EXAMINING DISTINCTIONS BETWEEN CORPORATE AND HIGHER EDUCATION CYBERSECURITY PROGRAM DEVELOPMENT: A NARRATIVE REVIEW

by

CHRISTOPHER D. ADAMS

B.S., Western Governors University, 2017
M.S., Western Governors University, 2018

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

Examining distinctions between corporate and higher education cybersecurity program development: a narrative review

Christopher Adams, *Middle Georgia State University, christopher.adams5@mga.edu*

Abstract

Modern higher education institutions must contend with a litany of cyber threats, regulations, and environmental dynamics. These institutions are increasingly being targeted due to the value of the data they possess and their historically permissive configurations that are intended to support academic freedom. Many universities are implementing and maturing their cybersecurity programs as part of broader risk management activities. As these programs progress, cybersecurity professionals are meeting the headwinds of complexity and resource constraints, challenging the effectiveness of their programs. This research is being performed to better understand the differences and similarities between corporate and higher education cybersecurity programs. By understanding how industry-specific and higher education needs overlap, mappings can be drawn between corresponding industry regulations and higher education requirements. Insight into these relationships will ultimately allow for a more effective transfer of best practices, knowledge, and threat intelligence, creating efficiencies for higher education cybersecurity programs beyond what could be reasonably attained on their own.

Keywords: cybersecurity program, information security management, cybersecurity governance, higher education risk management, cybersecurity regulation

Introduction

Within the realm of modern information systems, there may be no topic more important than that of cybersecurity. As such, a systematic approach to cybersecurity is needed for most organizations. According to Perry (2021), a comprehensive and documented cybersecurity program "includes security-related policies, procedures, manuals, codes of conduct, preparedness, and response communications" (p. 4). The efforts required to establish a cybersecurity program in a large enterprise are immense, time-consuming, and necessitate continuous adaptation. While there is an existing body of knowledge pertaining to cybersecurity programs and frameworks, there is little information available pertaining to higher education cybersecurity programs, and specifically, how they vary from program development in corporate environments. In addition to establishing a cybersecurity program, it is also necessary for higher education cybersecurity professionals to continuously update their programs to effectively manage risk (Cheng & Wang, 2022). The research performed in this review will better enable higher education institutions to understand what similarities and differences exist when comparing cybersecurity threats and program development to corporate environments. The resulting knowledge will encourage the identification and adoption of cybersecurity best practices in higher education environments and foster more efficient program development.

Problem Statement

Higher education technology leaders assume the difficult position to both create open environments conducive to academic freedom while simultaneously complying with a wide range of regulatory challenges and protecting populations of sensitive data. While a body of research pertaining to cybersecurity program development exists in the corporate setting, not all guidelines may be appropriate for application within the higher education setting.

Purpose of the Study

The purpose of this study is to perform a thorough review of existing literature pertaining to the cybersecurity domain and program development spanning both higher education and corporate environments. The findings of this review are then used to identify and examine the distinctions and similarities found while developing cybersecurity programs. The resulting knowledge will be used to aid higher education technology professionals to manage cybersecurity risks more efficiently and effectively in their organizations.

Research Questions

RQ1: What are the differences and similarities found when examining the cybersecurity landscape pertaining to corporations and higher education institutions?

RQ2: What are elements that can be translated from corporate environments into higher education cybersecurity program development?

Review of the literature

Motivations for Cyber Attacks

As technology continues to be a cornerstone of organizational operations and innovation, the data and importance of the work that corporations and higher education institutions perform continue to increase in value, making them appealing targets for threat actors. According to Al-Mohannadi et al. (2016), understanding the motivations of threat actors and their methods is critical to establishing an effective cyber defense. As detailed in the 2022 Verizon Data Breach Investigations Report (Verizon, 2022), financial gain has been the top motive for cyberattacks since 2015 when data on motives started being collected. Additionally, the sources of data breaches have changed over time. In fact, over the last 15 years, external sources of data breaches have increased compared to internal and partner-originated breaches (Verizon, 2022).

Corporations are often targeted for intellectual property theft which can be either sold or otherwise leveraged for economic gain, often by foreign or state-sponsored attackers (Andrijcic & Horowitz, 2006). Higher education institutions also maintain a great deal of sensitive data. According to Ulven & Wangen (2021), the most valuable information within higher education "are personally identifiable information (PII) on students and employees, financial data, research data, IP, student grades, and administration details" (p. 38). Higher education institutions that perform research hold a great deal of intellectual property and student information. This intellectual property and body of student records can similarly be sold for financial gain by threat actors. Although theft is a common motivator, state-sponsored threat actors and cyber terrorists may have more sinister intentions such as disrupting financial markets and negatively impacting an organization's productivity (Saini et al., 2012). The loss of proprietary trade secrets and reputational damage can cause an organization to lose its competitive advantage and market position (Blank, 2021).

Cyber Attack Vectors

The methods used to infiltrate and attack organizations are numerous in number and are well-established. The most common attack vector is the use of social engineering, which leverages human interactions, rather than technical prowess, to gain access to systems or information. As identified by Krombholz et al., (2015), advanced social engineering attacks against corporations can include the use of phishing, shoulder surfing, dumpster diving, reverse social engineering, water holing, persistent threats, and baiting (p. 117). Social engineering attacks are also a leading cause of cyber incidents within higher education institutions (Ulven & Wangen, 2021). The use of social engineering against universities can be particularly effective given the considerable number of faculty and staff as well as a transient student population. Eyadat (2015) posits that universities are motivated to establish information security programs to reduce the risks that are inherent in having such a wide range of users connected to the same networks.

While threat actors often exploit humans to gain unauthorized access to systems, internal networks, and server infrastructure are frequent attack vectors as well. It is common for both enterprises and higher education institutions to have a significant infrastructure footprint ranging from local area networks, servers, cloud infrastructure, endpoint computing systems, and other networked devices. An attack that leverages a system intrusion can be defined as "complex attacks that leverage malware and/or hacking to achieve their objectives including deploying ransomware" (Verizon, 2022, p. 24). Dudorov et al. (2013) suggest that any critical system connected to a public network, such as the internet, is at risk of a cyber-attack. Furthermore, advanced attackers may use multiple pathways to access company infrastructure, such as home PCs, mobile devices, or direct attacks against servers and services (Dudorov et al., 2013).

In higher education, it is normal for faculty, staff, and students to utilize personally owned devices, commonly referred to as a bring your own device (BYOD) program, for academic and personal use-cases (Afreen, 2014). Corporate IT environments have also begun to adopt and support BYOD programs, but adoption seems to lag the trajectory witnessed in higher education environments (Dhingra, 2016). The proliferation of personally owned devices and the challenges associated with ensuring their security posture adds varying levels of risk to critical systems and can be an unfortunately effective attack vector. To this point, the 2022 Verizon Data Breach Investigations Report shares that attacks leveraging system intrusions within the educational services sector outpace other industries and exhibit an upward trend (Verizon, 2022).

Security Frameworks & Regulatory Environments

The use of security frameworks and standards is not a novel concept for maturing information security programs in organizations. Various regulations and legal requirements often specify controls from established security frameworks to secure information systems environments. ISO 27001 is a common security framework that is published by the International Organization for Standardization and consists of a catalog containing over 114 security controls that span fourteen different domains. Although ISO 27001 is often used by higher education institutions, it is a generic framework, and as such, it is difficult to identify which elements are important to employ within higher education cybersecurity programs (Alexei, 2021). Despite evidence showing increased breaches, some universities utilize de-centralized information technology departments, adding complexity to the creation and implementation of security governance (Liu et al., 2020). These variables, along with others, highlight some of the unique complexities that must be considered as part of a higher education cyber security program.

As risk surrounding information systems has evolved, the desire to manage risk has often been approached by various authorities in the form of regulations. According to Marano & Grima (2018), "boards are facing increased pressure from internal and external stakeholders to oversee all types of enterprise-wide risks, which range from financial to reputational, to technology and to environmental or sustainability risks" (p. 25). Given that specific industries often have regulations that pertain to their operations, the types of regulations that different corporations must comply with will depend on the specifics of their business operations. For example, the banking industry is subject to a litany of regulations designed to provide stability and to avoid the impacts of financial crises (Vives, 2016). Similarly, higher education institutions have specific regulations that they must comply with and may fall within the domain of other regulations given the wide range of operations they conduct (Beaudin, 2015).

Methodology

To explore the literature pertaining to the research questions, a population of articles has been assessed using a thorough narrative review. As cyber security is an always-evolving subject, articles selected for review were limited to research published within the last 20 years. Articles considered for evaluation were not limited in origin to any specific geographic region, but only articles written in English were studied. Scholarly articles were sought using a combination of databases and keywords available within GALILEO and Google Scholar, and articles identified using relevant keywords were also used to identify additional related research using a snowballing approach (Wohlin, 2014). The initial articles returned were reviewed and retained based on their relevance to the research questions and were used to create a list of key articles. With a list of key articles selected, the articles were then decomposed to identify descriptive and analytic codes, which produced a high-level description of the articles' main points (Gibbs, 2007). The resulting codes were then reviewed to identify common themes based on the frequency of predominant and similar codes. The key articles were then compiled to create a key themes table (see Table 1) which details the author(s) & year of the article, the article's contribution to the research questions, and their resulting theme code (Ferrari, 2015). As the focus of this research is on cybersecurity program development in the risk management sense, articles pertaining to curriculum development were not assessed further. Additionally, articles containing conclusions that were redundant in nature to previously reviewed articles were excluded from further consideration.

Table 1: Key Themes

Authors (Year)	Contribution	Main Theme
Etzioni (2011)	Private sector organizations are integral to national security but are not regulated to the same level as public sector information systems making them a target.	1
Harknett and Stever (2009)	Success in the cybersecurity policy space will only be accomplished through effective strategy and knowledge sharing by government entities, private-sector professionals, and individuals.	1
Harknett and Stever (2011)	Cybersecurity guidance from several presidential administrations has been incremental in nature, rather than strategic, and cyber intelligence sharing has relied on self-interest rather than the public good.	1
Hiller and Russell (2013)	Private cybersecurity will only mature through the imposition of regulations and incentives combined with flexible approaches.	1
Hyla (2018)	The implementation of a dedicated agency with oversight of public and private cybersecurity may reduce costs, improve knowledge sharing, and provide customer data protection.	1

Maranga and Nelson (2019)	Institutions must invest in the proper resources, training, knowledge-sharing opportunities, and standards for the ethical conduct of its users and cybersecurity professionals.	1
Sales (2013)	Approaching organizational cybersecurity using an analytical framework based on regulations improves accountability and equity.	1
Aliyu et al. (2020)	The use of maturity models can be used to create a baseline by which changes in compliance can be quantified over time.	2
Arafat, Daiyan and Waliullah (2012)	A novel higher education security management plan is proposed that is designed to support academic freedoms, facts, and perspectives while adopting a proactive cybersecurity approach.	2
Bondoc and Malawit (2020)	The use of cybersecurity frameworks is necessary to ensure that resources and talent are aligned for effective implementations.	2
Bongiovanni (2019)	Information security programs within higher education institutions contend with a great deal of complexity and most new research has focused on the use of conceptual frameworks.	2
Doherty, Anastasakisa, and Fulford (2009)	Higher education security programs operate using an amalgam of disparate policies and standards that are overly technically focused which prevents a comprehensive approach from being feasible.	2
Hommel, Metzger, and Steinke (2015)	The understanding of effective risk management practices must be expressed in terms beyond high-level descriptions to be properly operationalized in higher education organizations.	2
Kam and Katerattanakul (2014)	Higher education institutions are heavily influenced by frameworks and regulations to mature their information security posture.	2
Merchan-Lima et al. (2021)	Frequent references to common frameworks, as well as hybrid frameworks, are present in the literature pertaining to information security management in higher education institutions.	2
Mishra et al. (2022)	The requirements for cybersecurity programs will differ based on the industry an organization operates in and can be determined by the information they process and store.	2
Rahman and Donahue (2010)	The convergence of enterprise security and information security as part of an overarching corporate risk management approach improves organizational productivity and sustainability.	2
Shackelford, Russell, and Haut (2015)	Although NIST is an output of the US federal government, it is being implemented at least in part by many nations around the world as part of their cybersecurity policymaking.	2

Arina and Anatolie (2021)	Significant events, such as the pandemic, can require substantial shifts within operations and the security approaches that must be considered.	3
Bandara, Ioras, and Maher (2014)	Technology platforms, such as e-learning systems, require a thoughtful approach to policy and cybersecurity to protect the data they contain.	3
Chabinsky (2010)	Establishes criteria for effective cybersecurity strategy and stakeholders' impacts on cybersecurity outcomes.	3
Ghelani (2022)	Combining management perspectives along with strategies to simultaneously secure physical, network, and compute resources can be used to create an effective preventative strategy.	3
Hina and Dominic (2020)	The alignment of information security management practices to business practices is often immature in higher education institutions and is impacted by a lack of awareness by campus populations.	3
Jarjoui and Murimi (2021)	A novel approach to cybersecurity risk management is proposed that uses a systems-based approach to link elements together providing a more holistic, adaptive, and interconnected security strategy.	3
Loonam et al. (2020)	Senior IT leaders must support a broad range of ideas and themes to create resilient cybersecurity programs in their organizations.	3
Reagin and Gentry (2018)	The evolving impacts of cybersecurity threats are forcing organizations to build defense programs rather than simply respond to incidents.	3

Results

Theme 1: External influences are necessary to promote and enforce cybersecurity maturity

The negative impacts and severity of information systems compromises have increased over time, throughout organizations from all industries. Organizational motivation for improving cybersecurity programs varies. In less mature or inadequately staffed organizations, cybersecurity may be approached as a compliance requirement, with programs focused on passing audit requirements. In more mature organizations, cybersecurity may be approached more broadly as part of a holistic risk management exercise (Rahman & Donahue, 2010). Cybersecurity attacks and breaches for organizations in nearly every sector can have widespread impacts, with consequences ranging from the loss of customers' personal information, the loss of proprietary information, and reputational damage impacting stakeholders and investors. In other sectors, the impacts can be more pronounced. For example, breaches affecting critical infrastructure providers or defense contractors can have national security implications (Hiller & Russell, 2013).

With the impacts of cyber-attacks having a blast radius that extends beyond the organization itself, one theme that emerged from the literature is a need for external influences to set cybersecurity requirements for organizations. Given that most infrastructure is operated by private entities and is intertwined with networks from other sectors, overarching solutions are difficult to achieve (Hiller & Russell, 2013). While some federally sponsored cybersecurity policy guidance efforts were made through multiple presidential administrations, the approaches taken have been viewed as cumulative and insufficient (Harknett & Stever, 2011). In addition, while regulations and public-private partnerships have seen some success in contending with cyber risk, these systems lack oversight and accountability (Hyla, 2018). Harknett & Stever (2009) posit that advances in this domain must be viewed as a public good rather than a private concern and can be accomplished by approaching cybersecurity as a civic duty and through information-sharing partnerships. Supporting this suggestion, Maranga & Nelson (2019) recommend that higher education organizations invest in conferences and exchange programs to share knowledge and learn best practices to help mitigate cyber threats. More directly, Hyla (2018) suggests that a single government agency dedicated to cybersecurity regulation would provide the best impact. In any of the suggested approaches, it is apparent that cybersecurity must be approached in a fashion that extends beyond the immediate sphere of a given organization, whether they are a higher education institution or a private corporation.

Theme 2: The vetting, selection, and implementation of frameworks are necessary to provide a structured, standards-based approach to cybersecurity programs

As evidenced by the number of articles identified as theme 2 that pertain to cybersecurity frameworks, it is apparent that the inclusion of frameworks as a pillar of effective cybersecurity programs is well established. In organizations, frameworks can offer a means to approach a wide range of abstract cybersecurity-related topics in a structured manner. The benefits of utilizing frameworks can include effectively organizing requirements, managing risk, measuring cybersecurity maturity, and prioritizing activities and resources (Bondoc & Malawit, 2020). The greatest challenge in the realm of frameworks may be the sheer quantity and variety of frameworks in use. Some frameworks are broad in nature and are designed to generally address the CIA triad, which is the protection of confidentiality, integrity, and availability of technology resources. Other frameworks, and subsequent standards, may be specific to certain types of risks, such as financial systems (Hommel et al., 2015). Given that information systems reside in both physical and virtual realms, such as data centers and cloud infrastructure, cybersecurity frameworks often have controls that specify physical security controls as well as secure software configurations. This convergence of risk management activities has encouraged some organizations to combine the efforts of physical security and cybersecurity professionals (Rahman & Donahue, 2010).

While the merits of frameworks are well-established, many organizations struggle to contend with the complexity of competing and overlapping frameworks. In higher education environments, standard frameworks face numerous challenges, including limited resources and budgetary allocations as well as the transient nature of student populations (Arafat et al., 2012). While contending with these challenges and managing risk in broad and dynamic environments, many universities elect to implement a portfolio of policies, most commonly starting with an overarching information security policy that enables subordinate policies, such as an acceptable use policy, and others (Doherty et al., 2009).

The nature of the business conducted by an organization also impacts the frameworks and governance required. For example, an access control policy will necessarily change depending on the type of data that is being processed. Healthcare providers will need to control access to specific types of data, such as patient medical records, whereas a financial sector organization may need to protect customer and business banking accounts (Mishra, 2022). These requirements may be clearer for organizations that work within one or a few sectors. Enterprises, such as large corporations and higher education institutions, face an exponentially larger challenge when the necessary frameworks and governance must encompass policies and protections for multiple data types.

Educational entities must comply with the Family Education Rights and Privacy Act (FERPA), which is designed to protect access to student data. Similar to certain financial sector organizations, universities that accept federal student aid money must comply with the Gramm Leach Bliley Act (GLBA) and institutions that offer certain counseling and medical services may also be required to comply with the Health Insurance

Portability and Accountability Act, commonly known as HIPAA (Kam & Katerattanakul, 2014). Each of these regulations is complex in its own right; in aggregate they are a heavy lift for organizations of any size or maturity. Interest in the use of frameworks is growing and can be particularly helpful for higher education institutions navigating the complexities of regulations. In fact, Bongiovanni (2019) noted that while research is sparse within the realm of higher education information security management, much of the literature published in this space since 2014 has focused on conceptual frameworks.

Theme 3: The continuous alignment of program strategy to dynamic environments and unique business requirements is necessary as cybersecurity risks change

While reviewing the literature, a third theme emerged which demonstrates the need for cybersecurity programs and governance to continuously align with changing environments and any unique business needs of the organization. Understanding how cybersecurity fits into an organization depends on many variables, some of which will be unique to the environment they support. As established by Loonam et al. (2020), cybersecurity leadership must extend beyond the technical configuration of information systems and integrate within organizational processes and structures. Features of cybersecurity programs must not only support secure system configurations, but also address human and behavioral factors. In fact, Jarjoui & Murimi (2021), suggest that while there is a great deal of literature pertaining to the implementation of frameworks, there is often a gap that exists between theoretical and practical implementations. This gap continues to expose organizations to risk (Jarjoui & Murimi, 2021). As use-cases, needs, and technological improvements occur over time, static frameworks and governance may not be suited to contend with new internal and external security concerns that come as a result (Ghelani, 2022). Furthermore, for cybersecurity programs to adopt an effective defense strategy, it will be important for program improvements to not only span technology, but also the processes and people that use these systems (Reagin & Gentry 2018). Chabinsky (2010) posits that a comprehensive strategy that considers supply chain, remote access, proximity access, and insider threats offers a means to reduce cyber risks, even as technology trends evolve.

While higher education institutions may be subjected to the same threats and vulnerabilities as corporate environments, they are often negatively impacted by poor governance, a lack of awareness of the value of the data they are holding, and poor monitoring & response which exposes these entities to increased risk (Hina & Dominic, 2020). There are many examples of information systems that are unique to educational environments. For example, educational entities must contend with a litany of security and privacy concerns arising from the use of e-learning platforms. E-learning systems are increasing in popularity due to their accessibility and effectiveness and they can be accessed by nearly any device that has internet connectivity. While convenience and accessibility are important, having such a wide range of potential configurations, data, and client device possibilities requires special consideration for security (Bandara et al., 2014).

In addition to unique systems, environmental changes also bring unique challenges for organizations to contend with. There may be no better example in recent memory than how technology was forced to quickly adapt to enable business operations during the COVID-19 pandemic. In addition to increased dependence on remote learning platforms, organizations quickly leveraged cloud computing services and video conferencing platforms to rapidly scale computing and communications capabilities as their students and employees transitioned to remote work (Arina & Anatolie, 2021). In each of these scenarios, information technology organizations were instrumental in ensuring business continuity. Understanding that information security programs must be malleable and adaptable to changing environments and requirements will continue to be necessary to manage cyber risks within organizations.

Discussion

While evaluating articles returned from keyword searches, analyzing retained key articles, and identifying the resulting themes, an assortment of information pertaining to cybersecurity program development has been compiled. The resulting information has been used to thoroughly contemplate the research questions, discuss implications from the findings, and offer a conclusion that includes the limitations of the study and identifies opportunities for future research. The research questions are evaluated from the perspective of the topics that emerged from thematic analysis.

RQ1: What are the differences and similarities found when examining the cybersecurity landscape pertaining to corporations and higher education institutions?

Corporate environments and higher education institutions both appear to benefit from external cybersecurity influences. An apparent reality is that most organizations struggle to grapple with the complexity of modern cybersecurity risks and governance. Part of this complexity comes as a result of a disparate combination of industry-specific regulations, varying international approaches to cybersecurity law and enforcement, and differing organizational motivations for cybersecurity. This combination has resulted in a largely decentralized cyber landscape that promotes a self-interested approach to risk management and lacks the unity that results from a common outcome (Harknett & Stever, 2011). The combination of decentralized cybersecurity approaches is particularly detrimental due to the intertwined nature of private and public networks. In aggregate, risks to these networks pose a significant threat to national security, despite being privately operated (Etzioni, 2011). Interfacing organizational networks with different approaches to cybersecurity and risk management may also provide an avenue for attacks to impact multiple sectors (Hiller & Russell, 2013). These challenges are amplified in higher education environments which rely on open architectures and large populations of users to operate (Bongiovanni, 2019). An overarching direction that reasonably sets baselines for cybersecurity activities stands to cut through some of the complexity and provide a consistent direction for corporations and higher education institutions that, despite differences in their business objectives, are realistically intertwined and operate in the same digital realms.

Virtually all cybersecurity risk management approaches in both corporate and higher education settings are similar in the use of frameworks to establish security controls. In fact, corporate and higher education environments frequently reference controls from many of the same security frameworks, such as those published by the National Institute of Standards and Technology (NIST) (Shackelford et al., 2015; Bondoc & Malawit, 2020). Additionally, corporations and higher education institutions enjoy many of the same benefits resulting from the use of frameworks, such as articulating requirements, aligning resources, measuring maturity, and establishing a list of security standards (Bondoc & Malawit, 2020). Although these frameworks are robust, they can be difficult to apply or scale throughout organizations of different sizes and complexity (Perry, 2021). The application of general frameworks in higher education environments has been particularly problematic. For example, poor alignment and complexity faced when implementing frameworks within higher education environments have brought forth suggestions for alternative information security models to be established (Kam & Katerattanakul, 2014). Additionally, new models are being organized to assist higher education institutions to measure their compliance with frameworks such as those published by the National Institute of Standards and Technology (NIST), the Payment Card Industry Data Security Standard (PCI-DSS), and the General Data Protection Regulation (GDPR) (Aliyu et al., 2020).

Perhaps the greatest difference that must be considered when developing cybersecurity programs for corporations and higher education institutions are the environments they must protect. While employee changes exist in corporate settings, the nearly continuous turnover of student populations within universities requires unique consideration. For example, students frequently connect their personal devices, which may be insecure, to university networks (Maranga & Nelson, 2019). This continuously changing student population can also make it difficult to effectively perform security awareness education, which is understood to be highly effective at preventing social engineering attacks, which are a leading attack method in the education sector (Borkovich & Skovira, 2019; Verizon, 2022).

RQ2: What are elements that can be translated from corporate environments into higher education cybersecurity program development?

While there are elements of program development that are unique to niche environments, cybersecurity programs supporting corporate and higher education environments have a great deal in common. These similarities can include the cyber threats organizations contend with, frameworks leveraged, and regulations that must be abided by. In terms of cybersecurity program development, this offers an opportunity for higher education institutions to benefit from best practices generated in the industry. In a broad sense, much of the knowledge and best practices in these areas can provide valuable guidance and examples for inclusion into higher education cybersecurity programs.

As noted in Table 2, many regulations exist that may be applicable in the corporate and higher education realms. For example, the Family Education Rights and Privacy Act (FERPA) is designed to protect student privacy. This regulation is unique to educational entities and is not often applicable in the corporate setting. On the other hand, regulations like the Health Insurance Portability and Accountability Act (HIPAA), are designed to protect patient health records. While this regulation is generally only applicable to corporations working in the healthcare space, universities that provide medical services may also be in scope. The same applies to other regulations, such as the Gramm–Leach–Bliley Act (GLBA). In the corporate world, GLBA would most commonly be applied to organizations in the financial services sector but is also applicable to certain systems and processes within higher education institutions that process financial aid distributions (Mishra et al., 2022).

Table 2: Example Regulation Applicability Matrix

Regulation	**Corporate Y/N**	**Higher Education Y/N**	**Applicability/Industry**
Family Education Rights and Privacy Act	N	Y	Education
Health Insurance Portability and Accountability Act	Y	Y	Healthcare
Gramm–Leach–Bliley Act	Y	Y	Financial Services
Payment Card Industry Data Security Standard	Y	Y	Payment Card Processing
General Data Protection Regulation	Y	Y	Privacy

The data in table 2 shows that higher education institution cybersecurity programs can incorporate elements from private entities across multiple sectors, as appropriate. As identified by Harknett & Stever (2009), multiple information-sharing entities, such as the FBI’s InfraGard and Information Sharing and Advisory Councils exist for the purpose of information sharing. While higher education institutions benefit from threat intelligence and information sharing within the realm of other higher education entities, expanding their networks to encompass other appropriate information-sharing entities can provide exposure to best practices and threat insights from organizations in the corporate world that function in overlapping regulatory domains. Providing higher education institutions access to the ever-expanding domain of cyber threat intelligence, especially across multiple regulatory domains, can provide exposure to actionable data that is useful to not only defend their networks, but also to strengthen their cybersecurity programs (Wagner et al., 2019).

Implications

The cyber threats that universities are battling continue to increase in frequency and intensity. As students embark and progress through their academic careers, it is more important than ever that their experience and growth are not impeded by cyber-attacks against university technology. In a 2019 higher education information security study performed by Jisc, only 52% of students felt confident that their personal data was protected by the university they attended (Chapman, 2019). Protecting the confidentiality, integrity, and availability of university information systems must be prioritized through the development, implementation, and continuous improvement of a thorough information security program. Information security management can be a challenge for many higher education institutions, particularly those that do not have adequate staffing or financial resources (Ulven & Wangen, 2021). For this reason, it is imperative that academic research continues to seek remedies that can bring knowledge and efficiency to higher education institution cybersecurity programs. As this research has shown, a tremendous amount of overlap exists between the corporate world and higher education institutions. While these environments will always have inherent differences, such as the necessity of academic freedom and experimentation, entities in these spaces are contending with many of the same burdens and we must strive to leverage the knowledge amassed by the cybersecurity community as a whole. This review has identified that the greatest difference between corporate and higher education cybersecurity programs is their regulatory environments. Higher education environments exhibit a many-to-one regulatory relationship, often finding themselves applicable to a broad range of regulations that individually would only be witnessed within specific industries in the corporate realm. This breadth of specialized regulations, combined with sparse resources, creates an environment that will only become more difficult to secure over time without substantial changes in efficiency and approaches.

Conclusion, Limitations, and Future Research

Higher education institutions are responsible and privileged to educate future generations of leaders. While protecting the tenants of academic freedom, research, and knowledge creation, modern universities are a frequent target of cyber-related attacks. Understanding the cyber landscape that universities exist in allows cybersecurity professionals to create and continuously improve their cybersecurity programs, which provides a systematic approach to managing risk. To gain insight into the current state of cybersecurity program development within corporation and higher education environments, this research studied a broad catalog of literature. The resulting literature was initially reviewed and coded, seeking to pair analytical and descriptive terms with the literature's findings. Using these codes, 3 main themes were able to be identified, showing commonality in the need for external influences, frameworks, and environments. Dissecting and evaluating these themes provides great insight into how corporate and higher education cyber environments and program development are alike and are also dissimilar. Fortunately, this research has demonstrated that these verticals have a great deal in common, ranging from the attacks they face to the regulatory environments they must comply with. This knowledge, combined with suggested industry pairings in the corporate realm, helps to pave a path for improved knowledge, understanding, and information sharing between corporate and higher education technology professionals. As these conversations progress, best practices, knowledge transfer, and threat intelligence sharing will create efficiencies for higher education environments, elevating cybersecurity programs to a level that would not be attainable on their own. This in turn will help protect the very environments that have been the backbone of knowledge and wisdom.

This literature review is not without limitations. First, a significant population of articles available for higher education cybersecurity programs focuses on curriculum development. A smaller population of research is available that examines the practical complexities of program development. Additionally, as is the case with many cybersecurity-related topics, a wealth of knowledge remains proprietary and is not shared within public or academic communities. While the leveraged sources (GALILEO, Google Scholar) offer a great volume of results for a literature review, I found quite a bit of the literature to be based on repetitive themes, offering a relatively narrow body of knowledge to draw from.

With many of the limitations of this research in mind, several research opportunities become apparent. First, and perhaps most importantly, cybersecurity researchers must find a way to peer around the curtain of secrecy that obscures cybersecurity knowledge and practices. As this article has shown, the cyber landscapes that corporations and universities occupy are quite similar and intertwined. As such, breaking down barriers and objectively collecting and publishing research to benefit organizations of all types will provide the greatest return on investment. Second, there is a great deal of literature that suggests the importance of overarching cybersecurity guidance, to create an equitable, common-good approach to the security of the critical infrastructure. The same literature, however, points out many flaws and a failure to meaningfully progress this narrative. Research pertaining to practical cybersecurity governance methods, gathered at an international scale, could provide a foundation for our legislators to establish more holistic cybersecurity guidance, improving the cyber landscape for all its inhabitants.

References

Afreen, R. (2014). Bring your own device (BYOD) in higher education: Opportunities and challenges. *International Journal of Emerging Trends & Technology in Computer Science*, *3*(1), 233-236.

Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016, August). Cyber-attack modeling analysis techniques: An overview. In *2016 IEEE 4th international conference on future internet of things and cloud workshops* (FiCloudW) (pp. 69-76). IEEE.

Alexei, L. A. (2021). Cyber security strategies for higher education institutions. *Journal of Engineering Sciences*, (4), 74-92.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, 10(10), 3660.

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk analysis*, 26(4), 907-923.

Arafat, J., Daiyan, G. M., & Waliullah, M. (2012). Emergence of robust information security management structure around the world wide higher education Institutions: a multifaceted security solution. *International Journal of Computer Science Issues (IJCSI)*, 9(4), 206.

Arina L. A., & Anatoli, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific and Technology Research*, (3), 128-133.

Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. In *ICERI2014 Proceedings* (pp. 728-734). IATED.

Beaudin, K. (2015). College and university data breaches: regulating higher education cybersecurity under state and federal law. *JC & UL, 41,* 657.

Blank, D. B., Hadley, B., & Unsal, O. (2021). Financial consequences of reputational damage: Evidence from government economic incentives. *Financial Review*, 56(4), 693–719. https://doi.org/10.1111/fire.12274

Bondoc, C. E., & Malawit, T. G. (2020). Cybersecurity for higher education institutions: Adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, *2*(3), 16.

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, *86*, 350-357.

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity inertia and social engineering: Who's worse, employees or hackers?. *Issues in Information Systems*, 20(3).

Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. *J. Nat'l Sec. L. & Pol'y*, 4, 27.

Chapman, J. (2019). *How safe is your data?: Cyber-security in Higher Education* (Vol. 12, pp. 1-6). Oxford, UK: Higher Education Policy Institute.

Cheng, E., & Wang, T., (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(192), 192. https://doi.org/10.3390/info13040192

Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science*, *78*, 179-184.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International journal of information management*, 29(6), 449-457.

Dudorov, D., Stupples, D., & Newby, M. (2013). Probability analysis of cyber attack paths against business and commercial enterprise systems. In *2013 European Intelligence and Security Informatics Conference* (pp. 38-44). IEEE.

Etzioni, A. (2011). Cybersecurity in the private sector. *Issues in Science and Technology*, 28(1), 58-62.

Eyadat, M. S. (2015). Higher education administrators' roles in fortification of information security program. *Journal of Academic Administration in Higher Education*, *11*(2), 61–68.

Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing*, *24*(4), 230-235.

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*.

Gibbs, G. R. (2007). Thematic coding and categorizing. *Analyzing qualitative data*, *703*, 38-56.

Harknett, R. J., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management*, 6(1).

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review*, 71(3), 455-460.

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, 29(3), 236-245.

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, 60(3), 201-211.

Hommel, W., Metzger, S., & Steinke, M. (2015). Information security risk management in higher education institutions: from processes to operationalization. *EUNIS Journal of Higher Education IT.*

Hyla, E. J. (2018). Corporate cybersecurity: The international threat to private networks and how regulations can mitigate it. *Vanderbilt Journal of Entertainment & Technology Law*, *21*(1), 309–338.

Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in cybersecurity management* (pp. 139-161). Cham: Springer International Publishing.

Kam, H. J., & Katerattanakul, P. (2014). Information security in higher education: A neo-institutional perspective. *Journal of Information Privacy and Security*, *10*(1), 28-43.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Liu, C.-W., Huang, P., & Lucas, H. C. (2020). Centralized IT decision making and cybersecurity breaches: evidence from U.S. higher education institutions. *Journal of Management Information Systems*, *37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2020). Cyber-resiliency for digital enterprises: a strategic leadership perspective. *IEEE Transactions on Engineering Management, 69(6),* 3757-3770.

Maranga, M. J., & Nelson, M. (2019). Emerging issues in cyber security for institutions of higher education. *International Journal of Computer Science and Network*, 8(4), 371-379.

Marano, P. & Grima, S. (2018). *Governance and regulations: contemporary issues*: Vol. First edition. Emerald Publishing Limited.

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications*, 76, 255-270.

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors* (14248220), 22(2), 538–N.PAG. https://doi.org/10.3390/s22020538

Perry, P. M. (2021). Establishing a cybersecurity program for my size entity. *Journal of Pension Benefits: Issues in Administration*, *29*(1), 4–9.

Rahman, M., & Donahue, S. E. (2010). Convergence of corporate and information security. *arXiv preprint arXiv:1002.1950.*

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity: Building a successful defense program. *Frontiers of health services management*, 35(1), 13-22.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Sales, N. A. (2013). Regulating Cyber-Security. *Northwestern University Law Review*, 107(4), 1503–1568.

Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks. *UC Davis Bus. LJ, 16*, 217.

Ulven, J.B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(39), 39. https://doi.org/10.3390/fi13020039

Verizon. (2022). *Data Breach Investigations Report (DBIR) 2022*. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigationsreport-dbir.pdf

Vives, X. (2016). *Competition and Stability in Banking: The Role of Regulation and Competition Policy.* Princeton University Press.

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589.

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering* (pp. 1-10).