The State of Cybersecurity in K-12 and Higher Education: Risk Assessment and Analysis

MS: Information Security Policy and Management Capstone Project

Mack Peterman, Regan McGovern, Jordan Christian, Lexi Rutkowski, Saurabh Pethe
Heinz College, Carnegie Mellon University

Abstract

On October 8th, 2021, the Biden Administration signed the K-12 Cybersecurity Act into law. This act aims to address threats to education, specifically the kindergarten through grade 12 levels. Created as a joint project between the Institute for Critical Infrastructure Technology (ICIT) and students of Carnegie Mellon University's Master of Science in Information Security Policy and Management program, this whitepaper seeks to provide a high-level overview of the current state of cybersecurity for educational institutions, both K-12 and Higher Education, in the United States. Through open-source research, interviews with subject matter experts and industry leaders, and Threat Intelligence work,, risks to both K-12 and Higher Education are identified, and recommendations to better strengthen the cybersecurity of these institutions are provided. Additionally, supplementary justification will be provided on whether Education should be named as a critical infrastructure sector under the Cybersecurity and Infrastructure Security Agency.

1 Executive Summary

This whitepaper is intended for all relevant stakeholders, including, but not limited to students, teachers, administrators, and government officials on the local, state, and federal level, in addition to other researchers. This document describes in its entirety what the current state of cybersecurity is within education and provides actionable recommendations for improving the overall cybersecurity posture. To begin, the authors define the scope of their findings, including what levels of education this paper focuses on and what the overall objectives of the document is. Next, current challenges, critical functions, key assets, high-value targets, and associated stakeholders are discussed in detail so as to provide a foundation for assessing risk in addition to highlighting the audience for which this document is most relevant to. The authors also seek to emphasize the value and impact of cybersecurity in education, which differs from an enterprise. Educational institutions' core focus is maintaining learning continuity. Furthermore, thorough research findings have been provided through open-source information gathering, interviews with industry experts, and threat intelligence work so as to appropriately demonstrate how and why educational institutions are a target. Lastly, the authors provide several recommendations that detail ways to handle risk and improve cyber maturity across organizations while also addressing the gaps that currently exist.

2 Scope and Objectives

This project seeks to assess threats to both K-12 education and Higher Education (HE) through identifying critical assets, key stakeholders, current practices and policies, and utilizing Threat Intelligence to in order to provide recommendations that address those threats. For the purposes of this document, a threat actor can be defined as a person or group that executes negative activities in order to disrupt, harm, or cause unintended consequences for an educational institution and its stakeholders via its information technology capability. Given that K-12 and Higher Education will frequently be used as blanket terms throughout this report, it is important to define specifically what falls under K-12 and Higher Education.

It is important to note that while the scope includes these

institutions, the whitepaper may not focus on everything listed below.

K-12 addresses educational institutions from the kindergarten through 12th-grade levels. This would include public, private, and charter elementary, middle, junior high, and high schools. Additionally, any special education, alternative, or subject-specific (art, technology, or trade schools) programs that fall within kindergarten and grade 12 levels are also covered.

Higher Education covers all post-secondary educational institutions. This includes both public and private, 2-year and 4-year colleges and universities in addition to trade schools, vocational programs, and any other post-secondary institutions. It covers any post-graduate degrees (Master and Ph.D.) in addition to post-secondary degrees (Associate or Bachelor).

Overall, the primary objective of this project is to develop scope-specific recommendations for identifying threats and risks to K-12 and Higher Education while accounting for cyber security posture as a whole, including the physical security element. Additional objectives include:

- Identifying high-value assets and targets for K-12 and Higher Education
- Providing a risk analysis that assesses the cost of implementation versus the cost of recovery
- Analyzing current threats to K-12 and Higher Education via Threat Intelligence research
- Providing justification for CISA to designate Education as a critical infrastructure sector

3 Current Challenges in Higher Education

Education as a "Soft Target": Ransomware and Cybersecurity Challenges

Educational institutions are privy to huge amounts of data about their staff, students and families. Despite this, they often lack the staffing, knowledge, and resources to actively protect all of this data. Rick Dakin, CEO of Coalfire, a cybersecurity and audit firm, said universities are soft targets for hackers because they have a "treasure trove of information assets" and often don't have the money to keep up with security safeguards. "They have always been targeted, but most attacks aren't publicly reported. Sometimes attacks aren't even detected," Dakin said [2]. Breaches of confidentiality, availability, and/or integrity can have massive implications, but it is well known that attackers seek the path of least resistance. As we will discuss further, there are a many factors that contribute to schools and universities being proverbial "low-hanging fruit".

Ransomware has quickly become one of the most common types of attacks against Educational institutions have the highest cost of recovery from ransomware attacks across industries, with an average cost of about $2.3 million dollars, which is 48% higher than the global average [1]. In 2020, 77 different educational institutions suffered attacks, and that number rose to 88 in 2021 [24] [25]. These issues are highly exacerbated by remote learning: schools of all kinds now have much larger, more distributed networks as faculty learn and teach from home. In addition, Bring Your Own Device (BYOD) and the public-facing nature of school networks makes it difficult to vet each device to ensure it meets proper security requirements [68]. Schools routinely struggle to find and retain cybersecurity talent, and overall awareness amongst students, faculty, and staff about cyber hygiene (defined as the implementation of basic cyber safeguards: for a robust discussion, see "Recommendations) remains low. The combination of these factors makes a variety of attack vectors (ransomware, phishing, etc) attractive to attackers.

Apples, Oranges, and Bananas

It is important to note as we explore the educational cybersecurity space that, while they technically all serve the same purpose of teaching the public, various types of educational institutions are actually very different. Whether it be pre-education, K12, undergraduate and graduate higher education, public, or private, each type of school will have its' own challenges, legal requirements, compliance regimes, and stakeholders. One of our initial interviewees referred to this as a "apples, oranges, and bananas" problem: while they are all technically fruits, people who work in each of these spaces are well-versed in the many nuances between types of educational institutions. [15].

Not only are educational institutions of all kinds facing challenges in the technology space: budgetary concerns are another major issue that will inevitably affect an institution's overall cybersecurity posture. K12 schools, especially public ones, already struggled with limited budgets, and then had to, and continue to, purchase new technologies to facilitate basic online learning [29].

Meanwhile, colleges of all kinds across the country face declining enrollment. Since the onset of the Coronavirus-19 pandemic, approximately 1 million fewer students are in college. Community college enrollment is down 13% since the fall of 2019, and overall undergraduate enrollment is down 6% [40]. These trends only reinforce an overall decline in college enrollment since 2012. This poses issues for colleges in terms of their resource allocation: they must provide more amenities to incentivize students to attend while facing a decline in revenues as fewer students enroll overall. The concept of resource allocation is and will continue to be a question when making cybersecurity spending decisions across all types of educational institutions, whether it be public schools constrained by lack of funding, or Higher Education institutions facing the issues discussed above. Our research will take these limiting factors into account as we make recommendations moving forward.

4 Identification of Critical Functions and Assets

4.1 Critical Functions of Education Institutions

Before thoroughly assessing an institution's asset inventory, it is important to first discuss the function and objectives of these institutions. Naturally, the main function of such organizations is to provide education and instruction to students in an effective and healthy environment. Additionally, some Higher Education institutions also focus significant efforts on research programs in a plethora of disciplines, ranging from energy and climate change to security and defense projects. Consequently, these K-12 and Higher Education institutions rely on a significant number of critical assets to support and drive staff's ability to educate, capacity to conduct research, and above all, facilitate student understanding and learning.

4.2 Identification of Critical Assets

To effectively assess and manage cyber risk that can impact critical functions, it is crucial to first attempt to identify all organizational assets. Without a significant understanding of what information, people, technology, and infrastructure the organization has, comprehensive identification of threats and areas of risk would be nearly impossible. The authors have identified critical assets for K-12 and Higher Education together, but have separated some areas out as particularly appropriate. Critical assets have been divided into four categories: Information, People, Technology, and Infrastructure.

4.3 Information

When identifying an organization's assets (or in this case, a set of organizations), it is important to consider not only physical components but information and digital assets as well. When it comes to cybersecurity risk, information is often the most critical asset to protect. For this reason, the authors have identified a list of information-based assets that are common to K-12 and Higher Education institutions.

Personally Identifiable Information (K-12 and Higher Education): With the success and progress of any education institution built around students and staff, any personal information should be considered crucial. This data relates to student and personnel names, addresses, social security numbers, schedules, and contact information. It is also worth noting that student grades and test scores are also identified as information assets, but they are not necessarily labeled as PII. However, they are generally linked to student names and associated accounts, indicating they can be at risk in the context of cybersecurity.

Financial Information (K-12 and Higher Education): Any information that relates to staff payroll, accounting, student payment accounts, or any other sensitive financial information can be classified as a critical asset. This data is necessary to pay personnel, process student payments (i.e. student lunch accounts), and activities to purchase or process other organizational resources.

Policies and Procedures (K-12 and Higher Education): At first glance, school policies and procedures may not seem to be critical assets. However, when looking at this from a malicious or attacker perspective, insight into how the institution handles certain situations can be valuable information used to gain unauthorized access to school systems. Malicious actors can leverage this information to gain a better understanding of an

institution's incident response procedures, security policies, and even student disciplinary measures. All of these can be exploited in some way to cause damage to individuals or the organization itself.

Projects and Research (Higher Education): In addition to the information discussed above, Higher Education institutions also support both student and faculty research and projects. Some institutions rely on such projects to maintain grants, funding, and partnerships with industry and governmental organizations. As an example, the authors consider Carnegie Mellon's numerous projects ranging from defense and security to robotics and energy. This information is often sensitive and valuable, meaning it could often be sought after by threat actors.

4.4 Technology

In today's hybrid and virtual learning (and teaching) environments, technology should be a crucial classification when evaluating critical assets. It not only provides the platform for students to learn and teachers to educate, but also the pathways for unauthorized access or control of school systems. In the context of this paper, technological assets can be both physical and virtual devices, which can be used to process and store information assets.

Hardware (K-12 and Higher Education): As is the case with any organization, physical assets are critical to daily operations and educational institutions are no exception. School hardware and physical devices are integral to not only administrative and staff activities, but the learning environment has come to rely heavily on technology. The list of hardware used by schools can be endless, but some noteworthy devices include computers, servers, communication equipment (phones, announcement systems, etc.), smart classroom devices (projectors, boards, etc.), and the associated connectivity equipment. Additionally, critical components that also merit consideration are power supply equipment, environmental control systems, and physical security measures taken by the institution.

Software- Programs and Applications (K-12 and Higher Education): Software, programs, and applications are as equally important as the hardware used to run them. (In some cases, virtualization is being implemented to replace hardware with software.) These digital assets are used by both students and staff and range from video conferencing and virtual classroom programs, to accounting and project management software. An introductory list of examples would also include student learning platforms, school websites, databases (as an asset that contains information, not specifically the information contained within), and security programs and controls used to protect school networks. With the increasing dependence on technological-based learning environments, software applications are becoming increasingly critical to education.

Networks- Wired and Wireless (K-12 and Higher Education): Networks provide the interconnectivity and infrastructure on which schools rely to provide their education and administrative services. As an example (which may differ depending on the institution), a wired network is physically located on school premises and consists of cabled connectivity between computers, servers (providing critical services to computers), and other network devices. Similarly, wireless networks are also a series of interconnected devices, but are connected via non-physical connections. Wireless is typically achieved through WiFi-enabled devices and provides a more convenient and accessible connection for both staff and students. However, this interconnection has made security more difficult; expanding the learning environment to points beyond school security controls, but within reach of potentially malicious actors. Although much more convenient, especially considering remote and hybrid learning models, wireless connectivity means that both authorized and unauthorized users are able to gain access from devices that are not easily monitored or tracked by security personnel.

4.5 People

It can be argued that any organization's most critical assets are its people, and for educational institutions, this is undoubtedly true. With the primary goal of educating young minds, the success and progress of an educational institution is constructed around people. Naturally, the most crucial assets in this context would be students and educators. However, this list should expand to include administrators, support staff (to

include custodial, cafeteria, and maintenance), and security personnel. It is worth noting again that each institution will be different and their respective lists will vary, but the basics of this category should include what has been discussed here.

Researchers and Subject Matter Experts (Higher Education): As previously mentioned in the Information section, Higher Education institutions generally fund and produce more research and projects for both faculty and students alike. Consequently, these organizations will typically have more researchers and subject matter experts who support and conduct research in critical areas of interest. These individuals play a vital role in student and institutional success.

4.6 Infrastructure and Facilities

The physical location of an educational institution and its associated facilities are also critical assets.This infrastructure includes school campuses, buses, and transportation vehicles and facilities, as well as sports and recreation facilities. Additionally, it is also important to highlight the physical safety and security measures that schools implement. These include (but are not limited to) metal detectors, alarm/alert systems, environmental control units, entry points (to include locking mechanisms), and access control points.
For the purposes of this paper, infrastructure and facilities are discussed in the context of cybersecurity. This infrastructure is used to house and secure many of the technology and information assets that have been highlighted above. The physical security of these facilities is vital to protect physical access to hardware, software, and information systems. These work centers also support research and facilitate work that leads to additional information technology-based assets.

Labs, Work Centers, and Shops (Higher Education): With a higher number of students With a higher number of students conducting research, projects, and other hands-on activities, Higher Education facilities will generally contain more laboratories, work centers, and workshops. These facilities are critical to both student and staff work and could house sensitive information and data, making them an asset as well as a target.

5 Primary Stakeholders

In the context of this project, the authors have identified stakeholders as individuals, groups, and organizations who can be affected by this research and its outcomes. Those identified can benefit, as well as lose as a result of increased cybersecurity for educational institutions (K-12 and Higher Education). Based on this definition, stakeholders will be anyone with an interest in education institution cybersecurity. It is imperative to consider all possible perspectives, therefore threat actors and malicious players will also be mentioned in this section. The following are considered stakeholders for both K-12 and Higher Education unless otherwise noted. It is also important to note that, like assets, stakeholders in this context are subjective and will vary from institution to institution.

Students
Naturally, students are considered major stakeholders. Schools are constructed around the education of students and the protection of their privacy is critical. Increased awareness of, and participation of cybersecurity in education will benefit students on multiple levels. This includes their privacy as well as their classroom experience overall. It is also worth noting here that parents, guardians, and caretakers of students should also be considered.

Administration
Administration will consist of all personnel who work for and with education institutions. Faculty, staff, and administrators are all considered due to their connection to the school. These individuals are also at risk as their personal information can also be a target, meaning they too can benefit from increased cybersecurity. Additionally, increased awareness in this regard can also help facilitate education and provide a safer and more secure teaching environment.

Communities
The communities in which these institutions reside also represent a vested interest. Specifically, increased cybersecurity could be double-sided: increased security could result in fewer attacks and fewer costs associated with attacks, but it could also lead to an increase in local taxes to support such projects, a reduction in services, and/or a consolidation of or closure of schools.

Conversely, lack of security could leave institutions vulnerable, creating more opportunities for ransomware attacks that may lead to an incident response that draws from taxpayer funding. Additionally, this also takes into account community leadership and associated organizations (i.e., school boards).

Non-educational Institutions

The communities in which these institutions reside also represent a vested interest. Specifically, increased cybersecurity could be double-sided: increased security could result in fewer attacks and fewer costs associated with attacks, but it could also lead to an increase in local taxes to support such projects, a reduction in services, and/or a consolidation of or closure of schools. Conversely, lack of security could leave institutions vulnerable, creating more opportunities for ransomware attacks that may lead to an incident response that draws from taxpayer funding. Additionally, this also takes into account community leadership and associated organizations (i.e., school boards).

Institute for Critical Infrastructure Technology

As America's "cybersecurity think tank," ICIT provides a wealth of information, education, and advisory services to a broad array of audiences, including government, private, and public organizations. As the overall project sponsor, ICIT will benefit from increased awareness and assessment of cybersecurity in education institutions by building upon this research and author recommendations.

Unauthorized Users and Malicious Actors

Although it may seem that apparent cyber threat actors are not actual stakeholders, the authors have chosen to include them as such to highlight the effectiveness of increased security awareness. These individuals or entities may not benefit from such research, but they can face loss in its success. With increased security awareness comes improved security culture, which can then lead to increased security for students and staff. This would make education a more difficult target to exploit, thus making attacks more difficult as well.

In the context of this research, the authors consider both internal and external threats as well as malicious and non-malicious users. Internal threat actors can be a disgruntled employee who steals payment information from the administration, a tech-savvy student applying some self-taught computer skills to access their grades, or simply an authorized user who accidentally makes changes to the system. External threat actors can also be malicious or non-malicious but are generally intending to cause harm. These can range from cybercriminals to hacking groups, and even state-sponsored entities.

6 Value and Impact

The intended impact of assessing the state of cybersecurity in education and providing actionable recommendations is to encourage increased awareness of cyber risk. One primary element to recognize is that educational institutions, while at times operating in a business-like fashion, are not businesses themselves [15]. Educational institutions reside in a very unique space, where its stakeholders' primary interest is not necessarily the bottom line. Instead, other metrics are prioritized like student performance, institutional ranking, implementation of new curriculum, and even the immersion of technology and new tools in the classroom. Educational institutions are much more concerned with learning continuity versus the standard business continuity [15].

With that said, in order to consider the value of prioritizing cybersecurity, specifically in education, one must consider how education views cybersecurity at the present. Unlike other industries, education, specifically public schools, colleges, and universities, receives a significant amount of its funding from federal or state programs. And while education has time and time again been an easy target for budget cuts or resource allocation, *money is not necessarily the key issue*. Essentially, the question becomes not **if** cybersecurity, in general, holds any form of value, but rather **how** educational institutions can recognize the value it holds within the field, not just in terms of money but in that primary goal of learning continuity [15]. In order for cybersecurity to hold value within educational institutions, it must be tailored to fit the unique needs of these institutions and their mission. Cybersecurity experts must pivot from trying to benefit education as a business and instead frame the benefit of cybersecurity as it relates to what educational institutions truly value.

And while money is not the primary motivation of education, these institutions still need a strong financial foundation in order to provide learning to its students.

Therefore, in terms of impact, one can look at the cost of recovery versus the cost of implementation. The cost of recovering from a cyber incident can vary greatly, especially when considering the attack type and the intended target. Over the past three years, the number of cyber incidents in education has grown. Exacerbated by the COVID-19 pandemic, education, like many other industries, was forced to pivot its traditional style of learning to a remote or hybrid model in order to adapt to mandatory lockdowns and quarantines.

Furthermore, when we look toward implementation, it is typical for enterprises to manage upwards of seventy security controls in order to safeguard the business from cyber threats [39]. With education, the responsibility of cybersecurity can vary by state and school district. There are no large security teams continuously monitoring activity. Under the Department of Education, the Readiness and Emergency Management for School Technical Assistance Center provides general information for schools on common types of malware, specific measures to take for preparedness, and tips on how to respond and recover if a cyber incident occurs [57]. But, there is no specific guidance on building, maintaining, and funding a cybersecurity program nor is there information on schools potentially outsourcing or forming outside partnerships to cover this type of work. With the increasing presence of and reliance upon technology in the classroom, whether it be for day-to-day instruction or testing, like the SAT, there is a pressing need for schools to keep up [30]. So, how exactly can these institutions continue to prioritize their mission while also creating a more secure environment for its students, teachers, and administration?

7 Risk Considerations

Two use case examples of a risk analysis, including a risk register, have been provided in order to understand the potential impact of cyber risks on an educational institution. A risk register is used to identify potential risks to an organization and includes the potential impact level of that risk and a specific response plan for that risk. There are four risk responses available: accept, avoid, mitigate, and transfer. The basis of these example risk registers is a result of research into current risk registers for education institutions. While many risk management frameworks exist, it is important to note that many of them are *enterprise-focused*. With that in mind, the authors have created a format specifically designed with schools in mind. When considering educational institutions, there are five main priorities: Safety and Security, Education and Instruction, Compliance, Financial, and Reputational. While the potential risks may differ depending on the type of institution, these five priorities should remain constant.

The use cases provided offer an example for both K-12 and Higher Education. The goal of presenting these use cases is to provide both a consideration of risk as well as a fairly straightforward method for these organizations to implement some form of a risk management plan. A proper risk consideration plan allows organizations to adequately prepare themselves for incidents that may arise in the future. For schools, learning continuity and the availability of operations to remain consistent is highly important.

It is important to note that these use cases are just examples of risk registers that have been developed through research. It is suggested that the concept of risk management be further developed for educational institutions at all levels beyond what is shown here (see Future Work). These example risk analyses can be found below:

7.1 K-12 Example - Public Elementary School

In this example, an elementary school is defined as educating grades 1 through 6.

When it comes to considering the potential risks associated with an elementary school, one must take into account the level of responsibility assigned to each stakeholder. With children ranging from age 6 to 12 years old, a specific level of responsibility is afforded to the faculty, staff, and administrators of the school during normal operating school hours and potentially during extended school hours or additional events and services. With that being said, there are specific risk areas that must be addressed.

In terms of Safety and Security, there may be potential risks to the physical, cyber, and information security of students, faculty, staff, and administration. Because of this, proper safety and security protocols in addition to the appointment of and collaboration with security personnel, relevant safety procedures, and local law enforcement is necessary in order to mitigate any risks. Any impact to the learning continuity and ability for the institution to deliver on its mission will have a low

risk appetite.This is also the case with physical security, in which the physical safety and wellbeing of students, faculty, staff, and administrators must be prioritized. Furthermore, there are many considerations that fall under the Financial priority, like elements of student development or additional services which could range from field trips, volunteer opportunities, and extracurricular activities. These components would have a high risk appetite, as they are non-critical to the maintenance of learning continuity.
The corresponding risk matrix for this example can be found in Appendix 1.

7.2 Higher Education Example - Private 4-Year University

As previously noted, assessment of organizational risks is subjective and will vary from school to school. In the example of a university, risk management considerations will largely remain the same as that of an elementary school. However, university students typically have more freedom and responsibility on their own. They can come and go as they please, make their own schedules, and generally have more control over their life at school. With that, universities assume less responsibility when compared to an elementary school, but still need to assess and address risks in the same way. Consequently, the risk register here follows a similar outline as that of an elementary school. The major difference between the two is that universities may assume less risk in some areas where students have more responsibility.
The corresponding risk matrix for this example can be found in Appendix 1.

8 Project Methodology

To ensure that research was both comprehensive and in keeping with the expectations set forth by ICIT, this project followed a four-phase plan. Those phases were organization, research, drafting, and revision. The authors' first team milestone was to establish a scope for the overall project, in collaboration with the project sponsor and appointed faculty advisor. Additionally, the K-12 Cybersecurity Act was explored in-depth, the passage of which motivated this research project. Finally, a robust outline was developed in order to serve as the basis for this final whitepaper.
Additionally, the authors established a schedule of two research phases: the primary research phase, spanning January 24th to March 7th, and the secondary research phase, spanning March 7th to April 17th. The primary research phase mainly consisted of open-source research gathering on a variety of topics. This included news publications, academic and industry journals, and technical Threat Intelligence gathering sessions. This phase also featured initial informational interviews with thought leaders in the cybersecurity space, both generally and those who have experience with the public sector, K-12, and Higher Education. Interviews are a major component of this final whitepaper, as they have allowed the authors real-world insight into educational services and the security industry. Some examples include ransomware recovery, zero-trust, remote access/learning considerations, and technology risk management. Additionally, this phase was used to explore existing best practices in the cybersecurity space as they apply. The secondary research phase was used to fill in any gaps uncovered during the revision of the first phase, to apply practical and novel Threat Intelligence information, and to conduct any out-standing interviews. Following the completion of the second phase, the paper was sent to interviewees to solicit final comments and revisions.

9 Research and Analysis

This section seeks to provide context and a foundation for cybersecurity in education, prior to presenting actionable recommendations. For research, three primary methods were utilized:

- Open source research in the form of news articles and other publications on recent cyber incidents and current policies and practices
- First-hand interviews with subject matter and industry experts
- Threat Intelligence research via a number of sources and tools

9.1 Case Studies

As previously mentioned, educational institutions have seen a dramatic increase in cyberattacks over the past several years. Since 2016 there have been over 1300 individual cyber incidents and in 2019, over 500 schools across the country were affected by

ransomware alone [61]. But ransomware is not the only attack type educational institutions are experiencing. These can range from targeted phishing campaigns for students, teachers, staff, and administration in addition to denial of service (DoS), data breaches, and other malware attacks [52]In 2020, the top states affected by cyberattacks were Texas, California, New York, and North Carolina, with Louisiana, Connecticut, Illinois, and Missouri as the next highest [13]. In Louisiana, the governor announced a state of emergency due to consecutive hits on three school districts across the state [12]. When looking toward Higher Education, universities have a history of being a target, which has only increased over the past three years with the shift to remote learning models. Some recent, notable incidents across Higher Education include two ransomware attacks, one at Butler County Community College (BC3), located in Western Pennsylvania, and the other at Howard University, located in Washington, D.C., both of which occurred in late 2021. Below are a few case study examples of recent attacks or threats to education ranging from ransomware, distributed denial of service (DDoS), identity theft, threats to third-party partnerships, and even an example of an attack against a university outside of the United States (U.S.).

Michigan State University: Two Attacks in Four Months

Over Memorial Day weekend of 2020, Michigan State University (MSU), located in East Lansing, Michigan, was the victim of a ransomware attack [70]. Attackers gained entry through the university's Department of Physics and Astronomy servers and demanded payment of the ransom, an amount which has never been disclosed, in order to prevent the leak of information [18]. MSU was one of many universities targeted by this particular malware, referred to as Netwalker. While the perpetrator of the ransomware was eventually detained, MSU was adamant about not giving in to the actor's demands and did not pay the ransom, as per discussions with law enforcement [18]. The university did not want to have a hand in perpetuating these types of attacks by paying the ransom. As a result, several records were released [18]. A few months later, in August of 2020, MSU was the victim yet again of a cyber incident, this time via their online school merchandise store [53]. Data compromised in this attack included financial information and other PII [53]. There is no evidence of a direct link between the ransomware attack and the hack of the school's merchandise store. However, it is possible that the school's post-incident recovery practices and policies may be called into question given the closeness in the timing of the two incidents.

Albuquerque Public Schools: Ransomware

In January 2022, Albuquerque Public Schools (APS) announced that they were the victim of a widespread ransomware attack [54]. As one of the largest school districts in the United States, covering 142 schools, the school district was forced to cancel classes for two days for its nearly 75,000 students across the district [54]. APS did not pay the ransom, under advisement from law enforcement, specifically, the Federal Bureau of Investigation (FBI) [54]. APS was not the only school district in New Mexico to be affected by cyberattacks at the time. Several other districts across the state were affected over the Christmas and New Year holidays [54].

Ventura and Conejo Valley School Districts: DoS Hits Southern CA

In September 2020, both the Ventura and the Conejo Valley School Districts, located in Southern California, were affected by a denial of service (DoS) attack [51]. At this time, the school was still operating via remote format. However, many teachers were working from school buildings, leading to them losing contact with their students for a few hours [51]. This, as result, had a major negative impact on the ability for learning instruction to be delivered, affecting the overall learning continuity for students. Because of the nature of the COVID-19 pandemic, and the requirement for students to stay home and attend classes remotely, valuable school time was lost during this attack, because teachers working on the school network were unable to deliver class [51].

Miami-Dade County: Insider Threat

The fourth-largest school district in the United States, Miami-Dade County, was the victim of several cyberattacks perpetrated by a student at South Miami Senior High School, located within the district [23]. This student-initiated eight distributed DoS (DDoS) attacks across the district, causing glitches and loss of connectivity for virtual classroom environments, effectively taking down the district's entire IT system [23].Students were not able to access virtual

classrooms, being inundated with error messages and a slew of technical issues for a few days. Teachers were able to pivot, employing other virtual platforms like Zoom or Google Classroom so as to not completely disrupt instruction [23]. The student who orchestrated the attacks was charged as a juvenile offender.

Calgary University: An International Example

While this document specifically addresses cybersecurity in K-12 and Higher Education institutions located in the United States, cyber threats and attacks have no borders. Therefore, consideration of international approaches to such incidents may provide lessons for incident handling and post-incident recovery. Looking at the ransomware attack on Calgary University in 2016, Trend Micro reported that this attack resulted in a payment of $20,000 in bitcoin to an unidentified perpetrator [64]. The university was unsuccessful in tracing who executed this attack, but was confident the attack came from an external source. While no personal or sensitive data was released by the attackers, the effect of the attack encrypted systems, rendering them unusable [7]. The university's justification for paying the ransom? To protect the integrity of the research performed at the university [7]. While paying ransom offers no guarantee that data will be recovered, the university was successful in decrypting and restoring function to their systems [64]. While their payment resulted in restoration, it begs the question if paying is truly the correct answer. Ransomware attacks have become incredibly prevalent, especially against education institutions, with attackers knowing a school's need to continue to maintain day-to-day learning instruction. Is paying ransoms ultimately setting these institutions up for the next attack?

New York City Hack: Breach via Third Party

In March 2022, the largest hack in the K-12 space occurred in New York City, with nearly 820,000 student records compromised [20]. These records contained four categories of information: biographic information (names, birthdays, ethnicity, etc.), special education information (disability information), sensitive information (family socio-economic status), and academic information (grades, teacher names, etc.) [20]. This massive violation of data confidentiality and availability was a result of security practices, specifically encryption, which were misrepresented by a third-party education platform, called Illuminate. Student records were not properly encrypted and as a result information was compromised and school grading operations across the city were halted for a week [20]. This incident was a clear violation of information security and a massive invasion of students' and their family's privacy. Given the recent nature of the breach, an investigation is still ongoing, specifically targeting Illuminate's pseudo-compliance with the New York City Department of Education and city laws [20].

9.2 Policies and Regulations

Regulatory Bodies

There are a wide variety of organizations that govern the operation of an educational institution. Which governance applies is influenced by where the school is located, the age group of students taught, the type of accreditation the school is seeking, and who provides the school funding, among other things. At the federal level, educational institutions are governed by the US Department of Education (DoE). From a cybersecurity perspective, relevant offices within the DoE include the Student Privacy Policy Office, and the Office of Student Technology. For public K-12 education there are multiple levels to the governance structure: State Education Agencies (SEAs), and then Local Education Agencies (LEAs), and then specific school districts and their elected boards, and finally the administration at a given school. Private K-12 schools are subject to some but not all of these bodies. For post-high school education at the state level, much is dependent on whether the college receives state funding or is private. Overall, this patchwork of regulatory bodies creates a great amount of diversity in a given educational institution's cybersecurity maturity and response preparedness. Such a landscape makes it difficult to issue blanket recommendations or standardize cybersecurity practices.

Relevant Laws and Regulations

At the federal level, two main laws which govern how student data is protected at schools and are therefore relevant from a cybersecurity perspective; FERPA and the PPRA amendment. As is the case with regulatory bodies, more specific laws and policies that schools are required to follow will vary widely across states and districts: only federal regulations will be addressed here.

Family Educational Rights and Privacy Act (FERPA): FERPA was originally passed in 1974, and applies to all schools which receive funding from the DoE for an applicable program. It codifies rights for both the parents of students and students themselves once they reach 18 years of age. The most relevant provision here is the prohibition of the release of student records to anyone other than a select list of excluded groups such as accrediting agencies and law enforcement [44]. As such, cybersecurity incidents in which student information is accessed by unpermitted third parties is a direct violation.

Protection of Pupil Rights Amendment (PPRA): The PPRA Amendment, sometimes called the Hatch Amendment, was passed in 1978. It protects the privacy of students as it relates to surveys, analyses, or evaluations and applies to any school which receives funding from the DoE for applicable programs. It governs the administration of gathering information on students that is related but not limited to, their political affiliations, mental illness, sexual orientation, and religious practices [43]. The amendment also protects and governs the disclosure of that information, which again is important from a data breach perspective.

Resource Constraint, Cyber Maturity, and Policy

Throughout both the open-source research conducted and the interviews held with people who work in the education space frequently, two themes became clear: a disparity across types of educational institutions in both their level of resource constraint and in their level of cyber maturity. At the inception of this project, the goal was to create or recommend a set of policy measures and applicable frameworks for use across institutions. However, as additional information has come to light, a uniform set of recommendations no longer feels appropriate. Beyond basic adherence to the regulations discussed above, schools vary widely in every aspect of their cybersecurity posture. To accommodate for this, recommendations will be divided into two categories: educational institutions with limited cyber maturity and resources (or a high level of resource constraint) and educational institutions with a higher level of cyber maturity and resources (or a low level of resource constraint).

Several factors influence the category into which a school falls: geographic location, local regulations and funding statutes, and type of education/age of the student. Common examples of educational institutions with high resource constraints include public K-12 or grade schools, especially in small communities and rural areas, state-funded or rural community colleges, and small private grade schools. In many cases, the security operations of these schools are run by a teacher or administrator with little to no technical background and a limited budget. [15] Examples of lower resource constraint institutions could include private schools which charge for tuition, especially in high-income areas and large private universities. Specific recommendations for high resource constraint institutions (namely good cyber hygiene) and lower resource constraint institutions which have already implemented basic cyber hygiene (frameworks and tools) can be found later in the paper.

9.3 Interviews

The individuals interviewed as part of this project ranged from cybersecurity experts to account managers who provide technology services to educational institutions. Each interview provided valuable insight and expertise to the authors and their research objectives. The following overview provides a brief summary of the interview process and whom the authors spoke to.

9.3.1 Methodology

Requests to interviewees were based on research into both educational and business institutions that the authors felt might have valuable insight into the overall goals of this paper, as well as by leveraging ICIT contacts. A set of questions were developed for each interviewee based on their unique backgrounds. Interview agendas were sent to interviewees in advance, which contained a brief overview of the project and the question set. Each interview lasted about an hour. A general overview of the types of questions asked is provided below, but again questions were tailored to interviewees' specific knowledge areas:

- What do you feel is the most pressing threat toward education, as it relates to cyber and information security? (Is this different from the most pressing threat in other sectors? Why or why not?)
- How has the shift toward a hybrid/remote learning model impacted education?

- How have you dealt with an unwillingness to invest in cybersecurity in your role?
- What are some attack trends you have seen over the past few years? (Has there been an evolution from simple, phishing or ransomware attacks to more sophisticated attacks?)
- How should smaller universities, colleges, or even K-12 institutions budget in order to prioritize cybersecurity (or any organization without a robust cybersecurity program)? In other words, what are the most prominent recommendations that you would provide for these institutions to implement?
- What are some current security policies that schools are implementing effectively? What policies or procedures do you think schools are lacking?
- In your opinion, would it be beneficial for Education to be added as a Critical Infrastructure Sector?
- Specific questions surrounding Threat Intelligence, APTs, and cyber attribution were asked of clients with a more technical background or expertise in those areas.

Additionally, it is also worth noting that the authors found willing participants to be few and far between. Due to the often sensitive nature of the subject, it is theorized that some organizations may have been reluctant to discuss their organizational security concerns with the authors. Of the roughly twenty organizations that were solicited, only seven responded and were willing to participate. However, the limited number of interviews provided vital information that ties into the author's recommendations that will be discussed in a later section.

9.3.2 Interviewees

Mary Ann Blair - Chief Information Security Officer, Carnegie Mellon University
Ms. Blair provided insight from an educational perspective, sharing her experience and expertise on threats that schools like CMU face. She also provided recommendations regarding how schools can implement security basics through general cyber hygiene practices.
Itzik Kotler - Co-founder and Chief Technical Officer, SafeBreach / ICIT Fellow
Mr. Kotler provided valuable information on cyberattacks that schools may face and provided real-world examples of how threat actors might target an education institution and why.
Katrin Hillner - President and CEO, PC Network Inc.
Ms. Hillner offered a different perspective on how to promote security in schools through effective communication and fostering a culture that supports resiliency. She also provided thoughtful suggestions on what a strong security program should entail.
Dr. Bruce Young - Governance Risk and Compliance (GRC) Practice Lead, PC Network Inc. / Professor of Cybersecurity and Information Assurance, Harrisburg University
Dr. Young brought a wealth of knowledge and expertise in cybersecurity, highlighting potential solutions to bring more effective security to education institutions by implementing centralized monitoring and response services.
Jim Routh - Chief Security Advisor, Virsec Systems / ICIT Fellow
Mr. Routh provided valuable experience and perspective from an executive level, illustrating how to bridge the gap between technology and management and promoting resiliency throughout the organization.
Bill Moss - Territory Account Manager, Infoblox
Mr. Moss's experience in managing security service accounts for education clients provided valuable insight into how some schools approach security and what type of services they outsource.
Ryan Cloutier - President and Principal Security Consultant, SecurityStudio
Mr. Cloutier's experience working to strengthen cybersecurity in education provided a critical perspective on how to best bridge the communication gap between schools and technology.

9.4 Threat Intelligence

In order to correctly evaluate the current state of cybersecurity in education and provide appropriate recommendations, it is necessary to understand current threat actors and the likelihood of these threats directing their resources towards K-12 and Higher Education. The Threat Intelligence methodology used by researchers consisted of a number of parts. It was necessary to explore several knowledge bases such as the MITRE ATT&CK repository [37], Red Canary's 2021 Threat Detection Report [6], Crowdstrike Threat Detection Report [17], and

information shared by the United States Government. Open Source Intelligence (OSINT) also aided research into cyber threats, cybercriminals, and Advanced Persistent Threats (APTs). Finally, insight was gained through numerous interviews with professionals in the industry. Some of the interviewees pointed researchers towards specific cybercriminals and APTs that have been further researched and detailed below.

The question that needed to be answered: Why is it important to understand threat actors that are targeting education? In a report, Microsoft detailed the percentage of devices with malicious encounters over the last 30 days [35]. Out of over 8 million devices with malware encounters, education accounted for over 80%. As of March 29th, 2022, the education industry has been the most targeted in comparison to other groups such as retail and consumer goods, healthcare and pharmaceuticals, telecommunications, financial services and insurance, and power and utilities. Threat actors acknowledge the opportunity due to the restricted budget for education, limited resources, and potential financial gain.

For Threat Intelligence, specific focus has been placed on malware, APTs, and Cybercriminals for both K-12 and Higher Education. While attribution can be very difficult, organizations often release warnings of malware, APTs, and cybercriminals targeting certain industries. This then raises the question: *What exactly differentiates Cybercriminals from APTs?*

Cybercriminals are typically part of an organized network of criminals attempting to attack an end target. Their technical abilities can vary but they tend to have greater resources and skillsets when compared to other malicious parties like script-kiddies, making them a much larger threat to organizations.

On the other hand, an APT is a cybercrime body that is backed by the state or government where the group originates. As a result, APTs generally have access to better infrastructure, resources, and funding. They are able to carry out more sophisticated attacks over longer periods of time, a luxury that may not be available to the average cybercriminal. They attempt to maintain persistence within their end target for a longer period and do not stop until they have succeeded. APTs typically use similar malware time after time with slight variations. This can be useful for analysts as they are able to derive patterns to better protect their systems. Moreover, the attack technique may remain similar even if the payload changes. Knowing the attackers, organizations may also be able to better anticipate their demands in case an attack or breach does occur.

Through information gathering, social media, interviews, and community sharing, several APTs and Cybercriminals that pose the biggest threat to K-12 and Higher Education have been identified. Some groups may be prevalent to both depending on a number of factors. In addition, it is important to recognize adversaries, both APTs and Cybercriminals, who have targeted the healthcare industry. Universities that have healthcare or health insurance affiliations could provide a vector for threat actors to move laterally into the institution, according to Infoblox Account Manager Bill Moss. This is largely dependent on how well the networks between the two are segmented [8]. Below are specific details of these groups and the malware associated with them.

9.4.1 K-12

The shift to remote education in 2020, driven by the pandemic, introduced a host of cyber threats to educational institutions. Unlike Higher Educational institutions, many K-12 schools were not as technically proficient and ready for this dramatic change making them even more vulnerable to cyber-attacks.

2020 saw a significant increase in the number of cyberattacks on K-12 institutions. According to the K-12 Cybersecurity Resource Center, 400 such attacks were reported [31] The pie chart in Appendix 5 depicts the distribution of the reported attacks:

1. Data Breaches: 36% of attacks reported were data breaches. These involved both student and staff data and were one of the most common types of attacks reported

2. Ransomware: Extortion demands made to schools may have significantly increased, in some cases far exceeding $1 million per incident. 12% of reported attacks were related to ransomware

3. Denial of service: These attacks involved denying students and staff access to resources, sometimes leading to the cancellation of classes

4. Phishing: In one commonly employed tactic targeting teachers, attackers abuse-free email services, including Gmail, Outlook, iCloud, and Yahoo, to create fake email accounts impersonating K-12 school personnel

5. Unattributed malware, class invasions and other disruptions: These attacks include unattributed malware, class and meeting invasions, email invasion, website and social media defacement, and a wide variety of related and/or low-frequency incidents and comprised 45% of all reported attacks

The first quarter of 2021 saw another increase in cyberattacks on the education sector. Nearly 10% of globally reported attacks targeted educational institutions, which was over a 30Latest reports suggest that this trend has only increased over the past couple of years [32]. Cybercrime researchers, Cybersecurity Ventures project cybercrime costs to rise to $10.5 trillion annually by 2025, up from around $3 trillion in 2015 [38]. Given the rise in cyber crime in the past few years, this estimate is certainly plausible.

9.4.2 Higher Education

Much like K-12 institutions, Higher Education institutions have witnessed a rise in attacks. The shift to remote education widened the attack surface and exposed millions of students to cyber threats. Most attacks are not reported and the exact impact is hard to estimate. However, some high-profile attacks were brought to light. Michigan State University was attacked with ransomware twice in four months [70]. In 2021, the attack on the University of Massachusetts Lowell forced the university to close completely for a week [11].
Mary Ann Blair, CISO at Carnegie Mellon University, spoke to us about how the loss in network visibility due to remote school made it hard to block some cyberattacks [9]. A shift to complete remote learning also makes it harder for universities to determine if students are falling for phishing attacks. A BYOD policy also increases vulnerabilities and brings around several compatibility issues.
Some of the observed malware, APT groups, and cybercriminals targeting Educational Institutions are covered below:

9.4.3 Malware:

In March 2021, the Federal Bureau of Investigation (FBI) issued a warning to Higher Education institutions, K-12 schools, and seminaries about the PYSA, also known as Mespinoza, ransomware. Upon encryption, victims see the following message "Protect Your System Amigo" [45]. This malware extracts user data while also encrypting sensitive files. The data is then used as leverage in negotiations to persuade the affected party in paying the ransom. Technical details regarding PYSA can be found in the Appendix.

9.4.4 APTs:

Name: Gold Lowell, Boss Spider
Attribution: Iran
Associated Malware: SamSam
Attack Vectors: Remote Desktop Protocol (RDP), File Transfer Protocol (FTP), Java Based Web Servers, Brute force attacks against weak passwords [42]
Details: SamSam malware is known for targeted attacks, does not spread by itself, and needs human involvement to run [36]. In November 2018, two Iran-based individuals were charged for attacks based on the SamSam malware. More than 200 victims included public institutions, hospitals, and municipalities [47]. Gold Lowell typically scans for vulnerabilities on Internet-facing systems. Once a presence has been established, malware such as SamSam can be deployed. From there, attackers have shown the ability to escalate privileges and move laterally across the network [66]. Gold Lowell also uses a number of open-source tools such as JexBoss, Mimikatz for credential theft, Wmiexec, RDPWrap, and NLBrute. Indicators of compromise (IOCs) from Gold Lowell can be found in the appendix.

Name: Winnti Group, APT41, WickedPanda
Attribution: China
Associated Malware: PlugX, ShadowPad
Attack Vectors: Brute Force attacks, RDP, Domain Name System (DNS) [28]
Details: In late 2020, the U.S. Department of Justice charged five Chinese citizens for hacking crimes committed in the United States and across the world. This scheme included a wide range of targets in the video game industry, universities across the world, and non-profit organizations. These citizens were linked to APT41 and were motivated by profit [34]. In the official documents released by the DoJ, a number of universities in the U.S. had been targeted [67]. APT41 has also been known to target the healthcare sector, and this is another vector that could be used to move laterally to HE institutions that have associated hospitals [28].

Name: Energetic Bear, DragonFly
Attribution: Russia
Associated Malware: Havex RAT, Oldera, LightsOut, Exploit Kit
Details: Energetic Bear has targeted some education institutions, but has primarily focused its efforts on industrial control systems [3]. However, given the current state of Russia's invasion of Ukraine and U.S. involvement in providing aid to Ukraine, the team believes Russia may attempt to retaliate against those aiding the Ukrainians. Given that Energetic Bear has some history of attacking educational institutions, it is necessary to include them as potential threats.

9.4.5 Cybercriminals

Name: Silver Terrier
Origin: Nigeria
Associated Malware: Information Stealers and Remote Access Trojans (RATs)
Details: It is not clear whether Silver Terrier can be classified as an Advanced persistent threat because there isn't any evidence at the moment to show that they are state-sponsored. However, they have been one of the most prolific hacking groups mainly targeting large businesses, as part of Business Email Compromise (BEC) attacks [58]. These actors have now collectively produced more than 81,300 samples of malware linked to 2.1 million attacks across the globe. The most common tools that SilverTerrier actors used to attack organizations once they infiltrated those networks were information stealers and remote access trojans (RATs).

Name: Vice Society
Origin: Unknown
Associated Malware: PrintNightmare (CVE-2021-1675)
Details: This gang is fairly new in the world of ransomware attacks, emerging is mid-2021. Vice Society was responsible for the attack on Butler County Community College (BC3). In line with common ransomware attacks, the cybercriminal group obtains sensitive data, encrypts the storage servers, and demands payment in exchange for not publishing the information. The attacks from Vice Society have been concentrated on mid-sized organizations, however, reports have shown this group to have a specific interest in public school districts as well as Higher Education institutions. Vice Society also operates a leak site on the Dark Web where they publish the information of those who refuse to pay [33]. Leak sites are a good source of information to discover if an organization's data has been released and sold.

Name: Netwalker
Origin: Unknown
Associated Malware: NetWalker Ransomware
Attack Vectors: Phishing
Details: NetWalker, also known as Circus Spider or Mummy Spider, is a cybercriminal gang that has been around since at least 2019 [16]. Their targets have included hospitals, law enforcement, school districts, and colleges and universities [46]. NetWalker has two separate parties involved in their activities, "Developers" and "Affiliates". The former create and update the ransomware used by the group while the latter identify and exploit what they believe to be high-value targets. As the COVID-19 pandemic has progressed, cyberattacks have increased against healthcare. As mentioned above, this could also be leveraged to attack an affiliated university. NetWalker did just this by breaching The University of California, San Francisco's school of medicine [62]. In the same year, NetWalker was also responsible for an attack on Michigan State University where information regarding a student's passport and two other financial documents were released on the group's leak site [14].

10 Recommendations

Having discussed the current cyber risk landscape for educational institutions, recommendations will now be provided which detail cultural, technical, and procedural ways to handle that risk and improve cyber maturity across organizations. The question of whether or not to consider paying ransomware, one of the leading issues amongst educational institutions, will also be discussed,

10.1 Mission Enablement: Maintaining a Learning Community

Mission enablement refers to the continued effort of an educational institution to uphold its mission statement and deliver on its promises to its stakeholders. Furthermore, mission enablement allows for the prioritization of learning continuity. Mission enablement includes:

10.1.1 Knowing Your Audience

As it stands, much of the language regarding cybersecurity and its impact is primarily enterprise-focused. With that being said, there is a learning curve that must be addressed when discussing cybersecurity in education. Security must be framed from an education perspective, focused on promoting learning continuity rather than revenue or business continuity [15]. In many ways, this can be interpreted as moving from "scare to care" [15]. Cybersecurity should not be framed as practices to shield innocents from the deep, dark, scary elements of the internet. Instead, cybersecurity should be instilled as a necessary measure to maintain a positive learning environment, in addition to protecting the students, faculty, and staff of an educational institution, akin to the locks on classroom doors.

Stating the effects of a cyber incident in terms of financial loss or disruption of the market is not applicable to schools. However, framing the concept of cybersecurity and the result of diminished cybersecurity around the inability to maintain normal learning environments may bridge the gap that currently exists between education and cybersecurity. Educators should be inclined to think of cybersecurity as no different than typical physical security: a necessity.

For example, if teachers came to school one morning only to find all of the doors locked, with no one possessing the keys, there would be major cause for concern. Normal school operations would not be able to resume until the doors were unlocked. Shifting the language to technology, if ransomware were to occur that locks all of the information a school possesses, including student records, payroll information, and learning systems, normal learning functions would not be able to operate.

Pushing this idea even further, the teachers remember that there is a backup set of keys located at the district's office across town. While there may be some delay to the school day, they will now be able to get the school unlocked and start the day. Shifting the cyber, in the case of ransomware, although the school is locked out of its current systems, they remembered that they set up offsite backups of most, if not all, systems. While there may be a delay in getting back on track, they are still able to maintain learning continuity.

Cybersecurity within education must be interpreted as a necessary component of learning operations, so as to provide the best possible educational experience for its students. Equipping a classroom with textbooks, desks, pencils, notebooks, and other materials is integral to academic performance and success. Given the increased presence of technology in the classroom, the importance of cybersecurity must be understood and tailored to the appropriate audience.

10.1.2 Fostering a Culture of Security and Resiliency

As the dependency on technology continues to increase across educational institutions, the idea of implementing appropriate security moves from a 'nice to have' to a 'critical need.' IT teams can implement technology-based controls that mitigate breaches to education systems, but this should only be part of a school's strategy and overall approach to security. To effectively respond to these risks, the administration needs to instill a culture and mindset that is focused on both security and resiliency.

ICIT Fellow Jim Routh explained that a culture based on resilience is much more effective and efficient than a culture of security [60]. A culture of resilience places greater emphasis on lessons learned, awareness, and transparency regarding security issues in order to ultimately learn how to address and mitigate risk instead of simply avoiding it (where possible). This mindset also emphasizes response measures in the event of a cyberattack or breach.

Furthermore, resiliency is also dependent on accountability. In a general sense, accountability is not to place blame but instead used to identify who has responsibility for specific activities and processes. This idea is instrumental to security but fundamentally extends to fostering organizational resiliency as well. According to Katrin Hillner, president and CEO of PC Network Inc., "accountability should be a staple in all security programs" [27].

It is important to note that these two ideas may be conceptually different when dissected, but are often interwoven into most cybersecurity programs. Security and resilience often go hand in hand in this context, with the overall objective of data, system, and network confidentiality, integrity, and availability. The biggest difference between the two lies in their fundamental perspectives. Routh illustrated this point through a relatable example (that the authors have adapted for a school's perspective); a malicious email sent to a school teacher with the

intent to gain access to the network.
In this example, a teacher received an email that was originally thought to be from the school's principal. After opening the email, it was revealed that the message was in fact a phishing attempt and the teacher was notified after clicking on an attached link. From this point forward, the teacher would avoid any and all emails coming from the principal based on the idea that they *could* be malicious. This approach exemplifies a security culture mindset; the teacher simply avoided any more emails from this sender because it was more secure to ignore them (you can't get caught in a phishing campaign if you don't take the bait). Instead, a culture of resilience mindset would use the event as a learning experience and subsequently be used to train employees on how to identify phishing attacks and what to do when they occur (how to spot malicious activity and how to respond to it).
Considering the similarities and differences between the two, the authors conclude that security and resiliency are largely codependent - an institution becomes more secure as it becomes more resilient. Effective security programs achieve that status by being more than just technological controls to prevent unauthorized usage. They grow out of a culture that emphasizes security and promotes resiliency. This mindset should be fostered at all levels; from administrators and staff to teachers and students. Promoting a culture of cybersecurity and resilience is essential for the protection of students and staff.
Instilling a culture of security and resiliency also relies on the overall approach to IT needs. According to Ryan Cloutier, Principal Security Consultant and President of SecurityStudio, IT and security departments of educational institutions are often '"siloed," citing that teams within these capacities are often preoccupied with their own functional area and prioritize this over other activities [15]. Generally speaking, this means that a networking team is composed almost entirely of network specialists and focused solely on networking, while the risk team is made up entirely of risk specialists and only concerned with risk.At first glance, this may appear to be beneficial, however, this leads to significant blind spots that can hinder effective security management across different IT functions. *(Note that this idea may not apply to all institutions. Higher Education organizations or K-12 with significant resources dedicated to IT and security functions may benefit from mixing their IT staff. Smaller organizations with fewer resources and personnel may not have this option.)*
Based on this realization, the authors recommend that educational institutions reorganize IT teams to include personnel from different specialties. This concept would support not only a broader understanding of the different functional areas but also how they can best complement each other to provide the most effective approach to security. This would also seek to promote a strong, secure, and more resilient mindset across departments, as well as with the leadership positions that would be managing staff from different specialties.

10.2 Frameworks and Policy

As discussed in the preceding sections, information that emerged throughout the process of drafting this report suggested that when making recommendations for how educational institutions should improve their cybersecurity posture, there is no one blanket answer. Instead, the varying degree of cyber maturity and patchwork of regulations means that there are two main types of institutions: those with a high level of resource constraint and those with a low level of resource constraint.
High resource constraint means that institutions have limited resources to devote to their cybersecurity programs, from both funding and staffing perspectives. Lower resource constraint organizations have fewer funding limitations, and more time and staff to devote to developing and maintaining cybersecurity programs. Factors that influence the category into which a school can include but are not limited to geographic location, local regulations and funding statutes, and type of education/age of students. Examples of educational institutions with high resource constraints include public K-12 or grade schools, especially in small communities and rural areas, state-funded or rural community colleges, and small private grade schools. For these schools, the overwhelming recommendation among the interviewees was to begin with a program of basic cyber hygiene. Examples of lower resource constraint institutions could include private K-12 schools which charge for tuition, especially in high-income areas, and large private or state universities. For these institutions, investments can be made into implementing, and potentially becoming certified in, a specific cybersecurity framework.

10.2.1 Cyber Hygiene

Cyber Hygiene does not have a single industry-standard subset of practices; Instead, it is the general concept of performing basic tasks which have the biggest impact on the overall cybersecurity health of an organization. As such, cyber hygiene is a more flexible and versatile option than choosing to follow a specific framework, and also has the ability to scale across a variety of funding and staffing levels. For educational institutions with limited resources, that scalability is vital. Compiled based on conversations with experts and additional research, the following is a list of recommended cyber hygiene practices. The listed is roughly sorted by importance, with actions that will best mitigate the attack vectors frequently experienced by schools listed higher.

Robust and Comprehensive Backups
Ransomware preys largely on the need for victims to access the only copies of their data that the ransomware has encrypted. Therefore, the most effective way to combat the effects of a ransomware attack is to create and maintain working backups of all data necessary for a school to operate.Those backups should be stored separately from the main network, and tested for completeness and operability every six months at minimum.

Multi-Factor Authentication (MFA)
There are three types of authentication: something you know (such as a password or PIN), something you have (such as an ID swipe, token, or secondary device), and something you are (typically a fingerprint or retina scan). Many systems utilize only something you know, most often a username or email and password combination. Multi-factor authentication utilizes two or more of these types instead of one. The most common application in a school setting is the secondary device/something you have: a sign-in attempt triggers the user to confirm their request on a linked cellphone app or via their email. MFA greatly reduces the ability of attackers to gain access to accounts via a stolen password or password guessing, because they do not have access to the second method of authentication.

Properly Configured and Enforced Password Management
Password management is a key aspect of good cyber hygiene, as passwords are the first line of defense in access to most systems. There are two aspects to password management: the front end, which interacts with users and enforces the password policy during creation and updating, and the back end which stores passwords and checks for correctness during log-in. On the front end, users should be required to set a password that contains at least 8 characters, with a letter and a number. Based on additional factors, the number of characters may be increased or dictionary words may be disallowed. Additionally, default passwords should not be allowed- changes should occur during device or account setup. On the back end, passwords should be stored as a salted hash, not encrypted or in plain text. A hash is a string of characters that only the user's specific password can create after being run through an algorithm. A salt is an additional string of characters added to the hash to prevent the creation of tables of pre-generated hashes. With this method, the school must only check to see if the two hashes match, preventing them from having to store a student or staff password in any capacity.

User Awareness Training
User awareness training helps to eliminate unsafe behaviors a user may carry out without knowing the full effect those actions may have. A prime example is training related to phishing: helping users understand what a phishing email looks like and what to do if they receive a potential phishing attack goes a long way toward preventing monetary and credential theft. For more information on user awareness, see the section "Creating a Culture of Security and Resilience". Implementing these measures greatly decreases the attack surface for the average educational institution, and makes recovering in the event of an attack much easier. Most of these solutions can be implemented with comparative ease or purchased as an off-the-shelf solution. That combination of benefits makes cyber hygiene an excellent first step for schools with limited time, staff, and funding resources.

Basic Patch and Update Management
PPatch and update management refers to creating a policy, procedure, and technical implementation to manage the installation of patches and updates across a network. Patches and updates should be ranked

according to severity, and implemented at a timeline representative of that severity. Patches or updates which contain fixes to major security threats should be implemented as a top priority, moving down the scale from there.

Acceptable Use Policy
Especially during a time of heightened remote access and work from home (WFH), it is critical for organizations of all kinds to have an acceptable use policy: this is no less true for schools, especially in districts that distributed computers to students and staff at the start of the pandemic. An acceptable use policy details the actions that can be performed on a computer, such as downloading additional software. This policy can be enforced both procedurally and technically depending on need. Preventing dangerous behavior on devices that have network access limits the opportunity for third parties to abuse that access and gain a foothold in the system.

Install Reputable Antivirus Software and Firewalls Antivirus software and virtual or physical firewalls are two technical methods to curtail unwanted behavior on a network. They monitor software/file downloads and network traffic. While not an all-encompassing solution, they help close the paths of least resistance for attackers and provide better visibility across the network, which can assist in making future cybersecurity plans.

10.2.2 Potential Frameworks

If an educational institution has consistently managed to achieve good cyber hygiene via processes that are well-documented, auditable, and repeatable, they should begin to consider adopting a more robust cybersecurity framework. Becoming certified on that framework when possible is also a potential follow-up step. It is most likely that educational institutions which are able to reach this stage, especially from a certification perspective, will be organizations with lower resource constraints. What follows is a detailing of potential frameworks for lower-resource constraint or more mature cyber programs to consider implementing:

NIST 800 Series
The National Institute of Standards and Technology (NIST) maintains a library of "guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities" which are published as part of the 800 series [49]. While they are technically published for use in the federal government, they are often used by other public and private organizations. Examples of 800 series publications include a Secure Software Development Framework (800-218), Developing Cyber-Resilient Systems (800-160) and a Workforce Framework for Cybersecurity (800-181) [50]. The most commonly used is NIST 800-53 or Security and Privacy Controls for Information Systems and Organizations. 800-53 "provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks" [41]. It is important to note that these documents are voluminous and will require time and consideration in order to tailor it to a specific scope.

NIST Cybersecurity Framework
The NIST Cybersecurity Framework (CSF), or "Framework for Improving Critical Infrastructure Cybersecurity" consists of five phases: Identify, Protect, Detect, Respond and Recover. Each of these components contains a subset of categories and subcategories which detail specific steps [48]. One of the main benefits of the NIST CSF is that actions are assigned into one of four tiers, and an organization can choose which tier they would like to be proficient in for each of the five phases, allowing for flexibility and prioritization of resources. The tiers are, from least to most advanced: Partial, Risk Informed, Repeatable, and Adaptive. Originally developed as a way for the nation's 16 critical infrastructure sectors to standardize their cybersecurity programs, the NIST CSF has become popular amongst other organizations as well to either follow specifically or use as a jumping-off point for their own programs.

ISO 27000 Series
Developed as a collaboration between the International Standards Organization and the International Electrotechnical Commission, the 27000 Series details the purpose and functions of an Information Security Management System. It provides best practice guidance on a variety of aspects of Information Security management, such as privacy/PII, network security, application security, and governance.

Information Technology Infrastructure Library
The ITIL framework provides broad guidance for implementing and managing information technology services. Created by the British Government following a survey of a variety of organizations, it establishes a common language of technology/cybersecurity definitions and goals, which is helpful when enhancing an organization's overall security posture [5]. Rather than providing technical detail, it serves as a best practice framework that can be adapted to specific educational needs.
The options presented here offer only a preview of the border cybersecurity framework ecosystem. However, they are some of the most common options currently in use by educational institutions that have reached a high level of cyber maturity [19]. They also provide broad name recognition and there are ample open-source and private/consultancy-based resources for implementation guidance for each.

10.3 Ransomware: To pay or not to pay?

Ransomware is an attack on a system in which malicious actors use malware to encrypt your data and hold it for ransom. Notably one of the most prevalent attacks facing users today, ransomware has also become a significant threat to education institutions. Through discussions with cyber experts and technical managers, the authors learned education institutions are targets for such attacks due to a lack of security measures in place, the sensitive nature of the information stolen, and the expectation that schools will likely pay to retrieve the data that was not sufficiently backed up. Regardless of the reason why one major issue that accompanies ransomware attacks is the question of whether or not to pay the ransom.
With an average ransom of about $140,000 and an average system downtime of roughly 23 days, the costs can add up quickly, especially for an institution that may have limited resources [21]. Although the ostensible solution may be to simply pay, the consensus among cybersecurity experts and industry professionals is *not* to pay. Payment does not guarantee full recovery and only 11% of schools that eventually paid their ransom saw a total restoration of data [1].
Considering this, the Federal Bureau of Investigation (FBI) also advises against paying the ransom and illustrates alternative response procedures in their guide, *How to Protect Your Networks from Ransomware* [22]. Furthermore, Jim Routh, ICIT Fellow and Chief Security Advisor for Virsec Systems, agrees that victims should never pay in the event of a ransomware attack, citing that prevention is the best response and organizations should invest in protecting their data recovery capabilities first [60].
It is worth mentioning that some organizations may not have the financial resources to implement sophisticated protection and security measures. However, Routh highlights that organizations should consider the cost of implementation of data recovery resilience versus the cost of ransom payments. Likewise, the FBI informs that "proactive prevention is the best defense" against ransomware [22]. With that, it is recommended that organizations invest as much as possible (and appropriate) in prevention instead of resorting to paying the ransom. In the long run, the upfront cost of prevention will likely be lower than that of any ransom payment and associated response costs.

10.4 Current Trends

10.4.1 Cloud Migration

Cloud migration involves moving most, if not all, local resources to a larger company that hosts data centers around the world. Some examples of Big Tech companies that offer cloud solutions are Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and VMware. The author's opinion is that migration to the cloud is not a matter of "if", but rather "when". The COVID-19 pandemic had a large impact on organizations across multiple sectors, however, it is reasonable to say that education institutions, both K-12 and Higher Education, felt this shift more than others [56]. At the drop of a dime, education systems had to scramble to accommodate remote work by both students and employees. Courses had to be modified to work alongside this sudden transformation.
For bigger, well-funded Universities, this accommodation was likely easier compared to small colleges and K-12 school districts. Many organizations in the education sector have small IT teams that often have help from students with varying degrees of experience, managing large systems. For those organizations, this adoption of online learning was incredibly difficult and often left large gaps in security. Another issue arises when core functions of a school or university such as student

records, housing, meal plans, human resources, finances, etc. are kept locally using legacy systems [56]. There can be specific details that are integrated and tailored to a given company that can make version upgrades rather difficult. Thoughts of cloud migration can often be daunting. It is important to make the transition well-thought-out over a period of time in addition to understanding the solution cost versus the staying cost. Stony Brook University is one example of how this strategic process worked well in the end. Their cloud migration took roughly five years but resulted in around $1 million in savings for the school over that time frame [56].
Other organizations such as Carnegie Mellon University, Northwestern University, University of California, Berkeley, Winnipeg School Division, and others have made the change to incorporate cloud solutions within their IT infrastructure.
A decade ago, this would have seemed impractical to do. Now, with the number of options, it is up to each organization to conduct their own research and find what is right for them. Given the lack of funding, lack of expertise, overhead needed to run local data centers, and the number of threats against K-12 and Universities, it may be time for these organizations to take a serious look at migrating some or all of their IT environment to the cloud.

10.4.2 Zero Trust

The digital transformation accelerated by the pandemic has changed the way organizations deal with data. It has also fundamentally changed the information distribution channels for educational institutions. Moving to a hybrid, cloud-based architecture makes it likely that an organization's resources are increasingly distributed over multiple IT environments. Each environment has varying levels of visibility and security. Having your data distributed over several different systems greatly increases the attack surface by introducing a host of risks and threats.
Zero Trust is the term for an evolving set of cybersecurity paradigms that transition cyber defenses from static, network-based parameters to more dynamic relationships between users, assets, and resources. The Zero Trust Architecture (ZTA) assumes no implicit trust granted to users based solely on their assigned roles, physical or network locations [59]. This security framework requires all users, internal and external, to be authenticated, authorized, and continuously validated in order to be granted access to applications, resources, and data [55]. The three core principles of ZTA are implementing least privileged access, assuming a breach has already occurred, and never trusting and always verifying an entity [65]. Switching to a ZTA requires significant resources in terms of capital and know-how.The costs to implement and maintain this architecture, along with the costs to train personnel can be out of reach for some institutions, especially if transitioning from legacy systems. On the other hand, implementing ZTA may save an organization over 40% on data breach costs according to some studies [63]Even partially implemented ZTA's have been shown to be effective in reducing breach-related costs.
Thus, in the short term, ZTA may be easier for larger, better-funded universities to transition to. However, most institutions should gradually make this transition to better secure their overall cybersecurity posture and make their organizations more resilient to emerging threats. The NIST SP 800-207 Zero Trust Architecture is a comprehensive, vendor-neutral lays the foundations for a Zero Trust Architecture and is meant to serve as a guide to understanding its principles. This standard ensures consistency in recommended defenses against modern attacks that most organizations should follow to achieve success [59].

10.5 Security as an Investment: Financial Considerations

One major question when any change is proposed to the norm is, "Can we afford this?". This is no different in the case of education and cybersecurity. Many schools, both at the K-12 and Higher Education levels, are concerned about budgets and how far they can be stretched. During discussions with Jim Routh, he noted the importance of financial support when it comes to education: Schools have assets, and you need money to support those assets [60]. With the increase of technology in the classroom and the interdependencies that technology supports, like security systems and even general business functions like payroll and human resources management, cybersecurity is a non-negotiable [60]. The more devices and attack surfaces brought into the classroom, the more attack types a malicious actor can leverage. Investment in controls, like a lock, is necessary.
This is especially important when considering the in-

crease of cyber-threats looking for financial gain, as is the case with ransomware. Schools are being used as pawns for economic warfare, and they are typically not the end target, but rather a launching pad for the "big fish". Bill Moss highlighted this when he mentioned the most valuable information, specifically within Higher Education would be health records [8]. With most states requiring college students to have health insurance coverage, and many of them covered via university-partnered plans, some interdependencies stretch far beyond grades and GPA scores. Specifically in Pittsburgh, Carnegie Mellon University has a partnership with Highmark Health, the company that offers student coverage. Furthermore, Highmark Health has a contracted partnership with the University of Pittsburgh Medical Center, a 40-hospital organization that serves as the largest non-governmental employer in the state of Pennsylvania [26]. With this vast web of interdependencies, the protection of these assets is a glaring necessity. And because of this, the need to seal each loose thread becomes increasingly important.

Investing upfront in cybersecurity allows for less cost needed over time, especially when looking at the cost of recovery from an incident. *Educational institutions have the highest cost of recovery when it comes to ransomware attacks, about 48% higher than the global average across a variety of industries* [1]. Because of this, cybersecurity must be accounted for in the total IT budgeting for schools, rather than as an add-on or afterthought down the line (usually post-incident). Budgeting for cybersecurity can add up, especially when factoring in the cost of labor and expertise in addition to various tools and systems. However, there are more reasonable investments that off-load some of the responsibilities onto a third-party vendor, like with cloud security solutions. Furthermore, there are also opportunities to centralize security, especially for K-12 schools. School districts have the ability to bundle technology devices and security services to ensure devices are managed safely and securely [4].

The goal of investing in cybersecurity is to ultimately receive a return on investment (ROI), but not in the traditional sense. ROI is typically interpreted as the point at which an investment becomes profitable. In this sense, ROI can be interpreted as the point at which an investment in security prevents a future incident from occurring, ultimately reducing any future losses or costs. The "return" for security is softening the blow, or preventing it entirely, when it comes to security incidents. Essentially, paying up now so you will not have to pay up even more in the future. That is not to say that investing in security has a 100% guarantee that incidents will not occur, but rather that when they do occur then the sting will not be as devastating.

10.6 Security Operations Center Concept

The next recommendation is a concept that is well-known in the security industry but its integration between K-12 and Higher Education has never come to fruition - a localized Security Operations Center (SOC). The logistics behind this is for Government agencies and Higher Education institutions to help K-12 districts become more resilient against cyber threats. After speaking with many experts in the security industry, there was a common theme centered around K-12's lesser ability to adequately protect themselves against the threats and attack vectors that have been articulated above. This localized SOC could be a partnership between the Government, a sponsoring University, and any number of K-12 schools deemed appropriate. This is not to suggest that IT professionals already working for school districts would simply lose their jobs. The SOCs would need experienced IT professionals to run, monitor, and teach willing students the path to being successful and knowledgeable members of the security community. University students with interest in security and some IT experience could serve as mentors to high school students that join them in working for the SOC. Appendix 4 illustrates this idea in more detail.

However, there are some difficulties with this idea. Primarily, this would take a large commitment from the Government, Universities, and K-12 schools to strategically plan, create, and operate these SOCs. Once created, it would not be overwhelmingly difficult to set up sensors in several locations throughout different school locations. Due to advanced cloud solutions (See subsection 'Cloud Migration' within 'Recommendations' section), there are a number of services that would make this transition easier. It is unlikely that this would require a complete overhaul of current data centers, but rather a small integration of a given service that moves security monitoring to the SOC and alleviates some pressure on IT managers of a given district. Another issue could be student retention. How would these SOCs motivate and keep students post-graduation? This would need to be

incentive-based, similar to the Scholarship for Service, that would guarantee college students a job immediately upon graduation and high school students admission to the University who sponsored their respective SOC. This type of incentive and partnership would help Universities gain students, help the Government maintain their public workforce, and most importantly improve the security and resiliency of K-12 school districts. Discussing with experts in the field, they believe some partnership and incentive is needed for this idea to be successful and sustainable.

11 Education as a Critical Infrastructure Sector

It is important to note that education does currently fall under the Government Facilities Critical Infrastructure Sector (CIS). However, education does not exist as a standalone CIS. There are both pros and cons to introducing education as a CIS.

Classifying education as a CIS opens the potential for increased federal funding and more government aid to institutions. These funds could be used to help strengthen the shift towards remote and cloud-based education while also strengthening the security posture of many institutions. This funding could be especially beneficial to smaller institutes with limited resources. However, others like Katrin Hillner, President and CEO of PC Network, point out that existing Critical Infrastructure sectors require more funding than they already receive [27]. Classifying education as a CIS would further strain the federal budget and prevent some sectors, like Healthcare and Public Health, Food and Agriculture, or Energy, from receiving the additional funding required.

Some experts, such as Bill Moss from Infoblox, believe that education should be treated as a long-term strategy for development [8]. They believe that this change is necessary as education is critical and has many interdependencies with other critical sectors. Itzik Kotler, co-founder & CTO at SafeBreach, claims that classifying education as a Critical Infrastructure Sector will bring about a certain level of standardization that is currently missing [10]. This could ensure a minimum security threshold for all institutions making them more secure. Jim Routh, Chief Security Advisor at Virsec Systems states intellectual property is a critical asset for the US which could be targeted by adversaries from China and Russia. However, he claims that targeting Educational Institutes could be counterproductive for these attack groups as they would hinder the progress of students from their countries studying in the US. On the whole, Jim argued that most attacks on education are for financial gain and are not on par with attacks on other CIS [60]. Other experts concur; Katrin Hillner also stated that many cybercriminal bodies specifically target Critical Infrastructure Sectors. She believes that classifying education as a CIS would draw further attention to this sector from such criminal bodies and APTs [27]. The move could thus prove counterproductive and cause more harm than benefit to the education industry as a whole.Classifying Education as a CIS could be beneficial but it could also end up doing more harm than good. While the consensus remains split, most experts we interviewed were of the opinion that education should not be categorized as a Critical Infrastructure Sector.

12 Future Work

The research into the overall state of cybersecurity and associated risks in education institutions has raised as many questions as it has answered. One of the biggest drivers in this regard is that many of the situations in this context are different with varied resources and needs. Each educational institution is unique and trying to assess them as a single entity is extremely difficult.

However, there are approaches to cybersecurity and risk management that schools can use to strengthen their resiliency and ensure the protection of students and staff in the digital space. Available frameworks and security services offer a plethora of tools for these organizations to implement, but there is still much room to grow. Specifically, many of these tools, technologies, and strategies are not widely known and/or are difficult to understand. Therefore, further research and categorization of what is available should be considered. The following outlines areas that could further expand upon the research and thoughts provided in this paper.

Educational Risk Management

The authors have briefly touched upon risk assessment and asset management for educational institutions, but these have been discussed at a high level and merit further consideration. It is clear that risk management is

a necessary tool in effectively addressing cybersecurity risk, but it is unclear what (if any) is currently being done in most schools with regard to risk and asset management. A deeper understanding of how schools address and identify risk would be necessary to further develop the ideas and recommendations that the authors have presented here. Cursory searches identified some risk registers and appetite statements, however, these were significantly different in their approach and many schools ostensibly have no such program in place. Additionally, it would also merit further research into how schools identify, classify, and manage their asset inventory.

Centralized Security Operations Centers

As previously mentioned, the idea of centralized security operation centers (SOC) is for one location to manage cybersecurity for multiple institutions and has been brought up in discussions with industry experts. Dr. Bruce Young, a cybersecurity professor at Harrisburg University and Governance Risk and Compliance (GRC) Practice Lead at PC Network, noted that some organizations have already been further developing this idea. Dr. Young illustrated that specialized security sensors could be integrated into school systems, which then report back to a centralized SOC [69]. However, he noted that such programs would require personnel with specialized experience to establish and monitor the sensors. Schools (specifically K-12) often lack the resources and expertise needed to implement and maintain effective cybersecurity programs, so this concept may be a viable solution that provides appropriate services. However, further research into the idea and how it could potentially be funded would require additional research.

The Educational Perspective on Cybersecurity

Though schools stand to benefit from this paper and the ideas expressed within, a deeper understanding of an education institution's perspective on cybersecurity and associated risks would further develop this project. To provide a comprehensive list of feasible solutions and approaches to addressing cybersecurity, it would be necessary to speak with institutions at all levels and sizes to better understand their views, objectives, and thoughts on this research and subsequent recommendations. Notably, the authors had a rather difficult time connecting with any such institutions. With that, communicating these ideas and learning more from schools themselves would only serve to benefit this research.

Education as a Critical Infrastructure Sector of its Own

One of the secondary focuses of this paper has been to assess whether Education should be considered a Critical Infrastructure Sector in the U.S. (alongside Transportation, Energy, Healthcare, etc.). The authors had the opportunity to ask cyber experts their thoughts on this with varied responses. However, no governmental organizations and only one school was able to weigh in their perspective. Potential future work in this regard would be to meet with government organizations to obtain their opinion and should also include speaking with more schools to assess this idea from an educational and administrative perspective.

Bringing Cyber Experience to Education

Through research and interviews with cyber and education experts, it is evident that, when compared to other industries, there is a dearth of cybersecurity expertise in educational institutions. This is due to a list of factors that include a lack of resources, funding restraints, or the fact that many cybersecurity experts navigate to positions within the tech or defense industries. Considering this, what could education institutions do to bring in more cyber expertise? Perhaps more can be done to incentivize cyber experts to fill these jobs? Any future work that builds upon this paper could dive deeper into these questions.

13 Lessons Learned

Reflecting on the project holistically, the team benefitted from maintaining a solid schedule that laid out specific goals and deadlines for milestones, in addition to open lines of communication with each other and the team's faculty advisor and sponsor. In terms of communication with the faculty advisor, the team had weekly meetings with the appointed faculty advisor to provide status updates on the progress of the project in addition to identifying any areas in which he could provide additional support. The team's project manager also kept in constant contact with the team's advisor, sending weekly status reports in order to provide a written record of progress. From the perspective of ICIT, our sponsors, the project

manager facilitated communication as needed. This prioritization of communication was crucial for the success of the project, especially given the need to manage several different schedules and unrelated responsibilities.
When it comes to difficulties the team faced in executing the project, there are several which may have at times hindered the team from receiving real-world expertise. The team specifically found it difficult to hear from potential victims of cyberattacks. Several leads ended up going nowhere, possibly due to an educational institution's own policies or simply a preference not to speak on cyber incidents that have occurred, regardless of the positive impact such information could provide.
Through the progression of the project, the team recognized several things regarding the topic area and scope that are also worth noting:

- Cyber hygiene is an important element of cybersecurity, but culture, awareness, and training are most critical. Without a security-positive attitude in place, controls will not have their intended effect.
- Many schools are underfunded when it comes to IT and cybersecurity resources, but funding is not the only reason security is not improved. There is also a significant lack of expertise, as many institutions, specifically K-12, only have 1-2 people managing their entire network and IT infrastructure.
- Compared to everything else school's already must deal with, cybersecurity sometimes falls by the wayside.
- The prioritization of cybersecurity in education remains a rapidly developing area of research, especially with the K-12 Cybersecurity Act. This fact provides some level of hope that while security is not where it needs to be, it is improving.

14 Conclusion

As a result of a rapidly changing world, impacted by developing technologies and the COVID-19 pandemic, education systems in the United States have seen a rising number of attacks. The resultant shift in remote learning has broadened a large number of existing attack vectors and weak points (legacy systems, underfunded schools, and lack of security professionals) within K-12 school corporations and Universities. As documented above, there are a large number of APTs and Cybercriminals looking to exploit these weaknesses and extort the organizations, which could be detrimental to their function. The education system needs more resources to broaden their security coverage Whether it is through adding education as its own Critical Infrastructure Sector, moving resources to the cloud, increasing federal funding, or a combination of a number of things, the overall security posture needs to be put first and foremost. Education in America is the rockbed upon which other industries lie. Should educational systems become the main focus of adversaries, it could have a rippling effect on all other sectors. By further examining the people, policies, and technologies which facilitate education, definitive improvement can be made.

Appendices

15 Appendix 1: Example Risk Appetite Statements

Example Risk Appetite for a Private 4 year University

Priority 1: Safety and Security of Students and Staff			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Information Security	Impact to protection of student and staff information.	Medium	**Mitigate** through proper security controls and policies.
	Impact to secure back-up services of individual and institutional data.	Medium	**Mitigate** through proper security controls and policies.
Cybersecurity	Impact to the student's online learning experience - virtual lectures, assignments, and/or virtual classroom platforms.	Low	**Mitigate** through proper security controls and policies.
	Impacts to school networks - school system configurations.	Low	**Transfer** services to a third-party via cloud solutions.
Physical Security	Impact to the physical learning and teaching environment - classroom and building safety and security.	Low	**Mitigate** through institutional security personnel, procedures, and controls.
Priority 2: Education and Instruction			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Education and Instruction	Impact to student's ability to learn and grow in the classroom.	Medium	**Accept** because not all risks can be mitigated or transferred in this context.
	Impact to the institution's ability to provide effective instruction.	Medium	**Accept** because not all risks can be mitigated or transferred in this context.

Priority 3: Compliance			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Compliance	Impact to remaining compliant with any local, state, or federal regulation.	Medium	**Mitigate** through routine audits of institutional processes and practices.
Priority 4: Financial			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Learning Continuity	Impact to the institution's ability to provide effect and continuous education and instruction.	Medium	**Mitigate** through budgeting and additional funding as needed.
Staff Compensation	Impact to the institution's ability to provide compensation to faculty and staff.	Low	**Mitigate** through budgeting and prioritization of funds.
Additional Services	Impact to the institution's ability to provide additional services outside of the learning environment - extracurriculars, sports, clubs, etc.	High	**Accept** because these services are non-critical to student learning. Although important to student growth and development outside the classroom, they are not the main focus of the institution.
Priority 5: Reputational			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Student Experience	Impact to student learning inside the classroom.	Low	**Mitigate** through effective contingency planning and prioritization of education and student learning objectives.
	Impact to student experience and life on campus.	High	**Accept** because some scenarios (i.e., the pandemic) limit campus activity and options for students outside the classroom.
Mission and Values	Impact to the institution's culture or core values.	Medium	**Mitigate** through a culture that highlights the school's mission and values.

Example Risk Appetite for a Public Elementary School

Priority 1: Safety of Students and Staff			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Information Security	Impact to protect information of students, staff, faculty, and administration.	Medium	**Mitigate** through proper security controls and policies.
	Impact to secure back-up services of individual and institutional data.	Medium	**Mitigate** through proper security controls and policies.
Cybersecurity	Impact to the student's in-person learning experience - inability for teacher' to deliver curriculum, failure of technology, etc.	Low	**Mitigate** through proper security controls and policies.
	Impact to the student's online learning experience - virtual class delivery platforms, assignment submissions, and/or virtual classroom platforms.	Low	**Mitigate** through proper security controls and policies.
	Impact of inappropriate use of IT by students, staff, faculty, and/or administration.	Medium	**Mitigate** through proper security controls and policies.
	Impacts to school networks - school system configurations.	Low	**Transfer** services to a third-party via cloud solutions.
Physical Security	Impact to the physical learning and teaching environment - classroom and building safety and security.	Low	**Mitigate** through institutional security personnel, procedures, and controls in addition to local law enforcement suggested best practices.
	Impact to the physical well being of student, faculty, staff, or administration (illness, injury, mental health, school lunch program, etc.).	Low	**Mitigate** through institutional security personnel, procedures, and controls in addition to local law enforcement suggested best practices.
Priority 2: Quality of Education and Learning Instruction			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Education and Instruction	Impact to student's ability to learn and grow in the classroom.	Low	**Mitigate** through proper learning continuity plans.
	Impact to the institution's ability to provide effective instruction.	Low	**Mitigate** through proper learning continuity plans.
	Impact to the delivery of special programs (tutoring, counseling, after school care, etc.)	Medium	**Mitigate** through proper learning continuity plans.

Priority 3: Compliance			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Compliance	Impact to remaining compliant with any local, state, or federal regulation.	Medium	**Mitigate** through routine audits of institutional processes and practices.
Priority 4: Financial			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Learning Continuity	Impact to the institution's ability to provide effective and continuous education and instruction.	Medium	**Mitigate** through budgeting and additional funding as needed.
Staff Compensation	Impact to the institution's ability to provide compensation to faculty and staff.	Low	**Mitigate** through budgeting and prioritization of funds.
Student Development	Impact to the institution's ability to provide goods and services to support the development of student's well-being and academic career (breakfast clubs, field trips, volunteer opportunities, etc.)	High	**Accept** because these services are non-critical to student learning. Although important to student growth and development outside the classroom, they are not the main focus of the institution.
Additional Services	Impact to the institution's ability to provide additional services outside of the learning environment - extracurriculars, sports, clubs, etc.	High	**Accept** because these services are non-critical to student learning. Although important to student growth and development outside the classroom, they are not the main focus of the institution.
Priority 5: Reputational			
Risk Category	**Risk Event**	**Appetite**	**Strategy**
Student Experience	Impact to student learning inside the classroom.	Low	**Mitigate** through effective contingency planning and prioritization of education and student learning objectives.
Mission and Values	Impact to the institution's culture or core values.	Medium	**Mitigate** through a culture that highlights the school's mission and values.

16 Appendix 2: PYSA Malware [45]

Tor URLs:
Pysa2bitc5ldeyfak4seeruqymqs4s-
j5wt5qkcq7aoyg4h2acqieywad.onion
Na47pldl5eoqxt42.onion
Indicators of Compromise:
.pysa file extension
SHA1 Hashes:

- 07cb2a3fe86414b054e2b002f283935bb0cb993c
- 52b2fc13ec0dbf8a0250c066cd3486b635a27827
- 728CB56F98EDBADA697FE66FBF7D367215271F10
- C74378a93806628b62276195f9657487310a96fd
- 24c592ad9b21df380cb4f39a85d4375b6a8a6175
- F2dda8720a5549d4666269b8ca9d629ea8b76bdf
- 6d390038003c298c7ab8f2cbe35a50b07e096554
- ffa28db79daca3b93a283ce2a6ff24791956a
768cb5fc791c075b638416b51f4
- 7e50f6e752b1335cbb4afe5aee93e317
- f69a4f9407f0aebf25576a4c9baa609cb35683d1
- 022f80d65608a6af3eb500f4b60674d2c59b1
1322a3f87dcbb8582ce34c39b99
- 58b39bb94660958b6180588109c34f51
- 7d21c1fb16f819c7a15e7a3343efb65f7ad76d85
- 88e344977bf6451e15fe202d65471a5f75
d22370050fe6ba4dfa2c2d0fae7828

Table 1: Aliases Associated with PYSA Malware

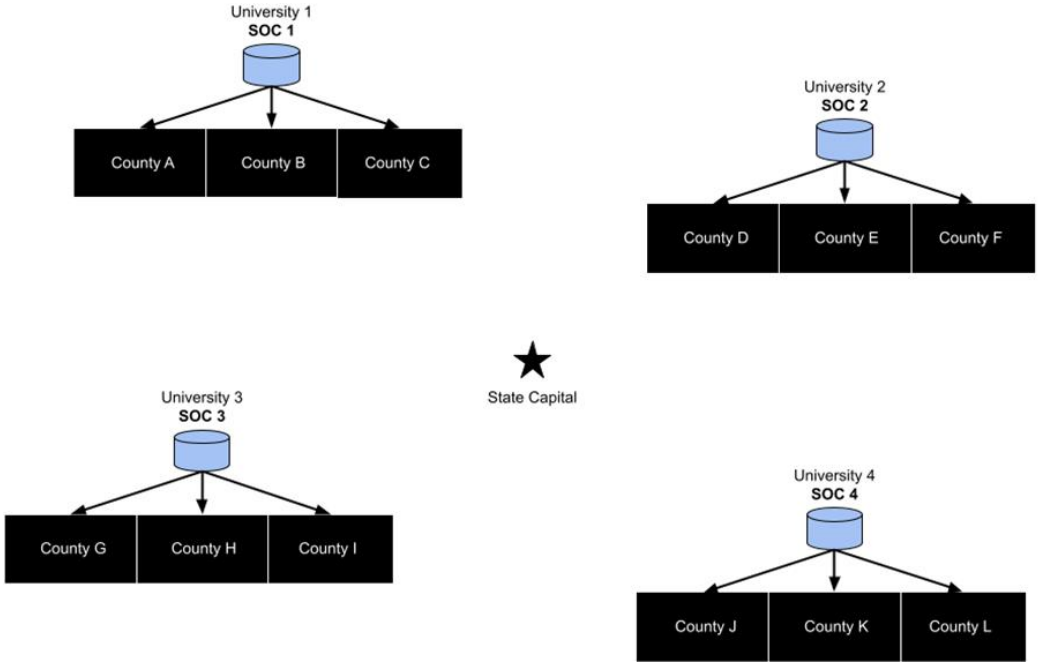
ced_ririele93@protonmail.com	veronabello@onionmail.org
irvingalfie@protonmail.com	giuliacabello@onionmail.org
gustaf.wixon@protonmail.com	avitacabrera@protonmail.com
ralfgriffin@protonmail.com	domenikuvoker@protonmail.com
korgy.torky@protonmail.com	mespinoza980@protonmail.com
masonhoyt@onionmail.org	izak.pollington@protonmail.com
willmottlem01@protonmail.com	Jamesy.kettlewell@protonmail.com
BettyRacine@protonmail.com	jarret.wharram@protonmail.com
Ohsgsuywb@protonmail.com	domenikuvoker@protonmail.com
Lojdgseywu@protonmail.copm	hewitt_rogers@protonmail.com
thorvald_beattie@protonmail.com	Johnbeamvv@protonmail.com
warden_riddoch@protonmail.com	rewhgsch@protonmail.com
cowland_lothaire@protonmail.com	lhdbeysdq@protonmail.com
merry.lane@mailfence.com	t_trstram@protonmail.com
astion11@protonmail.com	ellershaw.kiley@protonmail.com
PaulDade@onionmail.org	gareth.mckie3l@protonmail.com

17 Appendix 3: Gold Lowell, Boss Spider [66]

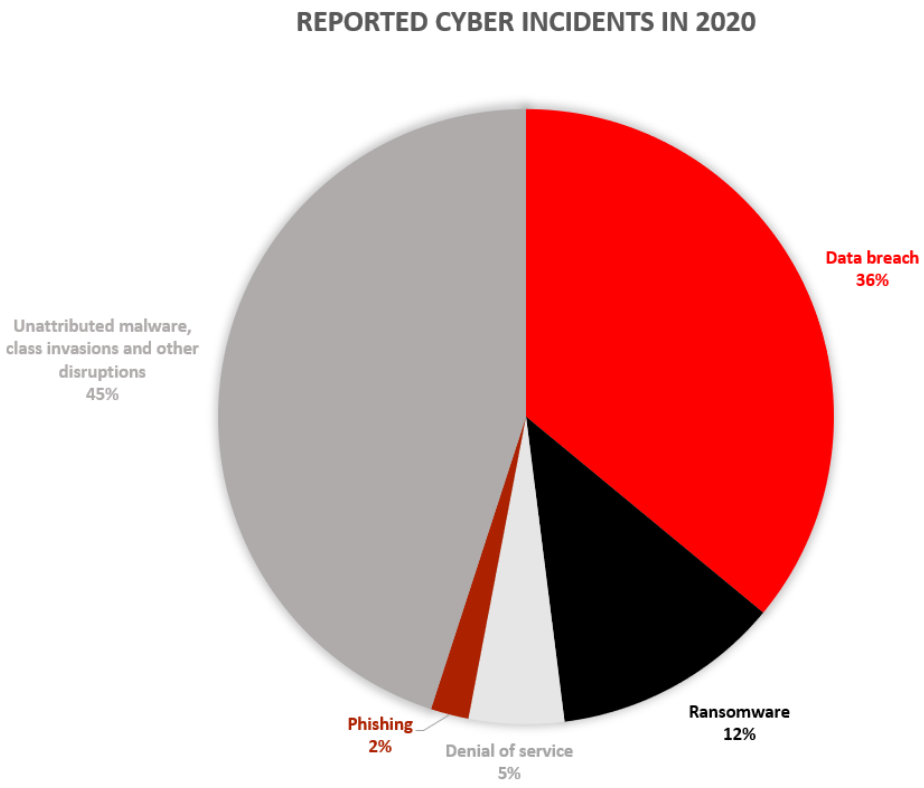
Files:
Nlbrute.exe
r45.exe
Hashes:

- 025c1c35c3198e6e3497d5dbf97ae81f

18 Appendix 4: SOC Example



19 Appendix 5: Cyber Incident Breakdown



References

[1] Sally Adam. The State of Ransomware in Education 2021, Jul 2021. https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/.

[2] Associated Press. ND Univ. system enlists FBI in help on Data Breach, Jul 2019. https://www.mprnews.org/story/2014/03/07/ndsu-enlists-fbi-in-help-on-data-breach-300000-affected.

[3] MITRE ATTACK. Dragonfly Cyber Espionage Group, May 2017. attack.mitre.org/groups/G0035/.

[4] Nadav Avni. Bundling Education Device Management for Schools, Dec 2021. https://districtadministration.com/bundling-education-device-management-for-schools/.

[5] Axelos. What is IT Service Management | ITIL, 2020. https://www.axelos.com/certifications/itil-service-management/what-is-it-service-management.

[6] Red Canary. 2021 Threat Detection Report, 2021. https://resource.redcanary.com/rs/003-YRU-314/images/2021-Threat-Detection-Report.pdf.

[7] CBCnews. University of Calgary paid $20K ransom to cyberattackers to Unlock Computer Systems, Jun 2016. https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979.

[8] Jordan Christian, Regan McGovern, Alexandra Rutkowski, Mackenzie Peterman, Saurabh Pethe, and Bill Moss. Interview with infoblox account manager bill moss, Mar 2022.

[9] Jordan Christian, Alexandra Rutkowski, Lexi McGovern, Mack Peterman, Saurabh Pethe, and Mary Ann Blair. CMU CISO Interview, Feb 2022.

[10] Jordan Christian, Alexandra Rutkowski, Regan McGovern, Mack Peterman, Saurabh Pethe, and Itzik Kotler. Interview with Itzik Kotler, Co-Founder & CTO at SafeBreach, Feb 2022.

[11] chum1ng0. MA: UMass Lowell closed due to cybersecurity incident, Jun 2021. https://www.databreaches.net/ma-umass-lowell-closed-due-to-cybersecurity-incident/.

[12] Catalin Cimpanu. Louisiana governor declares state emergency after local ransomware outbreak, Jul 2019. https://www.zdnet.com/article/louisiana-governor-declares-state-emergency-after-local-ransomware-outbreak/.

[13] Catalin Cimpanu. Over 500 US schools were hit by Ransomware in 2019, Oct 2019. https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/.

[14] Catalin Cimpanu. Michigan State University hit by ransomware gang, May 2020. https://www.zdnet.com/article/michigan-state-university-hit-by-ransomware-gang/.

[15] Ryan Cloutier. Interview with Ryan Cloutier - President, SecurityStudio, Mar 2022.

[16] Nathan Coppinger Nathan has always loved learning about cutting edge technology but didn't have the patience for coding. So. Netwalker Ransomware Guide: Everything you need to know, Nov 2020. https://www.varonis.com/blog/netwalker-ransomware.

[17] Crowdstrike. *2020 GLOBAL THREAT REPORT*. 2020.

[18] James David Dickson. Report: MSU Hackers release documents; school had refused to pay ransom, Jun 2020. https://www.detroitnews.com/story/news/local/michigan/2020/06/05/msu-hackers-release-documents-school-had-refused-pay-ransom/3153209001/.

[19] Educase and Higher Education Information Security Council (HEISC). Response to NIST RFI: "Developing a Framework to Improve Critical Infrastructure Cybersecurity", Jun 2017. https://www.nist.gov/system/files /documents/2017/06/06/040813$_e$*ducause.pdf*.

[20] Michael Elsen-Rooney. Data of 820,000 NYC students compromised in Hack of online grading system: Education dept., Mar

2022. https://www.nydailynews.com/new-york/education/ny-hack-illuminate-online-gradebook-compromised-personal-data-20220325-ahy3b3b3t5cjzajau63muqcniq-story.html?mod=djemCybersecruityPro&tpl=cy, journal=nydailynews.com.

[21] Liz Farmer. Cyberattacks keep targeting colleges. How can they protect themselves?, Nov 2021. dive.com/news/cyberattacks-keep-targeting-colleges-how-can-they-protect-themselves.

[22] FBI. Ransomware prevention and response for Cisos, Jul 2016. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

[23] Jacey Fortin. Student charged in cyberattacks at Miami-Dade Schools, Sep 2020. https://www.nytimes.com/2020/09/03/us/miami-dade-school-cyberattack.html.

[24] Jonathan Greig. Texas, California, New York, Louisiana, Missouri lead list of states with most ransomware attacks on schools: Report, Aug 2021. https://www.zdnet.com/article/texas-california-new-york-and-louisiana-missouri-lead-list-of-states-with-most-ransomware-attacks-on-schools-report/.

[25] Jonathan Greig. Ransomware: 2,300+ local governments, schools, healthcare providers impacted in 2021, Jan 2022. https://www.zdnet.com/article/2300-local-governments-schools-healthcare-providers-impacted-by-ransomware-in-2021/.

[26] Highmark Answers. Highmark and UPMC agreement. https://faqs.discoverhighmark.com/answers/highmark-and-upmc-agreement/.

[27] Katrin Hillner. Interview with Katrin Hillner - President and CEO of PC Network Inc., Mar 2022.

[28] Kyaw Pyiyt Htet. APT41, Sep 2019. https://attack.mitre.org/groups/G0096/, journal=APT41, WICKED PANDA, Group G0096 | MITRE ATT&CK.

[29] Pete Koczera. On the money: A look at it leaders' budget concerns, May 2021. https://edtechmagazine.com/k12/article/2020/06/money-look-it-leaders-budget-concerns.

[30] Eric Levenson. SAT will soon be all-digital and shortened from 3 hours to 2, Jan 2022. https://www.cnn.com/2022/01/25/us/sat-test-digital/index.html.

[31] Douglas A. Levin. The State of K12 Cybersecurity: 2020 Year in Review, 2021. https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf.

[32] Douglas A. Levin. The State of K-12 Cybersecurity: Year in Review, 2022. https://static1.squarespace.com/static/StateofK12Cybersecurity2022.pdf.

[33] Mezo. Vice Society Ransomware, Aug 2021. https://www.enigmasoftware.com/vicesocietyransomware-removal/.

[34] Trend Micro. U.S. Justice Department Charges APT41 Hackers Over Global Cyberattacks, Sep 2020. https://www.trendmicro.com/en_us/research/20/i/u-s–justice-department-charges-apt41-hackers-over-global-cyberattacks.html.

[35] Microsoft. Cyberthreats, viruses, and malware - microsoft security intelligence. https://www.microsoft.com/en-us/wdsi/threats.

[36] Marisa Midler, Kyle O'Meara, and Alexandra Parisi. Current Ransomware Threats: Carnegie Mellon University, May 2020. https://resources.sei.cmu.edu/assetfiles/WhitePaper/2020_019_001_645034.pdf.

[37] MITRE. Mitre ATT&CK, 2022. https://attack.mitre.org/, journal=MITRE ATT&CK.

[38] Steve Morgan. Cybercrime to cost the world $10.5 trillion annually by 2025, Nov 2020.

[39] Phil Muncaster. Organizations now have an average 76 security tools to man-

age, Dec 2021. https://www.infosecurity-magazine.com/news/organizations-76-security-tools/.

[40] Elissa Nadworny. More than 1 million fewer students are in college: Here's how that impacts the economy, Jan 2022. https://www.npr.org/2022/01/13/1072529477/more-than-1-million-fewer-students-are-in-college-the-lowest-enrollment-numbers-.

[41] NIST Joint Task Force. Security and Privacy Controls for Information Systems and Organizations, Sep 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[42] Noimos Group. What is Samsam Ransomware?, 2019. https://www.nomios.com/resources/what-is-samsam-ransomware/.

[43] US Department of Education. What is the Protection of Pupil Rights Amendment (PPRA)?, 2020. https://studentprivacy.ed.gov/faq/what-protection-pupil-rights-amendment-ppra.

[44] US Department of Education. Family Educational Rights and Privacy Act (FERPA), Aug 2021. https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[45] Federal Bureau of Investigation Cyber Division. Increase in PYSA Ransomware Targeting Education Institutions, Mar 2021. www.ic3.gov/Media/News/2021/210316.pdf.

[46] The Unites States Department of Justice. Department of Justice Launches Global Action Against NetWalker Ransomware, Jan 2021. https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.

[47] United States Department of Justice. Two Iranian men indicted for deploying ransomware to extort hospitals, municipalities, and public institutions, causing over 30 million in losses, Nov 2018. https://www.justice.gov/opa/pr/two-Iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[48] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[49] National Institute of Standards and Technology. Nist special publication 800-series general information, May 2018. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information.

[50] National Institute of Standards and Technology. NIST Special Publications 800 Series, 2022. https://pages.nist.gov/NIST-Tech-Pubs/SP800.html.

[51] Shivani Patel. Two Ventura County school districts affected by cyber attack Friday morning, Sep 2020. https://www.vcstar.com/story/news/2020/09/04/two-ventura-county-school-districts-affected-cyber-attack-internet-cybersecurity/5718588002/.

[52] Brandon Paykamian. Report: 'record-breaking' cyber attacks on schools in 2020, Mar 2021. https://www.govtech.com/policy/2020-marks-a-record-breaking-year-for-cyber-attacks-against-schools.html.

[53] Associated Press. Hackers Breach Customer Data at Michigan State Online Store, Aug 2020. https://www.detroitnews.com/story/news/local/michigan/2020/08/11/hackers-breach-customer-data-michigan-state-online-store/113014252/.

[54] Associated Press. A cyberattack in Albuquerque forces schools to cancel classes, Jan 2022. https://www.npr.org/2022/01/14/1072970219/cyber-attack-in-albuquerque-latest-to-target-public-schools.

[55] Kapil Raina. What is Zero Trust Security? Principles of the zero trust model, May 2021. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/.

[56] Arvind Rajan. Covid-19 accentuates the need for cloud migration in higher education, May 2021. https://www.govtech.com/sponsored/covid-19-accentuates-the-need-for-cloud-migration-in-higher-education.

[57] REMS. Cybersecurity Considerations for K-12 Schools and School Districts, 2017. https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.PDF.

[58] Peter Renals. Silverterrier: 2019 Nigerian business email compromise update, Mar 2020. https://unit42.paloaltonetworks.com/silverterrier-2019-update/.

[59] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero Trust Architecture, Aug 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final.

[60] Jim Routh. Interview with Jim Routh, Chief Security Advisor at Virsec, Mar 2022.

[61] K12 Six. The K12 Cyber Incident Map, 2022. https://www.k12six.org/map.

[62] Jeff Stone. California University pays $1 million ransom amid coronavirus research, Jul 2021. https://www.cyberscoop.com/ucsf-ransomware-payment-coronavirus/.

[63] Teramind. 5 stats that show the cost saving effect of Zero trust: Teramind blog, Sep 2021. https://www.teramind.co/blog/cost-saving-effect-of-zero-trust/.

[64] TrendMicro. Ransomware attack on university of calgary forces $20,000 payment, Jun 2016. https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/ransomware-attack-on-university-of-calgary-forces-20000-payment.

[65] John Turner. Zero Trust Architecture: 2022 comprehensive guide, Feb 2022.

[66] Secureworks Counter Threat Unit. Samsam ransomware campaigns, Feb 2018. https://www.secureworks.com/research/samsam-ransomware-campaigns, journal=Secureworks.

[67] United States Department of Justice. Seven international cyber defendants, including APT14 Actors, Charged, May 2019. https://www.justice.gov/opa/press-release/file/1317206/download.

[68] U.S. House. 117th Congress. PUBLIC LAW 117–47: K–12 Cybersecurity Act of 2021, Oct 2021. https://www.congress.gov/117/plaws/publ47/PLAW-117publ47.pdf.

[69] Bruce Young. Interview with Dr. Bruce Young - HU Professor and GRC Practice Lead at PC Network, Inc., Mar 2022.

[70] Samuel Zwickel. MSU: We won't pay hacker demanding ransom, threatening university over records, Jun 2020. https://www.freep.com/story/news/education/2020/06/03/michigan-state-hackers-ransom-breach-records/3134361001/.