Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity leadership for institutions of higher education

Bradley Fowler *

Dissertation Chair, Capitol Technology University, 11301 Springfield Rd, Laurel, MD, USA.

Global Journal of Engineering and Technology Advances, 2024, 20(01), 160–170

Publication history: Received on 02 June 2024; revised on 12 July 2024; accepted on 15 July 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.20.1.0122

Abstract

Research continues reporting an increase of cyber-attacks deployed against institutions of higher education. Unauthorized access to known vulnerabilities in software applications, institutions of higher education rely on, is providing external attackers ease of entrance points to access personal information assets. Information assets obtained enable external attackers to sell this information on the Dark Web, where anyone can purchase American Express, Visa, and Master Card details with CVV from the back of credit cards, as well as login and password information, expiration dates, mother's maiden name, and so on. Thus, utilizing qualitative grounded theory lite research enables the researcher's research study to be valid and significant. The researcher seeks to answer the question regarding why ineffective cybersecurity leadership advocates an attitude of tolerance for ineffective training and non-compliance. The researcher also desires to understand how to define improved cybersecurity and information security policy, institutions of higher education can rely on. As well as answer the question regarding what the best resolution is to decrease human error among executive leadership, administrators, faculty, and staff at institutions of higher education. After all, research proves human error is a leading cause of cyberattacks, particularly when institutions of higher education, information systems, technology, and/or cloud practitioners (ISTC) neglect to design effective training and technology usage policy. Thus, this research delivers a resolution supporting institutions of higher education need for increased cybersecurity leadership, delivered through an introduction, literature review, discussion, method of research, results, recommendations, and conclusion.

Keywords: Cybersecurity leadership; Institutions of higher education cybersecurity; Thwarting cyber-attacks higher ed; Higher ed IT practitioners; Higher education cyber resilience; Cybersecurity for colleges and universities

1. Introduction

In 2021, a research survey collected the number of cyberattack incidents deployed against institutions of higher education. The survey included 5,600 IT professionals, including 410 from higher education, across 31 countries. An estimated 74 percent of ransomware attacks deployed against institutions of higher education were successful [1]. Forty percent of institutions of higher education took a month or more to recover. However, this is not just an American issue. Institutions of higher education in Hong Kong were victimized in 2021, also. Hackers used a Sparkling Goblin advanced persistent threat (APT) [2]. This attack method enables attackers to access printers and email servers and embed malware. Alarmingly, minimum reports convey enough detail regarding this attack method and the extensive history of cyberattacks targeting institutions of higher education. In fact, looking back at a 2017, a research article titled *Why higher education institutions are a prime target for cyber-attacks*, Freedom of Information (FOI) figures reported by the TIMES, estimated 1,151 cyberattacks targeted institutions of higher education. Today, the number of attacks has increased. So much, British institutions of higher education are now experiencing an increase of threat, too [3].

Furthermore, research published in June 2023, from the Holistica Journal of Business and Public Administration, conveys that human error is playing a role in cybercriminals gaining access to institutions of higher education

* Corresponding author: Bradley Fowler ORCID: 0000-0002-8447-7898

information systems and information technology tools and applications. This article stresses current usage of cybersecurity policy, training, and awareness at institutions of higher education, inadequately prepares executive leaders, administrators, faculty, and staff on how frequent human error is the root cause of cyber incidents. Additionally, statistical research reported by IBM in 2019, shares details that three top root causes of cyber-attacks, include malicious criminal attacks, system glitches, and human error. In 2022, the United States FBI and CISA (Cybersecurity Infrastructure & Security Agency) reports convey that ransomware incidents escalated to 44%, rising to 2,297 attacks deployed weekly. Ransomware attacks targeting institutions of higher education are higher than attacks targeting healthcare organizations at 61%, businesses at 68%, and financial banking institutions at 58% [4].

Thus, utilization of qualitative grounded theory lite research, enables the researcher to answer three research questions. The first question is, why is ineffective cybersecurity leadership present in institutions of higher education? The second question is, why is cybersecurity and information security policy and non-compliance with such policy so prevalent in institutions of higher education? The third question asks how can cybersecurity leadership be improved at institutions of higher education? This research shares evidence supporting the researcher's reliance on this research method and makes recommendations to resolve these issues effectively. This research also provides details regarding the significance of utilizing qualitative grounded theory lite research, to convey its value to this on-going research study. Utilization of previously published peer reviewed documents supports the researcher's recommendations and confirms this resolution as accurate [5].

2. Literature Review

An effective method of defining this research as qualitative grounded theory lite, was determined after reviewing an article published by Delve & Limpaecher, who helped the researcher understand how qualitative grounded theory research differs from qualitative grounded theory lite research. The latter form of grounded theory research was introduced by Glaser and Strauss, who deployed scientific research on dying patients using a comparative research methodology that assessed data continually to define a theory. Typically, this approach helps create a theory from on-going recycling of data while it is being processed into data assets [6]. This includes usage of three methods of coding-open coding, which focuses on deciphering textual data into various parts; axial coding, which is correlating details from open coded data, and selective coding, which is the final phase of creating a new theory after deciphering details from all data sources during each coding phase. For instance, during open coding, data is collected from previously published scholarly journals, reporting information from information systems, information technology, and cloud practitioners, who work and manage these technology tools and systems for institutions of higher education, and who are responsible for managing the development and implementation of training for executive leaders, administrators, faculty, and staff, to increase awareness of cyberattacks and cybersecurity methodologies. Using this data helps establish the axial coding phase, which enables defining a theory regarding institutions of higher education being targeted with ransomware and other cyber-attack methods because human error incidents are high, due to irresponsibility in action and activity demonstrated by executive leaders, administrators, faculty, and staff, who willingly ignore current information security and information assurance workplace policy. The selective coding establishes another theory, proving ineffective compliance with workplace policy recommendations and guidelines, as well as federal and state laws regarding information systems and information technology usage. Additionally, selective coding helps prove this theory true, that ineffective cybersecurity leadership is demonstrated through the number of noncompliant policy issues, resulting in cyber-attack incidents, monthly and annually, at institutions of higher education.

Qualitative grounded theory lite research requires less rigorous assessment of coding details to define a theory. This approach enables researchers to utilize time better and avoid investing time focusing on establishing a formal theory. This approach is less resource intensive and requires less in-depth research study. Thus, usage of qualitative grounded theory lite research for this research, helps expedite proof regarding the accuracy of the author's theory that cybersecurity leadership at institutions of higher education must be improved, and helps cultivate a new directive of development and system architecture that should be implemented to enhance risk factor awareness and improve awareness training and information security policy development and compliance that reduces human error in institutions of higher education.

Researchers Rochette, Mériade, and Cassière reported that public policy implemented during the COVID-19 pandemic, delivered a unique Information Scientific study to help understand the role public policy plays in compliance and adherence [7]. However, instead of relying on concepts of theory to determine the success of policy implementation, this research examines the actions of those required to align their behavior with policy implemented, to pinpoint the origin of reason and to correct that reason with effective strategy. Additional research reported by D'Agostino, Viano, and Chin, supports the researcher's theory, by validating it with scientific proof and contributes knowledge towards

concerns institutions of higher education information systems, technology, and cloud practitioners and education executive leaders and administrators have, regarding methods of cyber-attack prevention and deterrence [8].

3. Method of Data Collection

Utilization of key search terms, quality of content, and reputation of scholarly journal publishers i.e., EBSCO & ProQuest were chosen to ensure data assets provided the quality of reference and validation required to support the researcher's research. Search terms were categorized based on research needs, including qualitative grounded theory, qualitative grounded theory lite, cyberattacks at higher education, cyber incidents at institutions of higher education, human error in the workplace, and noncompliance policy in the workplace. For instance, one reference collected was a scholarly journal document that helped reassess the researcher's theory, in pursuit of an effective resolution, but aligned with the requirements for this research method.

Thus, first method of measurement involved categorizing data by type of cyber incident, chrono logicalizing the number of incidents across region, and determining the correlation across incidents to minimize vulnerabilities in current technology applications relied on for institutions of higher education and their reliance on information systems, information technology, and cloud applications for data storage. Assessing the research documents compiled helped determine that current theories regarding institutions of higher education being targeted as weak entities, are validated across multiple regions, types of cyber incidents, and statistical reports. However, this theory also establishes another theory regarding the value of on-going training in all higher education institutions for executive leaders, administrators, faculty, and staff, to ensure alignment and compliance with information assurance and security policy. When end-users are not aware of vulnerabilities created by human error, they practice careless actions and activities that enable cyber attackers accessibility to sensitive environments to easily exploit weaknesses. This validates the researcher's theory that human behavior advocates for cyber incidents to occur in institutions of higher education.

In fact, one research study conducted on technology experts in Israel, through survey instruments-i.e., collected journals, articles, Web site post, and video surveys, depicting lethal and nonlethal cyberattack incidents, included experimental manipulation of activities to test participants response to cyberattack models deployed differently. This was implemented to arouse emotions about previously deployed cyber-attack incidents reported by participants or others in the workplace. The test measured how participant perception about each cyber-attack incident impacted their thought regarding compliance with workplace policy implemented to safeguard technology applications and tools relied on for business purposes, from victimization Gaining this knowledge invokes the establishment of new training methods and development of new training material that enables end-users to remain compliant. Thus, utilizing this approach enables an improved focus on defining a strategy to support institutions of higher education to improve cybersecurity leadership and methods of training executive leaders, administrators, faculty, and staff regarding human error and policy compliance.

4. Research Method

Qualitative grounded theory lite research is less rigorous than traditional grounded theory because no formal theory is required. This approach to research is shorter and utilized in small research projects. Since this research is utilizing previously published research regarding lived experiences of information system, information technology, and cloud computing architecture practitioners, working at institutions of higher education, as well as published validated articles from other researchers researching the impact of cyber-attacks on institutions of higher education, this research method best fits the needs of this research. Creating categories and concepts to understand relationships, without formulating a theory, is a key feature of this research method. In fact, research reports that utilizing this research method is still a valuable tool for developing a preliminary understanding of the topic relating to cybersecurity leadership for institutions of higher education. Thus, tools used for this research method included pen and paper for coding. Usage of highlighting tools in word document format, helped control the large scale of documents used to assess content relating to the topic of this research, which also helped define a theory correlating with the author's approach to understanding why institutions of higher education continue being victimized by cyber-attack incidents. The word processer was utilized to add comments and paraphrase as well as copy and paste content onto different word documents to be utilized in completing the research study. Consistent evaluation of facts relating to several reported articles published, including one specific on the EdTech online news site, who reported, that in March 2024 cyber-attacks deployed against institutions of higher education increased 70% [14].

Using the qualitative grounded theory lite research method helped understand that documented reports of cyber-attacks deployed against institutions of higher education in the United States, continue facing the daunting tasks of

improving executive leadership knowledge of ransomware attack strategies implemented by cybercriminals targeting institutions of higher education, as well as administrators, faculty, and staff. Due to the continued misalignment of effective cybersecurity leadership within institutions of higher education to better train executive leaders, administrators, faculty, and staff, cybercriminals are increasing their efforts to introduce new methods of attack, other than ransomware, which research conveys the highest paid ransomware attack earned cybercriminals well over $700,000 payload. The new attack method embodies malvertising.

Qualitative grounded theory lite research helped identify reported evidence found in more than 50,000 populated Google Web search inquires, proving risk of cyberattacks at institutions of higher education is consistently published globally. This research method also provided clarity that ineffective cybersecurity leadership remains a key factor resulting in institutions of higher education being targeted successfully by cybercriminals. Using key words to define search inquiry enables the author of this research to also learn more knowledge about the impact human error has on institutions of higher education and their crisis of cyberattack incidents.

In fact, research compiled from UpGuard's cybersecurity rating data, reporting on 1500 universities and 5000 university vendors, convey that institutions of higher education continue being victimized, as the author of this research initially thought, based on previous research collected. UpGuard reported that institutions of higher education suffer increased cyberattacks due to a lack of effective training of executive leaders, administrators, faculty, and staff. UpGuard also conveys that cyberattacks also increase due to a lack of maintaining updated software applications. In fact, UpGuard conveyed that their research discovered that 70% of institutions surveyed were utilizing software that had not been updated in 2 years [15]. This too, proves the author's theory that ineffective cybersecurity leadership exists in institutions of higher education.

Furthermore, this research method is validated by additional research compiled from The Voice of Higher Education Technology Community, who reported 30% of faculty and staff were victimized by phishing scams, because these personnel members lacked efficient awareness training. Assessing and recording collected documents to create a theory that is consistently reported in similar research defined with evidence, which backs the author's research regarding the inconsistent ineffective cybersecurity leadership that currently exist in institutions of higher education. This, too, proves that grounded theory lite research is useful in supporting the researcher's approach to defining an effective method of increasing cybersecurity leadership at institutions of higher education [16].

5. Results

The original research questions introduced by the researcher, to understand the primary, secondary, and exploratory analysis needed to define a resolution to deter cyberattack incidents from impacting institutions of higher education, include:

- What human behaviour is being deployed and/or neglected to be deployed by institutions of higher education, ISTC practitioners, from deterring cyberattacks against institutions of higher education?
- What impact can cybersecurity public policy have towards enforcing personnel compliance with cyber laws and policy in institutions of higher education?
- What characteristics of human behaviour is commonly shared among education administrators impacting their ability to comply with workplace information security policy?

To effectively utilize the qualitative grounded theory lite research method to answer each of these questions, requires assessing statistical research analysis compiled from research reported in documents, regarding the number of cybercrime incidents reported annually, the type of cybercrimes commonly committed towards institutions of higher education annually, the timeline for discovery of each cyberattack incident, and the timeline deployed to resolve the incident. Furthermore, an assessment must analyze types of human behavior demonstrated by ISTC practitioners at institutions of higher education and personnel, who utilizes institutional technology tools and assets. As a result, this research is validated with the researcher's exploratory analysis, in trying to establish a resolution to this global phenomenon. The result of this research ensures institutions of higher education can improve their rate of cybercrime victimization deterrence, by implementing effective cybersecurity leadership to decrease the growing threat of cybercrime victimization. To understand what human behavior is being deployed and/or neglected to be deployed by each institution of higher education, ISTC practitioners, requires usage of an information assurance risk analysis to manage organizational confidentiality, integrity, and availability under the CIA triad. Using an information usage profile categorizes information, provides a description of the information assets, as well as details the scale of sensitivity of the information, and instructs how to assess how this information is used or processed, and then, provides a list of the IT assets in use, including a list of each IT asset storing sensitive information. But even after achieving this clarity of these

subjects, attaining specifics regarding each ISTC practitioners, human behavior, enabling cybercriminals to successfully attack each individual institutions of higher education, remains null. Instead, this information enables an improvement of institutions technology assets tools and applications, usage, and security.

Conducting research through qualitative grounded theory lite reinforces facts from previously published scholarly articles relating to current trends in cyberattack awareness at institutions of higher education. The official search engine query deployed by the researcher, populated more than 50,000 Websites, scholarly journals, periodicals, and blogs, who report cybercrime incidents at institutions of higher education from 2022 to 2024, both domestically and internationally, as well as the type of cybercrimes committed at institutions of higher education-i.e., Distributed Denial of Service Attacks, phishing scams, ransomware attacks, malvertising, Zero-Day attacks, and malware.

Research also reports the turnaround time some institutions of higher education take to acknowledge an attack has occurred and to resolve the attack after discovery is too long in between the incident and discovery of the incident. However, no known research has populated the human behavior correlating from institutions of higher education, ISTC practitioners, to clearly assess the type of human behavior these practitioners are demonstrating individually on their job, or as a group across regions, domestically or internationally. What is known is that qualitative grounded theory lite research proves institutions of higher education are faced with a challenge of hiring qualified ISTC practitioners, and their inability to effectively train current personnel on the current trends of cybercrimes targeting institutions of higher education, as well as training faculty, staff, and executive leaders on what cybersecurity leadership means to institutions of higher education, and the role and responsibilities each of these leaders play in supporting the deterrence methods, strategies, and procedures institutions of higher education, ISTC practitioners should be knowledgeable of, to effectively protect and prepare their institutions from cybercrime victimization.

Additionally, this research method helped the researcher cultivate some of the resolutions needed for effective information assurance risk management, to support institutions of higher education, in deterring successful cyberattacks. First, the researcher discovered he needed to compile supporting documents from previously researched cyberattack incidents deployed against institutions of higher education, domestically and internationally [17]. The result of this research validated that cyberattacks increased from 48% in 2022 up to 164% in 2024.

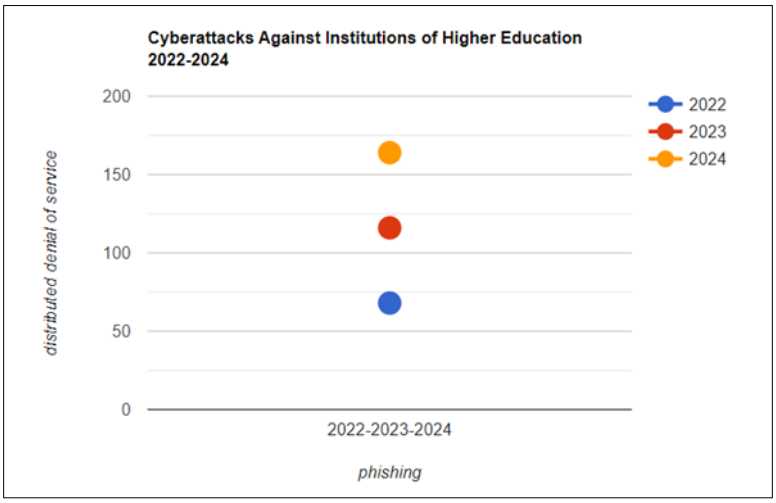

Figure 1 Types of Cyberattacks Against Institutions of Higher Education 2022-2024

Statistical research also validated that ransomware attacks cost a total of $3.58 million in 2023, compared with $570,000 in 2022. This increase of cost demonstrates that institutions of higher education are willing to make ransomware attack payments. This report also shows that institutions of higher education are good targets because they pay ransomware demands.

The researcher discovered that using a second analysis type should involve a risk factor table to understand what is at risk and to categorize the risks and the impact levels of such risks. Risks titles should include information extortion, human error, or failure to comply, compromise of intellectual property, technical hardware failures or installation errors, technical software failures or installation errors, technological obsolescence, sabotage or vandalism, forces of nature, theft, software attacks, vendor and third-party records, information system assets, cloud assets, telecommunications, and physical assets. A description of each of these risk factors must be provided, each risks

category should range from extremely high, high, medium, low, and each risk impact level should range from catastrophic, major, moderate, medium, or low.

Furthermore, a third analysis approach the researcher discovered includes assessing and understanding all known vulnerabilities woven in all software and hardware applications used across the organization and having a plan to patch and mitigate every technology tool, application, asset, and known vulnerability. This includes implementing auditing to ensure consistency is applied to each of these analysis types throughout the lifecycle of the organization, to deter successful exploitation of these tools, applications, and assets. Even with this information, there remains a lack of clarity regarding types of human behavior deployed by ISTC practitioners at institutions of higher education as well as a lack of understanding regarding the question: what characteristics of human behavior is commonly shared among education administrators, impacting their ability to comply with workplace information security policy.

What this research results provided was knowledge regarding how invaluable cybersecurity public policy is to institutions of higher education in helping personnel comply with information security policy to support deterrence efforts implemented by cybersecurity leadership. Learning this invokes the need to define effective policy compliance strategies that render effective in helping deter and control cyberattack incidents at institutions of higher education. The result of this discovery enables institutions of higher education to understand 10 primary privacy issues that must take precedent, including the collection of sensitive information, retention of data collected, logging of data collected and stored, generation of data, transformation of data for business usage, usage of consumer information, disclosure of sensitive information and privacy of that information, the sharing of sensitive information with third-party vendors, transmission of sensitive information disseminated via the Internet and WIFI, and the disposal of information.

Results of this research also shows that usage of a privacy compliance risks profile can be beneficial, when it includes details for each risk title i.e., computer viruses, malicious code, unauthorized access, phishing efforts, denial of service attacks, disruption and failure of technology services, safety failures, regulatory compliance failures, the inability to protect information assets, and reputational damage. A description of each risk title, a risk category, including people or computer/software, and the impact level: high, medium, and low, should guide the risk compliance risk profile development. Next, usage of a privacy compliance control profile should also be implemented. This profile should convey each risk title i.e., computer viruses, malicious code, unauthorized access, phishing efforts, denial of service attacks, disruption and failure of technology services, safety failures, regulatory compliance failures, inability to protect information assets, and reputational damage, as well as compliance risk mitigation strategy, which should be established for each risk title, and lists each NIST security control that each risk title asset should be assessed, configured, patched, or mitigated in alignment with.

As a result of this qualitative grounded theory lite research compiled, it was also discovered that a privacy compliance risk mitigation strategy be deployed, including a threat model to find security problems for each institution. Utilizing this model means an effective abstraction should be implemented to assess the whole picture, instead of codes alone. Usage of a diagram board should also be deployed. This is a great method to map out technology tools utilized, that need increased security methods, planning, and strategies to ensure effective management of internal and external threats and vulnerabilities. Trust boundaries should be set to establish who should and should not have control to sensitive information, including accounts, network interfaces, physical computer hard drives, virtual machines, artificial intelligence, cloud assets, and institutional boundaries. This invokes the need for effective steps to mitigate threats. This should include bug tracking systems. This can be achieved using open-source tools, such as Threat Modeler.

Furthermore, the results report that usage of an enterprise architecture IT strategy proves team management can be beneficial in reducing cyberattack incidents. However, to effectively achieve total risk management control, institutions of higher education, ISTC practitioners and executive leaders, should understand their disruptive technology, change management, IT value creation, have plans to manage vendor management, and effectively assess enterprise architecture artifacts, and have a firm vision of cybersecurity leadership. Most importantly, the results show that development and usage of a IT Strategy policy life cycle, should include setting an agenda, developing a policy formulation, improving decision-making success, provide methods of implementing policy and making updates to policy implemented, monitoring and evaluating policy and compliance, creating policy as needed, including acceptable use policy, access control policy, mobile device usage policy, change management policy, a scope, information security policy, remote access policy, email communication and security policy, email security policy, data management policy, documentation policy, disaster recovery policy, and establishing a policy management tool. In addition, there must be IT guidelines, procedures, standards, policies, policy compliance report cards, and policy enforcement strategies. Proven results for compliance with these recommendations can be significant when cybercrimes deployed against institutions of higher education have reported decreased numbers by 68% in 2025 and beyond. Otherwise, a reconsideration of assessment methods must be updated, and strategies revised to align with the recommended

guidelines and standards enacted by the National Institute of Standards and Technology, European Union, U.S. Department of Homeland Security, and federal and state laws and cybersecurity policy.

Finally, the results regarding the question: what impact can cybersecurity public policy have towards enforcing personnel compliance with cyber laws and policy in institutions of higher education? Research compiled by the researcher reported that current cybersecurity training in the public sector is inadequate based on the frequent number of human error incidents leading to successful cyberattacks. In fact, between 2014 and 2019, a study conducted by IBM reported that 95% of all security breaches were caused by human error. The cost of these incidents reached an estimated $3.56 million US dollars. This research was compiled by IBM based on 1000 clients in 133 countries. Although this research clarified the issue human error creates. The result of this qualitative grounded theory lite research study shows that, when cybersecurity leadership training is implemented by qualified ISTC practitioners, these leaders enable their institutions to define improved awareness training that empowers personnel and executive leaders to comply with cybersecurity policy. Usage of cybersecurity public policy that aligns with federal, state, and international law, relating to all components of information systems, information technology, and cloud applications, reiterates the value of cybersecurity policy and impacts the level of compliance end-user deploy to stay compliant with such policy [17].

However, for this to have the impact needed to reduce cyberattacks, ISTC practitioners and executive leaders must work in concert to ensure those held accountable under such policy, are operating daily business functions in alignment and compliant of such policy. Regardless of the behavior relating to human error. Noncompliance of cybersecurity policy at institutions of higher education is a result of ineffective cybersecurity leadership. Proving the research study valuable to the security of institutions of higher education.

6. Discussion

Cybersecurity leadership is essential to mandating regulations and policy at institutions of higher education, to help deter and thwart successful cyber-attacks from occurring. The growing threat of cyber-attack incidents reported since the year 2022 proves there remains a lack of effective cybersecurity leadership at institutions of higher education. But why? After all, in October 2022, reports conveyed that the Federal Trade Commission published a revised Safeguards Rule, regulating institutions of higher education, one-year to align their policy compliance with the new enacted cybersecurity protections and requirements for institutions of higher education [9]. The Safeguard Rule establishes standards for safeguarding customer information and was officially published in January 2022. This rule requires institutions of higher education to develop, implement, and manage an effective information security program that embodies administrative, technical, and physical methodologies to protect institutions access, collection, ability to distribute, process, protect, store, utilize, transmit, dispose of, or handle sensitive information belonging to customers- i.e., students, faculty, and staff. This imposed program must deploy effective methods to ensure security and confidentiality of customer information and ensure protection against potential threats or hazards that could impact the ability to safeguard customer's information [10]. Furthermore, this new rule requires institutions of higher education to designate a person or team to oversee, implement, and ensure the institution's information assurance and information security policy is current and enforced to ensure compliance with this new federal law. This also requires institutions of higher education to develop a written risk assessment regarding the methods of information security the institution is deploying, as well as develop and implement strategies and procedures conveying what methods of risk management control the institution is implementing to ensure their information assets are not vulnerable to cyber-attack incidents. This must include:

- Limiting access to technology and physical entrance to areas where technology is housed.
- Maintaining clearly written inventory of all IT hardware and software utilized, including strategies to safeguard such.
- Ensuring encryption is implemented on data in transit and at rest in technology infused storage capacities.
- Writing down effective procedures for methods of secure internal applications and how the institution will assess the security of external applications utilized in correlation with students, faculty, and staff information.
- Ensuring multi-factor authentication is deployed for all individuals accessing any technology tool hosting information assets belonging to the institution.
- Clearly conveyed procedures for securing the disposal of faculty, staff, and students information that is no longer necessary for managing business operations.
- Providing clearly written change management procedures.
- Maintaining logs in written format and digitized to support the implementation of the new information security program.

Additional requirements include establishing policy and procedures to ensure all staff, faculty, and students receive effective training regarding institutional cybersecurity awareness and policy compliance requirements. This requires implementing periodic auditing of the information security risks factors to ensure these factors are updated with current security methods. It is also required that written incident reports are maintained, as well as ensure that whoever is held accountable-either a person or a team of people, are required to develop a written report regarding key components of the institution's information security program and report and share such with the institution's governing board [11].

With the continued growth of cyber-attacks deployed against institutions of higher education in America and globally, it is obvious not all institutions of higher education are aligning their information security policy with the federal Safeguard Rule. So, how can federal regulators determine who to hold accountable, when each individual institution of higher education is responsible for developing, implementing, and managing their own information security audits and assessments, and maintain written logs regarding these efforts? Despite the alarming number of successful cyber-attacks and concerns of students and parents, who fear their children's information will be stolen and sold on the Dark Web. Seemingly, the inability to hire qualified cybersecurity leaders at institutions of higher education, continues plaguing these systems, impacting their ability to align with federal regulations. This alone is reason why institutions of higher education continue being victimized. However, there are methods that institutions of higher education can implement to decrease these threats and deter vulnerabilities woven in the technology software utilized.

For instance, institutions of higher education can partner with AWS Cloud for Higher Education, which provides access to equitable higher education teaching and learning tools and resources. Using AWS cloud application connects the campus community to systems and tools, improve stored data efficiently, and makes artificial data-driven decisions that save money and resources, as well as accelerate research efforts. In addition, utilization of a landing zone accelerator lets each institution of higher education improve regulating workloads and enforce complex compliance regulations. Usage of Amazon Simple Storage Service (Amazon S3), helps an institution of higher education deploy, operate, and secure all data in encrypted files, using AWS Key Management System. Configurable to all AWS Regions and can be integrated with up to 35 other cloud services, all to increase security and workplace compliance. Deployment of artificial intelligence enables automation to collect analytics to consistently implement improved training in areas of inconsistency due to successful cyber-attacks that occur over a period. Furthermore, this system is easily adaptable to each institution of higher education database needs, and configurable using an AWS Cloud Formation template. This template can ensure instructions are clearly conveyed and understood and are being deployed as recommended. The results exist because this method creates a Code Pipeline that establishes the Landing Zone Accelerator on the installation engine [12].

Although partnering with AWS is a choice, it is each institution's final decision to make. Making the decision to partner with Amazon Web Services (AWS), also must align with federal law and policy regarding institutions of higher education and their storage of information assets, domestically and internationally. This requires each institution of higher education to ensure whoever they put in the role of cybersecurity leader, is knowledgeable of what is required to effectively manage their role and responsibilities. Institutions of higher education in America, who offers online-asynchronous learning through learning management systems, are held accountable to domestic and international laws and policy regulating information systems, information technology, cloud computing applications, information asset security, information assurance, and privacy of confidential information. When these institutions enroll students internationally, each institution becomes accountable under federal laws and policy in each country, they are delivering educational services and products too. The same applies to international institutions of higher education, who renders online asynchronous learning through learning management systems, to students in the United States, Canada, Europe, Asia, etc. Thus, imposing laws and policy is ineffective when institutions of higher education do not comply with or adhere to such regulations, laws, and policy. Who should ensure each institution is adhering to these regulations, laws, and policy? The Chief Information Security Officers (CISO), Chief Information Technology Officer (CTO), and cybersecurity leaders.

Thus, the second ethical approach institutions of higher education, domestically and internationally, should align with is their information security programming and policy development, implementation, and management, with the National Institute of Standards and Technology recommendations and guidelines, which the NIST continues revising and adopting methods and strategies to ensure safeguarding of information assets hosted in information systems, information technology, and cloud computing applications; owned or leased by institutions of higher education are secure. Under NIST 800-171 Compliance Guide for Colleges and Universities, it is publicly known that institutions of higher education do not effectively impose cybersecurity measures to effectively secure information assets. This awareness validates the researcher's theory proving institutions of higher education neglect to implement effective cybersecurity leadership. When institutions of higher education align with the recommended guidelines under NIST

800-171, they can improve how they assess risk factors associated with the technology tools and applications relied on. When determining what risk level each technology tool or application utilized falls under, the risk levels are low-medium-high. Deploying effective risk assessments helps institutions of higher education determine the level or risk they need to control. The 14 control families established by the National Institute of Standards and Technology include: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, personnel security, physical protection, risk assessment, security assessment, system and communication protection, and system and information integrity [13].

NIST 800-171 enables colleges and universities to align with the following federal regulations:

- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach Biley Act
- Health Insurance Probability and Accountability Act (HIPAA)
- Higher Education Act
- NIST Risk Assessment and Audit Standards
- Payment Card Industry Data Security Standards

The U.S. Department of Defense requires NIST 800-171 compliance for all third-party government contractors to ensure security is applied to all federal data and documents. Thus, enforcing all United States and international institutions of higher education to comply with each of the above listed laws and adhere to the recommended guidelines under NIST 800-171, as a prerequisite to secure information systems, information technology, and cloud computing architecture, where data assets are stored, must be mandatory!

7. Conclusion and Recommendation

Cybersecurity leadership at institutions of higher education cannot be effective without effective cybersecurity leaders taking the initiative to assess, develop, implement, and manage all institutions technology hardware, software, and applications relied on for daily business operation. While grounded theory research requires the development of a new theory to ascertain resolution. Qualitative grounded theory lite does not require researchers to ascertain a theory. This approach to research benefits researchers interested in cybersecurity leadership at institutions of higher education and the resolutions needed to thwart and deter successful cyberattacks, because there is a limit to how research can be deployed to understand the central phenomena. This approach reduces the time needed to deploy such research to ascertain clarity of the issues, to propose a resolution to the phenomenon. Thus, qualitative grounded theory lite research provided enough information data collection, to determine the need for improved cybersecurity leadership at institutions of higher education, defined by regulations, laws, and policies enacted and mandated by federal, state, and international law and policy. Neglecting to do so will continue impacting the outcome of resolutions required to deter future cyberattack incidents. Thus, it is recommended that institutions of higher education improve their assessment of hiring qualified ISTC practitioners to play the role of CISO-Chief Information Security Officer, who has the responsibility to protect the information assets owned and leased by institutions of higher education. This leadership role aligns with cybersecurity leadership. In fact, these two roles are synonymous with effective cybersecurity management.

Furthermore, the CISO must implement effective training requirements for ISTC practitioners at institutions of higher education, to ensure these practitioners stay current with trends in cybersecurity public policy and understand why these policies are valued, and know how to assess what policy the institution needs to align with, and understand how to modify current information system, information technology, and cloud policy that ensures these systems and tools are secured and, usage of these systems and tools are being respected by end-users across the organization. When executive leadership is aware of the technology security threats and vulnerabilities, these leaders can help ISTC practitioners make better judgments in governing their decision-making support efforts to increase cybersecurity across organizational assets, as well as improve how institutions personnel respond to potential threats and methods of cyberattack deployed against them.

When personnel are trained and understand their roles and responsibilities in supporting the institution's need for cybersecurity leadership, each institution can begin reducing their risk and control the scale of attack, because their alignment with federal, state, and international policy for cybersecurity control and information assurance, will be current and capable of thwarting external attacks and internal human error incidents. In fact, to increase deterrence, institutions of higher education must increase cybersecurity leadership and enforce adherence to cybersecurity and

information security policy recommendations and guidelines, published by the National Institute of Standards and Technology, European Commission, and federal, state, and international law authorities.

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.

+References

[1] D'Agostino, S. (2022, July 21). Ransomware attacks against higher ed increase. https://www.insidehighered.com/news/2022/07/22/ransomware-attacks-against-higher-ed-increase

[2] Mascellino, A. (2022, September 14). Sparkling goblin APT targeted Hong Kong university with new linux backdoor. https://www.infosecurity-magazine.com/news/sparklinggoblin-hong-kong-linux/

[3] Quorom Cyber. (2021, August 31). Why higher education institutions are a prime target for cyber-attacks? https://www.quorumcyber.com/insights/why-higher-education-institutions-are-a-prime-target-for-cyber-attacks/

[4] Amorosa, K., Yankson, B. (2023). Human-error-A critical contributing factor to the rise in data breaches: a case study of higher education, Holistica Journal of Business and Public Administration, Vol 14, Iss, 1, pp.110-132

[5] Tie, C.Y., Birks, M. & Francis, K. (2019, January 2). Grounded theory research: A design framework for novice researchers. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6318722/

[6] Delve, Ho,L. & Limpaecher, A. (2021, September 17). The practical guide to grounded theory. Practical Guide to Grounded Theory Research. https://delvetool.com/groundedtheory

[7] Rochette, C., Meriade, L., & Cassiere, F. (2023, December 11). A grounded-theory base qualitative approach for examining local implementation of public health policies during crisis. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10630630/

[8] Keren L G Snider, Ryan Shandler, Shay Zandani, Daphna Canetti. (2021, October 7). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies, Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab019, https://doi.org/10.1093/cybsec/tyab019

[9] McKenzie, L. (2022, October 28). New federal IT requirements coming to higher ed, Educause says. https://edscoop.com/new-federal-it-requirements-coming-to-higher-ed-educause-says/

[10] Federal Register, (2022, January 10). Standards for safeguarding customer's information. https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information

[11] Cummings, J. (2021, December 2). Policy Analysis: revised, highly prescriptive FTC safeguards rule. https://er.educause.edu/articles/2021/12/policy-analysis-revised-highly-prescriptive-ftc-safeguards-rule

[12] Amazon Web Services, (2024, February) Landing zone accelerator on AWS. https://aws.amazon.com/solutions/implementations/landing-zone-accelerator-on-aws/

[13] Chin, K. (2023, February 23). NIST 800-171 Compliance guide for colleges & universities. https://www.upguard.com/blog/nist-sp-800-171-compliance-guide-for-colleges-universities#:~:text=The%20NIST%20800%2D171%20framework,171%20to%20its%20security%20policies

[14] Viano, A. (2024, March 15). Cyberattacks on higher ed rose dramatically last year, report shows. https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows

[15] Kost, E. (2024, January 18). The state of university cybersecurity: 3 major problems in 2024. https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges

[16] SteelCloud, (2024, May 6). Cybersecurity in higher education: don't let the hackers win. https://er.educause.edu/articles/sponsored/2024/5/cybersecurity-in-higher-education-dont-let-the-hackers-win

[17] Fowler, B. (2023). Information assurance and risk management strategies-manage your information systems and tools in the cloud (1st Ed). Apress, New York, N.Y.

[18] Amoresano, K. (2022, May). Addressing human error through effective cyber policy design. https://scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1002&context=honorscollege_ehc