International Journal for Business Education

Volume 163 | Number 1 Article 6

January 2023

Revisiting Cybersecurity Awareness in the Midst of Disruptions

Avideh Sadaghiani-Tabrizi
Center for Educational and Instructional Technology Research Center (CEITR) / School of Advanced Studies / University of Phoenix, avidehst@email.phoenix.edu

Recommended Citation

Sadaghiani-Tabrizi, Avideh (2023) "Revisiting Cybersecurity Awareness in the Midst of Disruptions," *International Journal for Business Education*: Vol. 163: No. 1, Article 6.
DOI: 10.30707/IJBE163.1.1675491516.833197
Available at: https://ir.library.illinoisstate.edu/ijbe/vol163/iss1/6

ISSN 2164-2885

Revisiting Cybersecurity Awareness in the Midst of Disruptions

Avideh Sadaghiani-Tabrizi (DM/IST)
Center for Educational and Instructional Technology Research Center (CEITR) / School of Advanced Studies / University of Phoenix

AvidehST@email.phoenix.edu

ABSTRACT

The awareness of cybersecurity and knowledge about risks from a variety of threats, which present harm or steal private information in internetworking could help in mitigation of vulnerabilities to risks of threats in safeguarding information from malware and bots. Revisiting cybersecurity awareness of every member and evaluation of organization's posture might help to protect sensitive or private information from a network of computers, working together and forming into botnets. The purpose of the qualitative case study narrative was to explore prospects for integrating cybersecurity education into elementary school children's curriculum through interviews of elementary schoolteachers, IT experts, and parents to gain feedback about perceptions on cybersecurity knowledge and awareness. The analysis of schools' organizational security postures related to all levels of education, recommending in raising awareness of the underlying and unprecedented security vulnerabilities. One area of greatest need is in protecting the wellbeing of people in securing private or protected assets and sensitive information, most valuable and vulnerable amid disruption. The possible lack of cybersecurity awareness in online settings could increase an organizational vulnerability to risks of threats and outsider attempts to install malware during a variety of cyber-attacks. Organizations with online ambiguity face a threat from botnets to infect networks. This qualitative exploratory single case-study into perceptions of teachers and leaders, information technology (IT) experts, and parents of elementary school children about cybersecurity awareness level of children in elementary schools helped to reinforce the important role of education in building foundational cyber-safety practices.

Keywords: Decentralized autonomous organizations, Digital transformation, Intrusion detection systems, Pervasive computing, Polymorphic malware, Search engine optimization, Social engineering, Threat actors, and Threat vectors.

The future of a cyber-secure and aware workforce will depend on integrating cybersecurity awareness and training in all levels of internetworking to contribute to safely using the internet for communication, social networking, completing assignments, conducting research and telework in the digital age. The education in cybersecurity and cyber-safety could help to handle acts of cyber-attacks through approaching to resolve the issues, which pertain to cybersecurity on a national level with offensive advantages against cyberthreats in triaging to respond to security events proactively during times of uncertainty. A focus on facilitating contents through collaboration among peers and the advancements in digital communication supported learning strategies for implementation of cybersecurity in education, directing attention to leaders' clear vision for security and skills to assess safety of personal cybersecurity in protecting sensitive or private information from harm.

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

A thorough research on conducting communication, learning online and telework with managed services at a time when global ambiguity became a focus for school leaders helped consideration for providing online safety for staff, faculties, and students to mitigate online risks from the communication networks by building digital or cyber-resiliency. Online safety could reduce loss and provide cybersecurity defense to protect sensitive or private information from a network of computers, which form into bots and thereafter botnets. Unaware internetworking could expose online vulnerabilities to trigger security incidents. Networks of bots comprise of computers with malicious code threaten endpoints, requiring the ability to triage, respond to security events proactively, and conduct correlation analysis to prioritize and identify security incidents by remediation of threats. The assessment of weaknesses and vulnerabilities in cybersecurity culture of organizations' information systems management assist in conducting formal risk analysis to evaluate, correct, mitigate, remove, or formally accept risk-events. Additionally, risk analysis could play an important role in reducing or mitigating risks of exploitation of hardware, software and data transmission through intelligences and analysis of system log data in helping identification of the security posture in organizations. End-users at every level of age and society are vulnerable to manipulation, in which they are tricked into installing malware that appears in a wide variety of guises. Encouraging societal development could reinforce continual awareness amid the digital transformation.

Leaders must create value by aligning the organizational information security (InfoSec) knowledge and awareness, operations, strategies, and the need for monitoring cyber-vulnerabilities and threat. The cybersmart initiatives during the national cybersecurity month of October reminded to raise awareness of everyone to work, learn, and play with vigilance. The governance to align organizations' mission with cybersecurity strategies in structuring performance and assessing the culture, and assets could help to reduce cybersecurity risks. Safety requires a continual audit of organizational cybersecurity in a decentralized ecosystem that relies on mitigating and overcoming a multitude of risks of threats, and malicious attacks when managing a crisis and helping organizations to protect identifying information and security online. Further, safety requires governance to align organizational mission with decentralized autonomous organizations' (DAO) cybersecurity strategies in structuring performance and assessing the organizational culture and assets.

Problem Statement

The various forms of targeted attacks on networks or devices could present forms of threats to end-user's privacy and safety, creating online trolling and vulnerabilities to risk exposing private information. The cybersecurity unaware people who could connect a variety of technologies to take advantage of the innovations in communication risk the poisonous character in living a balanced life for the dark aspect of communications technology (Mbinjama-Gamatham, 2020, p. 2). Risks of social engineering threats to end-users include neuro-linguistic hacking for building rapport in communication to gain information (Hadnagy, 2010). Recent advances in communication and processing information through developments in IT have contributed to changes in elementary school education (The Levin Institute, 2014). The continual improvements in telecommunication systems and awareness of organizational cybersecurity threats must encourage every member of an organization to exercise security awareness.

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

An analysis of organizational security postures could help resist unprecedented security vulnerabilities of private and protected assets. Precautions against cyber-bullying could further direct attention to the necessity of exercising personal safety and cybersecurity (Tabrizi, 2021), to build offense against the vulnerabilities or risks of potential exploitation in times of global turmoil. Specific steps are necessary to protect the wellbeing of people, particularly children, who are society's most valuable assets and are at risk during the maliciously motivated cyber disruptions. Networks of people have become vulnerable in an interconnected world.

Security vulnerabilities are risks of potential exploitation of identifiable information in times of global turmoil. Specific steps are necessary to protect confidential information about people, particularly children, who are society's most valuable assets and are at risk during the maliciously motivated cyber disruptions. Networks of people could risk jeopardizing wellbeing by exposure of public-or-private data, in an interconnected world "stolen by bad actors" (Cave, 2021, p. 1). The continuous possibilities of deceitful access to software and hardware require increased awareness about the risks of threat vectors and vulnerabilities (Valdetero & Zetoony, 2014). Achieving security might be difficult because of multiple potential access points in the cyber-domain of an interconnected world. Defeating the many forms of emerging vulnerabilities in a cyber environment may depend on individuals' discretion to keep safe and to protect organizational assets.

Organizational leaders can create value by aligning organizational missions with operations and culture, information security (InfoSec) knowledge and awareness, and strategies in monitoring cyber-vulnerabilities and threats in an increasingly threatening landscape. The opportunities and learning experiences from the year 2020 related to widespread disruptions could have enormous impact on societies around the globe. Leaders can master new challenges in cybersecurity by supporting resilience in threat environments. Emerging and immediate Internet threats present in the digital future require various leadership strategies to meet the needs of all faculties, educational staff, and students in the following generations: (a) baby boomers (born from 1946-1965), (b) generation X (born from (1966-1979), (c) generation Y or millennials (born from 1980-1994), and (d) digital natives or generation Z (born from 1995-2012) who could present a diverse culture in the innovative digital enterprise (Tabrizi, 2019). Findings from the present qualitative exploratory single case-study into perceptions about cybersecurity awareness level of children in elementary schools from the viewpoints of teachers and leaders, information technology (IT) experts, and parents of elementary school children helped to reinforce the importance of implementing cyber-safety education in all levels. The availability of cybersecurity research with a plethora of findings could contribute many improvements in an Upstate New York school district in monitoring Internet activities and teaching age-appropriate cybersecurity skills to raise student awareness, and judge and discriminate Internet content in order to avoid online threats.

The response to crisis might require triaging essential services to fill gaps through contingency and incident response planning systems with deterministic or machine learning artificial intelligence (AI) for cybersecurity in processing threat intelligence to gather insights on the noise from alerts with an increased speed in reducing response times. Business impact analysis (BIA) could help with processing organizational deliverables and information to establish facts in helping implement business continuity

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

plans (BCP) and prepare to respond to attacks through backup contingencies. The escalation of a variety of attacks on educational software emphasize the importance of integrating cybersecurity awareness training and raising cybersecurity awareness among all staff.

Incorporating a system to provide appropriate security capabilities could help to build upon software assurance through applying processes and technologies, in achieving confidence that software systems and services will function as intended, free from vulnerabilities. The awareness of cyber and computer literacy, and careful and aware internetworking might contribute to safe use of the Internet for communication, in handling Internet-of-things (IoT), social networking, and conducting and completing work assignments in the digital-age. An attempt to stay safe and secure, online could reduce exposure to malware (Tabrizi, 2019). Accordingly, the interviews of elementary schoolteachers, educational leaders, Information Technology (IT) experts, and parents of elementary school children helped to explore cybersecurity awareness of children.

The availability of research in cybersecurity augments organizations' efforts to minimize the risks of cyberattacks, by contributing improvements with an emphasis on current issues in the development of modules to improve monitoring of Internet activities and raising awareness of threats of cyber-attacks. Accordingly, the national cybersecurity awareness month 2019 (NCSAM 2019) toolkit, developed by the Department of Homeland Security's national initiative for cybersecurity careers and studies provided a comprehensive guide to ease engaging and promoting the following critical messages of core theme of cybersecurity awareness throughout the month of October: (a) own IT, (b) online privacy, (c) social media cybersecurity, (d) Internet-of-things, (e) secure IT, (f) creating a strong password, (g) a how-to guide for multi-factor authentication, (h) phishing, (i) e-commerce and e-skimming, (j) protect IT, (k) social media bots overview, (l) understanding foreign interference in five steps, and (m) identity theft and Internet scams (NCSAM, 2019). The awareness about potential dangers present during Internet-working, given modern cyber interconnected-world could promote safe-internetworking. Training staff in cyber-safety and cybersecurity could prepare workforce to handle acts of a cyber-attack to approach and resolve the issues pertaining to cybersecurity on a national level, directing attention to education in cybersecurity at all levels of employment.

Literature Review

The proposition to explore is the leaders' approach to support security by integrating cybersecurity awareness to help and remind staff, faculties, and students about handling risks of threats, in addressing cyber-crimes. Leaders' implementation of improvements could help educational advancements and developments in organizations, by promoting safe-online education. Threat actors who are motivated through collecting competitive information for "political, economic, technical, or military" gains (Giandomenico, 2017; Tabrizi, 2018) could target attacks in forms of threat vectors to spear-phish forms of hacking attempts to target an attack, to gain an advantage over vulnerable subjects (Ferrillo, 2015). Protecting the multiple layers of information and implementation of cybersecurity policies requires consideration of several factors to protect against attacks from "script kiddies, hactivists, nation state actors, insiders, and others" (Ciampa, 2017, p. 29), such as the telephone spammers who commit voice frauds. Accidental access to websites, encompassing artificial intelligence programs with use of modern

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

technologies to disguise, parse, and analyze information, might direct attention to greater emphasis on monitoring internetworking and exercise of cybersecurity awareness (Oltsik, 2018). Accordingly, the results from the abovementioned qualitative exploratory case study were helpful in determining leaders' use of information technology systems (ITS) improvements to help advancements in organizations. The future of a cyber-secure and aware workforce will depend on integrating cybersecurity awareness programs for students and staff at all levels in organizations.

The modern communication networks could use artificial intelligence programs to disguise, parse, and analyze data, necessitating awareness of threats to address the vulnerabilities through "data-security events, incidents, and the likelihood of [much harm because many unethical and] bad actors' malicious attempts might jeopardize privacy and data" (Tabrizi & Lao, 2018, p. 52). The introduction of mathematical decentralized algorithms in digital platforms blockchain technology has been disrupting societies by mining and managing identities' security, privacy, and usability (Tabrizi & Lao, 2018; Nabi, 2017), in an environment that viral hacking attempts to target an attack, to gain an advantage over vulnerable subjects (Ferrillo, 2015). The increases in security risks of threats to vulnerabilities for "political, economic, technical, or military" gains (Giandomenico, 2017, para. iv), motivate awareness against dangers posed by threat actors' targeted attacks in forms of threat vectors to spear-phish forms of hacking attempts to gain an advantage over intellectual property (Ferrillo, 2015). The increases in security awareness and precautions against digital manipulatives might direct attention to personal safety, and cybersecurity.

The education in cyber-safety and cybersecurity for all staff and faculties could help these users prepare and handle acts of a cyber-attack. The first era of computing was defined by the mainframe computer, in a multi-user single large, time-shared computer owned by an organization. The second era of computing was the PC, personal computer that was individually owned and used primarily by one person (Krumm, 2010). Many employees could be vulnerable to risks of social engineering, in which to become victimized to take a certain action to achieve goals, using neuro-linguistic hacking for building rapport in communication to gain information. Building knowledge systems structurally could provide systematic databases and helpful document storage tools for semi-structured knowledge systems, social media and other rich media.

The public workforce and leaders in U.S. seek to address many needs of all staff, in today's cyber-intense world, and surely no issue is more important than to provide competitive societal information-age and pertinent ITS training, to meet societal demands in a digitally interconnected world. Technological communications require everyone's diligent exercise to verbalize thoughts. Staff, faculties, and students could socialize with one-another through computer-mediated communications and social media, opening doors to compromise privacy of vulnerable subjects (Tabrizi, 2019). The use of search engines, such as Google, Yahoo or Bing, which use search engine optimization (SEO) to rank websites and enable Internet-users search for specific products or services ease accessibility to the Internet searches, which require cyber and information security awareness prior to remote work exposure.

Evaluating the systems architecture and development for analysis of threats, which might surface could play an important role for assessing the vulnerabilities and management of the various forms of

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

targeted attacks on networks or devices. Threat actors are motivated to gain competitive advantage by accessing information about "political, economic, technical, or military" proprietary knowledge (Giandomenico, 2017, para. iv), which could be present in forms of scientific and technological developments, and competitions. Threat actors target attacks in forms of threat vectors to spearphish forms of hacking attempts to target an attack, to gain an advantage over intellectual property (Ferrillo, 2015). The artificial intelligence programs use of modern technologies disguise, parse, and analyze information, directing attention to greater emphasis on monitoring internetworking and exercise of cybersecurity awareness (Oltsik, 2018). Appropriate perception of risk could drive assurance decisions to implement choices in policies, practices, tools, and restrictions, based on the perception and impact of threat. A variety of cybersecurity measures and recommendations, established through the National Institute for Standards and Technology Cybersecurity Framework could guide the organizations and institutions to analyze and measure the current state of security and assurance that might be necessary in an event to react and allow for recovery.

The analysis of organizational security postures could help to improve accuracy of the threat models, which could support organizations to maintain resilience in threat environments with efforts to gain insights and counter cyber-attacks against unprecedented vulnerabilities of assets. Monitoring predictive analytics through use of big data could raise the organizations' attention to details in information technology (IT) initiatives and implementation of security principles, and policies in every phase of enterprise-wide endeavors through prevention of private and protected data losses from cyber-crimes (Australian Government – Business, 2018, jul). A cybersecure and aware ecosystem's reliance on mitigating risks from a variety of cyber-threats from a network of computers might benefit from preemptive measures to prevent risks of cyber-attacks in internetworking. A variety of attacks from a network of computers, compromised with malware that could form into botnets, present in many forms through ambiguity might cause an end-user's unintended attempt of installing the malware.

Use of neural networks and AI could provide algorithms to correlate data in a timed-series deep learning for a classification to help ML to recognize patterns. The innovations in communication systems improve collaboration and organizational interactions by removing barriers in sharing information and increasing organization's sustainability, and business continuity to overcome the threats of catastrophic cybersecurity attacks, such as polymorphic malware that transform and conceal threats through AI. Incorporating public key infrastructures to detect intrusions through ensemble models' *digital signatures, network system activity logs, definitive activity and behavior of users' records and transactions, mobile devices, evidence of compromise, identification of data, intrusion detection systems* (Tabrizi, 2021, p. 155) could provide valuable machine data to ease decisions. Additionally, a combination of models in ML improve the performance of detecting intrusions in organizational networks.

Purpose and Method

The purpose of the qualitative design case study narrative was to explore prospects for integrating cybersecurity education into elementary school children's curriculum through interviews of elementary

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

schoolteachers, IT experts, and parents to gain feedback about perceptions on cybersecurity knowledge and awareness. Oversampling of 100 eligible participants helped this qualitative exploratory single case-study's findings through gathering inputs from 16 study participants to arrive at a common theme for monitoring children's internetworking while teaching children to exercise awareness and cybersecurity, in social-networking and gaming. The triangulation of perceptions of six elementary schoolteachers and leaders, six information technology (IT) experts, and four parents of elementary school children about anchored learning opportunities for cybersecurity awareness in children's elementary schools' curriculum provided the opportunity to reinforce the importance of implementing cyber-safety education in schools. Furthermore, the study's findings helped to explore a variety of vulnerabilities in people, in times of global turmoil when the risks for potential exploitation, necessitates protecting the wellbeing of children who are society's most valuable assets and are at risk during the maliciously motivated cyber disruptions. Accordingly, the qualitative exploratory case study's findings related to the study's focus on the future of a cyber-secure and aware workforce, establishing a parallel dependency on integrating cybersecurity awareness training and raising cybersecurity awareness among all educational staff in helping to identify the escalation of a variety of attacks on the society.

The research focused on a central phenomenon to consider children's cybersecurity knowledge and awareness through understanding "distinctive contribution, [and opinions,] joined to the data" for this research (Merriam & Tisdal, 2015, p. 17). The postmodernist and post-structural forms of the abovementioned qualitative research strived to make subjectivity of this research and participants, visible although the research did not instigate own influence. Accordingly, the subjectivity was not the focus of the qualitative study and the qualitative research could lack theory, failing to explain a phenomenon, adequately and cause research findings to explain the phenomenon. The preceding study's inductive findings helped to develop "themes, categories, typologies, concepts, tentative hypotheses, and even theory [through an inductive process] from observations and intuitive understandings gleaned from being in the" software development and security field (Merriam & Tisdal, 2015, p.17). Merriam and Tisdal (2015) depicted that "bits and pieces of information from interviews, observations, or documents are combined and ordered into larger themes, [to allow assessing the level of cybersecurity awareness instructions at schools and research development] from the particular to the general" (Merriam & Tisdal, 2015, p. 17). In this qualitative study, an exploration of central phenomenon occurred through analyzing the schoolteachers, IT experts, and parents' perspective of children's IS security knowledge and awareness, needs, and uses to suggest implementation of protective measures to preserve confidentiality, integrity, and availability of information.

Population and Sample

The sample site was a local school district, with many diverse cultures that volunteered to participate in this study and reflect upon the typical situation in the school (Kane, 2016). Additionally, a diverse group of schoolteachers, IT experts, and parents of elementary school children from the sample site provided rich descriptive data for explanations and recommendations (Yin, 2018). The goal of this research was to collect and evaluate elementary schoolteachers', IT experts', and parents' opinions about integrating IT and security awareness into elementary school education and to understand current program implementation. The study's participants agreed with the need to guide children to partake in positive

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

aspects of the digital communication, with an emphasis on training young children to ask for parental permission before accessing online content while training older children to exercise judgement to recognize, question, and identify unacceptable content.

Analysis

The present case study into the perceptions of elementary schoolteachers, IT experts, and parents of elementary school children allowed exploration into the cybersecurity awareness educational phenomenon through a combination of methods of data collection to investigate the problem under research and to provide answers to the central research questions and research question(s). Identification of sub-questions helped to refine the central research question to add value to the body of knowledge, in which "a small number of [sub-questions helped in refining] the central question" (Creswell, 2013, p. 140). Data was "not tested deductively [and the framework satisfied through learnings, inductively,] in the field" that allowed focus on the process of developing this study's themes through inquiry and interpretation of the initial questionnaire, face-to-face and phone interview data (Merriam & Tisdal, 2015, p. 17). In contrast, inductive reasoning was applied to understand participant comments and insights.

Research Questions and Findings

The individuals in the IT community who manage, process, or use information technologies for teaching, or personal use participated and expressed interest in reducing noise for resolving the challenging security dilemmas, which associated with children's levels of cybersecurity knowledge and awareness. The results from the abovementioned qualitative exploratory case study were helpful in determining educational leaders' use of information technology systems (ITS) improvements to help advancements in education. The technological innovations in educational processes directed attention to recognize present paradigm for incorporating cybersecurity awareness in elementary school children's active educational processes to acquaint children to exercise cybersecurity on the internet. The rigor in this study helped to understand advancements in education to investigate current technological improvements, specifically cybersecurity anchored teaching practices in elementary schools and kindergarten-through-sixth-grade children's education.

This study's objective was to focus this qualitative research study to explore perceptions of a stratified judgment sample of 15 elementary school teachers, five IT experts, and five parents of elementary school children to infer common themes among study participants within the school district. The following cybersecurity themes were arrived throughout this study's data collection efforts; (a) children's need of age-appropriate personal safety and cybersecurity awareness, (b) continuation of the current effective character, health and safety, and Internet safety education as opposed to standardizing integration of cybersecurity education into elementary schools' education, (c) continuation of the current cyber-bullying and awareness programs in elementary school children's character and Internet safety education in addition to continuing to teach parents to provide guidance during children's internetworking, and to monitor children's internetworking to decrease children's exposure to risks

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

during Internet gaming and social networking, (d) continuation of the current programs to help children develop the critical thinking ability to evaluate information and content, build children's recognition of the credibility of online research content, negative aspects of online gaming and communication, and awareness to exercise caution in the cyber-space, and (e) to continue to teach children to secure online accounts while teaching children to guard against giving-out personal information. Accordingly, a common dilemma in cybersecurity sectors and organizations is in the process of educating Cybersmart workforce to flourish cybersecurity knowledge for information retrieval and accessibility, development of educational software and Internet sites, online gaming sites, and to restrict unaware information use. The study intended to identify inclusion of IT security in the elementary school curricula and its effectiveness through exploring the answer to the following central research question:

1. How might integration of cybersecurity education into elementary schools reduce children's Internet risks?

The research question was answered through an analysis of data gathered during an IS security study of elementary schoolteachers, IT experts, and parents to assist with clarifying issues with computer education and proper use of handling information. Perceptions of elementary schoolteachers, IT experts, and parents about children's knowledge and awareness of cybersecurity helped to develop an understanding about children's cybersecurity needs. Additionally, the interview process clarified assessment of the following sub-questions:

1.1. How might cybersecurity education decrease children's risk of gaining exposure to online vulnerabilities?

The increases in security awareness and children's knowledge to take precautions against motives for cyber-bullying or online threats might direct children's personal safety and cybersecurity. The results from the present qualitative exploratory case study were helpful in determining educational leaders' use of ITS improvements to help advancements in education. Accordingly, the educational system could approach security by integrating cybersecurity awareness in societies to help with pervasiveness of technologies and addressing cyber-crimes (Business Solver, 2018). Interviews of elementary schoolteachers, educational leaders, Information Technology (IT) experts, and parents of elementary school children helped to explore cybersecurity awareness of children. Educational leaders' IT curriculum improvements are helpful in children's educational advancements and developments; meanwhile promoting safe-online educational websites. Children might accidentally access websites, encompassing artificial intelligence programs with use of modern technologies to disguise, parse, and analyze information, directing attention to greater emphasis on monitoring children's internetworking and exercise of cybersecurity awareness.

1.2. How might cybersecurity education teach children to protect personally identifiable information (PII) when engaging in online activities through electronic mediums, telecommunications, and computing?

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

The adoption of a measurable success in children's cybersecurity knowledge and awareness education was acknowledged to help children build confidence in handling risks of online threats with pervasive computing. Children's active participation to learn to protect themselves against vulnerabilities to online threats of phishing attacks, viruses, and adware could serve children as beneficial in protecting confidentiality of PII. Education about potential dangers present during internetworking, given modern cyber interconnected-world could promote aware-internetworking even when instances or numbers of Internet crimes may not be as high in comparison to other crimes present throughout the world.

Result of the Study

The results from the abovementioned qualitative exploratory case study were helpful in determining educational leaders' use of information technology systems (ITS) improvements to help advancements in education. This study's discoveries favored children's knowledge and awareness of Internet risks, however, this study's findings were mixed in validating the necessity of integrating new afterschool information security educational programs to supplement children's educational processes with additional cybersecurity awareness instructions. Elementary schools teach children to be safe on the internet meanwhile having current practices in-place to implement safeguards, which block certain websites on school networks and trigger alerts when accessing an unauthorized website. Different data analysis approaches helped understanding and analysis of narrative data to compare against study participants' responses to the questionnaire determined the effectiveness of current character, health and safety, and Internet safety education as sufficient as opposed to standardizing and integrating cybersecurity education into elementary schools' education.

This study's objective was to explore perceptions of a stratified judgment sample of 15 elementary school teachers, five IT experts, and five parents of elementary school children to infer common themes among study participants within the school district. This study's data collection helped to clarify instructional methods that the school district employs in improving elementary school children's knowledge and awareness to exercise cybersecurity on the internet. The findings of this study could not prove an advantage in children's education by supplementing children's present education with additional cybersecurity instructions, which benefit children who attend afterschool programs, only. All study participants agreed with the importance of teaching children age-appropriate security awareness of risks and Internet demeanor in schools. Internet safety education is taking place during DARE programs, and children's positive character education. A common concern among study participants centered on monitoring children's Internet activities or knowing how to encourage children to practice and learn positive Internet pursuits while discouraging children' negative exposure on Internet.

Study participants agreed with advancements in technology, unrestricted use, and the presence of social threats, which require children's sustainable cybersecurity awareness to meet present and future computing needs. The schoolteachers, IT experts, or parents' demographics and favorability of cybersecurity awareness in children were relative to age and, or grades of children. The cognizance about the Internet threats, which could present harm in the digital future and big data might require addressing the needs of the various generations in schools. Generation Z or Digital Natives (born from 1995 to 2012) might require different leadership strategies in incorporating a system to provide

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

appropriate security capabilities (Tabrizi, 2021). Furthermore, improvements in software assurance through applying processes and technologies could help achieving required level of confidence for software systems and services to function as intended, and free from vulnerabilities.

Recommendations of the Study

The awareness to detect the threat environment might help in an event that could necessitate recovery from intrusions, and failures to limit the vulnerability to risk of an attack. Additionally, awareness of cyber and computer literacy, and careful and aware internetworking might contribute to safe use of the Internet for communication, in handling Internet-of-things (IoT), social networking, and conducting and completing work assignments in the digital-age. The educational organizations could continue to monitor children's internetworking and cybersecurity practices before, during, and afterschool hours while increasing implementation of cybersecurity awareness education in children's character education and cyber-bullying prevention programs. Good educational processes could continue to promote children's cyber-secure online collaborative learning environment for all children, in grades kindergarten-through-sixth.

The present educational processes are advantageous in meeting children's research development in computing fields to help children with gaining essential awareness against unacceptable social threats, behaviors, and Internet bullying. All study participants agreed with the importance of introducing children to the age-appropriate use of technologies to help children's development of critical thinking abilities to judge disseminated information, recommending continuation of age-appropriate cybersecurity educational opportunities and safety measures for all children. The emphasis on elementary school children's need to learn to secure online accounts, limitations in children's cybersecurity knowledge and children's vulnerability to Internet risks were a common theme among educational leaders, IT experts, and parents because children do not have the ability to evaluate information and content, critically.

All study participants agreed with the necessity of children's recognition of the credibility of online research content, negative aspects of online gaming and communication, and awareness to exercise caution in the cyber-space. Children need to develop an understanding of risks, which may be present online, without getting discouraged to use internetworking tools. Lack of children's age-appropriate educational opportunities in gaining social, character, and cybersecurity awareness were not evident, in proving the necessity of supplementing elementary school children's DARE and character education that is offered to every child with extracurricular and additional cybersecurity awareness afterschool programs. However, learning good Internet safety habits by getting educated about security and positive Internet usage are essential in children's early education because children are trusting and need to learn to verify Internet content. Children's internetworking may present many risks as well as rewards, which children's cognitive ability may not allow them to judge information correctly and realize that the information obtained through friends, Internet, and other resources may not be factual. An attempt to stay safe and secure, online could reduce exposure to malware (Tabrizi, 2019). Accordingly, the interviews of elementary schoolteachers, educational leaders, Information Technology (IT) experts,

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

and parents of elementary school children helped to explore variety of vulnerabilities, necessitating cybersecurity awareness of children.

Conclusion

The need for the educational system to approach security by integrating cybersecurity awareness in societies could help to address cyber-crimes. Interviews of elementary schoolteachers, educational leaders, Information Technology (IT) experts, and parents of elementary school children helped to explore cybersecurity awareness of children. Educational leaders' IT curriculum improvements are helpful in children's educational advancements and developments; meanwhile promoting safe-online educational websites. The future of a cyber-secure and aware workforce will depend on integrating age-appropriate cybersecurity awareness in schools at all levels of education. Education about potential dangers present during internetworking, given modern cyber interconnected-world could promote aware-internetworking even when instances or numbers of Internet crimes may not be as high in comparison to other crimes present throughout the world.

The education in cyber-safety and cybersecurity for all children will prepare children to handle acts of a cyber-attack, in the modern computing era. The first era of computing was defined by the mainframe computer, in a multi-user single large time-shared computer owned by an organization. The second era of computing was the PC, personal computer that was individually owned and used primarily by one person (Krumm, 2010). Children could be vulnerable to risks of social engineering, in which to become victimized to take a certain action to achieve goals, using neuro-linguistic hacking for building rapport in communication to gain information (Hadnagy, 2010). Building children's knowledge systems structurally could provide systematic databases and helpful document storage tools for children's semi-structured knowledge systems, and other rich media, with built-in offense mechanisms denying persistent threats.

Summary

The public-school educators and leaders in U.S. seek to address many needs of all students, in all grade levels. In today's cyber-intense world, surely no topic is more important than to provide competitive societal information-age and ITS education within the United States, to meet societal demands in a digitally interconnected world. IT could help to reform educational means, facilitate efficiency to drive innovations, and channel effective exchange of information that might require children's awareness of social aspects, which surround Internet information access and retrieval processes (The Levin Institute, 2014). Children could socialize with one-another through computer-mediated communications. Additionally, children's use of search engines, such as Google, Yahoo or Bing, which use search engine optimization (SEO) to rank websites and enable Internet users search for specific products or services ease accessibility to the Internet searches, which require children's cyber and information security awareness prior to exposure. PCs and networks, saturated with viruses, "data-stealing programs[,] and financial scams [may allow risks of security vulnerability to various attacks through] e-mail, text message and surf the Internet" from mobile devices (Swartz, 2008, p. 2). Proactive awareness about safety

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

techniques on the internet is crucial to maintain proper conduct, limiting risk of unhealthy behaviors, such as engaging in social networking websites, disclosing personal information, or risk of victimization by an intruder.

Consumers, adolescents, adults, and marketers use of social networking websites to connect and interact with one-another and advertise services and goods could allow hackers to find vulnerabilities in victim's computers. Hackers detect flaws in websites to "compromise social-networking sites using unsecure Web 2.0 technologies to load malware onto the PCs of consumers" (p. 2). Cyber-crooks plant malicious code in vulnerable websites' JavaScript code on social-networking site to infect "a Web page," [with] "a snippet of malicious coding," [to redirect victims' browser] to a tainted webpage that "a hub server" [could download] data-stealing programs onto victims' hard drive (p. 3). Google search engine, Mozilla, and Facebook.com "are designed to steal user credentials or launch bigger attacks through the victim's social network of contacts" [through SQL injection] "to exploit users" (p. 2). A malicious code seems like a regular message from friends among Facebook friends and to cause preceding effects on the friends of the friends. Proper virus protection may help to defend against attacks to the personal data and avoid many problems (Swartz, 2008). Although Facebook, promptly, took care of the preceding issue, many social-networking users are subject to attacks because posting and sharing personal information could lead to instances of malware and various social-networking risks (Swartz, 2008). The above-mentioned attacks spread quickly and led to more security risks because people share personal information, and eventually allow intruders to expand attacks (Swartz, 2008). Cyber-crooks want a foothold on users' machines, by gaining entry to users' personal profiles. Accordingly, one out of four administrators do not permit social networking, by blocking harmful content while quarantining the users' access, compared against two out of three administrators who acknowledged users could download malware and transfer the malware to the organizational systems (Swartz, 2008). In today's cyber-intense world, surely no topic is more important than to provide competitive societal information-age and ITS education within the United States, to meet societal demands in a digitally interconnected world.

IT could help to reform educational means, facilitate efficiency to drive innovations, and channel effective exchange of information that might require children's awareness of social aspects, which surround Internet information access and retrieval processes (The Levin Institute, 2014). Children could socialize with one-another through computer-mediated communications. Additionally, children's use of search engines, such as Google, Yahoo or Bing, which use search engine optimization (SEO) to rank websites and enable Internet users search for specific products or services ease accessibility to the Internet searches, which require children's cyber and information security awareness prior to exposure. The various forms of targeted attacks to networks or devices, which children could use are present in forms of threat actors, motivated through collecting competitive information for "political, economic, technical, or military" gains (Giandomenico, 2017). Additionally, threat actors target attacks in forms of threat vectors to spearphish forms of hacking attempts to target an attack, to gain an advantage over intellectual property (Ferrillo, 2015). The artificial intelligence programs use of modern technologies disguise, parse, and analyze information, directing attention to greater emphasis on monitoring children's internetworking and exercise of cybersecurity awareness (Oltsik, 2018). The dangers of cyberattacks are abundant and the recurrent threats with any new technology, or

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

revitalization of an old technology within the ecosystem of digital world (Valdetero & Zetoony, 2014), for both the adult world of computer interface and in the programs that children utilize.

References

Australian Government - Business (2021, mar 15). How to protect your business from cyber threats. Retrieved from https://www.business.gov.au/risk-management/cyber-security/keep-your-business-safe-from-cyber-threats

Business Solver (2018). State of empathy 2018 executive summary: Strengthening business for sustainable success. ®Businessolver.com, Inc. 2018. Retrieved from https://info.businessolver.com/hubfs/empathy-2018/businessolver-empathy-executive-summary.pdf?hsCtaTracking=7e237aa9-1d60-4cfb-b9a9-2b881143391a%7C0c012412-b9e0-488a-8f56-4c153450c4fa

Cave, B. (2021, Aug 24). Privacy, vulnerabilities, and breaches, oh my. Bryan Cave Leighton Paisner (BCLP). Retrieved from https://www.bclplaw.com/print/content/1502892/Privacy-Vulnerabilities-and-Breaches-Oh-My.pdf

Creswell, J. (2013). Qualitative inquiry & research design: Choosing among five approaches (3rd ed.). Thousand Oaks, CA: Sage

Ferrillo, P.A. (2015). Navigating cybersecurity storm: A guide for directors and officers. Advisen, Ltd. Retrieved from https://www.weil.com/~/media/files/pdfs/navigatingcybersecuritystormbookfinal.pdf

Giandomenico, A. (2017). Know your enemy: Understanding threat actors. CSO: Fortinet. Retrieved from https://www.csoonline.com/article/3203804/security/know-your-enemy-understanding-threat-actors.html

Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.

Krumm, J. (2010). Ubiquitous computing fundamentals. CRC Press.

Merriam, S. D., & Tisdal, E. J. (2015). Qualitative research: A guide to design and implementation (4th ed.). San Francisco, CA: Jossey-Bass.

Nabi, A. (2017). Comparative study on identity management methods using blockchain. Retrieved from https://files.ifi.uzh.ch/CSG/staff/Rafati/ID%20Management%20using%20BC-Atif-VA.pdf

NCSAM 2019 (2019, October 8). October is national cybersecurity awareness month (NCSAM)! Retrieved from https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

Oltsik, J. (2018, March). An all-source approach to threat intelligence using recorded future. Retrieved from https://go.recordedfuture.com/hubfs/solution-briefs/esg.pdf

Tabrizi, A. S., Lao, T. (2018). The Refractive Thinker: Volume XV – Generations: Strategies for managing generations in the workforce anthology. In C. Lentz (Ed.), Chapter 4: Rethinking cybersecurity measures: Managing nonprofit inevitable cyber-vulnerabilities (pp. 69 to 86). Grayslake: IL: The Refractive Thinker Press.

Tabrizi, A. S. (2019). The Refractive Thinker: Volume XVI - Generations – Strategies for managing generations in the work force anthology - Information technology security gap: Consideration of a diverse multi-generational cybersecure workforce. The Lentz Leadership Institute.

Tabrizi, A. S. (2019, Jan). Cybersecurity awareness education: Rethinking measures to develop the next generation. School of Advanced Studies, University of Phoenix. International technology and distance learning.

Valdetero, J., & Zetoony, D. (2014). Data security breaches: Incident preparedness and response. Bryan Cave LLP. Washington Legal Foundation © 2014. Retrieved from https://www.bryancave.com/images/content/2/2/v2/2285/DataBreachHandbookValdeteroand Zetoony.pdf

Yin, R. K. (2018). Case study research: Design and methods (6th ed.). Thousand Oaks, CA: Sage Publications.

ACKNOWLEDGEMENTS / AUTHOR BIOGRAPHY

The author, Dr. Avideh Sadaghiani-Tabrizi, thanks the Center for Educational and Instructional Technology Research, College of Doctoral Studies, University of Phoenix, for supporting the preparation of this article.

Dr. Avideh Tabrizi is from the Capital Region in upstate New York and holds several accredited degrees: a Doctorate of Management in Organizational Leadership with Specialization in Information Systems Technology (DM / IST) and a Master of Science in Computer Information Systems (MS / CIS) from the School of Advanced Studies of the University of Phoenix. Dr. Avideh Tabrizi is a security expert and a portfolio architect at the Office of Information Technology Services – Chief Technology Office – Architecture Design - Research & Development, participating in design and maintenance of enterprise systems with over 20 years of service at the New York State government. She enjoys travel and likes to engage in various physical fitness activities when possible.

Dr. Avideh Tabrizi's doctoral study entitled Integrating Cybersecurity Education in K-6 Curriculum: Schoolteachers, IT Experts, and Parents' Perceptions, provided her the opportunity to gain a deeper

ISSN 2164-2877 (print)
ISSN 2164-2885 (online)

understanding about academic needs of children, to suggest and facilitate improvements in the school district. Additionally, the continual publishing efforts through the University of Phoenix - Center of Educational and Instructional Technology Research has enabled her much mastery in her style of publications. To reach Dr. Avideh Tabrizi for information on consulting or doctoral coaching, please e-mail: avidehst@email.phoenix.edu.