Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

Global Journal of Engineering and Technology Advances
eISSN:2582-5003
Global Scholar Press, INDIA

(Review Article)

Cyberpsychology can improve cybersecurity leadership in higher education

Bradley Fowler *

Capitol Technology University, Dissertation Chair, Laurel, MD, USA.

Global Journal of Engineering and Technology Advances, 2024, 20(01), 036–044

Publication history: Received on 27 May 2024; revised on 02 July 2024; accepted on 04 July 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.20.1.0116

Abstract

Cyberpsychology has grown exponentially in supporting researchers understanding of the significance of human behavior in correlation with social media technology as a tool for business communication and engagement. Research coupled with quantitative and qualitative statistics, notes that cyberpsychology is woven in social media and is a key factor of social engineering. Additional research conveys cyberbullying is a key area of importance aligning with cyberpsychology, which helps researchers begin to understand the motive behind cybercriminals malicious activities. However, there is limited research providing the correlation between the role cyberpsychology plays in cybersecurity leadership for these institutions and the malicious attitude cybercriminals have that invoke this human behavior. Therefore, this research enables readers to comprehend the nexus regarding the utilization of qualitative grounded theory lite research in providing answers to three questions. First question is, what role does cyberpsychology play in correlation with institutions of higher education cybercrime victimization, in alignment with social media and social engineering activity deployed by higher education executive leadership, administrators, faculty, and staff that invoke cyberattacks? The second question asks, what attitude and human behavior do executive leaders, administrators, faculty, and staff, have towards completing and adhering to cybersecurity awareness training provided at institutions of higher education as a deterrence method? The third question asks, how can qualitative grounded theory lite research help the researcher understand how cyberpsychology can improve cybersecurity leadership for institutions of higher education? Thus, this research provides an introduction, research method, results, discussion, and answers to these questions, including a list of references.

Keywords: Cyberpsychology; Cyber Social Engagement; Social Media Cyberpsychology; Cyberpsychology Cybercrime; Human Behavior in Social Media.

1. Introduction

Since the inception of research engulfing cyberpsychology began in the late 1990s early 2000s, consistent research has provided clarity regarding the collaboration of psychology and cyber applications, tools, and attacks. In 2024, psychologists continue providing details regarding the impact cyberpsychology has in helping understand human behavior, emotions, and activities involving technology and cybercrime. One pioneer Cyberpsychologist that continues improving knowledge sharing in the field of cyberpsychology is Dr. Mary Aiken, author of *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online.* Dr. Aiken enables readers to grasp knowledge regarding how cyberpsychology has become a force to reckon with. Dr. Aiken leads us to acknowledge the impact cyberpsychology has on social media and social engineering. This information has become a bridge to deciphering how to better assess, define, implement, manage, and control risk when using social media [1]. However, with the growing number of cyber incidents targeting institutions of higher education, impeding their ability to thoroughly understand social engineering as it correlates with safeguarding sensitive information assets from cybercriminals. There is a growing need to understand how to resolve this issue. Thus, to derive at a resolution that can be universally implemented, the researcher chose qualitative grounded theory lite research. In doing so, the researcher discovered

* Corresponding author: Bradley Fowler

that qualitative grounded theory research is commonly utilized in social research and is inductive and conceptual [2]. Research also reports this research method is scalable because it emphasizes correlating data collection and analysis, while providing tools for deploying theories [3]. Unlike traditional qualitative grounded theory research, qualitative grounded theory lite research does not require deriving a theory from the correlating data collection and analysis. Instead, this research method helps validate research data collection by focusing on developing a preliminary comprehension of a topic, i.e., cyberpsychology to help improve cybersecurity leadership at institutions of higher education. In addition, this research model requires defining categories and concepts, and assessing the relation between the two, minus the need to define a formal theory [4]. But to effectively develop a preliminary comprehension of the central phenomenon requires defining categories and concepts of human behavior deployed by cybercriminals and assessing the type of cyberattack incidents deployed against each institution of higher education, targeting executive leaders, administrators, faculty, and staff, through social media and social engineering.

Furthermore, it is important to determine the concepts of cybersecurity leadership currently installed at each institution of higher education, worldwide, and assess the relationship executive leaders, administrators, faculty, and staff share through social media and social engineering at each institution, without formulating a theory. However, when you consider the limited resources and time to survey all institutions of higher education, worldwide, including their executive leaders, administrators, faculty, and staff; to effectively determine the current scale of cybersecurity leadership at each institution of higher education, through the lens of cyberpsychology, based on two variables- i.e., social media and social engineering; utilization of qualitative grounded theory lite research is a best fit.

Qualitative grounded theory lite research is a good fit, because this approach aligns with limited resources and time constraints required to complete the research study. Given the scale of research needed to assess all institutions of higher education, worldwide, this research method eliminates the need for a broad scope research study. This research is less rigorous. This research is less resource-intensive and can clarify the central phenomenon. This grounded theory method is used when research is exploratory in nature. Therefore, utilizing this research enables the researcher to align this study using a coding system traditionally utilized in grounded theory research, including open coding, axial coding, and selective coding.

Open coding involves compiling collected documents and creating excerpts from such to compare and contrast with additional excerpts. This method is called consistent comparative. This approach requires comparing documents relating to the central phenomenon reported by the same person and comparing similar excerpts compiled by and authored by different individuals, and comparing those experiences with similar excerpts, to compare excerpts as they differ consistently. For example, using a collection of journal articles regarding cyberpsychology and its role in human behavior, and comparing those collected articles with articles on a similar subject, but authored by other writers, who, too, should be compared with the delivery of content provided by each of the published authors. Enables the researcher to group similar discoveries of details and events to begin comparison and creating concepts of validity.

The next phase of grounded theory research is axial coding, which involves discovering a correlation between multiple codes, which are grouped and categorized. This helped the researcher discover the correlation of varies codes together. For instance, previously, the researcher mentioned usage of collected documents to compare published article content from various authors that were similar in reporting details regarding the central phenomenon. Yet, during a constant comparison, it is imperative to also analyze content to determine codes of categories that can support the continued development of a theory that derives from the content of these collected documents. This will begin to prove some content contradictory, increase theories, and support existing codes and categories, the researcher already created. This enables the researcher to improve his/her approach to developing a resolution to the central phenomenon.

With selective coding, the researcher is required to connect all his/her codes and categories into one category. This category should represent the central focus of the research and becomes the core concept of the research study. This core concept can also establish new grounded theory. But since the research for this study is rooted in qualitative grounded theory lite, there is no need to define a new theory. Instead, the researcher hopes to answer questions relating to the central phenomenon, by examining attitudes and human behavior of lived experiences delivered via a collection of documents published by peer reviewers, who, too, have an interest in answering how cyberpsychology can be helpful in establishing cybersecurity leadership at institutions of higher education. Most importantly, this enables the researcher to assess how cyberpsychology can improve cybersecurity leadership at institutions of higher education. Thus, this research provides answers regarding the role cyberpsychology plays in correlation with cybercrime victimization through social media and social engineering actions deployed by executive leaders, administrators, faculty, and staff. This research also answers the questions regarding the attitudes and human behavior of executive leaders, administrators, faculty, and staff, towards completing and adhering to cybersecurity awareness training as a deterrence method. Finally, this research answers the question regarding how cyberpsychology can help improve cybersecurity leadership for higher education.

However, to thoroughly comprehend this research topic requires understanding what cyberpsychology is and how cyberpsychology can improve cybersecurity leadership at institutions of higher education. Cyberpsychology encompasses a method people use to interact using computers or digital applications and devices, in alignment with their individual or group emotions correlating with brain activities. Dr. Mary Aiken believes cyberpsychology can help solve cybercrimes. Through the central phenomenon, cyberpsychology can also be instrumental in helping deter cybercrime from impacting institutions of higher education, as well as improve cybersecurity leadership. Cyberpsychology can also be useful when studying human engagement with emerging technologies, such as the internet, mobile devices, gaming consoles, virtual reality, and other technology (i.e., artificial intelligence). Additionally, cyberpsychology assesses the impact of evolving concepts and trends as they relate to individuals. To be useful in supporting a resolution to the central phenomenon, it is invaluable to determine the human behavior commonly exercised by cybercriminals targeting institutions of higher education, as well as the human behavior and attitudes of executive leaders, administrators, faculty, and staff at institutions of higher education, to pinpoint how such persons are being targeting successfully and victimized, through social media and social engineering. Thus, the researcher presents details of his findings via his research method.

2. Research Method

Utilizing grounded theory open coding, enabled the researcher to collect and compare documents published reporting similar concepts regarding the central phenomenon. The first collected document derives from Standford University and was reported by Stu Sjouwerman, who explains that an estimated 49% of employees admitted they are almost sure they have made mistakes at work that may have led to security breaches at their organization [5]. These security breach incidents resulted from phishing attacks. Phishing attacks are deployed to confiscate personal information, including organizational confidential data [6]. When an attacker has duplicated the behavior of legitimized Websites, he/she sends text messages, email messages, or connects with victims in social networking sites. This action enables attackers to collect sensitive data from executive leaders, administrators, faculty, and staff, including their user account login information and credit/debit card numbers, when such persons are not trained by their institution's cybersecurity leaders, to understand how to decipher the difference between a real person they know and someone emulating such an individual.

The number of phishing attacks deployed against institutions of higher education soared between 2021 and 2024. Reports convey that in 2021 institutions of higher education in the United Kingdom were targeted by cyber-criminals, resulting in an increase in cybercrime incidents. However, when using axial coding, the researcher compared and contrasted reports of cyberattack incidents at institutions of higher education, in the two previous years, to determine the compared activities and human behavior continually deployed by cybercriminals and executive leaders, administrators, faculty, and staff. This enabled the researcher to learn that in 2023, the number of successful cyberattacks deployed against institutions of higher education reached a staggering 2.2 million reported breached credentials that were made readily available on the dark web [7]. Furthermore, a UK report shared 22 higher education institutions reported that cybersecurity and information governance was a top reported risk factor. Then in September 2023, 100 UK institutions, which 56% registered institutions belong to Russell Group Universities, a group of prestigious, research-intensive universities, including Oxford and Cambridge, experienced an estimated 500,000 credentials being stolen [8]. This resulted in an 85% increase in phishing attacks deployed against institutions of higher education in the UK. Additional types of cyberattacks deployed against institutions of higher education between 2021 and 2024, worldwide, include ransomware, malware, viruses, and spyware. Ransomware attacks deployed against institutions of higher education in 2021 reached a staggering 56% compared with ransomware attacks deployed in 2018-2020. These attacks were even higher from 2022 to 2023, with numbers reaching 80%. The average pay-out for ransomware attacks in 2023 reached $3.5 million [9].

Thus, understanding how institutions of higher education can deter these attacks from happening remains puzzling. In fact, research reports increased usage of cybersecurity policy and awareness training has become essential tools in helping higher education institutions slow-down this growing threat. However, although this strategy has been discussed and implemented in some higher education institutions, particularly in the United Kingdom, with 90% of higher education institutions reporting implementing such. Additional research must be deployed to understand the success rate of institutions using this strategy to thwart and deter successful cyberattacks.

Furthermore, when selective coding is implemented, the researcher was able to compile all theories derived from formal research published on the central phenomenon determine that utilization of cyberpsychology can improve cybersecurity leadership at institutions of higher education. The researcher's research method also shows that common cyberpsychology human behavior attitudes cybercriminals share involve the feelings and emotions of greed, envy, and narcissism. After all, the type of human behavior cybercriminals engages in when targeting institutions of higher education, include ransomware attacks, business email compromise, distributed denial of service attacks, and invasion of online learning management platforms and institutional virtual meeting rooms, groups, and discussions [10]. Research reports that an estimated 90% of cybercrime incidents targeting institutions of higher education involve money as a reward for ransomware attacks. Research also reports that cybercriminals act of attack align with the emotion- envy, which research reported by Dr. Neel Burton, conveys that envy is a personal feeling of pain caused by an inner desire for the advantages of others. Dr. Burton explains that envy is embedded in all the human psyche. Dr. Burton believes that envy is deployed when a person feels they must compete with someone, or they desire to have what others have. When this is assessed in correlation with institutions of higher education, it is common these institutions bred competitiveness, which alludes to some people being incapable of being accepted into many institutions of higher education, due to a lack of academic excellence, or their inability to compete with undergrad and graduate-level learners. Thus, it can be determined that cybercriminals targeting institutions of higher education are doing so because they envy others ability to be competitive and demonstrate academic excellence. This type of envy is camouflaged through acts of resentment, attempting to use an advanced skill (i.e., hacking) to prove one can compete with enrolled students at institutions of higher education, while not attending. This also demonstrates cyberbullying.

Additionally, cybercriminals deploy cyberattack through narcissism, by demonstrating an inflated sense of self-importance and an inability to empathize with others [11]. In fact, Dr. Burgo explains that narcissistic people tend to consider themselves winners and everyone else losers. Dr. Burgo reports that narcissistic people will stop at nothing to prove they are better than those around them [12]. This correlates with the latter ideology that envy also plays a role in cybercriminal behavior. This form of cyberpsychology can be useful in supporting consistent research regarding these three areas of focus, to begin adopting methods of deterrence that decreases the value of cybercriminals. Thus, using cyberpsychology empowers institutions of higher education to think effectively in meeting the needs of their institutional network security, including their information assurance, information security for information systems, information technology, and cloud applications. While no two institutions will be modifying their approach and deploying methodologies identically. This approach helps organize improved strategies that rise above typical methods of cybersecurity and employ cybersecurity leadership fit for each individual institution's technology and cybersecurity leadership needs.

Furthermore, when assessing the attitude and human behavior of executive leaders, administrators, faculty, and staff at institutions of higher education, enabling cybercriminals to successfully victimize institutions of higher education through social media and social engineering. Research reported by Harvard Business Review authors Keri Pearlson and Nelson Novaes Neto, convey that Boards of Directors often are not aware of current trends in cybersecurity leadership they should be knowledgeable of, or aware of how cyberattacks can be prevented [13]. Pearlson and Neto also explain that 50% of responses collected from a survey shared with Board of Directors regarding their role in helping thwart cyberattacks, reported there is no current consensus about their role and responsibilities [14]. Thus, when utilizing cyberpsychology as a method of determining the attitude and human behavior of executive leaders and administrators at institutions of higher education, the common attitude is bewilderment. Bewilderment is commonly displayed through indecisiveness. People who are bewildered have an inability to think clearly [15]. Human behavior differs greatly because no two executive leaders, administrators, faculty, or staff, at any institution of higher education, worldwide, can compare. This leads to an inconsistency of facts that can also lead to contradictory, as pointed out previously in relation to using grounded theory research.

When applying the qualitative grounded theory lite research method, it is proven valid that the attitude and human behavior of executive leaders, administrators, faculty, and staff at institutions of higher education, towards completing awareness training regarding cybersecurity leadership as a deterrence method, is often welcomed with a positive attitude. However, the difference across each institution, is that awareness training can be developed and delivered ineffectively, leading to inconsistency of human behavior to ensure safeguarding of sensitive information. When aligned with usage of social media and social engineering tactics deployed by cybercriminals, targeting institutions of higher education, research reported by Clayton State University in the United States, reports that spear phishing has become a sophisticated attack method much advanced than phishing. This approach enables threat actors to collect information on key people through targeting institutions and assessing the BIO details on a university website to gain names of executive leaders, administrators, faculty, and staff. This enables attackers to craft personalized email that encourages and invoke targeted employees to render confidential details and share sensitive information. Spear phishing is personalized in alignment with traditional spam, and using reputation filters consistently fails to detect the malicious files embedded in such emails [18]. Research also conveys that business email compromise, which was mentioned previously, is also known as CEO fraud or whaling. This method of attack involves attackers emailing accounts belonging to high-profile executive leaders and requesting financial funds be transferred into bank accounts controlled by the attacker. The target victims for this fraud type include executive leaders, payroll officers, and human resource staff with responsibilities governing institutions of higher education [16].

The cyberpsychology human behavior commonly demonstrated by all executive leaders, administrators, faculty, and staff, include attention span, which the Parliamentary Office of Science and Technology explains that too much information boggles many people into a workplace that is ineffectively managed. This impacts their ability to remember certain things, particularly, issues relating to cyber deterrence when most needed. This also includes perception, which each person carries their own ideology of what cyberattacks are and how they are deployed. What one executive leader may perceive as a safe email from an assumed executive leader. Another executive leader will raise an eyebrow and question the reliability and validity of the email content. Thus, unless effective awareness training is consistently provided, attendees are not effectively assessed on their awareness practice and comprehension of the information provided during training. Perceptions are easily modified. Furthermore, memory also differs from person to person. If we train ten executive leaders to remember what phishing and spear phishing is and how they differ, and neglect to assess the memory of each person trained, how can any institution ensure their personnel are knowledgeable and capable of adhering to what they have been trained to comprehend. Another human behavior commonly shared with executive leaders is logical reasoning. Research reports that failures in reasoning and decision making often embody severe consequences for complex systems, including cybersecurity leadership at institutions of higher education [17].

Thus, qualitative grounded theory lite research helps understand the reality of human behavior through the lens of researched documents that report similar content relating to the central phenomenon. This enables cyberpsychology to improve how cybersecurity leaders at institutions of higher education assess, develop, implement, and manage cybersecurity leadership and implement cybersecurity policy and compliance regulatory that impacts adherence and helps reduce cyber-attack incidents. When cybersecurity leadership is created with knowledge-based framework, correlating with the psychological behavior commonly known, and provides resolution through a systematic development of training, management, and penalties. The rate of successful cyberattack incidents begins to decrease. In fact, the researcher shares his results in the next section.

3. Results

As a result of this qualitative grounded theory lite research, it is proven that cyberpsychology can benefit institutions of higher education in adopting new methods of awareness training, and auditing human behavior of executive leaders, administrators, faculty, and staff, to decrease successful cyberattacks externally and internally. Research compiled from institutions of higher education in the United States, Europe, and Asia, proves that these incidents of attack are similar. This similarity has provided clarity regarding the type of cybercrimes institutions of higher education are experiencing, as well as conveys the statistical measure of attack, and the rate of response time deployed across various institutions of higher education, to determine how any institution executive leadership will respond to cyberattack methods, in alignment with the scale of knowledge their IT practitioners and cybersecurity leaders provide through training. When these individuals lack the essential skills and awareness training to effectively prepare others in their institution to be aware and prepared to defend the network assets against cyberattacks, this, too, stagnates their ability to thwart and deter cyberattack incidents. Research reports that common human mistakes deployed in a workplace account for 88% of cyberattack breaches. Research also reports that businesses and institutions of higher education lack widespread knowledge regarding adequate cybersecurity policies, training, and awareness to ensure protection of information systems. Research also adds that a security breach can occur throughout an institution from anywhere and result in a severe catastrophic incident. Furthermore, it is reported that ineffective management of system vulnerabilities and mispatching of known vulnerabilities impacts the success of deterrence methods commonly implemented by institutions of higher education IT practitioners. Alarmingly, many institutions of higher education are limited in hiring adequate IT professionals, who are knowledgeable of cybersecurity requirements, strategies, methods, and policies that must be adhered to in alignment with federal, state, and global law and policy, relating to information systems, information technology, and cloud services, infrastructure, and platforms. This, too, adds to the pressure of cybersecurity leadership that thwarts cyber-attack incidents correctly and effectively.

As a result of this information, it is valid that qualitative grounded theory lite research enables the researcher to answer the primary three questions presented, regarding how cyberpsychology can be useful in helping institutions of higher education implement cybersecurity leadership, as well as in answering the question regarding the attitude and human behavior cybercriminals deploy when targeting institutions of higher education executive leadership, administrators, faculty, and staff, and the attitude and human behavior these personnel members embody towards adherence to workplace cybersecurity policy awareness and training. This research method also provided results that lead the researcher to answer what role cyberpsychology plays in improving cybersecurity leadership at institutions of higher education.

After all, the researcher shared that cyberpsychology aligns with social media and social engineering and the human behavior correlating with such, to enable cyber attackers to create strategies that provide detailed information to connect with their targets. Using a university Web site to gather information has been one approach. Using social media, such as LinkedIn, where many institutions of higher education executive leaders, administrators, faculty, and staff maintain professional profiles consistently promoting their place of work, activities, events, and sharing personal and professional feedback and comments in their posts. Enables cyber attackers to profile and social engineer these targets and craft their scheme of approach.

The researcher also used the research method to understand the attitude and human behavior deployed by cybercriminals and executive leaders, administrators, faculty, and staff. The coding methods deployed shared in grounded theory research enabled the researcher to collect documents, assess the correlation shared within these documents, and determine what attitudes and human behavior is commonly, including greed, envy, bewilderment, carelessness, and forgetfulness. These attitudes and human behaviors are key tools to improve methods of deterrence in cyber attackers' ability to attack and improve the type of training needed at institutions of higher education, to effectively deter successful attacks. These results play a key role in what needs to be done to resolve this problem adequately and consistently. Thus, the researcher shares a discussion regarding his resolution.

4. Discussion

Using cyberpsychology to assess cybercriminals attitude and human behavior as it correlates with successful cyberattack incidents, can be achieved in several ways. First, cyberbullying is a common thread of cyberpsychology. Knowing that cybercriminals are targeting institutions of higher education demands institutions of higher education improve cybersecurity leadership. Consider cyberbullying cybercriminals. To achieve this requires entrapping cybercriminals, gaining access to their technology devices and tools and crippling them. Through usage of intrusion detection and intrusion prevention (IDIP) software, cybersecurity leaders can begin collecting vital information regarding the attacker's primary location of attack, including their IP address. IDIP software operates like an alarm system. This alarm notifies network administrators when unusual activity is detected and helps prevent successful intrusion. Research reports that when a system embodies IDIP, the system can stop attacks by terminating the network connection and the attacker's user session. This also modifies the security environment via reconfiguring network devices, including firewalls, routers, and switches that block access to the targeted systems, as well as modify the attacker's content by making it benign [18]. IDIP is also instrumental in rendering a mechanism that severs the communication circuit, when the institution is attacked by a Distributed Denial of Service Attack, which is another common method of cyber-attack currently being used. Institutions of higher education must be knowledgeable that their IT staff and cybersecurity leaders have knowledge of these techniques and strategies, to be effective. There are host-based IDIP applications that work best with classifying various categories of systems and data files [19]. Then there are network-based IDIP applications, which rest in a host and monitor only activities on the host and monitor network traffic. This is essential to key prevention. The setback to utilizing this approach is that IDIP applications can generate false alarms. Using a host-based IDIP enables the organization to monitor multiple computers at once. This is a benefit to an organization working with a small scale of IT professionals. There is also a signature-based IDIP, which operates like an anti-virus software application. This approach examines the traffic for anything matching the signature, which compromises preconfigured and predetermined attack patterns. To be successful in usage requires consistently updating the signatures as new attack methods are discovered. Neglecting to do so enables new attack methods to be successful. Thus, it is recommended IT personnel collect and analyze data over a long timeline; this requires scalability. Scalability is commonly available through cloud application storage. Then there is anomaly-based IDIP, which is a behavior-based system, which collects data from normal traffic and establishes a baseline. This includes collecting samples of network activity and utilizing statistics and comparing samples to the baseline to ensure improved awareness of potential threats to the network. If any traffic falls outside the baseline, the IDIP alerts the system administrator, rendering time to patch the vulnerabilities before they can be exploited. Baseline variables tend to include CPU usage, network packet types, and packet quantities [23]. Thus, it is recommended that institutions of higher education IT personnel and cybersecurity leaders effectively manage and configure the IDIP system using a consolidated enterprise management service, which enables the practitioners to collect responses from all IDIP systems, to identify cross-system probing deployed by cybercriminals, who often ping a network to assess weaknesses and move on to another network segment of computer host, hoping to exploit another weakness. This helps decrease the success of probing altogether. Aligning deployment of IDIP systems with National Institute of Standards and Technology 800-94 special publication, Guide to Intrusion Detection and Prevention Systems, is a sure way to ensure the IT staff is aware of how to assess the IDIP, aware of how to align usage of such with their institution and stay current with recommended guidelines to ensure effective usage of IDIP in cybersecurity leadership for their institution.

It is also important that clearly developed awareness training is offered throughout the school year at institutions of higher education, to ensure executive leaders, administrators, faculty, and staff are deploying daily communication activities in alignment with the standardized procedures implemented by the institution. This awareness training should also include penalties for unacceptable human behavior that correlates with potential risk for cyberattack incidents. It is recommended by information security experts that alignment with NIST 800-14 regarding InfoSec policy, should include: Enterprise information security policy (EISP), Issue-specific security policies (ISSP), and System-specific security policies (SSSP). Developing the EISP first is common because this is the highest level of policy. To learn more about these policies, please review NIST 800-14. Furthermore, the United States Cybersecurity Infrastructure Security Agency provides free online training that supports the needs of institutions of higher education in training personnel regarding the current trend of cyberattack methods, including phishing, spear phishing, malware, and ransomware. Accessing this open-source information can save time with developing training material. Most of the training provided is rendered via online and can be utilized daily. This enables institutions of higher education IT staff and practitioners to define improved methods of awareness training and assess the comprehension of end-users consistently to determine what scale of knowledge base trainees need to improve focus on. The current list of training provided via this agency, includes Cybersecurity Performance Goal Assessment training, ensuring active antivirus and anti-malware protections are active, cybersecurity best practices to protect yourself from tracking technologies and spyware, formulating stronger passwords and pin codes, cyber resilience review/external dependency management training, getting the best out of cloud storage and services while minimizing risks, high value asset assessment training, how to communicate securely on your mobile device, how to protect the data that is stored on your devices, how to implement user account control to protect your personal computer, how to keep your operating systems and applications up to date, and managing application permissions for privacy and security. While these are recommended training tools, it is essential to be aware that all training provided by the CISA can be utilized by any institution of higher education, worldwide.

5. Conclusion

Utilization of cyberpsychology as a tool for effective cybersecurity leadership, is a benefit that can serve institutions of higher education. First, cyberpsychology enables assessment of both attitude and human behavior of technology usage, internally and externally, among executive leadership, administrators, faculty, and staff. Cyberpsychology enables the knowledge collection of attitudes and human behavior commonly shared among cybercriminals, to improve how effective cybersecurity deterrence methods must be, to thwart successful cyberattacks targeting these institutions. Research collected from Carnegie Mellon University Deitrich College of Humanities and Social Sciences reports that utilization of artificial intelligence and machine learning does not provide the key tools to stop cyber-attack incidents altogether. Researchers at this institution are pursuing cognitive models to emulate the behavior of cyber antagonists. In doing so, they believe they can improve the rate of deterrence, using psychological insights to leverage insights to cyber defense. Assessing patterns of information left behind by cyber attackers can enable researchers to assess bias deployed by attackers, to help create traps for cyber attackers. But to be successful requires cybersecurity leaders at institutions of higher education to be diligent in pursuing awareness training externally of their institutions, attending conferences to stay aware of what is being tried at competitor institutions of higher education, and building stronger alliances with institutions globally, to stay aware of new methods and strategies implemented from institution to institution. Thus, continued research must be deployed to ensure this methodology is considered and utilized as often as possible to ensure compliance and awareness of these tools, ideas, and concepts. This can be a vital asset to secure institutions of higher education from cyberattacks.

Most importantly, utilization of the security event information management system (SEIM), which collects log data derived from various servers and network devices to interpret, filter, correlate, analyze, store, and report data. This type of data collection provides cybersecurity leaders with valuable management functions deployed in log storage, such as log rotation, log archival, log compression, log reduction, log conversion, log normalization, log file integrity. This also provides results collected from the log analysis, including event correlation, log viewing, and log reporting. Managing logs are also relied on because it is imperative to ensure data storage can effectively manage the amount of data generated via the configured log activities [20]. Due to the mass amounts of strategies required to effectively implement a dynamic scope of cybersecurity leadership, it is imperative to remain consistent in researching what is being deployed and how it is being deployed across institution to institution. This includes staying aware of laws and policies that consistently evolve and adapt to trends of cyber-attack incidents. Ensuring cybersecurity leadership is implemented with the required process and procedures can ensure increased vulnerability awareness is controlled and does not impact the ability to configure correctly, technology software, hardware, tools, and applications. This includes effectively planning for contingencies. To effectively achieve this goal, it is important to review NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems. Institutions of higher education that partner with the United States Department of Education and receive federal funding to cover tuition cost of student attendance at these institutions, must align their information systems contingency plans with this recommended framework. The four key areas of this plan should include a business impact analysis, incident response plan, disaster recovery plan, and business continuity plan. While these efforts may seem applicable as primary mitigation strategies. It is invaluable to diligently research additional applications, frameworks, and methods of deterrence. After all, there is no 100% way to stop cyber-attacks.

Compliance with ethical standards

Acknowledgments

A special "Thank You" is extended to Dr. Ian McAndrew for his consistent support and professionalism. I also extend a special thank you to Dr. Mary Aiken, Dr. Rich, Dr. Shaw, and Dr. Maranga for his due diligence in supporting life-long-learners. Additionally, I thank Capitol Technology University, University of Arizona Global Campus, University of Maryland Global Campus, University of Phoenix, American Public University System, and Bellevue University for rendering the quality education I attained to soar as an expert in my fields of study.

Disclosure of conflict of interest

There is no known conflict of interest in publishing this content.

References

[1] Aiken, M. (2016). The cyber effect. https://www.maryaiken.com/cyber-effect

[2] Mohajan, K. H. (2022, December 26). Classic grounded theory: qualitative research on human behavior. Research Gate https://www.researchgate.net/publication/366593525_Classic_Grounded_Theory_A_Qualitative_Research_on_Human_Behavior

[3] Mohajan, K. H. (2022, December 26). Classic grounded theory: qualitative research on human behavior. Research Gate https://www.researchgate.net/publication/366593525_Classic_Grounded_Theory_A_Qualitative_Research_on_Human_Behavior

[4] Delve, Ho, L., & Limpeacher, A. (2021, September 17). The practical guide to grounded theory. practical guide to grounded theory research. https://delvetools.com/groundedtheory

[5] Sjouwerman, S. (2024, March 4). Security awareness training blog: 88% of Data Breaches Are Caused by Human Error. https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

[6] Basit, A., Zafar, M., Liu, X., Javed, R.A., Jalil, Z. and Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. National Library of Medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7581503/

[7] Know Be 4, Inc. (2024, May 27). United Kingdom" exponential growth in cyber-attacks against higher education institutions.https://www.knowbe4.com/hubfs/Exponential-Growth-In-Cyber-Attacks-Against-Higher-Education-Institutions-WP_EN-us.pdf

[8] Impact Networking, Inc. (2021, May 27). 15 cybersecurity in education stats you should know. https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

[9] Department for Science, Innovation and Technology. (2024, April 9). Cyber security breaches survey 2024: education institutions annex. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

[10] Artic Wolf. (2024, May 8). 10 cybercrimes against colleges and k-12 schools, and how to prevent them. https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/

[11] Burton, N. (2014, August 21). The psychology and philosophy of envy. https://www.psychologytoday.com/us/blog/hide-and-seek/201408/the-psychology-and-philosophy-envy

[12] Burgo, J. (2015, October 5). Why narcissism, greed, and power go hand in hand. https://www.psychologytoday.com/us/blog/shame/201510/why-narcissism-greed-and-power-go-hand-in-hand

[13] Pearlson, K. & Neto, N.N. (2022, March 4). 7 pressing cybersecurity questions boards need to ask. https://hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask

[14] American Psychology Association. (2018, April 19). Confusion. https://dictionary.apa.org/confusion

[15] Clayton State University. (2024, May 31). Social engineering. https://www.clayton.edu/its/it-security/cyber/index

[16] Parliamentary Office of Science and Technology. (2001, June). Managing human error. https://www.parliament.uk/globalassets/documents/post/pn156.pdf

[17] Amoresano, K. (2022). Addressing human error through effective cyber policy design. University at Albany, State University of New York. https://scholarsarchive.library.albany.edu/honorscollege_ehc/3/

[18] Whitman, E. M. & Mattord, J. H. (2017). Management of information security. (5ed). Cengage Learning, Boston, MA.

[19] Cybersecurity Infrastructure & Security Agency. (2024, June 4). Training. https://www.cisa.gov/resources-tools/training?f%5B0%5D=training_topic%3A68&page=0

[20] Carnegie Mellon University. (2024, April 5). Leveraging human psychology to thwart cyberattacks. https://www.cmu.edu/dietrich/news/news-stories/2024/april/gonzalez-ai.html#:~:text=Throughout%20a%20cyberattack%2C%20the%20behavior,develop%20more%20effective%20network%20defenses.