EJTAS
ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Synopsis of Cybersecurity and Risks Associated with Cybercrime to Susceptible and Blameless Global Citizenries

Dr. David O. Egete
Department of Computer Science, University of Calabar, Calabar, Nigeria

Dr. Bassey I. Ele
Department of Computer Science, University of Calabar, Calabar, Nigeria

Mr. Ceasar E. Eko
Department of Computer Science, University of Calabar, Calabar, Nigeria

Suggested Citation

Egete, D.O., Ele, B.I. & Eko, C.E. (2023). Synopsis of Cybersecurity and Risks Associated with Cybercrime to Susceptible and Blameless Global Citizenries. *European Journal of Theoretical and Applied Sciences, 1*(5), 475-487. DOI: 10.59324/ejtas.2023.1(5).37

Abstract:

Cybercrime, a collapse of the world economy, social and economic insecurity are all continual threats to the global society. Our interconnected, global civilization will soon be affected negatively and economically by the rapidly evolving cybersecurity challenge. Leaders of both developed and developing countries must be ready to launch a defence strategy against those who carry out cybersecurity attacks. In the past, local, national, and worldwide communications relied on radio networks, conventional mail systems, and fax machines to send data and documents. This paper critically performed a synopsis of cybersecurity and the risks associated with cybercrime to susceptible and blameless global citizenries. The world's transmission and communication processes are now controlled by the culture of high definition television, broadband direct connection, electronic mail, Internet access, and cyber-technology. All segments of the global innocent population are constantly at risk as a result of the excessive rate of advancement in cyber-technology. Attacks on blameless people in Paris and San Bernardino serve as a reminder to leaders of developed and developing countries to develop cyber security-savvy workforces in order to avert future catastrophes. Cybercrime poses a grave threat to the physical wellbeing of innocent members of the society worldwide. Individuals, governmental bodies, businesses, financial institutions, and higher education systems are all at risk from cybercriminals operating in isolation. The establishment of a unified front to cooperate via confidence, dedication, and commitment must be among the most credible and reliable approaches to stop cybercriminals today and in the future. All facets of international organizations and educational settings are being affected by cybersecurity concerns. The exchange of ideas, values, and beliefs as well as the teaching and learning process are all parts of the culture of the educational enterprise. Presidents, vice chancellors, professors, instructors, and other educators are urged to develop a plan of action to safeguard the infrastructure, critical data, and other assets of the entire educational system against cyber-attacks. The unanticipated events in Paris, France, and San Bernardino, California, in the United States, are a persistent trend and a decisive step that empowers national and higher education leaders, professors, instructors, and allied educators to put in place a well-organized action plan, efficient security measures, and workforces to neutralize perpetrators' malign intent to destroy all the institutions of human civilization. According to the research findings, a Global Collaborative Partnership (GCP) should be established with policies and directives to offer steady security to vulnerable global citizens.

Additionally, as part of the GCP ground plan, software designers must have preventative built-in capabilities to deter cybercriminals.

Keywords: *Synopsis, Cybercrime, Cybersecurity, Cyber-technology, Cyberspace, Cybercriminals, Blameless Global Citizenries, Susceptible Citizens.*

Introduction

Through the creation and ongoing development of communications, the world has been reduced to a global village or community today. The development of cyberspace has accompanied improvements in political collaboration, economic prosperity, and educational achievement. However, these developments have also almost given criminals and terrorists the power to use this improved communication to harm and obstruct humanity's continued advancement. Each request for progress has resulted in an equal or greater increase in criminal activity. Cybercriminals are constantly improving their skills and increasing their resolve to disrupt the relative calm that allows us to enjoy and promote these achievements. Therefore, each idea for a new development that is in the works must be developed concurrently with strategies to thwart and avoid criminal attempts to undermine and use these developments against the people who they were intended to benefit. In their study on treasury and trade solutions, Mcintosh, Petries, and Rejesh (2013) emphasized that tight and effective security measures must be put in place in order to lessen hackers' planning techniques in a digital society. To ensure that data, information, and network system resources are sent, digital services require powerful security measures. According to Mcintosh, Petries, and Rejesh (2013), the bulk of cybercrimes and the hazards they pose are intrusion-based crimes, where the attackers are usually found on the perimeters of organizations. Security breaches are uncommon when they originate from within an organization or from people who have access to sensitive data, security measures, and all system transactions. Recent cybercrime and cyber security researchers like Mcintosh, Petries & Rejesh (2013) and Kessler (2013) recommended that government agencies, corporate organizations, financial institutions, and higher education systems implement operational behaviour analysis tools to flag anomalies in employees' network activities and to keep track of when behaviour veers off the bounds of their regular responsibilities and access rights. In order to track internal cybercrime and anomalies among present personnel, operational behaviour analysis methods were developed (Kessler, 2013). Since the warnings are issued in real-time when the employee is participating in illicit behaviour on the network, the technique enables institutions to prevent employees from stealing intellectual property or destroying data. It follows logically that operational execution and monitoring of employee behaviour analysis will unquestionably reduce the worrisome rate of intellectual property theft, sensitive data leaks, and classified information theft by present employees and cybercriminals.

Cybersecurity Processes

The process of preventing unwanted computer access, as well as modifying and destroying data and information on corporate network systems and security breaches, is known as computer security. Illegal computer network access, including illegal access to communications from individuals and companies, financial information, and deliberate shutdown of network file servers at organizations, constitute a security breach (Assenter & Tobey, 2021). Cybersecurity has been developed in reaction to this weakness to prevent information theft and harm done to vulnerable populations by criminals. Networks, computers, devices, software programs, resources, information, and data are all protected by cybersecurity, which is a

collection of technologies, procedures, developments, and activities. 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 (Cheng, Lin, Huang, & Yang, 2016). With the growing volume and sophistication of cyber-attacks, urgent attention is required to protect sensitive information from being uncovered or proselytized. Due to the unpredictable nature of cyber-attacks, it is a difficult task to coordinate an efficient response. Measures taken to safeguard and manage the flow of data and information into other countries and organizations are closely tied to cyber security. Large amounts of private information are frequently maintained and stored on computers by governmental organizations, the military, businesses, financial institutions, healthcare industries, and educational organizations. They are also frequently transmitted to other computers via networks. Due to the frequency and sophistication of cyber-attacks, it is vital to take action to prevent the exposure or proselytization of sensitive information.

Long ago, dial-up telephones were the primary means of contact, and the global community managed to function extremely well in a setting of peace, quiet, and relaxation. For transmission and communication, regular mail and fax machines were employed, and the radio system was used for local, national, and international news. Global transmission and communication activities have been taken over by the culture of high definition television, broadband-direct connection, electronic mail and Internet access, cyber technology, telemedicine, tele-surgery, cyberbullying, and cyberstalking. Inadvertently driving citizens and inventors to focus on these advancements at the expense of security flaws, the exponential rise of cyber-technology now threatens innocent people throughout the world. The September 11, 2001 attacks (also known as 9/11) in New York, Pennsylvania, and the District of Columbia in the United States, the Paris attacks of November 13, 2015, and the San Bernardino, California, shootings of December 4, 2015 were all made possible by these security lapses.

In addition to other minor incidents, the three incidents made citizens aware of the reality of criminals' malign intentions and the necessity of putting in place well-thought-out plans of action of active security measures to stop or prevent cybercriminals' malicious intent to completely destroy the institutions of human development. A detailed examination of the three horrifying images shown below plainly demonstrates the likelihood that many lives could be lost during unanticipated cybercriminal strikes. The world's nations, members of the legislative branch of government, and Human Intelligence must be fully united and steadfast on a common front of confrontation against cruel cybercriminals in order to stop and eradicate it.

Cybersecurity risks are at the center of every newscast, television program, news bulletin, and radio talk show in today's technology-driven and internet-provoked society (Arthur & Rousseau, 2019). Conversations on cybersecurity and related threats are frequent. Institutions, organizations, and government bodies advise staff members not to open ambiguous or ambiguous emails, to make strong, unique passwords, and to adopt other well-considered security measures to secure organization data and information. Insecpro.com estimates that there are 556 million cyber victims annually, 1.5 million victims every day, more than 232 million characteristics exposed, and as many as 120,000 repetitive botnets "zombie" charges of creating and sending spam and infected emails every day (Evans & Reeder, 2020).

Figure 1. The World Trade Center Burns after Being Hit by a Plane in New York in this File Photo on September 11, 2001

Figure 2. November 13, 2015 in Paris, France

A deeper look at www.insecpro.com/index.php/cyber-crime-statistics exposes infographic data proving that in 2013, 59% of ex-employees acknowledged to stealing data and information from organizations after leaving their jobs. The incidents in Paris and San Bernardino act as a point of reference for betrayal and disloyalty against the institution of human civilisation. These incidents have put law enforcement officials and other state and federal government agencies on alert and threatened the safety of innocent worldwide people. To acknowledge the impending cyber risks, leaders of the united global community, legislative bodies, chief executive officers, and decision-makers of public and private companies are strongly urged. Global economic collapse, cybersecurity risks, and issues with social prosperity are all pervasive in the global environment. Threats to cybersecurity are here

to stay, and they could have significant economic repercussions for a linked global society. Therefore, global leaders must be prepared and willing to take the initiative in developing a cutting-edge strategy for protection against digital intrusion (Roach, Kidd, & Freeman, 2019). Cybersecurity risks have an effect on lawful activities by disrupting them, denying them service, sabotaging, causing direct financial loss, harming one's reputation, losing one's attractiveness, stealing trade secrets, and eroding confidence among clients, staff members, shareholders, and business partners.

Figure 3. December 4, 2015 in San Bernardino Attack, California, United States

Combating Cybercrime Threats

Cybercrime perpetrators have a long history of engaging in asymmetric and classic forms of maximum cyber-threats against defenceless people all around the world. The usage of related cyber-devices including smartphones, Internet, emails, and microcomputers supports the alarming rate of the impending cyber security concerns. In actuality, every country has its own unique set of regulations and practices to strengthen cyber security against these dangers. Manufacturers of computer operating systems (OS) and network operating systems (NOS) must be included in the specified regulations in a systematic manner. Hardware, software, email, and internet providers must actively participate in the cooperative effort to defeat all cyber-threat agents in a never-ending and protracted worldwide conflict with those who pose a threat to cyber security. Millions of technologies, including emails, smartphones, and the internet, are being distributed by producers of hardware, software, emails, and the internet that, regrettably, are now being used as weapons by cybercriminals. The international community is experiencing very stressful circumstances, and world leaders and their counterparts cannot ignore secret factors that are crucially influencing the spread of international violence. The majority of cyberterrorist activities are currently evolving towards encryption formats with improved cyber-technologies, code-named as asymmetric, and prepared to launch callous attacks on defenceless civilians.

Threats to humankind, which are comparable to cybercrime, have existed since the dawn of our species' civilisation. Since its inception till the present, the institution of human civilisation has experienced instability, mayhem, and upheaval. The conflict between Cain and Abel, Esau and Jacob, and other rebellious encounters from the times of Sparta, Alexander the Great, Pompeii, Julius Caesar, Genghis Khan, Napoleon, Wellington, Allenby, World War I, World War

II, Yom Kippur, 1982's Falklands War, 1990's Iraqi War, 2001's attacks on New York and Paris, and 2015's San Bernardino terrorist attacks have all been experienced by the human race. According to the aforementioned list of unpleasant encounters, cybersecurity threats are creating new fronts for conflict and war with impunity, forcing world leaders to embrace and execute cooperative data, information collecting, and sharing to tackle these dangers against humanity. Cybercriminals are cold-blooded, outdoor convicts with blatantly punitive aims who target innocent citizens and public events with suicide bombers. Leaders of the world's nations are fervently urged to join in all-inclusive measures to punish cybercriminals in order to stop and eradicate cybercrimes. They require complete cooperation, funding, qualified employees, and citizens who are aware of the true threat posed by cyber-attacks and insecurity. Cyber operations do indeed cross national and geopolitical borders because they exist and are carried out there. Therefore, it is imperative to see this crime from a position of "borderlessness" (Popescu, 2016).

Cybercrime Framework

Cybercriminals frequently use the 24 hours a day, 7 days a week (code-named 24/7) network connections to gain contented access and enough time to freely plan to experiment with user names and passwords and identify the kinds of user datagram protocol (UDP) and transmission control protocol (TCP) ports that are vulnerable to criminals. Unquestionably, since the allocated (IP) address frequently remains the same and unaltered, it is almost stress-free for cybercriminals to start cold-blooded attacks on wireless network systems. Increased connectivity speed is ingrained with unrestricted and limitless direct access. The standard 56Kbps dial-up and analog modem has a connection speed that is essentially slow, expensive, and time-consuming. However, the quick development of direct access communication has given wired and wireless cable manufacturers the ability to provide greater download and upload rates. Transfer rates at all stages of direct connections, regardless of carriers and manufacturers, should be limited to 128Kbps by wired cable providers and to somewhere between 128Kbps and 764Kbps by direct connection providers, according to Mcintosh, Petries, and Rejesh (2013) and Kessler (2013).

In order to close the gap and limit the dissemination of cyber security threats to companies and unprotected workers and infrastructure, the practice of exchanging actionable data, information, and intelligence acquisition is unavoidable (Kim 2014, and Chen & Whisnant 2020). This plan calls for the sharing of data gathered to combat cybersecurity threats, the tenacity to put in place global, round-the-clock monitoring systems to take down cybersecurity offenders, and preventative and proactive measures to defeat them everywhere and make them the watchwords of all leaders. Empowering law enforcement officers, conducting intelligence operations, and exchanging information specifically relevant to impending risk are all necessary components of all-encompassing hard work. As a result of cybercrime's constant invisibility and persistence, those responsible for such acts must be separated from international organizations. Communities around the world must continuously be attentive, vigilant, and prepared for an immediate response to cyber security threats. When implementing the President of the United States' Executive Order (E.O.) 13636, which places a strong focus on cooperation and swift action, alertness, preparedness, and willingness are crucial:

In order to improve the timeliness and quality of the cyber threat information shared with vulnerable private sector firms, the U.S. Government has developed systems and procedures. We place a lot of emphasis on agencies with a domestic response mandate working together as a team.

Educational Settings and Cybercrime

Every aspect of society is facing difficulties as a result of cybercrime, including educational

institutions. The culture of the educational enterprise includes instruction, educational endeavours, and the sharing of ideas, values, and beliefs. The infrastructure, critical data, and critical information of the entire educational system must be protected from exploitation and abuse, and presidents, vice presidents, professors, instructors, superintendents of school districts, principals, and other related educators are urged to develop measurable plans of action. These administrators and the associated stakeholders must be ready, willing, and able to develop compliance and regulatory standards in order to combat cyber security risks effectively. The idea that information technology (IT) divisions are in charge of handling concerns about cybercrime is a limited and wrong approach to the problem (Koo, & Miner, 2019). It is an escape tactic to avoid addressing urgent issues. Utilizing every organizational unit's assistance and treating them as partners in the corporation's protection is the most effective strategy to put complete cybersecurity measures into place. The price of doing nothing is much higher than the price of putting appropriate cyber security measures in place to combat dangers of cybercrime and confidentiality breach. In order to develop trustworthy cyber liability insurance and benefits and to create a simple contract with outside vendors to protect organizational financial records, the planned actions must involve a variety of organizational units, including the financial affairs and human resources departments. Due to the recent distribution of foreboding and threatening emails on December 12, 2015, two of the largest school systems in the United States—Los Angeles and New York—experienced academic break-ins.

Threats from cybercrime are constantly emerging, endangering the stability of institutions of higher learning. In colleges and universities, there is significant support for the expansion of degree programs in computer science and computer information technology. However, the envisioned growth and new course offerings must include subjects like a network for cyber security, an introduction to cybercrime problems, and computer forensics and investigations. As a result of the digital age, higher education institutions all around the world are going through various digital transformations and data breaches. Because of new technologies that alter how data and information are backed up, stored, accessed, and maintained, cybercrime threats have become more sophisticated (Shelly, Gunter & Gunter, 2012).

Academic deans of computer science (CS) and computer information technology (CIT), also known as computer information systems (CIS) or Homeland Security, are strongly encouraged to form an academic alliance with experienced members of a variety of law enforcement agencies, including police officers, state troopers, the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI), who will serve as official guest instructors under the supervision of full-time faculty members (Vermaat, 2014). Through this partnership, professionals who deal with these issues on a daily basis will give the staff and students the necessary information. This information exchange will be a starting point in the fight against cybercrime. Cyber criminology is a relatively recent invention created to provide the necessary knowledge and skills to look into and stop breaches of security standards in computer network systems. Graduates from the new cyber security programs will have the knowledge and skills necessary to defend institutions of higher learning against dangers of theft, misuse, and vulnerabilities by aiding with forensic examination of cyber occurrences.

Human and financial resources must be used to assist cybersecurity attack prevention and defence strategies. The majority of enterprises struggle with insufficient financial support and a disjointed cadre of professional development programs as a result of the rapidly expanding field of cyber security. In their empirical study on cyber security, Hoffman, Burley, and Toregas (2011) proposed that national and state governments, businesses, and academic stakeholders undertake continuous professional education development as a national security initiative. Sadly, there isn't any first-hand information or documentation on how to

respond to cyber security assaults. According to Hoffman, Burley, and Toregas (2011) and Honig (2011), the field of cybersecurity today is comparable to the practice of medicine in the 19th century, when doctors were frequently self-taught and had a range of skill sets. These professionals worked in a developing field that was closely tied to a complicated, dynamic, and somewhat unpredictable environment with few or no professional performance requirements.

The advancement of cyber security and its integration into higher education's core curriculum will aid in preparing the present and following generations to respond to cybersecurity attacks more effectively. The concept calls for the creation of an all-encompassing, cogent action plan that includes K–12 students, academic professors, associated educators, higher education administrators, and professionals from both the science and non-science fields. Given the transient nature of cybercrime, it stands to reason that the culture of cyber security includes global components and necessitates a multidisciplinary style of approach. Naturally, traditional degree programs last four to eleven years of study. Sadly, none of these are concerned with cyber security or how to counter attacks to it.

Hoffman (2010), Kessler (2013), Kim and Lee (2014) have proposed 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. This is due to the constantly evolving nature of cyber-attacks. To allow for the long-term, educational contexts necessary to address job-specific issues, such curriculum must contain curative rather than palliative approaches. Additionally, they need to put in place a variety of distribution strategies for instructional modules that make the best use of current technologies to train the cyber security workforce of the future. This article's goal is to build policies and strategies for the academic cyber security program that incorporates a thorough, collaborative, and career development preparation approach.

In fact, the academic setting offers significant incentives for research that adheres to rather strict disciplinary limits. Without any point of reference or classified or unclassified documents on how to defend against cyber security attacks on defenceless civilians, cybercriminals operate without warning. In their research on applying a comprehensive development approach to develop the cyber security workforce, Hoffman, Burley, and Toregas (2011) included the evolution of cyber security assaults to the legal and medical fields. They further asserted that an ongoing, step-by-step strategy must be developed in order to provide opportunities for ongoing professional development and to create successful educational efforts across a variety of subject areas in light of the culture of cybersecurity risks. In fact, the proposed universal methodology necessitates the formation of a long-lasting relationship between institutions of higher learning and the federal, state, and allied governments. A non-environmental project, cyber security is a result of the revolution in computer networks, the Internet, routers, emails, and Web servers.

Higher Education Strategy of Action for Cybercrime

The rapid proliferation of newer, better, quicker technologies around the world is one of the most striking features of the rising information technology operations (IT) (Kessler, 2013). For IT professionals, end users, and members of the global community, the rapid development of new technology is rife with difficulties. The situation has become more convenient for cybercriminals, who exploit computer networks and the Internet for a variety of unlawful activities (Kessler, 2013). Direct-connection technologies having the potential to make computer use appropriate and beneficial include wireless computing and broadband. Measurable performance and results should be backed by a broad spectrum of commitment and dedication that is customized to the sacrifice of security. Cybercriminals are well-versed in and ready to attack wireless network systems using broadband technologies including digital

subscriber line (DSL), cable modem, and satellite Internet services. Computers connected to DSL and broadband networks typically operate differently from dial-up telephone systems, according to Mcintosh, Petries, and Rejesh (2013) and Evans & Reeder (2020). Cybercriminals are more likely to employ new technologies to gain unauthorized access to DSL and broadband networks, thus customers of these services should be more concerned about security than those who use dial-up.

The attractive way of operation, high speed, twenty-four hour (24/7) connectivity everywhere and anytime, is a major foundation for DSL and broadband networks. Since a direct connection network is constantly linked to an external network, it is susceptible to attacks. Long ago, people and companies used analog modems or, possibly, dialup connections over the integrated services digital network (ISDN) to access the Internet. Since the system was only accessible to outsiders when in use, the vulnerability to attacks by hackers was managed and controlled during the process. After finishing its routine tasks, the network system was disconnected and vanished from the Internet. The majority of Internet service providers (ISP) assign dialup users internet protocol (IP) addresses via the Dynamic Host Configuration Protocol (DHCP). Broadband and DSL are categorized as unmatched connected technologies. Digital operation "code-name" (direct) has made it possible for people and businesses to connect to the Internet around-the-clock (24/7), unlike analog (dial-up) connections, broadband, and DSL. In fact, it expedites and enhances all stages of data, information, transmission, communication, and unfettered access to Internet resources. Additionally, unfettered access has improved IT professionals' capacity to set up, monitor, and share data and information remotely across a network system (Frenkiel, Badrinath, Borres & Yates, 2010).

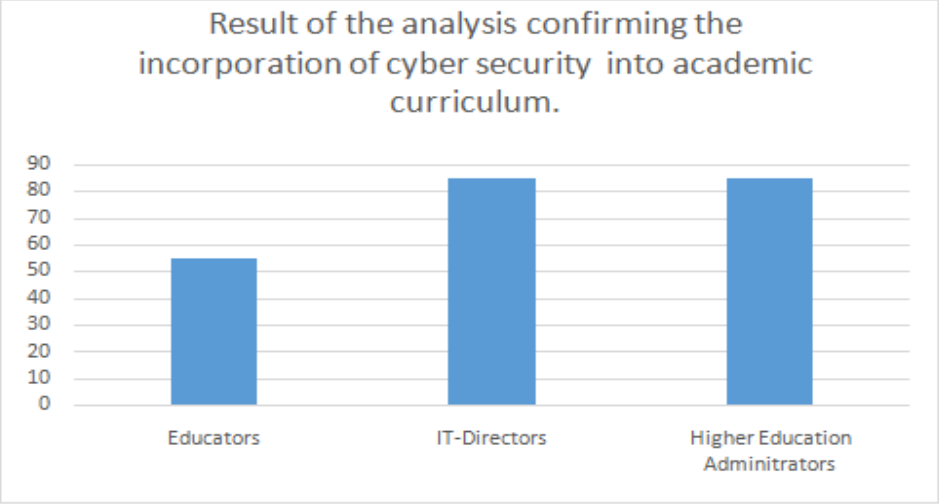

Figure 4. A Bar Chart the Result of the Analysis Confirming the Incorporation of Cybersecurity into Academic Curriculum

The National Cyber Security Alliance (NCSA) performed research early in 2015 and released a number of suggestions to secure everyone at home, on college, university, and school campuses, as well as advice on how to integrate lessons on cybersecurity, computer forensics, and cyber-ethics into academic curricula. The survey's goals were to better understand and raise awareness of cybercrime, cyber ethics, cyber safety, cybersecurity, and computer forensics as safeguards and minimum standards for American grade schools, high schools, and undergraduate degree programs. The study's findings showed that there is a large gulf in

opinion regarding the value of cyber education in educational settings between teachers, administrators, and information technology (IT) specialists. However, 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. Fifty-five percent (55%) of educators strongly agreed to include cyber security in the academic curriculum (Honig, 2011).

The fact that nearly forty-five percent (45%) of educators surveyed by NCSA reported being wary and unprepared to prepare students for the abrupt integration of cyber education into the educational systems suggests that higher education administrators and IT directors have a cooperative agreement, according to Henig's study. Two thirds of the educators polled had no formal training in internet education, and only 40% had attended workshops lasting three hours or fewer. This idea was developed with the intention of ensuring that teachers who prepare students for cyber education are also fully capable of using cyber education. As a result, when preparing the next generation for protection against cyber-attack threats, special emphasis must be made to cyber-related skills and competence.

At all levels of educational instruction and learning endeavours, cyber literacy initiatives and courses such as networking system security, digital and cybercrime forensics, cyber security planning and management, intrusion detection and defence, and internet technology security must be included in light of the growing threats posed by cybercrime. Ample human and financial resources must be available to support the planned activities. Thankfully, there are several colleges and institutions in the United States that have integrated cyber-security programs. Most of these sessions are provided as technical courses nested within professional certification programs. According to Bellavita (2008), the Homeland Security Act of 2002 requires universities to actively participate in homeland security education. The Homeland Security Act's purview must be seen as a segment of the larger field of information security. The paradigms that are anticipated include integrating cyber security into the academic curriculum and defensive strategies against threats from hackers. Education is a process that broadens people's perspectives on their own competences, specialized knowledge, critical thinking, and critical understanding of terrible and life-threatening risks from cybercriminals. Cyberspace threats can be prepared for by taking proactive steps to prevent incidents from happening in the future, reactive measures to respond to them when they do, and defensive measures to guard against them. Indeed, the defensive paradigm of preparing students to become useful, resourceful, and task-oriented citizens is deeply ingrained in education. Higher education institutions cannot afford to ignore the need to include a cybersecurity curriculum in their course offerings. Current students and future graduates will benefit from cyber education by receiving the knowledge and skills necessary to defend societal institutions and the global community from cybercrime threats. Threats to cyber security can be reduced by good management, collaborative projects, and extensive employee and public participation. To combat the many threats posed by cybercrime, organizations and enterprises have a plethora of policies and procedures in place today. All planned courses of action must be anchored by particular standards and norms. The workforce and staff of organizations need to be trained and cultured to adapt, comply, realize, and accept the reality that there are no methods that can be used universally to safeguard business data and information from cyber security risks. The general public, business organizations, religious groups, and governmental institutions must be included in an active plan of action, workshops, and professional training against cybercrime threats (Stair & Reynolds, 2016). The core of any organizational structure is protecting and preventing intrusions into the repository of data and information. Individuals, institutions of higher education, organizations, and governmental bodies must be willing, prepared, and ready to share intellectual information, expertise, and procedures with low enforcing agencies in order to combat the architects of cyber security threats, taking into account the

seriousness of the threats and the perpetrators' unwavering resolve.

Combating Cybercrime

Cybercrime measures have crossed international borders and will do so in the future. Because terrorism and cybercrime are global phenomena that cross national borders, global collaborative partnerships (GCP) are essential to prevent cybercriminals from exacting revenge on innocent members of global communities (Popescu 2016). The GCP will provide a revolutionary framework for an international environment that is dependable, consensus-based, and interoperable. Global leaders will be able to unite in the face of cyber security threats, keep an eye on how data and information are transmitted in and out, and impose limits on the extent of internet freedoms by adopting and successfully implementing GCP. Adoption and implementation of upgraded, state-of-the-art cyber-deterrent technologies as soon as possible in both public and commercial facilities will provide value and enable coordinated responses to cyber security threats (Kim, 2014).

The goal of GCP is to offer plans and instructions to protect the welfare of the general public's most vulnerable members. An exhaustive analysis of the attacks on innocent bystanders in Paris and San Bernardino serves as a wake-up call to leaders of developed and developing countries to create workforces that are knowledgeable about cybercrime. Hardware and software vendors need to pay more attention to developing cyber security-savvy workforces (CSSW). Software and hardware vendors must be urged to build in preventive features to thwart cyber security criminals' plans to interfere with and disrupt the rights of global citizens as part of GCP's ground strategy. Cybersecurity threats are one of the most incredible technology issues of our day. Parents, academics, allied educators, religious institutions, commercial companies, and governmental organizations are all actively involved in CSSW's culture of digital challenge, which is a significant step in raising public awareness of the dangers posed by technologically skilled criminals.

Expected Solution

Previously, computers were electronically networked and connected to one another, where specially trained personnel were positioned in secret locations with spying devices, where classified information was stored, and where counterfeit information was concealed in a mini camera and smuggled out, making the work extremely risky, expensive, and physically taxing (Evans & Reeder, 2020). Thousands of cybercriminals are currently positioned around cutting-edge computers and surveillance equipment with high-resolution screens in completely air-conditioned buildings with the ability to detect people entering and exiting the property, waiting everywhere.

The expected solution to this security breach issue should involve having existing employees' fingerprints taken. A sworn affidavit promising not to hack into the organization's system or steal sensitive information must be included in exit interviews with former workers. This is crucial because the majority of cybercriminals have the capability to steal sensitive data from firms' facilities located millions of miles away. The installation of properly designed surveillance equipment by businesses, governments, and institutions of higher education is strongly advised in order to track down and deter cybercriminals.

Conclusion

There is a common belief that there is nowhere fortified and safe to hide from cyber security dangers, and that no simulation is safe from impending cyber-assault. The path to containing this weakness, however, lies in concerted measures to counter threats of cybercrime, vulnerability, and to deter cybercriminals' attempt to unleash their malign intentions on the world's defenceless inhabitants. Nation leaders are strongly urged to uphold global collaborative partnerships by supporting measures to defend

the well-being of the vulnerable international citizens in order to protect the residents of the world from the malicious intentions of cybercriminals.

Reviewing the physical assaults in Paris and San Bernardino and the untimely deaths they caused serves as a warning and a reminder to leaders of wealthy and developing countries to be steadfast in protecting the global community from risks of cyber-attacks. These assaults are unforeseen, undetectable, and catastrophic to infrastructure, human life, and the advancement of civilisation worldwide. If technocrats and politicians, educators and organizations do not stand steadfast and decisive against those forces of destruction, the world risks losing in a few hours what it has worked so hard for years to design or build.

References

Assenter, M. & Tobey, D. (2021). Enhancing the Cybersecurity Workforce. IT Professional, 13(1), 12-15. https://doi.org/10.1109/MITP.2011.6

Arthur, M. B. & Rousseau, D. M. (2019). (eds.). *The Boundary less Career: A New Employment Principle for a New Organizational Era.* New York: Oxford University Press.

Bellavita, C. (2008). Changing homeland security: What is homeland security? *Homeland Security Affairs Journal, 4*, 1.

Cheng, S. M., Lin, P, Huang, W. & Yang, S. R. (2016). *A study on distributed and centralized scheduling for wireless mesh network.* In Proceedings of the international Conference on Wireless Commun. Mobile Computer. 599–604.

Chen, S. I., & Whisnant, R. K. (2020). *Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors.* In Proceedings of the International Conference on Dependable Systems & Network, Washington, D.C.

Evans, K. & Reeder, F. (2020). "A Human Capital Crisis in Cyber Security." Center for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/human-capital-crisis-cybersecurity

Frenkiel, R., Badrinath, B., Borres, J. & Yates, R. (2010). The infestations Challenge: Balancing cost and ubiquity in delivering wireless data. *IEEE Personal Communications., 7*(2), 66–71. https://doi.org/10.1109/98.839333

Hoffman, L. (2010). Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development. GW Cyber Security Research and Policy Institute Report (GWSPRI). Retrieved from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs5851/files/downloads/2010-3a_building_the_cyber_security_workforce_of_the_21st_century_0.pdf

Hoffman, L. J., Burley, D. & Toregas, C. (2011). Thinking Across Stovepipes: Using a Holistic Development Strategy to Build the Cybersecurity Workforce. (Report GW-CSPRI-2011-8). Retrieved from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs5851/files/downloads/stovepipes_gw_cspri_report_2011_8_0.pdf

Honig, D. (2011). The Importance of Cyber security Training. *Journal of Homeland Security Education. 2.*

Kessler, G. C. (2013). Paradigms for Cybersecurity Education in a Homeland Security Program. *Journal of Homeland Security Education, 2*(35).

Kim J., Lee, K., & Lee, C. (2014). *Design and Implementation of Integrated Security Engine for Secure Networking.* In Proceedings of International Conference on Advnaced Communication Technology. https://doi.org/10.1109/ICACT.2004.1292914

Kim, H. (2014). Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System. *IEEE Transactions on Consumer Electronics, 50*(1), 214-224. https://doi.org/10.1109/TCE.2004.1277865

Kim, J. M. & Tarokh, V. (2013). Variable rate space-time Blocary PSK systems. *IEEE J. Sel. Areas Commun, 21*(3), 362–373.

Koo, D. & Miner, K. (2019). Outcome-Based Workforce Development and Education in Public Health. *Annual Review of Public Health, 31*, 253-269. https://doi.org/10.1146/annurev.publhealth.012809.103705

Mcintosh, S., Petries, E., & Rejesh, S. (2013). Treasury and Trade Solutions Digital Security: CTTI's Corporate Banking Channels, United States. Retrieved from https://www.citibank.com/tts/solutions/digital-channels-data/digital-security/

Popescu, G. (2016). Borders in the era of globalization. Border Crossings: *A Bedford Spotlight Reader*. Ed. Catherine Cucinella. Boston: Berdford/Saint Martin's.

Roach, A., Kidd, J., & Freeman, T. (2019). Achieving professional practice change: From training to workforce development. Drug and Alcohol Review, 1(28), 550–557. https://doi.org/10.1111/j.1465-3362.2009.00111.x

Shelly, G. B., Gunter, G. A., & Gunter, R. E. (2012). *Teachers Discovering Computers Integrating Technology in a Connected World*. Boston: MA, Cengage Learning Course Technology.

Stair, R. M. & Reynolds, G. W. (2016). *Principles of Information Systems*. Boston: MA, Cengage Learning Course Technology.

Vermaat, M. E. (2014). *A Fundamentally Combined Approach: Discovering Computers & Microsoft Office 2013*. Boston: MA, Cengage Learning Course Technology.