INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD"
April 2021 (№17). Volume 7; Issue 2; Page No. 15-27
https://doi.org/10.36475/7.2.2
www.lawandworld.ge
ISSN: 2346-7916 (Print); ISSN: 2587-5043 (Online)

CYBER RISK MITIGATION IN HIGHER EDUCATION

George B. Liluashvili
Assistant Professor, MA in Criminal Justice, USA
Farmingdale State College, The State University of New York

ABSTRACT

The importance of having robust cybersecurity risk mitigation techniques in this rapidly evolving technological world cannot be overstated. Educational organizations hold an immense amount of personal data, and in the event of a data breach, it can cause serious damage to the organization. Similar to other organizations, educational organization data breaches occur in many forms, such as unauthorized access, ransomware, malware, physical theft, financial theft, or merely unintended disclosure of information. When higher education becomes the target of a cyberattack, the damage goes beyond the loss of personal identifiable information (PII) of faculty, staff, or students. According to the U.S. Department of Homeland Security, the cyberattack damage for higher education can include reputational, financial, and even national security, as some higher education installations work on defense research projects. The ability to safely connect to educational systems is an essential component of a supportive and safe learning environment. Cyberattacks are a constant threat for higher education institutions, especially after the COVID-19 pandemic shut down university campuses worldwide, forcing students, faculty, and staff to move online. With higher education shifting its operations online, both academic and IT systems face difficult challenges. The higher education entities need to have proper risk mitigation techniques, including defense strategies and effective security policies to safeguard the educational environment from data breaches and targeted cyberattacks. This article provides an overview of data breaches and risk mitigation techniques and strategies in higher education organizations.

KEYWORDS: Cybersecurity, Cyberattacks, Cyber Risk Mitigation, Data Breaches

INTRODUCTION

Cyberattacks on higher education institutions and effective threat mitigation strategies have not been fully explored and pose many unanswered questions. According to the news organization Comparitech, from 2005 to 2020, there have been 1,327 breaches in the educational system in the United States, including K-12 schools, colleges, and universities, and it is estimated that 24.5 million records have been stolen or compromised.[1] According to IBM's data breach calculations by the industry, it can cost around $140 to $260 on average per stolen record in the educational system.[2] This cost can reach billions of dollars; the exact costs can depend on the extent of a data breach, how much time it took to identify and contain the breach, compensating victims, and resolving lawsuits. Conducting proper research on cyberattacks and threat

1 Cook, S. (2020). US schools leaked 24.5 million records in 1,327 data breaches since 2005. Comparitech. Retrieved November 22, 2020, from https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/

2 IBM. (2020). How much would a data breach cost your business? Retrieved November 23, 2020, from https://www.ibm.com/security/data-breach

mitigation on higher education institutions is crucial as it has the potential to identify and isolate the factors that make higher education institutions more prone to cyberattacks.

Given the inevitable vulnerability and the seriousness of losses associated with cyberattacks in the Higher Education system, understanding the effective risk mitigation strategies, including managing and recovering from cyberattacks, can be essential and beneficial for higher educational institutions. The article explores: (1) Background of cyberattacks in higher education; (2) Cyber vulnerabilities in higher education institutions; (3) Cyber risk mitigation strategies in higher education; (4) Effective cyber risk mitigation framework for higher education.

BACKGROUND OF CYBERATTACKS IN HIGHER EDUCATION

Cybercriminals have extensively targeted higher education institutions for the past twenty years—the lack of cyber awareness, physical security, and cyber risk mitigation techniques resulted in several major data breaches. This paper will discuss only the most common cyber vulnerabilities in higher education institutions. One of the earliest known cyberattacks happened at the university in 1988, when the Cornell University graduate student Robert Morris while at MIT launched a computer worm, known as the Morris Worm, which replicated and spread rapidly. Morris wanted to demonstrate the weaknesses existing in security measures on computer networks. In 1989, Morris was the first person indicted for violating the Computer Fraud and Abuse Act (CFAA) and was sentenced to three years of probation. The Morris Worm was a wake-up call for the rapidly approaching digital age, and it inspired countless hackers to continue plaguing our digital systems to this day.[3]

In 2002, Princeton Ivy league University staff members gained unauthorized access to the Yale Universitas website and downloaded the list of prospective Yale students from the admissions database. Princeton university staff members used social security numbers and birthdates of Princeton applicants to apply to Yale University to access the system. Whether it was a result of ruthless competition between ivy league universities to boost student enrollment or calculated targeted espionage, it left the privacy of many (exact number unknown) prospective Yale and Princeton students compromised. The 2002 cyber-attack on Yale university is one of the first recorded cyberattacks in a higher educational institution. Ironically, the attack was conducted by another higher education institution.[4]

In 2003, California was the first state to pass a data breach notification law requiring companies to disclose personal information breaches to consumers whose personal information was compromised, including social security, driver's license, credit card number, and medical and health insurance information, passport numbers, and person's unique biometric information, such as a fingerprint, or image of a retina or iris.[5] In June 2005, after the indictment of a former library employee at the University of Hawaii by federal law officials, the university administration encouraged their students, faculty, staff, affiliates, and patrons to take protective measures against identity theft and obtain free credit reports to monitor their accounts for unusual activity. In 2003, the former librarian had access to the university's library patron database containing personal information, including social security numbers.[6] On March 11, 2005, from the Graduate Division office at the University of California, Berkeley, a laptop was stolen, which contained information on 98,369 individuals who applied to graduate school between fall 2001 and spring 2004. The computer's files included names, dates of birth, addresses, and Social Security numbers. The same year, a California university had another computer security breach when hackers broke into the housing and food service computer system, which contained vital information about 59,000 students, faculty, and staff. Boston College was also hacked in March 2005, and 120,000 alumni information was compromised, including names, addresses, and Social Security numbers.[7]

3 Vaughan-Nichols, S. (2018, November 2). The day computer security turned real: The Morris Worm turns 30. Retrieved November 23, 2020, from https://www.zdnet.com/article/the-day-computer-security-turned-real-the-morris-worm-turns-30/

4 Garroson, J. (2002, July 26). Yale Accuses Princeton in Hack Attack. Retrieved November 24, 2020, from https://www.latimes.com/archives/la-xpm-2002-jul-26-na-yale26-story.html

5 Attorney General Becerra and Assemblymember Levine Unveil Legislation to Strengthen Data Breach Notification Law. (2019, February 21). State of California Department of Justice. Retrieved November 24, 2020, from https://oag.ca.gov/news/press-releases/attorney-general-becerra-and-assemblymember-levine-unveil-legislation-strengthen

6 UH issues identity theft alert. (Jun 17, 2005). Retrieved November 24, 2020, from https://manoa.hawaii.edu/news/article.php?aId=1121

7 Gamio, L., Alcantara, C. (2017, September 7). How Data Breaches Grew to Massive Proportions in 12 Years. Retrieved November 23, 2020, https://www.washingtonpost.com/graphics/business/the-scale-of-large-hacks/

Oracle PeopleSoft human resource and financial management systems are extensively used in higher education and are implemented in more than 2000 universities and colleges worldwide. In 2007, three students installed keylogging software on computers at Florida Agricultural and Mechanical University and used the passwords to access the PeopleSoft system to modify grades and in-state residency status. In 2012, hackers broke into the PeopleSoft system at the University of Nebraska, exposing Social Security numbers and other sensitive information on about 654,000 students, alumni, and employees and bank account details of 21,000 individuals. The hacker, a former student, pleaded guilty to one count of intentionally damaging a protected computer. In 2013, Salem State University in Massachusetts notified 25,000 students and employees that their Social Security numbers were possibly compromised. PeopleSoft application architecture is complex and results in vulnerabilities in managing the system. It is difficult to patch the system without adding the custom functionality, and hackers can exploit the weaknesses and access the system. The perimeter security measures prevent employees from accessing harmful applications outside of the organizations but cannot prevent inadvertent privacy breaches and Organizations granting users inappropriate access rights. These threats are located within the organization and cannot be protected by perimeter security.[8]

The most extensive data breach in higher education institutions occurred in 2013 at Maricopa County Community College District (MCCCD) in Arizona. Data breach exposed 2.4 million records of current and former students, faculty, staff, and third-party members. Compromised records included names, dates of birth, addresses, social security numbers, and bank account information. It is suspected that student and faculty academic information, including grades and projects, have been exposed. The lawsuit filed against the MCCCD claims that before the 2013 cyber-attack, the FBI has repeatedly warned the MCCCD administration that several college databases have been compromised and information from these databases being offered for sale on the internet. After the data breach in 2013, it took MCCCD seven months and seven million dollars to notify the affected parties. The total cost of the 2013 data breaches as of 2019 is 14 million dollars.

Today's cybercriminals are often demanding ransom. In 2019, a cyberattack disabled Monroe College's technology systems. Hackers demanded $2 million in Bitcoin to restore access. In 2019, the Stevens Institute of Technology, Grinnell, Oberlin, and Hamilton Colleges were also targeted with ransomware attacks.[9] This year, the University of Utah experienced a ransomware attack at the College of Social and Behavioral Science network and decided to pay a $457,000 ransom to stop a hacker from disclosing stolen data.[10] Universities have the challenge to defend against multiple types of threats such as spam, phishing, and ransomware. Hackers target universities to retrieve sensitive information stored in their systems, including personal information, Social Security numbers, credit cards, and proprietary research data. The foreign actors often target scientific, medical, defense research, and academic work on public policy matters, nuclear issues, and economics. In 2018, nine Iranian hackers were charged for their attempt to steal the passwords of hundreds of thousands of professors in a phishing scam that ran from 2013 to 2017.[11] In 2019, Chinese hackers targeted 27 institutions and researchers with expertise in undersea technology in the U.S., Canada, and Southeast Asia, including Pennsylvania State University, the University of Hawaii, Duke University, the Massachusetts Institute of Technology, and the University of Washington. However, institutions did not confirm publicly if they have been compromised in the attacks. Research data can be vulnerable to cyberattacks because different department research repositories are often not managed by the office of information technology.[12]

8 McCoy, L. (2020, November 20). Why PeopleSoft System Security is Vital. Retrieved November 24, 2020, from https://www.sentinelsoftware.com/why-peoplesoft-system-security-is-vital

9 McKenzie, L. (2019, July 15). Hackers demand $2 million from Monroe College in ransomware attack. Retrieved November 27, 2020, from https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack

10 Olenick, D. & Ross, R. (August 21, 2020). University of Utah Pays Ransom to Avoid Data Disclosure. Retrieved November 19, 2020, from https://www.bankinfosecurity.com/university-utah-pays-ransom-to-avoid-data-disclosure-a-14871

11 Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps. (2018, March 23). Retrieved November 23, 2020, from https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

12 McKenzie, L. (2019, March 6). On Red Alert. Retrieved November 27, 2020, from http://www.insidehighered.com/news/2019/03/06/report-top-universities-us-targeted-chinese-hackers

CYBER VULNERABILITIES IN HIGHER EDUCATION INSTITUTIONS

At higher education institutions, chief information security officers are responsible for protecting, securing, and storing sensitive information, including financial aid applications with student personal information, proprietary research information, intellectual property, courses on online learning portals, and operational data. The higher education institutions are at risk for a variety of cyberattacks aimed at obtaining confidential information. It is advised that chief information security officers work closely with cybersecurity teams on the internal and external levels to prevent, protect, mitigate, respond to, and recover from different cyberattacks to the institution networks and systems. There are many different definitions of cyber vulnerabilities. After comparing several different cyber vulnerability definitions, a definition that covers most of the areas in cyber vulnerabilities and is most comprehensive to different types of the audience is by ISO 27005, which defines cyber vulnerability as: „Vulnerability is a weakness of an asset or group of assets that can be exploited by one or more threats, [where an] asset is anything that has value to the organization, its business operations, and their continuity, including information resources that support the organization's mission." Talabis states that this definition is readily applicable to various scenarios and recommends using it for governmental and civil environments.[13] The cyber vulnerabilities in the higher education system such as colleges and universities do not differ from other organizations; however, due to a large number of students and faculty who have limited or no security awareness can amplify the cyberthreat.

Ransomware encrypts computers by locking down files preventing the owner from accessing the content unless they pay and ransom for decryption. Ransomware is classified as an illegal money-making scheme embedded into files, emails, or many different types of contents, disguising itself as legitimate. The damage done by ransomware worldwide exceeds five billion dollars.[14] According to National Cyber Security Centre (NCSC) in the United Kingdom, Ransomware is one in the third place of the top five cybercrime issues in schools and universities across the United Kingdom, and because of the increased number of attacks in 2020, ransomware will be on the second place by the beginning of 2021 (NCSC 2020). As Moallem states, many higher education institutions are often forced to pay ransomware attacks because they cannot justify delaying or canceling educational activities. On June 1st, 2020, the Netwalker criminal gang attacked the University of California San Francisco (UCSF) using ransomware. Despite UCSFs IT staff's attempt to physically unplug the computers from the network and power, the malware spread through the systems paralyzing the medical research institution on COVID-19 research. BBC news reporter Joe Tidy anonymously witnessed the negotiations between cyber-criminal gang Netwalker and members of UCSF to relinquish the system control caused by the ransomware. According to Tidy, it cost UCSF 1.14 million dollars in ransom to regain control of the medical research institution systems and resume work on COVID-19 research.[15]

Distributed Denial of Service (DDoS) attacks common occurrences in colleges and universities across the world. The DDoS attack is a malicious attempt to disrupt a targeted computer (server), service, or the entire network by redirecting and flooding the internet traffic to the targeted system overwhelming the system, leaving it paralyzed. The DDoS Attacks can cost schools and universities up to $50,000 per attack. The damage from DDoS Attacks goes far beyond monetary, seriously affecting the educational institution's reputation. One of the most significant issues when it comes to DDoS attacks is that most students, faculty, and staff do not have basic IT awareness training and are powerless to stop the DDoS attack resulting in the loss of research-related work materials.[16] Between 2014 and 2016, Rodgers University in Newark, New Jersey, was subjected to Multiple DDoS attacks. DDoS attacks can cause devastation in an educational environment such as schools as universities. The DDoS attack on the Rutgers University system effectively shut down the central authentication server, paralyzing the getaway portal and online platform used by faculty, staff, and students to conduct discussions and submit assignments. Other affected systems included a Wi-Fi network, university email system, and

13 Talabis, M., Martin, J. (2012). Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis. Netherlands: Elsevier Science, pp. 1-2.

14 Morgan, S. (2017). Global Ransomware Damage Costs Predicted To Exceed $5 Billion in 2017. Retrieved November 27, 2020, from https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

15 Tidy, J. (2020). How hackers extorted $1.14m from University of California, San Francisco. Retrieved November 21, 2020, from https://www.bbc.com/news/technology-53214783

16 Moor, M. (2017). Cybersecurity Breaches and Issues Surrounding Online Threat Protection. United States: IGI Global, pp. 144-146.

library database. As a result of DDoS attacks, actual classes and exams had to be canceled. Besides physical damage, students filed lawsuits against Rogers University demanding tuition reimbursement and restitution for their compromised devices. According to Kremling and Park, a DDoS attack on Rutgers University cost around 8.6 million dollars in damages and led to the arrest of 22 years old Paras Jha, the architect of the famous Mirai Botnet. This malware can turn the networked devices into remote-controlled subjects, „Bots," and coursing the devices to attack designated targets. Even though the perpetrator was arrested, the damage done to Rutgers University was high, including the immeasurable loss to reputation and business that followed afterward.[17]

Phishing is categorized as one of the most common social engineering attacks directed to steal user data such as login information, credentials, including banking information such as credit card and account numbers. Webster dictionary defines phishing as a „scam by which an Internet user is tricked (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly." Phishing occurs when hackers disguise themselves as trusted entities and trick a victim into opening the email and clicking on a specific link. By clicking the link, the recipient allows the malware software to be installed and activated on a specific computer or device, resulting in the loss of personal or sensitive information. Phishing attack turns into ransomware attack locking the computer of an unsuspected recipient and hacker demanding the payment to release the system's control. From 2014 to 2019, phishing email attacks cost around 12 billion in damages to organizations worldwide.[18]

According to Twede and Marion, after analyzing 3.5 million spear-phishing attacks in 2020, it was discovered that more than 1,000 educational institutions, including schools and universities, fall victim to phishing attacks in the United States. Twede and Marion describe the two most common types of phishing attacks in educational instructions, Spear Phishing and Business Email Compromise attack. Spear Phishing is a type of attack directed at specific departments or individuals within the targeted organization. Business Email Compromise (BEC) is a type of attack when the attacker disguises itself as a trusted entity and attempts to obtain financial information such as organization or employee bank accounts, invoice information, or credit card information. Large scale BEC attack that occurred on December 2nd of 2018 at Cape Cod Community College (4Cs) in Barnstable, Massachusetts, fell victim to the phishing scam. The phishing scam was a large scale involving multiple departments and computer devices of faculty, staff, and students. The cybercriminals could access one of the computers in the Nickerson Administration Building and stole the information used to transfer $807,130 of school funds from the bank illegally. Only $278,887 was recovered after investigation. According to the digital forensic investigators, the entire scam was made possible by an unsuspected employee clicking what seems to be a harmless email attachment, causing the malware to be installed on the computer, compromising both the computer and personal information of dozens of employees. Like the 4Cs attack in 2019, hackers used phishing BEC attacks to gain access to Monroe College at New Rochelle, New York, locking down the computer systems in the cashiers' office, paralyzing the Monroe College New Rochelle campus financial transactions. Hackers demanded the 2 million dollars to release control of computer systems to Monroe college staff. Thankfully, the IT staff's quick thinking was able to isolate the incident, and the damage was minimal. However, according to Twede and Marion, it caused substantial chaos in the organization and barely avoided serious data Brach which would compromise the financial records of tens of thousands of Monroe College students, faculty, and staff.[19] One of the famous Direct-Access Attack cases is Aaron Swartz's case, one of the Reddit social news platform's principal founders. In 2010, Swartz was a visiting student at the Massachusetts Institute of Technology (MIT) and used his JSTOR digital library account to download „hundreds" of academic articles in PDF format and distribute them for free. Swartz gained direct access to the networking switch at one of the server rooms at MTI, creating the direct connection to his laptop computer, which he left hidden on-site, and initiated the download of academic articles. MIT Police arrested Swartz on breaking charges. Investigation in Swartz's case showed that the Direct-Access Attack on JSTOR overloaded its server, causing the university-wide outage of the JSTOR database.[20]

17 Kremling, J., Parker, A. M. S. (2017). Cyberspace, Cybersecurity, and Cybercrime. United States: SAGE Publications, pp. 143-163.

18 Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. United Kingdom: Wiley, p. 87.

19 Twede, J., Marion, N. E. (2020). Cybercrime: An Encyclopedia of Digital Crime. United States: ABC-CLIO. Retrieved November 20, 2020, pp. 126-133.

20 Lessig, L., Swartz, A. (2016). The Boy Who Could Change the World: The Writings of Aaron Swartz. United States: New Press, p. 26.

The Direct-Access Attack is a type of attack when a cybercriminal physically gains unauthorized access to the computer or network and performs various illicit functions, such as stealing the data by directly copying the information from the hard drive or install the malware to trace the user activities and intercept communications from the targeted computer. According to Convey, due to many untrained staff and employees, Direct-access attack is a common phenomenon in large organizations, including schools and universities. In an educational environment, Direct-access attack is not always a product of the criminal mind; it can be caused by the student's mischievous behavior, but the result is compromised data.[21]

CYBER RISK MITIGATION STRATEGIES IN HIGHER EDUCATION

Cyberattacks in higher education often occur not because the systems lack protection but because many institutions are large, complex, have different, sometimes outdated, operating systems and software, and users are accessing the network with their tablets or cell phone, making the implementation of security protocols difficult. Higher education institutions utilize different types of cyber risk mitigation methods, from software and hardware hardening to network access control, including traffic and intrusion detection systems.

The campus leadership has ultimate authority over cybersecurity strategy. Gearhart, Abbiatti, and Miller developed a survey administered to 150 college presidents to determine how senior college leaders are involved in cybersecurity. Study findings revealed that the leaders have significant concerns about the safety of the financial, student, faculty, and donor affairs data and that about half of the college leaders talk about cybersecurity-related issues 2-6 times per week. The president is often seen as an individual who delegates responsibility for the cybersecurity operations to the most appropriate individual on staff. The survey respondents strongly agreed that cybersecurity responsibilities should be assigned to the CIO position, who should be responsible within the campus structure for this work. The survey results demonstrated some ambivalence regarding when and how professional development training should occur. It was a moderate agreement to conduct online training sessions coordinated by professional associations to facilitate forward-thinking training programs that bring the campus leaders, faculty, and staff into the continued conversation of protecting sensitive data on the campus.[22]

There are some steps that institutions can take to make themselves safer. An entire institution should collaborate to protect it from cyberattacks. Academic research institutions contain valuable research data that must be safeguarded against hackers. To protect sensitive information, researchers must work in strategic partnership with technology administrators. Universities could create working groups, including department heads, researchers, and critical information security staff. It is essential to maintain a proactive approach to ensure that necessary security measures are implemented to protect sensitive personal information and proprietary research data. It is difficult for any institution to completely prevent a well-trained, funded, high-level group of attackers from gaining some level of access, and institutions should not focus entirely on prevention and concentrate on early detection and response strategies. It is imperative to use multi-factor authentication for login to systems. Information Technology departments often have well-managed and maintained servers, but the most significant risk is that they often have no insight regarding the depth of their security risks in different schools, departments, and labs.[23]

One of the most critical parts of an organization's cybersecurity is to have an appropriate cyber risk mitigation strategy. Due to its extensive scope and applicability to almost any type of organization, including higher educational institutions such as colleges and universities, the National Security Agency's (NSA) cybersecurity mitigation strategies are recommended. NSAs Cybersecurity Mitigation Strategies or PP-18-0120 was drafted in 2018 and included five core functions and ten strategies. NSAs Cybersecurity Mitigation Strategies are designed on the NIST Cybersecurity Framework, and its primary function is to counter a broad range of cyber threats by Advanced President Threat (APT) actors. NSAs Cybersecurity Mitigation Strategies is designed to promote the organization's defense-in-depth security posture and manage security risks. Five core components of NSAs

21 Convery, S. (2004). Network Security Architectures: Expert Guidance on Designing Secure Networks Indianapolis: Cisco Press, p. 77.

22 Gearhart, G. D., Abbiatti, M.D. & Michael T. Miller, M.T. (2019, April). Higher Education's Cyber Security: Leadership Issues, Challenges, and the Future. Volume 10, Issue 2, pp. 11-16.

23 McKenzie, L. (2019, July 15). Hackers demand $2 million from Monroe College in ransomware attack. Retrieved November 27, 2020, from https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack

Cybersecurity Mitigation Strategies are: Identify, Protect, Detect, Respond, and Recover. [24]

As higher education institutions evaluate new ways to store and share information, many institutions have adopted cloud computing services to create a virtual repository of data through which information can be disseminated. Although cloud computing is an ideal environment for student and faculty collaboration in the virtual environment, the use of cloud computing increases institutions' risk for data breaches due to sensitive personal information, operational, or financial data stored on third-party servers accessible over the Internet. Cloud security is a comprehensive set of policies, technologies, and controls deployed to protect data, applications, and cloud computing's associated infrastructure. Institutions must develop and revise their cloud security policies to protect networks managed by third-party vendors. Higher Education Cloud Vendor Assessment Tool was developed by The Higher Education Information Security Council (HEISC), which institutions can use to assess the quality of cloud computing services provided by third-party vendors.[25]

The software should be regularly updated at all times, and the updates should be automated if possible. The automation is necessary because harmful parties quickly exploit the new update and find the vulnerabilities and can be as harmful as before the update exploits. The software update should be received directly from the vendor and never from the unknown source or third-party software „Auto updates." The software update is an important mechanism that adds security changes and improvements made for the software. Software update practice encompasses various mechanisms, policies, and technologies necessary for proper software operation. Frances explains various software used in the educational environment and the importance of keeping the software up to date to ensure a safe and secure environment for students, faculty, and staff members.[26]

To maintain IT operations, technology users must be assigned appropriate access privileges based on their exposure risk. Using Privileged Access Management (PAM) solution is necessary to automate credential management and fine-grained access control. The alternative way is to manage user privilege through tiered administrative access in which each higher tier provides additional access to the desired, however, limited to fewer users. It is essential to create procedures to securely reset credentials such as passwords, Tokens, and tickers. Any privileged account must be under constant monitoring because cybercriminals target administrative credentials to access high-value assets and gain more control in exposed networks. According to Phillips, compartmentalizing user privileges and account access to specific individuals is necessary to maintain a proper cybersecurity posture for any organization. If one compartment is compromised, the damage will be minimal due to the threat actor's limited access capabilities. Educational institutions utilizing the system have fewer cases of full network paralysis.[27]

The organization must utilize modern operating systems that enforce signed software execution policies such as scripts, executables, device drivers, and system firmware updates in the process of maintaining the list of trusted certificates to detect and prevent the use of injection of illegitimate executables depositing malware. Execution policies can assure system integrity if used in conjunction with a secure boot capability. Application controlling whitelisting should be utilized with signed software execution policies providing improved control. Unsigned software should not be allowed to activate due to the threat of malicious code injection in the system, which will establish its control over it. According to Lee Holmes, it is essential that organizations use an updated operating system. An outdated operating system exposes the user to outdated security protocols allowing malware executables to operate in the system without any restraints. Holmes states that many educational facilities are still using outdated operating systems that can compromise the entire network's security.[28]

Exercising, creating a new or reviewing system recovery plan is necessary to ensure the proper restoration of data as part of comprehensive disaster recovery strategy. The plan's primary function should be to protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events or hardware failures. For enhanced data protection,

24 NSA's Top Ten Cybersecurity Mitigation Strategies. (2018, March). Retrieved November 27, 2020, from https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm

25 EDUCAUSE. Cloud Security. (2016). Retrieved November 21, 2020, from https://library.educause.edu/topics/cybersecurity/cloud-security

26 Frances, A. (2017). Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop. United States: National Academies Press, p. 5.

27 Phillips, R. (2013). Cyber Security for Educational Leaders: A Guide to Understanding and Implementing Technology Policies: Taylor & Francis. Retrieved November 27, 2020, p. 49.

28 Holmes, L. (2010). Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's New Command Shell. O'Reilly Media, p. 342.

backups should be encrypted, stored offsite and even offline when possible. Also, support full system recovery and reconstitution of all devices. IT staff should perform systematic testing and evaluate the backup plan. The backup plan should be updated periodically to accommodate the ever-evolving network technology environment. The recovery plan, as mitigation technique for both natural disasters as well as man made malicious threats. According to Snedaker, the most basic system recovery plan should include assessing backup needs, deciding how to conduct data backup, formulating a plan for asset recovery, and conducting a regular test of plan to isolate any internal software or hardware issues.[29]

A regular inventory of network devices should be taken. Removing any unwanted, unneeded, or unexpected hardware and software from the network. This reduces the attack surface and establishes control of the baseline of the operational environment. The active management should be conducted on operating systems, applications, security configurations, and hardware devices. To adapt to dynamic threat environments while scaling and streamlining administrative operations, it is necessary to utilize active enterprise management. According to Ding, besides software and hardware management, active enterprise management should be including any third-party entities connected to the organization's network. Ding states that third party entities are the leading cause of most network system compromises in the organization. Limiting access and setting up the proper privileges for third-party entities should be taken under immediate consideration as a part of systems management and configuration.[30]

It is important to take active steps to detect, contain, and eliminate any malicious software within the network. Enterprise-level organizations should constantly assume that the network system has been compromised and use all measures to continually seek out, contain, or eliminate threat actors within the network. The organization should utilize passive detection mechanisms such as logs, security information, and Event Management (SIEM) products, including Endpoint Detection and Response (EDR) solutions and other dedicated data analytic capabilities tools to find malicious or anomalous behaviors within the network environment. Active measures include hunt operations and penetration testing using documented reports within the system and address any discovered security vulnerabilities. The established proactive steps in network security will transition organizations beyond basic detection methods, implementing real-time threat detection and elimination as a mitigation strategy. According to Weidman, it is invaluable to the cybersecurity of the organization to regularly conduct the system penetration testing. Penetration testing is the best method in detecting system vulnerabilities and allowing IT staff to isolate the issues.[31]

Utilizing the hardware security features such as Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware (HVR) virtualization. If applicable, they are scheduling older devices for a hardware refresh. Modern hardware utilities increase the boot process's stability, boot process integrity, system attestation, and support features for high-risk application containment and elimination. Use of modern operating systems on outdated hardware results in a reduced ability to protect the system and critical data, including user credentials from threat actors. According to Bhunia and Tehranipoor, any outdated hardware that should be discontinued within the organization should be discontinued. Updating software on outdated hardware can cause security issues due to slowdowns or even hardware failure, paralyzing the system. For an optimized computer work environment, the hardwires age and degradation should be continuously monitored, and manufacturer-issued manuals should be consulted before any major software or hardware upgrade.[32]

For segregating critical networks and services, it is imperative to utilize application-aware network defenses to block improperly formed traffic and restrict unauthorized content, according to organizations' policy and legal authorizations. Traditional intrusion detection based on „known bad" signatures is rapidly decreases its effectiveness due to encryption and obfuscation techniques. Threat actors conceal malicious actions and eliminate data over common protocols, making the need for sophisticated, application-concentrated defensive systems critical for modern network environments. The IT staff must automate the monitoring of suspicious traffic within the network. Manual monitoring is not recommended due to high volume network traffic with the large organization, re-

29 Snedaker, S. (2011). Business Continuity and Disaster Recovery Planning for IT Professionals. Burlington: Elsevier Science. p. 361

30 Ding, J. (2016). Advances in Network Management. Boca Raton: CRC Press, p. 105.

31 Weidman, G. (2014). Penetration Testing: A Hands-on Introduction to Hacking. San Francisco: No Starch Press, p. 2-3.

32 Bhunia, S., Tehranipoor, M. (2018). Hardware Security: A Hands-on Learning Approach. Cambridge: Elsevier Science, p. 469.

sulting in unnecessary resources from the IT staff.[33]

It is essential to utilize multi-sourced threat reputation services for files, URLs, DNS, IPs, and email addresses. Reputation services help identify and prevent malicious events and allow for rapid global responses to threats, reduce exposure from known threats, and provide access to much larger threat analysis and tipping capability than an organization can provide on its own. Whether targeted or global campaigns, emerging threats occur faster than organizations can handle, resulting in inadequate coverage of new threats. Multi-source reputation and information-sharing services can provide a more timely and effective security posture against ever-changing threat actors. Integrating threat reputation services is an excellent threat deterrent tool that detects and isolates the threat before the user activates and infects the network or particular device.[34] Multi-Factor Authentication (MFA) is designed to prioritize user accounts with elevated privileges, remote access, and/or used on high-value assets. Physical and software token-based authentication systems should be utilized in addition to knowledge-based factors such as passwords and PINs. To create a robust cybersecurity environment, organizations should move away from single-factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems. The importance of MFA security cannot be overstated. MFA improves security by adding an extra layer of protection, reducing the intruder's ability to hack the system. As Grimes states, it is beneficial for organizations to implement MFA, and, in some cases, it is required and part of the compliance.[35]

When facing cyber threats, Federal Information Security Management Act (FISMA) guidelines recommend that chief information security officers and cybersecurity mitigation and response teams identify cyber risk areas, implement safeguards, detect cybersecurity threats, respond to a potential incident, and recover and restore systems. Institutions need to have an adequate risk mitigation framework to emphasize prevention, protection, and mitigation, response, and recovery processes implemented and approved by the leadership and the governance.

CONCLUSION

In this rapidly evolving technological ecosystem, it is essential to have robust cybersecurity mitigation techniques in higher educational institutions such as colleges and universities. Higher education institutions provide a unique environment for cybercrimes; whether it is a professional cybercriminal who wants to steal the data for their personal gain or a student who is just getting into the field of IT and wants to challenge their skills by conducting the computer system penetration, the data breach is usually the final outcome. Universities hold a vast amount of personal data on students, faculty, and staff. Besides personal data, universities contain government-contracted research, and when breached, the exposed sensitive information compromises institution security. The core component of the educational cybersecurity system is the ability for students, faculty, and staff to connect to educational systems safely. Cyberattacks on the higher education system and effective threat mitigation strategies have not been fully explored and pose many questions. The literature review on the background of cyberattacks in higher education points to common vulnerabilities, such as ransomware, DDoS attacks, phishing, social engineering attacks, direct-access attacks. When vulnerabilities are understood, higher education risk mitigation strategies can be utilized to combat the cyberthreat. The common mitigation strategies include software update procedures, defending user privileges and accounts, enforcing signed software execution policies, formulating system recovery plan, actively managing systems and configurations, continuously hunt for network intrusions, leverage modern hardware security features, segment networks, and deploy application-aware defenses, integrate threat reputation services, and transition to multi-factor authentication system can be effective countermeasures against cyberthreats in higher education.

Cyberattacks on colleges and universities are increasing in frequency and level of damage incurred. With institutions rapidly expanding remote systems and networks to support staff, faculty, and students working from home, hackers also take advantage of increased security vulnerabilities to steal data, generate profits, and cause disruption. Cyber threats to higher education are likely to grow for the foreseeable future. It is imperative to meet the challenges posed by cyberattacks with a robust cybersecurity team, meticulous planning, strategic thinking, and collaboration. Cyber threats are continually evolving, and there is no guarantee that the threat higher education institutions face today and the strategies for mitigating them will

33 Kott, A., Wang, C., Erbacher, R.E. (2015). Cyber Defense and Situational Awareness. Springer International Publishing, p. 193.

34 Ulsch, M. (2014). Cyber Threat! How to Manage the Growing Risk of Cyber Attacks. New Jersey: Wiley, p. 185.

35 Grimes, R. A. (2020). Hacking Multifactor Authentication. New Jersey: Wiley, p.137.

work in the future. Understanding vulnerabilities, how and why cyberattacks occur and preventing such attacks is fundamental to creating a more secure future for higher education. The cybersecurity challenges facing higher education are significant, and the cost of solving them is steep. Institutions across the higher education landscape find that effective cyber risk mitigation solutions protect colleges and universities from potential financial and reputational risks that come with insufficient defense.

BIBLIOGRAPHY:

1. Cook, S. (2020). US schools leaked 24.5 million records in 1,327 data breaches since 2005. Comparitech. Retrieved November 22, 2020, from https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/ (In English)
2. IBM. (2020). How much would a data breach cost your business? Retrieved November 23, 2020, from https://www.ibm.com/security/data-breach (In English)
3. Vaughan-Nichols, S. (2018, November 2). The day computer security turned real: The Morris Worm turns 30. Retrieved November 23, 2020, from https://www.zdnet.com/article/the-day-computer-security-turned-real-the-morris-worm-turns-30/ (In English)
4. Garroson, J. (2002, July 26). Yale Accuses Princeton in Hack Attack. Retrieved November 24, 2020, from https://www.latimes.com/archives/la-xpm-2002-jul-26-na-yale26-story.html (In English)
5. Attorney General Becerra and Assemblymember Levine Unveil Legislation to Strengthen Data Breach Notification Law. (2019, February 21). State of California Department of Justice. Retrieved November 24, 2020, from https://oag.ca.gov/news/press-releases/attorney-general-becerra-and-assemblymember-levine-unveil-legislation-strengthen (In English)
6. UH issues identity theft alert. (Jun 17, 2005). Retrieved November 24, 2020, from https://manoa.hawaii.edu/news/article.php?aId=1121 (In English)
7. Gamio, L., Alcantara, C. (2017, September 7). How Data Breaches Grew to Massive Proportions in 12 Years. Retrieved November 23, 2020, https://www.washingtonpost.com/graphics/business/the-scale-of-large-hacks/ (In English)
8. McCoy, L. (2020, November 20). Why PeopleSoft System Security is Vital. Retrieved November 24, 2020, from https://www.sentinelsoftware.com/why-peoplesoft-system-security-is-vital (In English)
9. McKenzie, L. (2019, July 15). Hackers demand $2 million from Monroe College in ransomware attack. Retrieved November 27, 2020, from https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack (In English)
10. Olenick, D., & Ross, R. (August 21, 2020). University of Utah Pays Ransom to Avoid Data Disclosure. Retrieved November 19, 2020, from https://www.bankinfosecurity.com/university-utah-pays-ransom-to-avoid-data-disclosure-a-14871 (In English)
11. Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps. (2018, March 23). Retrieved November 23, 2020, from https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary (In English)
12. McKenzie, L. (2019, March 6). Top universities in U.S. targeted by Chinese hackers. Retrieved November 27, 2020, from http://www.insidehighered.com/news/2019/03/06/report-top-universities-us-targeted-chinese-hackers (In English)
13. Talabis, M., Martin, J. (2012). Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis. Netherlands: Elsevier Science (In English)
14. Morgan, S. (2017). Global Ransomware Damage Costs Predicted To Exceed $5 Billion in 2017. Retrieved November 27, 2020, from https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ (In English)
15. Tidy, J. (2020). How hackers extorted $1.14m from University of California, San Francisco. Retrieved November 21, 2020, from https://www.bbc.com/news/technology-53214783 (In English)
16. Moor, M. (2017). Cybersecurity Breaches and Issues Surrounding Online Threat Protection. United States: IGI Global. (In English)
17. Kremling, J., Parker, A. M. S. (2017). Cyberspace, Cybersecurity, and Cybercrime. United States: SAGE Publications. (In English)
18. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. United

Kingdom: Wiley. (In English)
19. Twede, J., Marion, N. E. (2020). Cybercrime: An Encyclopedia of Digital Crime. United States: ABC-CLIO. (In English)
20. Lessig, L., Swartz, A. (2016). The Boy Who Could Change the World: The Writings of Aaron Swartz. United States: New Press. (In English)
21. Convery, S. (2004). Network Security Architectures. Switzerland: Cisco Press. (In English)
22. Gearhart, G. D., Abbiatti, M.D., Michael T., Miller, M.T. (2019). Higher Education's Cyber Security: Leadership Issues, Challenges, and the Future. Retrieved November 24, 2020, from https://www.researchgate.net/publication/333055605_Higher_Education's_Cyber_Security_Leadership_Issues_Challenges_and_the_Future (In English)
23. McKenzie, L. (2019, July 15). Hackers demand $2 million from Monroe College in ransomware attack. Retrieved November 27, 2020, from https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack (In English)
24. NSA's Top Ten Cybersecurity Mitigation Strategies. (2018, March). Retrieved November 27, 2020, from https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm
25. EDUCAUSE. Cloud Security. (2016). Retrieved November 21, 2020, from https://library.educause.edu/topics/cybersecurity/cloud-security (In English)
26. Frances, A. (2017). Software Update as a Mechanism for Resilience and Security: Proceedings of a Workshop. United States: National Academies Press. (In English)
27. Phillips, R. (2013). Cyber Security for Educational Leaders: A Guide to Understanding and Implementing Technology Policies: Taylor & Francis. (In English)
28. Holmes, L. (2010). Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's New Command Shell. O'Reilly Media. (In English)
29. Snedaker, S. (2011). Business Continuity and Disaster Recovery Planning for IT Professionals. Burlington: Elsevier Science. (In English)
30. Ding, J. (2016). Advances in Network Management. Boca Raton: CRC Press. (In English)
31. Weidman, G. (2014). Penetration Testing: A Hands-on Introduction to Hacking. San Francisco: No Starch Press. (In English)
32. Bhunia, S., Tehranipoor, M. (2018). Hardware Security: A Hands-on Learning Approach. Cambridge: Elsevier Science. (In English)
33. Kott, A., Wang, C, Erbacher, R.E. (2015). Cyber Defense and Situational Awareness. Springer International Publishing. (In English)
34. Ulsch, M. (2014). Cyber Threat! How to Manage the Growing Risk of Cyber Attacks. New Jersey: Wiley. (In English)
35. Grimes, R. A. (2020). Hacking Multifactor Authentication. New Jersey: Wiley. (In English)