INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 2 | Issue 2 [2024] | Page 396 - 415

A STUDY ON THE IMPACT OF CYBERSECURITY CHALLENGES AND HOW AI REINFORCES EMERGING TECHNOLOGIES IN THE FIELD OF DIGITAL EDUCATION

- **Dev Kaur**[1] **& Himanshu Bhargava**[2]

ABSTRACT

In today's era of education, there is an extreme adoption of cyber technologies resulting in efficient teaching and learning environments, contributing in extraordinary approach towards information and inventive teaching tools. However, this change in digital era leads to major cyber security challenges that are become barriers towards education and also impact negatively towards the privacy, integrity and availability of these educational resources. Educational institutions are also targeted negatively in this digital era, cyber-attacks, ransomware, data breaches and phishing are committed for the purpose of stealing cognizant information and disturb the educational processes. To overcome from these challenges and convert into safest environment in respect of education, Artificial Intelligence (AI) is a leading powerful tool which strengthen cybersecurity measures and helps in the evolution of strong digital education platforms. The said research explains the complicated threats of cyber security over digital education and explores how AI-driven tools increase the security protocols, safeguard data and secure the continuity of educational services. From the use of AI technologies in the educational institution which helps in finding and combating cyber threats which resulted in promoting a protected and more effective digital learning environment. This research study explains some measures that is taken by the government and leading stakeholders like industry leaders and academicians for the purpose of defeat the skill gap in the cybersecurity knowledge expertise. Through these measures which is supported by sufficient funding, practical policies and a strong curriculum can defeat the skill gap in education.

Keywords: Cybersecurity Challenges, Digital Education, Data Breaches, Ransomware Attacks, Artificial Intelligence (AI).

[1] Research Scholar, Dr. Bhim Rao Ambedkar University, Agra.

[2] Post Graduate, Renaissance University, Indore.

INTRODUCTION

In our education system, education related to cybersecurity is very important for some important reasons. Cybersecurity education helps students to reduce online risks, understand the career interest in cybersecurity and help towards the filling of skill gap. Jobs related to cybersecurity are very much in demand according to the CYBER.ORG and the Ed Week Research Centre but the contribution of qualified professionals is inadequate. As a result, early education has an important role towards students for their foundational knowledge and skills (Cyber.org). The set of practices and the step taken by individuals which helps to maintain the health and security of their digital information and devices are known as "Cyber Hygiene". Cyber Hygiene is related to personal hygiene, which brings out dynamic measures towards the protection from cyber threats. This Cyber hygiene is important for those students who regularly uses shared networks and such devices to protect their personal and academic information. In this digital world where the importance of cyber security is increasing day by day, is very important to provide necessary tools and knowledge so that they teach the concept of cyber security very effectively. Towards student careers and their future in the field of cyber security, teachers training is also very important so that students can protect their data in this digital world. The breach of cybersecurity directly impacts upon educational institutions with an increase in the cyber-attacks and their numerous challenges. When the COVID-19 arises, this issue is aggravated because all the education system and schools shifted towards online learning, this leads to more and more cyber threats because of the use of technology and devices (Bravura Security 2024). In every educational institution, cybersecurity has become a critical matter because as the time changes this institution increasingly adopting advanced network technologies for efficient learning. Because of this digital change in the education system, it leads to intensify risks and making of strong cybersecurity policies. This dependency upon digital platforms for education has requirement the need of strong online safety measures. Online safety of students involve knowledge about cyber risks and how to enforce policies and tools to protect their own data. Cybersecurity is an important aspect towards protecting information and systems from cyber-attacks. As cybersecurity develops, cyber threats are also evolved, for that purpose strong cybersecurity measures are very important for safeguarding the data, privacy maintenance and secure the integrity of the digital infrastructures. In educational institutions data privacy is a very important issue because the institution handles very sensitive personal information such as social, academic records, health related information and financial data for every student. For protecting students and maintain their trust it is important to ensure privacy and security of this data. Skill gap under cybersecurity is a major issue that affects different sectors, including

education. Cybersecurity skill gap under education means gap between the professionals and the available skilled work force.

CYBERSECURITY AWARENESS AND EDUCATION IN K-12 SCHOOLS

The study focuses on the challenges of cybersecurity in education. In today's era, school education from kindergarten to twelfth- grade converted to online mode from traditional offline mode, that leads to increasing to the risk of cyber-attacks and cybercrimes. The main of this study is to making strategies that education institutions can implement for the purpose of cybersecurity awareness and motivates them to pursue as a career.

Teachers and students from K - 12 educations are most in danger from these cyber-attacks. The time where these risks increased, when COVID - 19 pandemics evolved, all the youngsters are fully dependent upon the digital technology and spent their all-time online. As well as United States of America is also troubled with shortage of cybersecurity professionals. The rise of cyber-attacks is increasing day by day and there is also a need of cybersecurity professionals is an intensive effort towards teachers to integrate the cybersecurity education towards the K- 12 curriculum. The target for the year 2025 is that all the aspiring educators from whole of the country are ready to prepare combined age-oriented concepts of cybersecurity, career awareness in their curriculum nevertheless of their area or any specialization.

CURRENT STATE OF CYBERSECURITY EDUCATION

In the United States, according to a National Survey, there is a significant gap in cybersecurity education across the K - 12 schools. According to that survey less than half of the K - 12 students experience with any form of cybersecurity education and also the accessibility of these resources differs very much. Schools which are located at small or high poverty districts or regions, where there is no cybersecurity companies or universities are there, they are less likely to offer education in cybersecurity (cyber.org). This type of inconsistency leads to more and more widespread initiatives related to cybersecurity education.

INTEGRATION INTO CURRICULUM

Education in cybersecurity is consolidated with broader curriculum, not being offered as a single course. Curriculum method in cybersecurity involves subjects like technology, computer science and even social studies. However, under this approach, many interpretative topics like cryptography, system engineering, Artificial Intelligence and electricity are not covered. (cyber.org).

EXTRACURRICULAR ACTIVITIES

For the student's benefit, extra-curricular activities such as competitions, camps and cybersecurity clubs are productive for understanding the student's interest and field. Extra-curricular activities include practical, hands-on experience that motivates the students to choose cybersecurity in career. Students engages in competitive and collaborative cybersecurity challenges, which is an initiative by National Cyber Cup (cyber.org).

CYBER HYGIENE PRACTICES AMONG STUDENTS

ESSENTIAL CYBER HYGIENE PRACTICES

Regular Software updates: It is very important to keep your software up-to-date, because of updates include security patches for their weakness. This practice of updating is not limited towards operating systems but also applicable towards applications and plugins (ERAU Scholarly Commons 2020) (Illinois.edu 2024).

Strong passwords: For intensify security features, we have to use password that is a combination of letters which is both uppercase and lowercase, numbers and special characters. It is also very important to not use your same password on different websites. To detain and manage your difficult password with security, password manager is a very helpful tool for this purpose (Illinois.edu 2024).

Awareness of Phishing Scams: Method which is used by cybercriminals to steal sensitive information is known as "Phishing". While using suspicious websites, which asks for any type of personal information and uninvited emails and messages, student should be very cautious while using these websites. In a website, recognizing the signs of phishing, such as poor grammar and mismatched URL's can prevent the attacks (Illinois.edu 2024).

Safe Browsing Habits: While using any websites or sharing information online, students should be more attentive about those websites. Also, they have to check the website they used is secure (look for "https" and a padlock symbol), while entering their personal information, is very important. To reduce the risks, students have to keep away from untrusted websites (Illinois.edu 2024).

Use of Antivirus Software: While using antivirus and anti-malware software's we have to keep update the software's from time to time, which protects and mitigate from cyber threats. Antivirus

and anti-malware software's helps to detect and remove malicious software's and prevent from data breaches (Illinois.edu 2024).

CYBER HYGIENE IN EDUCATIONAL CONTEXTS

Many researches elaborate that, most of the students have seen that, they have a lack of awareness in the cybersecurity practices, which results into greater risks of cyber incidents. These cybersecurity knowledge gap among students is found by the study of Majmaah University, which highlighted the need for efficient education and training among students (MDPI 2021).

TEACHER TRAINING FOR CYBERSECURITY EDUCATION

CURRENT INITIATIVES AND PROGRAMS

National Initiative for Cybersecurity Education (NICE) K12 Cybersecurity Education Roadmap. To intensify the education in cybersecurity, the NICE roadmap provides an analytical approach. The roadmap focuses on students towards increasing their career awareness, engagement of students through incorporative approaches, restoration of innovative educational methods, encouraging career pathways and categorize research (nist 2021).

CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY (CISA) RESOURCES

Numerous resources for K-12 educators, including of professional development workshops, cybersecurity curriculum and various educational tools were offered by CISA. The various resources offered by CISA focuses on to help teachers integrate cybersecurity into their lesson plans and motivates students to choose their career in this field (niccs. cisa 2024).

NCYTE CENTER PROGRAMS

NCyTE Centre helps towards expansion and distribution of cybersecurity curriculum and essential resources for the educators. The centre provides workshops, lessons, plans and modules that was created for the cybersecurity concepts into the classroom. "Girls Go Teach" workshops and cybercamps like programs are mainly for the students.

IMPACT OF CYBERSECURITY BREACHES ON EDUCATIONAL INSTITUTIONS

TYPES OF ATTACKS AND THEIR CONSEQUENCES

Ransomware: In this digital world, ransomware attacks are frequently targeted the educational institutions, which leads to block the access towards sensitive data until the ransom is being paid. Ransomware incidents form K-12 education towards Higher Education enlarge by 105%, in the year 2023, have a worst year on records due to these cyber-attacks (EdTech Magazine 2024) (Bravura Security 2024). The disturbances arise from these attacks may terminate the education activities and also the sensitive data may be compromised.

Phishing: Phishing attacks are those attacks, where cyber criminals pretending as the authorized legal entities, to steal their sensitive information, which is the most regular cyber threats faced by the school entities (Bravura Security 2024). Results of these phishing attacks are illegal access to username, passwords and related financial information.

Distributed Denial-of-Service (DDoS) Attacks: These types of attacks me create negative impact over the schools, caused destruction towards online learning platforms and other digital resources (Bravura Security 2024).

IMPACT ON INSTITUTIONS

Financial Loss: As a result of these ransomware attacks, financial loss conclusion includes ransom payments, costs recovery and potential fines for data breaches. An institution my sustain hundreds of thousands of dollars due to the single ransomware attack (EdTech Magazine 2024) (Bravura Security 2024).

Reputation Damage: Ransomware attacks or any breach in cyber security my leads to harm towards educational institutions, destroying the trust among the students, their parents, teachers and their staff. The disclosure of any personal sensitive information and financial data lead to reputational harm in long term.

Operational Disruption: Ransomware attacks lead to create disturbances in the educational processes and also termination of classes and the loss of instructional time. These disturbances may occur during the time of examinations and admissions (EdTech Magazine 2024).

CONTRIBUTING FACTORS

Limited Resources: Most of the educational institutions spent less than 8% of their IT budgets towards cybersecurity education, as a result of this, there are non-efficient protection measures and untrained faculties (Bravura security 2024).

Increased Attack Surface: Very wide user base that includes students, faculty and the administrators increases the possibilities of such cyber criminals. Cyber threats which are internal, such as students and staff with malafide intention, again complicated the security efforts (Bravura Security 2024).

MITIGATION STRATEGIES

To mitigate these cyber threats various methods or strategies are to be adopted by educational institutions, that are:

Regular Cybersecurity Training: To increase the institution's security, educators, staff members and students doing best practices against cyber threats (keeper password manager& digital vault).

Advanced Security Measures: Enforcing security framework with zero-trust, access management solutions and confidential access management systems helps to combating the risks of cyber threats (Keeper® Password Manager & Digital Vault).

Incident Response Plans: Developing and frequently updating cybersecurity incidents, make sure that education institutions are well prepared to control security breaches effectively (bravura security 2024).

CYBERSECURITY POLICIES IN EDUCATIONAL INSTITUTIONS

KEY COMPONENTS OF CYBERSECURITY POLICIES

Zero-Trust Security Model: This zero-trust security model presume that no one, whether inside or outside the network, be easily trusted. Under this security model it is necessary to continuous verification of user identities and access permissions.

Implementation: The method of implementation includes using of multifactorial authentication, monitoring of behavior and analysis of networks. However, examine data traffic for anomalies can helps in identify and combat cyber threats easily (EdTech Magazine 2024).

Benefits: Zero-trust model increases the security through limiting the access towards only what is necessary, however it containing major breaches towards main segments of the security network.

CYBERSECURITY TRAINING PROGRAMS

Purpose: Acknowledging phishing attempts and how to use safe internet, through instruct students, educators and staff members, towards efficient practice in cyber practice.

Methods: Conducting workshops on regular basis, imitate phishing attacks and compulsory cybersecurity courses, helps in mitigating the risk of human error, that is the most fragile link in cybersecurity (CISA 2023).

INCIDENT RESPONSE PLANS

Importance: An effective incident response plan makes sure that, education institution can easily and efficiently acknowledge to cybersecurity incidents to reduce the damages.

Components: The incident response plan should include the ideas for identify the cybersecurity breaches, communications protocol and also includes the necessary steps for recovery and system restoration (CISA 2023).

INVESTMENT IN SECURITY MEASURES

Priority: Educational institutions need to categorize investments in the most efficient cybersecurity measures, with the limited budgetary concern.

Actions: Placing of multi-factor authentication, combating the known weakness and executing the regular backups are the most important steps. As well as manipulating state and federal grants help in provide important financial support towards institutions (CISA 2023).

COLLABORATION AND INFORMATION SHARING

Strategy: Co-operation with federal states as well as local agencies and taking part in information-sharing organizations e.g. Multi-State Information Sharing and Analysis Centre (MS-ISAC), which helps to intensify situational awareness and resource allocation (ED.gov 2024) (CISA 2023).

Benefits: The collaborations with such agencies and states helps toward remain updated with the cyber threats and also encourage for acquire resources and support mechanism.

ONLINE SAFETY FOR STUDENTS

IMPORTANCE OF ONLINE SAFETY

Protection from cyberbullying, phishing, identity theft and mitigating the inappropriate content all of these encompasses through the concept of "Online Safety". It is also important for the students to take knowledge more about technology, understand how to safely used internet, is very important to mitigate these risks (Edutopia 2024) (Cybersecurity Guide 2024).

KEY STRATEGIES FOR ONLINE SAFETY

Education and Awareness: Daily basis discussion on cyber threats and risks and awareness behavior can help the students to become more conscious about their internet activities. Educators should also encourage the students for cyber safety matters with the help of various subjects. (NSPCC Learning 2024).

Creating Strong Passwords: Teaches the students to make lengthy and unforgettable passwords, instead of using the difficult passwords, that is very complex in nature and difficult to remember, that leads to unsafe storage practices. To mitigate credential stuffing attacks, students have to use different password for their multiple accounts (Cybersecurity Guide 2024)..

Two-Factor Authentication (2FA): For better safety and add an extra layer of security, implements the 2FA, that is a second form of verification process. This method of implementing 2FA, protects the account even if the password is compromised (Cybersecurity Guide 2024).

Privacy Settings and Data Protection: Encouraging the students to daily check and also updates their privacy settings on social media and other platforms. They have to understand, what permission is being given and it is being used is very important towards protection of their personal information (Edutopia 2024).

Use of Antivirus and Safe Browsing Practices: Students have to ensure that their devices are up-to-date and having an antivirus software, that helps against viruses and malwares. Teachers' duty to teach students towards not click on unknown links and not download any matter from untrusted websites. Give knowledge about safe and secure browsing like being aware while using public wi-fi and so on (Edutopia) (NSPCC Learning 2024).

Resources and Tools: Utilize available resources like Google's "Be Internet Awesome," which offers interactive activities on cyber safety, and Common-Sense Media's lessons on internet safety.

These tools can make learning about online safety engaging and effective for students (blog. Google 2024) (Edutopia 2024).

POLICY IMPLEMENTATION IN SCHOOLS

Filtering and Monitoring Systems: Schools should implement tiered filtering systems to restrict access to harmful content and monitor online activities to identify and mitigate risks. This helps create a safer online environment for students (NSPCC Learning 2024).

Regular Training for Staff and Students: Continuous training for teachers and students on the latest online safety practices ensures that everyone stays updated on emerging threats and protection strategies. Workshops and seminars by external experts can supplement the school's efforts (NSPCC Learning 2024).

Incident Response Plans: Developing clear incident response plans for cyberbullying or data breaches ensures quick and effective action. Schools should have protocols for reporting and managing online safety incidents to minimize their impact on students (NSPCC Learning 2024).

ROLE OF TECHNOLOGY IN ENHANCING CYBERSECURITY EDUCATION

In today's digital world, the role of technology become enhancing day by day in cybersecurity education, because of the complexities and frequency of cyber threats also grow. Technological advancements in cybersecurity education are transforming is how the cybersecurity is taught and practised:

ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

In revolutionizing the cybersecurity education AL and ML are the tools which provides advanced threat analysis and response. These AL and ML technologies helps towards the real-time analysis of data sets, which help towards identifying and mitigate cyber threats very efficiently. In cybersecurity training AI-driven tools and labs are now an integral part of the cybersecurity training and also helps students to experience with real-world scenario (Acronis 2024) (Splash top 2024).

QUANTUM COMPUTING

In cybersecurity education, Quantum Computing have potential risks towards present encryption methods, and also gives more opportunity offers. It helps to increase the understanding level of difficult cryptography systems and also improve the evolution of quantum-resistant algorithms.

This concept of Quantum computing is incorporated by educators while preparing their curriculum towards students for their future challenges and innovation in cybersecurity (Splash top 2024).

GENERATIVE AI

Generative AI which includes ChatGPT that is being used to develop realistic cyber threat structure and associated training environments. Generative AI tools help the students and their professionals to develop their skills in responding to advanced cyber threats. As well as, Generative AI tools can help in expand the educational content, creating cybersecurity learning more effective that helps towards individual needs (Gartner 2024).

VIRTUAL AND AUGMENTED REALITY (VR/AR)

VR and AR technologies, which provides interesting learning experience, that allows the students to connected with real experience of cyber-attacks and their defence methods. These types of technologies maintain the gap between the theoretical knowledge and practical application, which makes cybersecurity education more effective. (Splash top 2024).

BLOCKCHAIN TECHNOLOGY

Blockchain's technology reduce the most effectual education during making of vigorous cybersecurity protocols. (Gartner 2024).

DATA PRIVACY IN EDUCATIONAL INSTITUTIONS

Data protection and data security are very important in learning institutions. Over one's school time, educational facilities accumulate much private data regarding a student. This data is considered to be very attractive for fraudsters to use it for their sinful identity stealing actions, so this type of data should be defended. Updating systems as simple as the student information systems (SIS), remains inevitable as it helps in improving both data security and the general user interface for staff, teachers, and students, (Campus Safety Magazine 2024).

Compliance with Laws and Regulations: There are several data protection laws including but not limited to CCPA, HIPAA, FERPA that institutions have to adhere to. High requirements to the admissibility of data operations and non-disclosure of information are set by these regulations, and violation of such bans may entail serious legal and financial consequences (Campus Safety Magazine 2024) (EDUCAUSE Review 2021).

Best Practices for Data Privacy: Reducing the amount of information also reduces the possibilities of leakage as it only collects information that is useful and discards it when it is not anymore. Since it guarantees that institutions only collect and retain the data that is required in every part of a student's academic journey, this practice complies with the aspect of data minimization (Campus Safety Magazine 2024).

Openness and Informed Consent: Thus, transparency when it comes to the collection and use of data promotes trust. Organizations should openly communicate why data is gathered, to whom it is collected, and how it is utilized. Regulators' business objectives are improved due to the use of consent and preference management platforms that enhance student trust (Campus Safety Magazine 2024) (EDUCAUSE 2020).

Frequent Evaluations and Vendor Management: This is why it is important to continue to learn using various evaluations of data privacy policies and well-enshrined vendor management frameworks. To ensure the third-party suppliers conform to institutional standards, third party assessment tools such as the Higher Education Community Vendor Assessment Tool (HECVAT) facilitate in evaluating the security and privacy compliance of the vendors (Help Net Security 2022)
.

CYBERSECURITY SKILLS GAP IN EDUCATION

Security professionals as well as those specialized in cybersecurity are scarce and much needed in today's global market. In other words, the cybersecurity industry should have four million more employees in order to sufficiently guard digital structures (World Economic Forum 2024).

CHALLENGES AND RECOMMENDATIONS

Several challenges make it difficult to achieve effective implementation of cybersecurity education in K-12 schools and facilities. These include; lack of qualified staff, poor financial endowment, and limited access to up-to-date educational resources. In an effort to address these issues, the following suggestions have been put forth:

It is advised that students take the following actions to improve their cyber hygiene:

Include Education on Cybersecurity: Introduce topics based on Cybersecurity in the curriculum to ensure that children get factual information in their day-to-day life and are aware of the importance of good Cyber hygiene practice.

Frequent Training and Awareness Programmes: Organize training sessions where priority is given to how not to violate the rules of the World Wide Web and what threats exist at the moment.

Make Use of Campus Resources: Take advantage of what university IT departments can provide in the maintenance of appropriate cyber hygiene; for instance, putting up and updating antivirus software on the campus gadgets.

By following these procedures, students have a great opportunity to decrease their vulnerability to cyberattacks and protect their academic and personal information:

Limitations on Resources: Resources are always limited especially when it comes to expenditure in institutions of learning; therefore, it becomes hard to implement adequate security measures for combating cyber criminals.

Complex Networks: One of the features of networks in the educational institutions that complicates their protection is their structural and functional diversity, which means that networks can host multiple user groups and contain several access points.

Government Support: Additional resources and guidance can be acquired from the government for instance, cybersecurity grants and Government Coordinating Council (GCC) (ED. Gov 2024).

Constant Improvement: Security is something that needs to be worked on all the time. It has been postulated that in order to counter emerging risks, the possible changes to policies must be made more often, as well as introducing new technologies (EdTech Magazine 2024).

Allocation of Resources: As for the issue of privacy, it is usually a part of the CISO's portfolio, which means that he has limited time and resources to work on distinct and detailed privacy programs. As the complexity of data security issues increase institutions must consider creating roles uniquely for privacy (EDUCAUSE 2020).

Education and Awareness among Students: As much as one would like to believe this is not the case, many students do not understand how organisations use their data. For them to have full control during the process of reaching such decisions and for them to have a clue of the consequences of data gathering, students ought to be educated on data privacy, ethics, and literacy (EDUCAUSE Review 2021) (EDUCAUSE 2020).

Adaptation to Regulatory Changes: It means establishments must ensure that they continue knowing the latest innovations in the laws that govern data privacy, and adjust accordingly. This includes being conscious with foreign regulation that has potential impact on the American universities that offer courses to students globally (Help Net Security 2022).

Cyber Threats Are Changing: Email fraud, computer viruses, and hacking are some of the modern and evolved threats to educational institutions. Thus, such honours are important in order to perceive and prevent these risks and react properly to them, if any (World Economic Forum 2024).

Insufficient Training Programmes: Many universities do not teach a lot of their training courses in the field of cybersecurity. The current force is often not ready to deal with the present-day challenges in cybersecurity as conventional academic courses are often unable to overcome with the fast-changing picture of threat landscapes (SANS Institute 2024).

Resource Limitations: Schools especially experience limited funding when it comes to financing state-of-the-art cybersecurity policies and training programs. As a result, when it comes to the hiring and retention of cybersecurity talent, organisations face significant challenges and this creates an even bigger skills gap as highlighted by the World Economic Forum.

APPROACHES TO MEETING THE SKILL DEFICIENCY

Stressing Certifications: The field of cybersecurity truly is starting to wake up to the fact that certificates are worth more than diplomas. Just as the cybersecurity threats are modern, the knowledge which is needed for their repelling is also of practical and, at the same time, immediately applicable kind, so the certifications from the organizations such as GIAC and SANS Institute (SANS Institute 2024).

Improved Courses of Study: This requires developing sort of needful specialized training programs that can cater for the demand of the market. For these programmes to be beneficial to the graduates, the focus should be on the application programmes with special reference to practical application (SANS Institute 2024, World Economic Forum 2024).

Collaboration between the academic institutions and cybersecurity companies can help in creating relevant curricula and provide work experience for students. By means of internships, apprenticeships, and cooperative education programmes the above-mentioned gap can be minimized (SANS Institute 2024, World Economic Forum 2024).

Government-led Initiatives: Thus, investing in adequate education and training, government prompted programs like White House Office of the National Cyber Director try to update the cybersecurity workforce. These programmes recruit more people to the profession by giving categorical assistance towards formation of sound cybersecurity programmes (SANS Institute 2024).

CONCLUSION

Thus, one can conclude that financial viability, management efficiency, and reputational URN assets of educational institutions are threatened by cyber threats. Focusing on cybersecurity training and investments, schools may minimize these threats that increase year by year (GOV.UK 2024) (EdTech Magazine 2024) (Bravura Security 2024). This means that there is a need for educational institutions to have good and elastic cybersecurity policies because the threats are continuously evolving and increasing. When it comes to developing a safe academic environment more has to be invested in: implementing zero-trust security architecture; funding necessary security controls; training all the users; promoting collaboration with external entities. Still, these issues are solvable and educational institutions are able to achieve a much higher level of cybersecurity protection with the help of governmental grants and proper planning. The protection of student's internet usage therefore requires a combination of the use of technology, enforcement of policies and training.

It is also possible to help students to exist in the digital environment without becoming a part of its negative aspects by creating a culture of protection. Cyber defence is a complex process that requires a series of measures comprehending reliable policy, monitoring, user awareness, and technological enhancements. Organisations could potentially fortify the safeguard of the digital assets and ensure that security stays lasting by continuing to evolving the risks and through adding adequate preventions. The student's privacy in educational institutions is safeguarded using a multi-faceted approach that includes legal obligations, data minimization, transparency, and consistency in improvement. The following are the best practices that an institution can adopt to retain the confidence of the community and also protect the sensitive student's information. There is need for a multiple-anvil approach in an endeavour to develop meaningful and sustainable solutions to the problem of the lack of a well-coordinated cyt org in education today, where training programs, business partnerships, and supportive government policies are the pillars that can help. Through emphasis on certification, the establishment of versatile training, and the formation of industry relations, future educational institutions are posed to train the future generation of cybersecurity personnel in order to counter the rising incidents of cybercrime.

REFERENCES

- Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, *3*(1), 47-67. http://journal.gmpionline.com/index.php/ijses/article/download/132/112
- Dawson, K., Antonenko, P., Xu, Z., & Wusylko, C. (2022). Promoting interdisciplinary integration of cybersecurity knowledge, skills and career awareness in preservice teacher education. *Journal of Technology and Teacher Education*, *30*(2), 275-287.https://www.learntechlib.org/primary/p/221089/paper_221089.pdf
- Baraković, S., & Baraković Husić, J. (2023). Cyber hygiene knowledge, awareness, and behavioural practices of university students. *Information Security Journal: A Global Perspective*, *32*(5), 347-370. https://doi.org/10.1080/19393555.2022.2088428
- Chen, W., He, Y., Tian, X., & He, W. (2021, October). Exploring cybersecurity education at the K-12 level. In *SITE Interactive Conference* (pp. 108-114). Association for the Advancement of Computing in Education (AACE). https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1062&context=itds_facpubs
- AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754. https://www.researchgate.net/profile/SalehAldaajeh/publication/360670552_The_Role_of_National_Cybersecurity_Strategies_on_the_Improvement_of_Cybersecurity_Education/links/661e81c9f7d3fc287466271f/The-Role-of-National-Cybersecurity-Strategies-on-the-Improvement-of-Cybersecurity-Education.pdf
- Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382. https://pdfs.semanticscholar.org/f24d/d9d57c7c3c4a14cedfd4eb38073b78124d96.pdf
- D. Guillén-Gámez, F., Martínez-García, I., Alastor, E., & Tomczyk, Ł. (2024). Digital Competences in Cybersecurity of Teachers in Training. *Computers in the Schools*, 1-26. https://doi.org/10.1080/07380569.2024.2361614
- Alrabaee, S., Al-Kfairy, M., & Barka, E. (2022, March). Efforts and suggestions for improving cybersecurity education. In *2022 IEEE Global Engineering Education Conference*

(EDUCON) (pp. 1161-1168). IEEE. https://doi.org/10.1109/EDUCON52537.2022.9766653

- Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. https://www.mdpi.com/2078-2489/13/4/192
- Jawaid, S. A. (2022). Cyber security threats to educational institutes: a growing concern for the new era of cybersecurity. https://www.preprints.org/manuscript/202211.0128/download/final_file
- Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137-154. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1973526
- Kendall, C. L. (2022). The Openness of Higher Education and Implications on Cybersecurity.https://search.proquest.com/openview/628bf9ae362721c1afea428ac3f51732/1?pq-origsite=gscholar&cbl=18750&diss=y
- Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), 538. https://www.mdpi.com/1424-8220/22/2/538
- Hina, S., & Dominic, D. D. (2017, July). Need for information security policies compliance: A perspective in Higher Education Institutions. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.https://www.researchgate.net/profile/SadafHina/publication/311788432_Information_security_policies_Investigation_of_compliance_in_universities/links/65670adbb1398a779dc492cd/Information-security-policies-Investigation-of-compliance-in-universities.pdf
- Zufić, J., Zajgar, T., & Prkić, S. (2017, May). Children online safety. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 961-966). IEEE. https://www.researchgate.net/profile/JankoZufic/publication/318695892_Children_online_safety/links/60aa0efea6fdcc6d626abb4b/Children-online-safety.pdf
- Tomczyk, L., & Eger, L. (2020). Online safety as a new component of digital literacy for young people.https://www.researchgate.net/profile/JankoZufic/publication/318695892_Children_online_safety/links/60aa0efea6fdcc6d626abb4b/Children-online safety.pdf

- Lazarinis, F., Alexandri, K., Panagiotakopoulos, C., & Verykios, V. S. (2020). Sensitizing young children on internet addiction and online safety risks through storytelling in a mobile application. *Education and Information Technologies*, *25*, 163-174. https://link.springer.com/article/10.1007/s10639-019-09952-w
- Walsh, K., Pink, E., Ayling, N., Sondergeld, A., Dallaston, E., Tournas, P., ... & Rogic, N. (2022). Best practice framework for online safety education: Results from a rapid review of the international literature, expert review, and stakeholder consultation. *International journal of child-computer interaction*, *33*, 100474. https://www.sciencedirect.com/science/article/pii/S2212868922000150
- Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122). https://www.researchgate.net/profile/JosephEkstrom/publication/220707262_The_role_of_cybersecurity_in_information_technology_education/links/00b7d517e8c671a6df000000/The-role-of-cyber-security-in-information technology-education.pdf
- Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in human behavior*, *29*(1), 26-32. https://www.agnesday.com/wp-content/uploads/2012/10/Slonje-Cyberbullying.pdf
- Chisholm, J. F. (2014). Review of the status of cyberbullying and cyberbullying prevention. *Journal of information systems education*, *25*(1), 77. http://jise.org/volume25/n1/JISEv25n1p77.pdf
- Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16*(3), 263-279. https://www.academia.edu/download/57958447/Achieving_big_data_privacy_in_education.pdf
- Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information Systems Education*, *34*(1), 94-105. https://jise.org/Volume34/n1/JISE2023v34n1pp94-105.pdf
- Blažič, B. J. (2021). Cybersecurity skills in eu: New educational concept for closing the missing workforce gap. *Cybersecurity threats with new perspectives*. https://www.intechopen.com/chapters/75922
- John, S. N., Noma-Osaghae, E., Oajide, F., & Okokpujie, K. (2020). Cybersecurity Education: The Skills Gap, Hurdle. *Innovations in Cybersecurity Education*, 361-376. https://link.springer.com/chapter/10.1007/978-3-030-50244-7_18

- Chen, L., Chen, P., & Lin, Z. (2020). Artificial intelligence in education: A review. *Ieee Access*, *8*,7526475278.https://ieeexplore.ieee.org/iel7/6287639/6514899/09069875.pdf
- Jaiswal, A., & Arun, C. J. (2021). Potential of Artificial Intelligence for transformation of the education system in India. *International Journal of Education and Development using Information and Communication Technology*, *17*(1), 142-158. https://files.eric.ed.gov/fulltext/EJ1285526.pdf
- Alam, A. (2021, November). Possibilities and apprehensions in the landscape of artificial intelligence in education. In *2021 International Conference on Computational Intelligence and Computing Applications (ICCICA)* (pp. 1-8). IEEE. https://www.emerald.com/insight/content/doi/10.1108/lht-07-2021-0242/full/html
- Okunlaya, R. O., Syed Abdullah, N., & Alias, R. A. (2022). Artificial intelligence (AI) library services innovative conceptual framework for the digital transformation of university education. *Library Hi Tech*, *40*(6), 1869-1892. https://www.emerald.com/insight/content/doi/10.1108/lht-07-2021-0242/full/html.
- https://www.nist.gov/
- https://www.nist.gov/news-events/news/2021/12/roadmap-k12-cybersecurity-education
- https://niccs.cisa.gov/education-training/cybersecurity-teachers
- https://commons.erau.edu/db-srs/2020/poster-session-grad/6/
- https://publish.illinois.edu/educationblog/2024/02/19/understanding-cyber-hygiene-basics-every-student-should-know/
- https://www.mdpi.com/2504-2289/5/2/23https://doi.org/10.3390/bdcc5020023
- https://cyber.org/
- https://www.bravurasecurity.com/blog/the-impact-of-security-breaches-on educational-institutions
- https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows
- https://www.keepersecurity.com/blog/2024/01/22/why-higher-education-needs-to-prioritize cybersecurity-in-2024/
- https://www.bravurasecurity.com/blog/the-impact-of-security-breaches-on-educational-institutions
- https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024

- https://edtechmagazine.com/higher/article/2024/02/what-do-higher-education-institutions-need-know-about-zero-trust
- https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- https://www.ed.gov/news/press-releases/us-department-education-launches-government-coordinating-council-strengthen-cybersecurity-schools
- https://www.edutopia.org/article/teaching-students-cyber-safety
- https://cybersecurityguide.org/resources/internet-safety/
- https://learning.nspcc.org.uk/online-safety/online-safety-for-schools
- https://blog.google/outreach-initiatives/education/safer-internet-day-2024/
- https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
- https://www.isaca.org/resources/news-and-trends/industry-news/2024/the-top-5-cybersecurity-threats-and-how-to-defend-against-them
- https://www.jpmorgan.com/technology/news/top-cybersecurity-trends-to-watch-2024
- https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
- https://www.campussafetymagazine.com/insights/navigating-student-data-privacy-in-higher-education/134476/
- https://er.educause.edu/articles/2021/2/data-privacy-in-higher-education-yes-students-care
- https://www.helpnetsecurity.com/2022/03/03/higher-education-data-privacy/
- https://www.educause.edu/ecar/research-publications/the-evolving-landscape-of-data-privacy-in-higher-education/introduction
- https://www.weforum.org/agenda/2024/04/cybersecurity-industry-talent-shortage-new-report/
- https://www.sans.org/press/announcements/white-house-sans-institute-chart-path-to-close-cybersecurity-skills-gap/
- https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home