Webology (ISSN: 1735-188X)
Volume 19, Number 3, 2022

# Cybersecurity Technologies And Practices In Higher Education Institutions: A Systematic Review

**Ayman Bassam Nassoura**

City University College of Ajman, UAE.

**Abstract:** Higher education institutions (HEIs) handle vast amounts of valuable research and sensitive personal information, making them an ideal target for cybercriminals, spies, and hackers. HEIs are suffering a great deal as a result of the COVID-19 epidemic. In April 2020, the pandemic began to spread. The use of technology is crucial for keeping HEIs connected. Secure and trusted cyberspace is essential to the digital age's full potential. In the year since the World Health Organization declared CoviD-19 a pandemic and developed new management methods and immunizations for COVID-19, the use of digital technology by higher education institutions has increased. As the world becomes more interconnected, a secure and reliable internet is essential. A growing number of people are becoming aware of cybersecurity risks. The current pandemic has created skepticism, particularly among internet users (students, staff, and faculty). HEIs can use study findings to understand how the pandemic impacts cybersecurity and how they attempt to address cybersecurity in the context of the pandemic. HEIs must evaluate their cybersecurity policies and practices as the world changes.

**Keywords:** Cybersecurity, Higher education institutions, cyberattacks, cybersecurity technologies

## I. INTRODUCTION

Cybersecurity refers to the protection of systems, programs, and networks from digital threats [1]. Cybersecurity is considered to include the security of the Internet infrastructure, the devices that connect to it, and the tech platforms and apps from which they are built [2]. Because anybody who connects to the network is a target, higher education institutions cannot entirely safeguard their networks from hackers [2]. HLIs, on the other hand, can reduce the risks of these assaults by using the cybersecurity strategies and technology discussed in this study. Higher education institutions (HEIs) have become profitable targets for cyberattacks, and many high-impact events have already occurred [2, 3, 4, 5]. Since HEIs handle vast amounts of valuable research and sensitive personal information, they are ideal targets for cybercriminals, spies, and hacktivists [3, 2] . In today's dangerous landscape, opportunists are looking for quick cash, as well as state-funded organizations seeking to steal trade secrets. HEIs have been a popular target for cybercriminals [7, 8]. Since

2005, 1,327 data breaches in the educational field have resulted in the disclosure of 24.5 million records [5, 2]. Three-quarters of the breaches occurred in higher education. Furthermore, the institutions' information security concerns are exacerbated by the free flow of workers and annual rotations of new students, visitors, and employees. Despite the fact that HEIs face significant information security risks at their institutions, implementation of information security solutions varies [6, 4]. Security measures as well as academic openness and free exchange of knowledge are among the cultural issues HEIs are addressing [6, 7].

In industry sectors, and particularly in HEIs, there is a growing demand for cybersecurity specialists. Companies are posting more cybersecurity openings and providing better wages than ever before because it is difficult to find strong, skilled employees in this industry. Highly technological occupations such as cybersecurity professionals and developers have various chances in cybersecurity organizations [2]. Many multinational corporations are organizing their own cybersecurity taskforces and hiring more cybersecurity professionals. HEIs will rely on cybersecurity specialists as a backbone in ten years, and the cybersecurity workforce will have more than doubled during the same period [3] . With a greater focus on strategic and collaborative initiatives among HEIs to regulate cybersecurity measures, students, staff, and professors will be more aware and proactive about securing their devices and networks. [7, 6].

The Covid-19 pandemic had a significant impact on the way studies were organized in higher education institutions (HEIs) [5, 7, 8, 2]. Distance learning has been the only way to continue learners study since March 2020. Due to the Covid-19 pandemic, cloud computing, eLearning platforms, and video conferencing apps were previously underdeveloped at HEIs, but are now the major assets for doing online studies. The study focused on identifying the kind of attacks that have the most impact on assets, as well as giving recommendations for improving cyber security in eLearning environments. Update systems and manage security updates, set access controls at the application or resource level, classify information, and use cryptographic protocols are all common recommendations.

In the last 20 years, the need for cyber security has grown in tandem with the increased usage of modern technologies around the world. With the Covid-19 pandemic in 2020, however, this requirement became genuinely revolutionary [4]. The modern world is hyper-connected and complicated, involving a variety of technologies, the influence of which on cybersecurity is still unknown. Users (students, staff, and faculty) are protected from the threats associated with the use of current communication technologies by cyber security. According to the Ponemon Institute [1], which performs cybersecurity research, the average loss for a global data breach in 2020 will be $ 3.86 million, with the health sector ($ 7.1 million) and the United States ($ 8.64 million) being the most affected. A data breach costs an average of $ 137,000 more than it used to due to the Covid-19 pandemic's effects on remote work. As a result, the average data breach loss is around $ 4 million.

Based on the findings of the same study [1,] it can be estimated that the cost of a data breach in the sector of education would be $3.90 million in 2020. A somewhat high figure when compared to the research industry, where data breach losses in 2020 were $1.53 million. Higher education institutions (HEIs) are increasingly vulnerable to cyber-attacks, [15]. Students and staff are targeted by cybercriminals interested in stealing personal data as well as gaining access to devices and resources [2]. Remote access and online learning platforms can be used to get access. The main goal is not to get access to a personal account, but to utilize personal information to launch fresh phishing or spam campaigns, as well as to steal money in the future.

HEIs were unprepared for such a dilemma, and a slew of issues occurred, including a lack of technological adoption, unskilled teachers for online courses, and students lacking the requisite hardware or a fast internet connection to watch video streaming media [5]. Organizations lacked specialized cybersecurity procedures to secure assets, employees, and students while they engaged in online activities. As a result, Microsoft Security Intelligence [2] pointed out that the previous 30 days, enterprises encountered 61 percent of the 7.7 million malwares that originated from HEIs, a far higher percentage than any other industry. After most higher education institutions implemented an online teaching style, or at best, a hybrid system that comprised offline hours for reduced events and online courses for tens or hundreds of students, ensuring cyber security for the new reality is vital.

Companies and businesses, as well as HEIs, who wish to protect themselves from cyber-attacks are encouraged to use cybersecurity principles. It's a 10-step guide created by the National Center for Science and Technology [8]. As a result, any HEIs interested in achieving successful cybersecurity should study the NCSC's 10-step guidance (See figure 1). Taking these ten steps as a whole, HEIs have taken action on a number of them, but they still have a long way to go before taking action in all ten areas [9].

### A. System of Risk Management (SRM):

Risk management policies and practices should be established, simplified, and clearly understood by all students, faculty, staff, and suppliers in order to ensure everyone understands the policy. For instance, how decisions are made, risk limits, and so on. It is important to support the risk management regime with a solid governance structure, including directors and senior members with relevant experience.

### B. A Secure Configuration:

Set policies for securing the organization's security zone, as well as a secure foundation and methods for configuration management [8]. The system should also be disabled or removed from unneeded functionality, as it is the primary cause of security breaches [7]. It is essential to update all software and systems regularly to avoid security gaps. If any of the above techniques are not used, the risk of system and information compromise increases.

### C. System Make:

A HEI's systems could be attacked or infected by bugs if they interact with an unsecure system over the internet, like HTTP. In order to serve as a networking foundation, policies and appropriate technical and functional responses must be developed. HEI's firewall rules will be protected as a result of the import and export networking rules. Implementing these metrics can help businesses reduce their risk of becoming victims of cyberattacks. The institution network should also be supported by a SIEM platform (security information and event management).

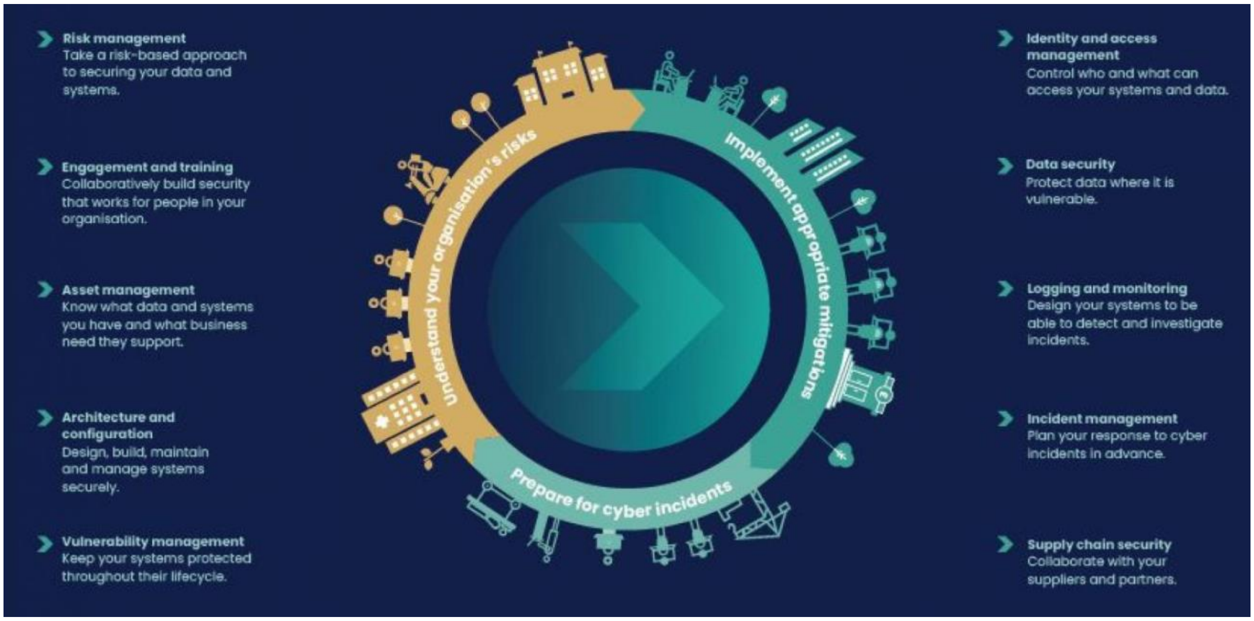
Risk management
Take a risk-based approach to securing your data and systems.
Engagement and training
Collaboratively build security that works for people in your organisation.
Asset management
Know what data and systems you have and what business need they support.
Architecture and configuration
Design, build, maintain and manage systems securely.
Vulnerability management
Keep your systems protected throughout their lifecycle.
Understand your organisation's risks
Implement appropriate mitigations
Prepare for cyber incidents
Identity and access management
Control who and what can access your systems and data.
Data security
Protect data where it is vulnerable.
Logging and monitoring
Design your systems to be able to detect and investigate incidents.
Incident management
Plan your response to cyber incidents in advance.
Supply chain security
Collaborate with your suppliers and partners.

**Figure 1: 10 Steps to Cyber Security**

### D. User Privileges Management:

Students, staff, , and professor should have access to the appropriate level of privileges, so that they can complete their tasks without interruption [16, 5]. Data security will be compromised if students, staff, and professors are granted more access than they need [2, 5]. A very close eye should be kept on the distribution of privileges at significantly elevated levels [2, 5].

### E. User Awareness and Education:

Keeping a HLIs safe and secure relies on staff, students, and professors. Students, staff, and professors will be unable to comply with these rules if they are unaware of the policies and risk management protocols established and articulated by the business. It would be beneficial to train staff, students, and professors regularly about the organization's security policies and the risks that could result in a security breach [6]. When a breach occurs, the institution's cybersecurity professionals need to be well-trained and capable of going into war mode at any time [2].

### F. Incident Handling:

HEIs should adopt effective incident management to ensure security at all points, including those at rest (like computers) and those in motion (such as laptops, mobile phones, etc.) [6, 16].

### G. Malware Prevention:

It entails the implementation of regulations addressing the most vulnerable business processes to malware infection, such as email, web, personal devices, and USB [9]. Depending on the scenario and demands, for example, a policy restricting USB access to computers should be implemented; similarly, a policy restricting outbound internet requests should be implemented, and so on. In order to protect users (students, staff, and faculty) from malware, separate expertise solutions must be established, such as email threat protection for emails, mobile security profiles to monitor end users' mobile devices, and so on.

### H. Monitoring:

In order for HEIs to have a complete picture of their overall security, a tracking strategy and solution needs to be implemented. The monitoring solution can create a solid incident report if, for example, an HEI's endpoint solution discovers malware but cannot prevent or destroy it [6, 2]. All import and export traffic, as well as the logs from the firewall, endpoints, and other solutions, will be integrated [15].

### I. Media Controls That Can Be Removed:

The use of removable media should be kept to a minimal, and each institution's external hard policy should be stated. A policy should specify the types of media and materials that can be used in specific circumstances if their use is required.

### j. Networking at Home and on the Go:

The company's LAN and WAN are no longer available to students, employees, and professors at home and on the road [12]. Because HEIs have no control over the internet, this poses a network vulnerability [2]. Therefore, mobile and remote work should be governed by risk-based regulations. The HEI can also have access to the user's data stored on their smartphone or their PC, and manage the information on the smart phone or the PC.

Data breaches are one of the most significant sources of risk for HEIs, so it's not surprising that privacy and security concerns topped the list of concerns for IT departments at HEIs even before the epidemic [1]. However, in the spring of 2020, when teaching and learning migrated to homes and parking lots, students, staff, and faculty security protection became more difficult to control, but even more necessary to sustain [4]. The first section of this article identified the key technologies used in online education activities. In a survey of 154 higher education institutions, more than 40% said security tasks had become substantially more critical in the last year. The widespread adoption of remote work and learning during the epidemic increased institutional security and privacy vulnerabilities in a variety of ways [5]. The second section focused on the security risks associated with key assets. The final segment was set aside for recommendations and debates aimed at reducing the effect of security breaches in HEIs related to online learning [7]. According to [9], the top ten ideas for improving cybersecurity in HEIs setting are as follows:

- Ensure that all of HEIs operating systems and platforms are current. Security updates are frequently included in updates.
- Install anti-virus software on each device that will be used in the remote education process.
- Upgrade software to the most recent versions recommended by the manufacturer, as the presence of non-updateable hardware and software jeopardizes computer network security.
- Make regular backup copies of all of HEIs data.
- Make a policy for passwords. According to cybersecurity experts, passwords should be updated every 90 days.
- Enable the two-step verification function to keep student, staff, and professors account safe from hackers [2].
- Make strong passwords: A strong password is a combination of numbers and letters, both uppercase and lowercase letters, with at least eight characters. In contrast, personal information such as phone numbers or dates of birth should not be included in the password [2].
- Cybersecurity experts advise that only non-sensitive information be shared on social media.
- Never click on anonymous links in emails because they are one of the most common ways computers are hacked.
- Use a tool to protect the camera. Duct tape is commonly used to protect the cameras on laptops and cellphones. It is also possible to use software that provides safeguards against unauthorized camera access and operation.

## II CYBERSECURITY TECHNOLOGIES AND PRACTICES IN HEIs

Institutional security was expected to be influenced by technologies and practices [21]. In light of the significant external and internal trends shaping higher education, it is possible that information security professionals and HEIs should begin planning now for specific technology solutions and practices to remain competitive in the future. The importance of recognizing that these technologies and practices can actively reshape future higher education landscapes, instead of simply reacting to what is currently taking place, must be underscored. During this study, technologies and practices believed to have a significant impact on higher education information security were identified. Six key technologies and practices have been identified based on this study.

### A. Cloud Vendor Management (CVM):

A key component of higher education Information Technology operations has traditionally been vendor management, as HLIs try to balance in-house and third-party systems and solutions. IT leaders should understand the importance of managing the vendor's relationship with the institution continuously and thoughtfully over time, as the integration of the vendor into the institution's environment poses ongoing challenges and questions about the vendor's "fit" with the institution's culture, values, budget, and needs. HLIs are affected in a variety of ways by CVM when it comes to cybersecurity. This strategy has a significantly greater impact on an institution's cybersecurity posture than its perceived risk and cost. One of the main driving factors for institutions considering vendor solutions in this area is cost. The institution also perceives that vendored solutions are low risk due to its relatively hands-off involvement in the management of these services by an outside vendor, along with the vendor's vast resources, staff, and experience.

### B. Artificial Intelligence (AI) and Machine Learning (ML):

Cybersecurity is one application of AI [6]. Globally, Norton research showed that the average recovery cost from a data breach is $3.86 million. A company recovers from a data breach on average in 196 days, according to the survey [6]. Due to this, HEI should invest in AI to avoid wasting time and money. By spotting trends in data, AI, ML, and threat intelligence can help security systems learn from their mistakes. The use of AI and ML allows HEIs to reduce response times for incidents while maintaining a high level of cybersecurity [6, 7]. A traditional security technique relies on signatures or other evidence of compromise to identify threats. While this method may be effective against threats that have already been identified, it does not work against threats that have not yet been discovered. The use of signature-based techniques can detect 90% of attacks. AI can be used to increase detection rates by up to 95%, but false positives will skyrocket. HEIs should combine traditional approaches with AI [7]. Detection rates can be increased to 100% and false positives reduced.

### C. Endpoint Detection and Response:

Throughout HLIs, students, faculty, and staff use laptops, desktop computers, smartphones, tablets, and other devices to interact with the institution and perform their responsibilities. As well, they serve as an entry point through which HEIs are exposed to cyber risk, as well as threats of incidents that endanger the safety of the HEIs. Cybersecurity professionals will become even more critical to institutions' overall security posture as the number of these devices increases and their reach expands into our daily lives and across our campuses.

It is essential for institution-level endpoint security to be able to address the safety concerns of students, faculty, and staff using this complex web of devices and networks. However, most students and faculty do at least acknowledge the importance of security when using their devices and connecting to network networks, and these expectations, which may lead to a decreased awareness of or shortcuts in safety, may in fact contribute to institutions being at risk of hacking and other security breaches. In addition, students, staff, and faculty need to be educated. Students and faculty should be taught how to keep their technology up-to-date, such as patching out-of-date software. They should also be taught how to recognize malicious-looking emails to prevent them from falling victim to phishing and social engineering [9]. Additionally, most HEIs require students, staff, and professors to install certified security software and an app provided by the university to help protect the network on their devices [10].

By 2020, most higher education personnel, instructors, and students will be working remotely from home and other off-campus locations adding to these issues. The use of personal devices by faculty, students, and staff to access their personal areas and network is increasing and will continue to grow going forward. It will become significantly more important to use cloud-based endpoint protection platforms (EPPs) for managing institution security, enabling remote monitoring of network and device activities, and performing remote repairs when endpoints fail [15].

### D. Single Sign-On (SSO) / Multifactor Authentication (MFA):

Academics, staff, and students increasingly require access to a number of applications and systems. This has led to a growing need and expectation for solutions that simplify authentication while protecting accounts. Right now, SSOs and MFAs may not play a defining role on campus, but they could in the near future [6]. Due to the complexity of a typical HEI's IT system, despite the challenges of implementing such tools, HEIs should find ways to simplify access so that academics, staff, and students have the most convenient and secure authentication process. Using MFA and SSO will stop users (students, staff, and faculty) from writing down usernames and passwords on paper, storing them on devices, or keeping them in password lockers [7].

### E. Multi-factor authentication (MFA):

MFA is a method of verifying a user's identity that is frequently used for a single app. A second factor, in addition to the one provided for the login, is necessary. A user may know (PIN, answers to personal questions), they may have (a physical token, smartphone), or they may not know (biometrics such as fingerprints, retina scans, etc.) [6, 7]. Users (students, staff, and faculty) can authenticate once and have access to multiple platforms and applications within one system or across multiple systems using SSO [6, 3]. SSO simplifies system navigation for faculty, students, and staff by eliminating multiple logins that require complex usernames and passwords. A lost, forgotten, or stolen password reduces the risk of security breaches. Combining SSO with MFA is a powerful way to protect sensitive institutional data [7].

### F. Preserving the Authenticity and Integrity of Data:

Data authenticity is determined by the capacity to demonstrate that data was not corrupted after it was created [8]. In a strict sense, the integrity of any data prepared or distributed to students, faculty, and staff has been compromised. It is necessary to clean (and, in a technical sense, corrupt) raw data in a real world before they can be used without compromising what they actually represent. Authentic data is data that is exactly as it should be [3].

Even when stringent data authenticity is compromised, data integrity can be maintained if individuals editing or deleting data are permitted to do so [9, 10]. Human agency, whether unintended or deliberate, is responsible for many of the dangers to data integrity. Maintaining file permissions, user access, and version control, as well as establishing/recording rules for data alteration and deletion, becomes vital [9, 10]. Information security teams will need to devote more resource to mechanisms for validating authenticity and pay more attention to the data itself in the future. Validating data based on risk, designing business continuity plans, verifying inputs, selecting systems and service providers, and archiving data regularly are among the activities described.

### G. Student Data Privacy and Governance:

HEIs amass a great deal of information about their students, staff, and professors [16]. When students apply for admission, or even before they submit their applications, data is gathered. A student's academic career is tracked by multiple data points, including their use of their learning management system, their recreational center visits, their cafeteria selections, and their library resource usage. In addition to collecting data about alumni, HEIs also maintain contact information on them. A robust data governance system should be created and managed by every institution to ensure that concerns regarding students' privacy and security are addressed.

Students, professors, and staff will desire greater control and agency over their data as they become more aware of what information institutions collect about them and how that information is used. A privacy management system makes it easy for businesses to conduct audits of compliance with privacy regulations, to track breaches of sensitive personal data [2], to document users' understanding of privacy policies, and to monitor how their data is used. A privacy management system with more advanced dashboards will allow professors, students, and staff to approve which data institutions can collect and use.

In order to manage and govern professors, student, and staff data privacy, HEIs can follow three basic steps. To begin with, HEIs must prioritize student data protection, secure storage, implementing MFA/SSO and enforcing strong password policies and standards. As well as ensuring compliance with legislation, HEIs should evaluate existing and upcoming contracts. To protect student data privacy, leading institutions may collaborate with state legislators to draft laws that would allow students greater access to and control over their data.

Second, in order to be more transparent with students' personal data [2], HEIs should inform them of what data they collect, how it is used, and protected, and obtain informed consent.;

students' ability to view, update, and opt out of school data collection and use; and ability to view, update, and opt out of school data upon request. Third, to keep students informed of current security measures, protect data privacy, and identify potential threats, HEIs can launch campus-wide information security awareness campaigns [6]. Regular security and privacy reports enable students to make informed and proactive decisions regarding their personal data [2], improving their confidence in the institution. As soon as the students arrive, start these efforts.

HEIs may face some challenges in ensuring the privacy of student, staff, and professor data and establishing data privacy governance. Some HEIs may not be able to afford the human, financial, and technical resources required to support privacy proposed measures and tools at this time. In addition, in order to honor student requests to opt out, HEIs will have to determine the extent and content of all their data repositories where they may store and use information about students, staff, and professors. It takes time and money to integrate data across systems and define rules, definitions, and responsibility lines. As a result, the institution needs to define guidelines for gathering data and determining what can (and cannot) be erased in order to properly educate and assist its students. HEIs should be prepared to adapt their algorithms and/or identify alternate ways to assist students who have been masked or influenced by such algorithms if they opt out of the collection, use, and storage of their personal data [2].

### H. Behavioral Analytics (BA):

Following the Facebook Data Breach, the use of data mining for behavior analysis has become well known. This methodology is normally used in social media and digital marketing to attack the appropriate demographic. Surprisingly, behavioral analytics is being researched rapidly in the development of superior cyber security technology [16]. By identifying themes in a system's and network's activities, BA aids in the detection of potential and current cyberattacks. For example, a significant rise in data transfer from a single user device could suggest a possible cyber security threat [16].

### I. Zero-Trust Model (ZTM):

This cyber security assumption means that a network has already been compromised. If users (students, staff, and faculty) do not trust the network, both 'internal' and 'external' security must be strengthened. In the end, both internal and external networks are vulnerable to compromise and require the same level of security. It consists of identifying and charting business-critical data, isolating it logically and physically, and executing policies and controls through automation and monitoring systems [16].

### J. Data Loss Prevention (DLP):

Using DLP, an institution can determine whether the data it gives out could disrupt their business. This technology is usually used to verify that sensitive information is not being sent outside of the institution when data is sent by email. [9]. All emails and attachments are closely examined using high-tech to guarantee that all material transferred outside of the organization is acceptable and not personal data.

### K. Intrusion Detection System (IDS):

IDS is application that analyzes all network traffic entering an organization to guarantee it is not harmful. It can also be used to manage traffic and notifications to see if they are malicious or the consequence of a potentially untrustworthy cause. This method is primarily concerned with inspecting traffic in order to assess whether it should be approved in the first place.

### L. Intrusion Prevention System (IPS):

IPS is a system or tool that detects and responds to unauthorized traffic detected by IDS. When a packet is flagged as unreliable by the IPS, it is meant to leave the system. It acts as a first line of defense, preventing hostile traffic from entering the organization's network. It is the IPS's obligation to ensure that all traffic seeking to access the gives structure with the organizations' policies, ensuring that the system's operation is not jeopardized in any manner. The Network IPS resides on the edge of the HEIs' networks and the internet, protecting them against harmful traffic from outside the HEIs. The IPS allows HEIs to defend their wireless networks by providing sophisticated threat detection [22]. Adaptive security and cutting-edge protection against advanced and emerging network threats are provided by the campus IPS. Furthermore, dynamic security, which uses behavior analysis rather than statically specified rules, enables flexible protection. Finally, with the usage of campus virtual private networks, it offers mobility for wired and wireless devices even when they are off-site [22]. According to the Global Threat Landscape Report (2020), the HEIs have the highest IPS activity of any industry, with a noteworthy surge in malware activity when classes are in session [23].

### M. Security Incident and Event Management (SIEM):

SIEM's primary purpose is to generate an alert whenever something unusual occurs on the network of the organization. By integrating many techniques into SIEM, any potentially harmful activity can trigger an alert so that the security team can respond and protect the internal environment. The network's security is also determined by logs. Additionally, it can serve as a central point of connection for other devices. The devices act as peers and defend the network in their own way.

### N. Firewall:

A firewall serves as the first line of protection for any system or network. The classification of a firewall is determined by its function. Web application firewalls safeguard the program online, whereas network nodes protect the internet. This technology was created to keep the internal infrastructure safe from illegal transactions and to ensure that nothing harmful could get through. The technique ensures that the terminals are only opened when they are needed and that no insecure data is entered into the system.

### O. Antivirus:

Another sort of cybersecurity technology is antivirus software. It safeguards the PC from viruses. A computer virus is software that enables a user (students, staff, and faculty) or system to behave abnormally. It's part of a system that can be used to protect access points. To protect against viruses, antivirus software can be installed on all p2p devices. To determine if the file was a virus, the antivirus examined characteristics stored in its database. Modern antivirus software detects irregularities and is able to stop infections immediately by detecting irregularities.

## III. DISCUSSION, SUGGESTIONS, AND RECOMMENDATIONS

A shortage of current cyber security experts, poor education in cyber security and information security principles in computing courses, a lack of well-trained academics, and a lack of structured career opportunities into the field are all concerns that HEIs must solve [12, 34]. HEIs must take a number of coordinated actions to ensure a steady supply of qualified cyber security experts who meet the necessary standards and certification to operate safely and securely. In collaboration with HEIs, professional bodies, and trade associations, industry plays a critical role in developing diverse and appealing employment and training opportunities [8, 6, 6, 35]. Create a skills advisory board comprised of professional organizations, education providers, and HEIs to strengthen coherence across these critical sectors and acknowledge the collective challenge HEIs face in closing the skills gap. This committee will help to build a long-term policy that will account for changes in the broad field of digital skills while also addressing cyber security concerns. Providing opportunities for businesses and higher education institutions to collaborate on training and education [11, 7, 5], as well as facilities for skill maintenance and exercise. To solve these challenges, industry and academia must work together effectively.

Although the issues that HEIs face may appear to be insurmountable, there are numerous approaches to properly defend IT networks. A proactive strategy protects the security of the massive amounts of data stored by HEIs. As hackers become increasingly competent at stealing information, HEIs must increase their efforts to protect their highly sensitive systems and data [34]. To overcome these security issues, HEIs will need to set up an information security program. To create a good information security program, HEIs must take the following steps:

- Produce an information security team: A successful information security management program begins with identifying the institution's security team. An ideal IT security team would be a cross-functional group that manages day-to-day activities and an executive group that sets goals and drives the program.
- Defining information assets: To establish control, it is essential that all of the institution's information assets, including data from third parties, be classified. When classifying the catalog, the relevance of the stored data should be considered [36].

- Assess the current overall security: The HEIs should conduct a detailed study of potential cyberthreats after classifying all information assets.
- Attacks and risks should be prioritized in terms of their likelihood and impact. In most cases, a thorough risk register will include a list of all potential flaws as well as the critical controls required to mitigate them [36].
- Supervise all power grids: If power grid is not monitored, many schools may be vulnerable to surprise attacks. Monitoring software monitors network activity to detect illegal activity as soon as it occurs [31]. They also keep an eye on all network devices for activity, such as security systems, access points, and data centers, whereas log analyzers may keep an eye on all event logs.
- Develop a plan to respond to incidents: In the event of a security breach, a well-planned incident response plan defines what must be done, who must be notified, and the procedures to be followed. A recommended approach is to identify the tools needed at numerous levels of risk management, such as a help desk program to log notices and assign personnel.
- Convene trainings and raise awareness: The success of the entire security program is ensured by conducting frequent training and awareness exercises for all stakeholders. Internal risks remain one of the weakest areas in security protocols across HEIs, thus all professors, staff, and students should receive regular cybersecurity training [12, 8, 6, 36].
- Although the issues that the education sector faces may appear to be insurmountable, there are numerous approaches to properly defend IT networks. A proactive strategy protects the security of the massive amounts of data stored by HELs. Effective access controls, security mechanisms, and regular administration of all data-storing databases can all assist HEIs in meeting their cybersecurity objectives.

## IV. CONCLUSION

The cyber landscape will continue to evolve as technology advances and our adversaries try to exploit it, posing new challenges. However, the goal of this study is to explore a set of technologies, tools, and skills that will enable HEIs to adapt rapidly and flexibly to new challenges as they occur. The threat will continue to exceed HEIs' ability to defense themselves if they fail to act appropriately. At all levels, HEI may expect a surge in threat capability. Conversely, if HEIs achieve these goals, all aspects of HEIs, business, and society will contribute to the overall cyber security of education. HEIs and organizations would have less need to be concerned about cyber security if security was incorporated and embedded in by default into commodity technologies. Malicious hackers who want to create instruments and attack techniques for critical functions and data will simply have to put more effort to get past the multi-layer security that protects them [34]. Even in the best-case scenario, addressing some of the cyber concerns that HEIs face, whether in terms of scale or difficulty, might take over than five years. Nonetheless, this study gives HEIs with the tools they need to improve our future safety and stability in the digital age.

## REFERENCES

[1] Winbuzzer, "Cyber Security in Universities: Identifying Risk, Threats, and Vulnerabilities," 2021.

[2] Internet Society, "Major Initiatives in Cybersecurity: Public & Private Contributions Towards Increasing Internet Security," 2020.

[3] Veracode, "Veracode Tackles Cybersecurity Skills Gap with Launch of The Hacker Games," 2021.

[4] E. Rantanen, "Cybersecurity in Higher Education: Understanding the Threats & Adopting A Zero Trust Approach," 2021.

[5] India Today Web Desk, "Importance of Cybersecurity in the education sector," 2021.

[6] Cisco, "What Is a Cybersecurity Specialist?," 2021.

[7] D. Nahila, "What educational institutions need to do to protect themselves from cyber threats," 2021.

[8] P. Florin and C. Olivia, "Increasing the Competence and Resilience of Industrial Cybernetics by Involving the University Environment," Romanian Cyber Security Journal, vol. 1, no. 3, pp. 65-69, 2021.

[9] SecurityScorecard, "What is HECVAT and Why is it Important?," 2021.

[10] E. Povejsil, "Cybersecurity in Higher Ed: Understanding Vulnerabilities and Preventing Attacks [Infographic]," 2021.

[11] Reciprocity, "Cybersecurity Challenges Facing Higher Education," 2021.

[12] S. Bocetta, "Artificial Intelligence is Solving Cybersecurity Staffing Shortages in Higher Education," 2020.

[13] EDUCAUSE Horizon Report, "021 EDUCAUSE Horizon Report, Information Security Edition," EDUCAUSE Horizon, 2021.

[14] Gurnani, "From education to cybersecurity: Technology can create good businesses," 2020.

[15] J. Chapman, "Cyber security in universities and colleges is improving, but there's no room for complacency," 2020.

[16] Adam, "John Hurst, Public Sector Sales, CyberArk, explores the cybersecurity risks that higher education institutions are facing," 2021.

[17] O. Jeremiah, R. Anthony and L. Samuel, "A Framework For Secure University Networks For Effective Business Continuity," International Journal of Innovative Research and Advanced Studies (IJIRAS), vol. 7, no. 10, pp. 54-61.

[18] NCSC, "Further ransomware attacks on the UK education sector by cyber criminals," NCSC, 2021.

[19] National Cybersecurity Center, "Pikes Peak SBDC and National Cybersecurity Center Announce Cybersecurity Day on October 19th," National Cybersecurity Center, Nevada, 2021.

[20] Department for Digital Culture Media and Sport, "Cyber Security Breaches Survey 2021," Department for Digital, Culture, Media and Sport (DCMS), London, 2021.

[21] F. Donald, "A Look at Local Government Cybersecurity in 2020," 2021.

[22] D. Schaffhauser, "Educause Report Tackles Cybersecurity and Privacy in Higher Ed," 2021.

[23] Global Perspectives & Solutions, "Managing Cyber Risk with Human Intelligence: A Practical Approach," Global Perspectives & Solutions, 2019.

[24] UC Berkeley Extension, "Cybersecurity in Education: What Teachers, Parents and Students Should Know," 2020.

[25] K. Brian, "Cybersecurity in higher education: going from ‘no’ to ‘know’," 2021.

[26] S. Grajek, "EDUCAUSE COVID-19 QuickPoll Results: Information Security During the Pandemic," EDUCAUSE Research, 2020.

[27] E.-T. Amr, "Tips on Cybersecurity for Students and Teachers," 2021.

[28] E. Segal, "The Impact of AI on Cybersecurity," 2021.

[29] Toneimage, "Cyber attacks: Protecting universities and solving cyber security issues," 2019.

[30] D. Robb, "What Is Single Sign-On?," 2019.

[31] Fortified Health Security, "Single Sign-On vs. MFA: Do You Know The Difference?," 2020.

[32] B. Genge, P. Haller and D. drian-Vasile, "Engineering security-aware control applications for data authentication in smart industrial cyber-physical systems," Future Generation Computer Systems, vol. 4, p. 91, 2018.

[33] C. Cezarina, "Data Integrity: What It Means and How to Maintain It," 2021.

[34] B. Chris, "What is Data Integrity? Definition, Best Practices & More," 2020.

[35] S. Cook, "US schools leaked 24.5 million records in 1,327 data breaches since 2005," 2020.

[36] C. S. Cybercrime, "The 5 Latest Cyber Security Technologies for Your Business," 2019.

[37] University of Michigan, "Intrusion Prevention System (IPS)," University of Michigan, 2021.

[38] M. Steve, "How higher education can overcome the expanding threat landscape," 2021.

[39] H. Singh, "Cyber security in universities: Threats, threat actors and defence," 2021.

[40] Tripwire, "Could Universities' Use of Surveillance Software Be Putting Students at Risk?," 2020.

[41] P. John, "5 emerging security technologies set to level the battlefield," 2021.