due to constant changing nature of the cyber-attacks, Hoffman (2010), Kessler (2013), Kim and Lee (2004) have suggested long term traditional educational approaches with curricula that produce strong, desired skills for market-ready workers that prepare the cyber security worker with a full set of skills that truly address the problem. Such curricula must include curative rather than palliative approach to enable job-specific challenges to be addressed in long term, educational environments. Furthermore, they must inculcate different delivery mechanisms for education modules that take full advantage of today's technology capacity to prepare the cyber security work force of the future.

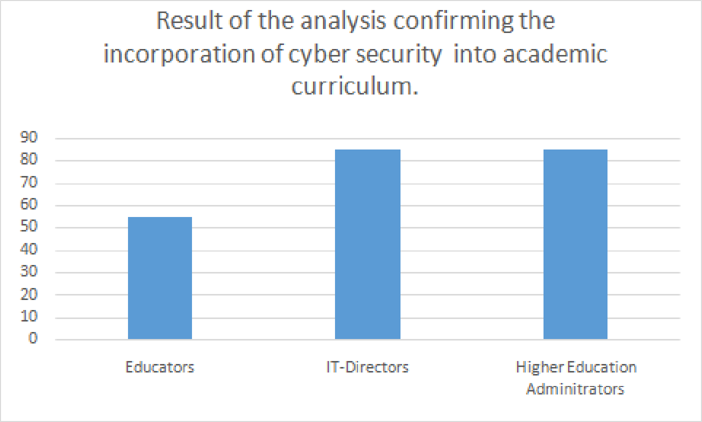
The intent of this article is to formulate guidelines and stratagems that speak to the academic cyber security program designed to include a comprehensive, collaborative and career development preparation approach. Indeed, the academic environment provides strong incentives for research, which stays within fairly rigid discipline boundaries. Cybercriminals operate without notice and the global communities are operating without any point of reference, or classified or unclassified documentation on how to rebuff cyber security attacks on innocent citizens. Hoffman, Burley and Toregas (2011), in their studies on using a holistic development strategy to build the cyber security workforce, annexed the evolution of cyber security attacks to law and medicine professions. They further posited that the culture of the cybersecurity threats requires an enduring step-wise approach designed to provide continuous professional development opportunities and to develop effective educational initiatives in different subject areas. Indeed, the projected universal methodology requires establishing enduring partnership between higher education administrators, professors, allied educators, organizations, federal and states government agencies. Cyber security is a non-environmental initiative and a consequence of computer network, Internet, routers, emails and Web server's revolution.

VI. HIGHER EDUCATION PLAN OF ACTION

Oneof the greatest characteristics about the emerging information technology operations (IT) is the whirlwind pace at which newer, better, faster technologies are spreading across the globe (Shinder, 2008). The evolution of rapid new technologies is entrenched with challenges for IT professionals, end-users, and citizens of the global community. According to Shinder (2008) and Shinder (2002) the new trend of IT has made the situation convenient for cybercriminals, who use computer networks and Internets for a variety of illegal activities. Technologies designed for direct connection such as broadband and wireless computing are deep-rooted with potential to make computer usage suitable and productive. Measurable outcomes and performance should be supported by wide range of dedication and commitment tailored to the sacrifice of security. Cybercriminals are highly savvy in and prepared to use broadband technologies such as digital subscriber line (DSL), cable modem and satellite Internet services to attack wireless network systems. Mcintosh, Petries, and Rejesh, (2013) and Shinder (2002, 2008) noted that computers attached to DSL and broadband networks tend to function differently from dial-up telephone systems. Cybercriminals are more often exploiting new technologies to gain unauthorized access to DSL and broadband network, therefore, broadband and DSL users must be more security conscious than dial-up Internet consumers.

The DSL and broadband networks are based largely on the attractive method of operation, high speed, twenty-four hours and seven days (24-7) connectivity anywhere and anytime. Direct connection network is vulnerable to an attack since it is always connected to an outside network. Long ago, individuals and organizations connected to the Internet using analog modems; perchance, dialup using integrated services digital network (ISDN) connections. In the process, the vulnerability to attacks by cybercriminals was regulated and controlled since the system was available to outsiders only during the time of usage. Upon completion of the normal activities, the network system was disconnected and disappeared from the Internet. The majority of the Internet Service Providers (ISP) use the Dynamic Host Configuration Protocol (DHCP) to assign internet protocol (IP) addresses to dialup users. Shinder (2008) further noted that broadband and DSL are classified as unmatched connected technologies. Unlike analog (dial-up) connections, broadband and DSL, digital operation "code-name" (direct) have helped individuals and organizations to connect to the Internet 24 hours a day, 7 days a week (24/7). Indeed, it makes all phases of data, information, transmission, communication and unrestricted access to the Internet resources faster and more comfortable. Furthermore, the unlimited access has reinforced IT professional ability to install, configure and manage network servers, and to share data and information remotely on the network system.

Early in 2015 the National Cyber Security Alliance (NCSA) conducted and published numerous guidelines to protect everyone at home, university, college and school campuses to include education on cyber ethics, cyber safety, and cybersecurity and computer forensics in the academic curriculum. The objectives of the survey was to search for better understanding and awareness about cybercrime, cyber ethics, cyber safety, cybersecurity and computer forensics as safeguarding and standard requirements for grade and high schools and undergraduate degree programs in the United States (Honig, 2011 &Kessler, 2013). The report of the study revealed a significant disconnect among teachers, administrators, and information technology (IT) specialists regarding the relevance of cyber education in the education settings. Fifty-five percent (55%) of educators strongly agreed to incorporate cyber security into the academic curriculum, but eighty-five percent (85%) of higher education administrators and eighty-five percent (85%) of IT professionals strongly supported the incorporation of cyber security into the educational systems (Honig, 2011).



The cooperative agreement among higher education administrators and IT directors in Henig's study is probable due to the fact that virtually forty-five percent (45%) of educators surveyed by NCSA reported being apprehensive and unprepared to educate students on the sudden incorporation of cyber education into the educational systems. Two third of educators surveyed had not received formal training in cyber education, while only 40% had received only three hours or less of workshop on cyber education. The rationale of this theory was to ensure that educators who prepare students for cyber education are themselves fully competent in applying cyber education. As a consequence, considerable attention must be paid to cyber-related skills and expertise in preparing the new generation for defense against threats of cyber-attack.

Given the increasing threats of cybercrime, it is essential to incorporate cyber literacy initiatives and courses such as networking system security, digital and cybercrime forensics, cyber security law and ethics, cyber security planning and management, intrusion detection and defense, internet technology security at all levels of educational instruction and learning endeavors. The projected initiatives must be supported by adequate personnel and financial resources. Fortunately, cyber-security programs are integrated into some of the United States colleges and universities, where the majority of these classes are offered as technical courses nested within professional certification programs. The Homeland Security Act (2002) mandates academia to take an active role in homeland security education (Bellavita, 2008). The scope of the Homeland Security Act must be viewed as a subset of the broader discipline of information security. The projected paradigms will include defensive mechanisms against threats of cybercriminals and integration of cyber security across academic curriculum. Education is a process of expanding the horizons of individual competencies, specific skills and expertise, critical thinking, systematic understanding of critical life-threatening and horrifying attack by perpetrators of threats of cybercrime. Threats of cyberspace occur in multiple dimensions and gives room to preparation for reactive response to future occurrence, proactive measures to stop the incidence and defensive procedures to protect against activities. Indeed, education is entrenched with defensive paradigm of training learners to become functional, resourceful and task-oriented citizens. Institutions of higher education cannot afford to overlook the act of incorporating cyber security curriculum into the academic course offerings. Cyber education will equip current and future graduates with the needed skills and expertise to protect the institutions and global society against threats of cybercrime.

The threats of cyber security are potentially intricate, aiding the propagation of cybercrime, vulnerabilities and breach of confidentiality. Cyber security threats can be abated through effective management, shared undertakings and wide-ranging participation of organizations' personnel and the general public. Today, policies and procedures of organizations and businessesare saturated with strategies to bring to an end numerous threats of cybercrime, and all projected course of actions must be entrenched with specific standards and guidelines. Organizations' personnel and workforces must be trained and cultured to adjust, comply, recognize and acknowledge the fact that there are no universal stratagems to protect organization data and information against threats of cyber security. Active plan of actions, workshops and professional training against threats of cybercrime must include the general public, private organizations, religious bodies and government agencies. Safeguarding and preventing intrusions into storehouse of data and information is the center piece of any organization system. Grounded on severity and the perpetrators' unwavering determination, individuals, institutions of higher education, organizations and government agencies, must be willing, prepared and ready to share intellectual information, expertise and procedures with low enforcing agencies to battle architects of cyber security threats.

VII. COMBATING CYBERCRIME

Cybercrime measures have encroached and will continue to trespass global international boundaries.Global collaborative partnerships (GCP) are imperative to stop cybercriminals from taking vengeance on innocent members of the world communities because terrorism and cybercrime is an international phenomenon that does not respect boundaries or borders (Popescu 2016). The GCP will serve as ground-breaking landscape for interoperable, consensus and reliable international environment. The adoption and successful execution of GCP will enable global leaders to form a united front to fight perpetrators of cyber security threats, monitor the outgoing and incoming transmission of data and information, and restrict extensive internet freedoms. Immediate and urgent adoption and deployment of improved state-of-the-art cyber-deterrent devices in public and private facilities will provide extra value to enable unified responses to cyber security threats (Kim 2004).

The objective of GCP is to provide strategies and commanding directives to safeguard the well-being of the vulnerable general public. All-inclusive review of Paris and San Bernardino's assault on innocent citizens is an urgent warning and announcement, a wakeup call, to leaders of developed and developing nations to develop cybercrime-savvy workforces. The emphasis of cyber security-savvy workforces (CSSW) must be extended to hardware and software manufacturers. As a part of GCP (G—C---P) ground strategy, software and hardware developers must be encouraged to include preemptive built-in capabilities to deter cyber security culprits' plan to disrupt and interfere with the rights of the world citizens.Threats of cyber security are astonishing digital challenges of the modern time. The culture of digital challenge associated with CSSW is an active process involving parents, professors, allied educators, religious bodies, private organizations and government agencies and a milestone to expand general public awareness of digital savvy threats.

VIII. PROJECTED SOLUTION

Formerly, computers were electronically networked and linked together, where specially -trained personnel, equipped with spying devices, were securely positioned in unrevealed locales, where classified information was stored, and where rip-off information was placed in a mini camera, smuggled out making it very dangerous, overpriced, and backbreaking (Enghelberg, 2003). Today, thousands of cybercriminals are waiting everywhere, around ultramodern computers and surveillance devices with high-resolution display screens in fully air conditioned facilities with capability to detect persons coming in and leaving the property.

Projected solution to this problem of security breach should include fingerprinting of current employees. Exit interviews of former employees must include sworn affidavit not to directly or indirectly engage in cyber-attack and rip-off of classified data and information on the organization's system. This is very important because most cybercriminals tend to have the ability to rip-off classified information millions of miles away from organizations' facilities. Organizations, government agencies and higher education institutions are strongly encouraged to install a well-configured surveillance equipment to monitor and stop cybercriminals.

IX. CONCLUSION

It is a widespread contention that there is no fortified and tenable location to hide from cyber security threats and no simulation remains unaffected from imminent cyber-assault. However, the steps towards containing this vulnerability lie in collaborative efforts to combat threats of cybercrime, vulnerability and to trip-off cybercriminals' attempt to unleash their malicious intents on the innocent citizens of the world. In order to safeguard the global residents from mischievous intents of cybercriminals, nation leaders are strongly encouraged to adhere to global collaborative partnership by supporting strategies to protect the well-being of the vulnerable international citizens. A review of Paris and San Bernardino's physical attacks and untimely loss of lives is a forewarning and reminder to leaders of developed and developing nations to stand firm in defending the world communities against threats of cyber-attacks. These attacks are unpredictable, invisible and devastating to human life, infrastructure and to global civilization and development. The world stands to lose in a few hours what it has struggled for years to invent or construct, if the technocrats and politicians, educators and organizations do not stand form and resolute against those forces of destruction.

CITED REFERENCES

[1]. Assenter M. & Tobey, D. (2011). "Enhancing the Cybersecurity Workforce," IT Professional, (13),1, pp. 12-15. Http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5708280.

[2]. Arthur, M. B.& Rousseau, D. M. (1996). (eds.), "The Boundary less Career: A New Employment Principle for a New Organizational Era," New York: Oxford University Press, http://findarticles.com/p/articles/mi_m4035/is_3_43/ai_53392863/.

[3]. Bellavita, C. (2008). "Changing homeland security: What is homeland security? Homeland Security Affairs Journal. Washington, D.C. Retrieved from , www.hsaj.org/full .

[4]. Cheng, S. M., Lin, P, Huang, W. & Yang, S. R. (2006). A study on distributed and "centralized scheduling for wireless mesh network." International Conference on Wireless Commun. Mobile Computer. (599–604).

[5]. Chen S., Iyer R.,& Whisnant, K. (2002). "Evaluating the Security Threat of Firewall Data

[6]. Corruption Caused by Instruction Transient Errors," In Proceedings of the International Conference on Dependable Systems & Network, Washington, D.C.

[7]. Conway, J., McMillan, M. & Becker, J. (2006). "Implementing workforce Development in Health Care: A Conceptual Framework to Guide and Evaluate Health Service Reform. ," Human Resource Development International, vol. 9, no. 1, pp. 129-139. Retrieved from , http://www.tandfonline.com/doi/abs/10.1080/13678860500522975#preview.

[8]. Esin, J. O. (1991). "High Level of Teachers' Apprehension (HLTA): About the Use of Computers in the Educational Process." Journal of Educational Media & Library Sciences (JEMLS) Vil. 29 No. 1: 15-21.

[9]. -------------(2011). The Evolution of Instructional Technology. Bloomington, IN: I-universe.

[10]. ------------ (2013). "Global Education Reform." Bloomington, I universe, Inc.

[11]. ------------(2014). "The Discovery of Computer Information Technology Is an Avenue For Educational In A Changing Society of Today and Tomorrow." International Organization of Scientific Research-Journal of Engineering. (IOSR-JEN) Vol.4, Issue 12 (1-6).

[12]. Evans, K & Reeder, F, (2010). "A Human Capital Crisis in Cyber Security." Center for

[13]. Strategic and International Studies. Retrieved from http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity.

[14]. Enghelberg, H. (2003). Ciberterrorismo Edicion En Castellano. Biblioteco,Nacional. De Venzuela

[15]. Frenkiel, R. Badrinath, B., Borres, J & Yates, R. (2000) "The infestations

[16]. Challenge: Balancing cost and ubiquity in delivering wireless data". IEEE Pers. Commun., vol. 7, no. 2, (66–71)

[17]. Gupta, S. Islam, Shahinur, N., Kawser, H., Mohammad, S. & Hasan,

[18]. Z. (2012). Design & Implementation of Cost Effective Wireless Power Transmission Model: Good Bye Wires. International Journal of Scientific and Research Publications, Vol. 2, Issues 12.

[19]. Hoffman, L. (2010). "Building the Cyber Security Workforce of the 21st Century:

[20]. Report of a Workshop on Cyber Security Education and Workforce Development," GW Cyber Security Research and Policy InstituteReportGWSPRIhttp://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/20103a%20Building%20the%20Cyber%20Security%20Workforce%20of%20the%2021st%20Century.pdf

[21]. Hoffman, L. J. Burley, D. & Toregas, C.. (2011) "Thinking Across

[22]. Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce." (Report GW-CSPRI-2011-8).

[23]. Honig, D. (2011) "The Importance of Cyber security Training."Journal of Homeland Security Education . Vol. 2 Washington, D.C

[24]. Hoisington, C. (2015). Technology Now. Boston: MA, Cengage Learning Course Technology.

[25]. Huang, H & Valenzuela, R. (2005). "Fundamental Simulated performance of downlink

[26]. fixed wireless cellular networks with multiple antennas in Proc". IEEE 16th Int. Symp. Pers. Indoor Mobile Radio Commun vol. 1, (161–165).

[27]. Kessler, Gray C. (2013) 35 "Paradigms for Cybersecurity Education in a Homeland Security Program." Journal of Homeland Security Education Volume 2 no 35 Washington, D.C

[28]. Kim J., Lee K., & Lee C. (2004) "Design and Implementation of Integrated Security Engine

[29]. for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology.

[30]. Kim H. (2004). "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics,

[31]. vol. 50, no. 1.

[32]. Kim, J. M. & Tarokh, V. (2003) "Variable rate space-time Blocary PSK systems." IEEE J. Sel. Areas Commun, vol. 21, no. 3, (362–373).

[33]. Koo, D. & Miner, K. (2009) "Outcome-Based Workforce Development

[34]. and Education in Public Health," Annual Review of Public Health, pp. 253-269,http://www.annualreviews.org/doi/pdf/10.1146/annurev.publhealth.012809.103705.

[35]. Lun, D. S., Koetter, Medard, R. Koetter, & Effros, M. (2008) "On coding for

[36]. reliable communication over packet networks". Phys. Commun., vol. 1, no. 1, (3–20). Jiang, A. (2006) "Network coding for joint storage and Transmission with minimum cost". IEEE Int. Symp. Inf. Theory, Seattle, WA, (1359–1363).

[37]. Mansfield, K. C.& Antonakos, J. L. (2010). Computer Networking from LANs to WANs: Hardware, Software, and Security. Boston: MA, Cengage Learning Course Technology.
[38]. Meguerdichian, S, Koushanfar, F., M. Potkonjak, & Srivastava, M. (2001
[39]. "Coverage problems in wireless ad-hoc sensor networks." 20th Annual Joint Conference. IEEE Computer Commun. Soc. vol. 3, (1380–1387).
[40]. Mcintosh, S., Petries, E., & Rejesh, S.. (2013). Treasury and Trade Solutions Digital Security: CTTI's Corporate Banking Channels, United States.
[41]. Morley, D. & Parker, C. S. (2013). Understanding Computers Today and Tomorrow. Boston: MA, Cengage Learning Course Technology.
[42]. Oz, Effy, (2009). Management Information Systems. Boston: Course Technology, Massachusetts.
[43]. Paul, S., Yates, R., Raychaudhuri, D. and Kurose, J. (2008) "The cache-and-forward network architecture for efficient mobile content delivery services in the future internet."
[44]. 1st ITU-T Kaleidoscope Acad. Conf. Innovations in NGN: Future Network and Services, (367–374).
[45]. Partnership for Public Service and Booz Allen Hamilton, (2009).
[46]. "Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce," http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf.
[47]. Popescu, G. (2016). Borders in the era of globalization. Border Crossings: A Bedford Spotlight Reader. Ed. Catherine Cucinella. Boston: Berdford/Saint Martin's.
[48]. Raychaudhuri, D & Mandayam, N (2011). "Frontiers of Wireless and Mobile Communications." Proceedings of IEE, Vol 100, No 4 (824-840).
[49]. Roach, A, Kidd, J, & Freeman, T (2009) "Achieving professional practice change: From training to workforce development," Drug and Alcohol Review, vol. 28, pp. 550–557. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1465-3362.2009.00111.
[50]. Schneider, F. & Mulligan, D. (2011). "A Doctrinal Thesis," EEE Security & Privacy Magazine, vol. 9, pp. 4- 3. Http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5968081&tag=1.
[51]. Shelly, G.B., Gunter, G. A & Gunter, R. E. (2012).Teachers
[52]. Discovering Computers Integrating Technology in a Connected World. Boston: MA, Cengage Learning Course Technology.
[53]. Stair, R. M. & Reynolds, G. W. (2014). Fundamentals of Information Systems.
[54]. Boston: MA, Cengage Learning Course Technology.

[55]. Stair, R. M. & Reynolds, G. W. (2016). Principles of Information Systems. Boston:
[56]. MA, Cengage Learning Course Technology.
[57]. Vermaat, M. E. (2014). A Fundamentally Combined Approach: Discovering Computers & Microsoft Office 2013. Boston: MA, Cengage Learning Course Technology.
[58]. U.S. Congressional Commission on the Advancement of Women and Minorities in
[59]. Science, Engineering and Technology Development. (2000). "Land of Plenty: Diversity as America's Competitive Edge in Science, Engineering and Technology," http://www.nsf.gov/pubs/2000/cawmset0409/cawmset_0409.pdf.
[60]. White House Report, (2009) "Cyberspace Policy Review: Assuring a Trusted and Resilient Trusted and Resilient Information and Communications Infrastructure," p. iii ,http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf