Emperor International Journal of Library and Information Technology Research

ISSN:2582-6972 Mayas Publication ® www.mayas.info

Volume - V Issue - 09 September-2024

Securing the Future: Information Security imperatives for Higher Educational Institutions

Sethukkarasi, R
Librarian, Government Law College,
sethu.ram2000@gmail.com
Tirunelveli-627 011.

Abstract

Data breaches at Indian educational institutions have grown to be a concerning problem, impacting millions of students, professors, and their families' private and sensitive data. As educational institutions depend more and more on digital platforms to handle student information, academic records, and administrative tasks, the dangers of cyber attacks and data theft have increased. These breaches put people at risk for identity theft, financial fraud, and other security risks in addition to compromising their privacy. Furthermore, there is an urgent need for stronger cyber security measures given the growing number of data breaches in the education sector. Sensitive data must be protected by institutions implementing advanced security methods including encryption, multi-factor authentication, and frequent security audits. But technological fixes are insufficient on their own. There is a critical need for increased awareness and training among staff, teachers, and administrators to recognize potential threats, such as phishing attacks and ransomware, and to take proactive steps to protect digital infrastructure.

Keywords: Information Security (IS), Data Protection, Awareness of IS, Education Sectors

I. INTRODUCTION

Higher education institutions are depending more and more on technology in today's quickly changing digital environment to manage administrative, academic, and personal data. The amount of sensitive data that is saved and sent through educational systems has increased dramatically, ranging from financial information and intellectual property to student records and research data. However, there is a growing risk of cyber attacks associated with this digital revolution. The higher education industry, which is sometimes seen as a soft target, has many difficulties, such as ransomware attacks, data breaches, and other cyber security risks.

Information security in higher education is now a strategic priority that affects the financial stability, reputation of the institution, and privacy of staff, teachers, and students. It is no longer just a technical problem. As schools and universities continue to use digital resources, cloud services, and online learning platforms, it is crucial to have strong cyber security measures in place to protect sensitive data and provide a safe learning environment. Institutions of higher learning that do not prioritize information security run the danger of losing important data as well as losing the confidence of their stakeholders.

In order to safeguard the digital infrastructure of the higher education industry, a comprehensive strategy to information security that incorporates cutting-edge technologies, robust regulations, and awareness campaigns is needed.

Significant Cyber security Incidents (2014-2024)

In 2023, India had 5.3 million compromised accounts, placing it fifth on the list of nations with the highest hacking rates. A total of 299.8 million accounts were compromised worldwide, with the United States ranked First and accounting for 32% of all breaches from January to December. Russia came in second, followed by France in third, Spain and India in fourth. The Research of data breaches by Surfshark revealed that the breach rate in India was 56% lower in 2023 than it was in 2022, while the global trend indicates an 18% decline.

India's educational institutions were the regular targets of serious cyber security incidents from 2014 to 2024. With the growing use of digital platforms for student data, learning management, and administration, schools, colleges, and universities became more susceptible to cyber attacks.

Indian educational institutions have become popular targets for hackers since they frequently handle enormous databases containing sensitive data, including financial, research, teacher, and student information.

Here are some of the most significant cyber security incidents in India's educational sector during this period:

AIIMS Ransomware Attack (2022)

Medical professionals and students can receive education at Delhi's All India Institute of Medical Sciences (AIIMS), despite it being a medical school. In 2022, a significant ransomware assault disrupted AIIMS's digital capabilities, affecting not just patient data but also employee and student records. The attack revealed the vulnerability of educational infrastructures interwoven with public service sectors like healthcare, even though the target was healthcare disruption.

Ed Tech Platform Unacademy Data Breach (2020)

Unacademy, a well-known EdTech company in India with millions of users, had a significant data breach in 2020. On the dark web, the private information of more than 22 million users including instructors and students was made public and offered for sale. Particularly during the COVID-19 pandemic, when EdTech services expanded nationwide, the hack brought to light the dangers of an increasing dependence on online learning platforms.

Student Database Breaches at Prestigious Universities (2021)

Hackers reportedly targeted several Indian universities in 2021, including well-known establishments like Delhi University. Students' names, phone numbers, email addresses, and academic records were among the compromised personal information that was made available for purchase on the dark web. These instances highlighted the need for more robust data protection measures by exposing the susceptibility of even India's most esteemed educational institutions to cyber threats.

Maharashtra SSC Board Exam Data Leak (2019)

A major cyber security incident involving the online leak of sensitive information pertaining to the SSC (Secondary School Certificate) exams, including exam-related records and student personal Information

occurred in 2019 at Maharashtra's State Secondary and Higher Secondary Education Board. This raised serious concerns about the security and privacy of examination procedures in India.

CBSE Data Breach Scandal (2018)

In 2018, a significant data breach occurred at the Central Board of Secondary Education (CBSE), one of the biggest educational institutions in India. Students who took the CBSE board exams were impacted by this breach. Addresses, roll numbers, student names, and other private information were among the sensitive data that was compromised. Serious questions were raised by the hack regarding the capacity of educational authorities to protect student data as well as the wider ramifications for student privacy and exam integrity.

Aadhaar Data Breach Impacting Schools (2018)

Reports of hacked Aadhaar-linked data from multiple schools surfaced in 2018. Numerous Indian institutions used Aadhaar data to identify students, and security lapses involving this data sparked concerns about the improper use of children' biometric and personal information. Stricter data management procedures are required in educational institutions as a result of this incident, which highlighted the dangers of integrating vital identity systems like Aadhaar with student records.

Ransomware Attacks on Indian Universities (2021-2022)

Between 2021 and 2022, a number of Indian universities reported ransomware attacks, which followed worldwide patterns showing an increase in ransomware targeting educational organizations. Operations, including access to digital services and scholarly resources, were interfered with by these attacks. Ransomware attacks caused temporary shutdowns of IT systems at institutions including Banaras Hindu University (BHU) and private universities in Maharashtra.

Phishing Scams Targeting EdTech Companies and Students (2020-2021)

Online learning grew commonplace during the COVID-19 pandemic, making Indian EdTech enterprises like Vedantu and Byju's great candidates for phishing assaults. Attackers tried to steal login

passwords and personal information by sending teachers and student's phony emails and links.

These occurrences made it clear that the educational sector has to raise awareness of cyber security, particularly while using online platforms.

Tamil Nadu Directorate of Technical Education Data Breach (2021)

Hackers breached the database of Tamil Nadu's Directorate of Technical Education in 2021, exposing the private information of thousands of students enrolled in technical schools. Increased examination of public educational institution cyber security procedures resulted from this incident, which revealed the susceptibility of government-run education boards to cyberattacks.

Examination Paper Leaks and Cyber Breaches (2014-2023)

Over the course of the decade, there were multiple incidents in which hackers gained access to testing systems in different states, resulting in the release of test papers before of significant public examinations. These events, which included leaks in the state board and engineering entrance exams, had a serious negative effect on the legitimacy of the Indian examination system. Hackers frequently used shoddy web portals to obtain exam-related data, highlighting the dangers associated with insufficient cyber security measures in educational testing systems.

Key Factors Driving Cyber Attacks on Educational Institutions

Some of the major reasons for cyber attacks in the education sector include:

Sensitive Data and Personally Identifiable Information (PII)

Personal Identifiable Information (PII) of students, teachers, staff, and even parents is stored in large quantities by educational institutions. This information includes social security numbers, addresses, contact information, academic records, health information, and occasionally financial information. Hackers target this information for identity theft, financial fraud, and even sale on the dark web.

Research and Intellectual Property

Advanced research and innovation are concentrated at many universities and other higher education institutions. In order to steal intellectual property linked to important research, especially in areas like technology, health, and military, cybercriminals including nation-state actors, frequently target these organizations. It is a profitable target since research data can be used for political or competitive advantage.

Outdated Security Infrastructure

Since many educational institutions have little resources, they do not give priority to or make sufficient investments in modern cyber security measures. This results in old software, unpatched vulnerabilities, and out-of-date systems that are simpler for attackers to exploit. In the absence of appropriate security measures, organizations are vulnerable to cyber attacks.

Lack of Cyber security Awareness

Faculty, staff, and students at educational institutions are frequently varied and might not be familiar with cyber security best practices. Users are more vulnerable to popular attack vectors including ransomware, phishing, and social engineering attacks when they lack training. Attackers may gain access to students and staff if they unintentionally click on harmful links, download malware, or fall for hoaxes.

Rise of Remote Learning and Digitalization

Particularly during the COVID-19 epidemic, the growing dependence on digital tools has increased the attack surface in the educational sector. New risks have been brought about by remote access to university networks, cloud services, and online learning platforms. Since many institutions lacked strong security for remote operations, hackers have taken advantage of these weaknesses, leaving them vulnerable to attacks and data breaches**.**

Inadequate IT Security Teams and Budgets

Resources for IT and cyber security are scarce at many educational institutions, especially smaller ones. IT departments frequently lack the resources or personnel necessary to adequately handle security risks. Successful cyber attacks are more likely as a result of the shortage of specialized cyber security staff.

Use of Third-Party Vendors

Third-party vendors are frequently used by educational institutions to provide services including cloud storage, student information systems, and learning management systems. Attackers may use these vendors as access points if they don't have robust cyber security measures in place. Vulnerabilities in third-party systems are frequently used by cybercriminals to enter institutional networks.

Ransom ware Attacks for Financial Gain

Ransomware attacks, in which cybercriminals lock users out of computers and demand ransom payments to unlock them, frequently target educational institutions. Institutions may face pressure to swiftly pay ransoms in order to regain control of their systems due to the vital nature of educational data (such as research, academic records, and administrative data). Because of the possibility of quick compensation, hackers target colleges and universities.

Increased Use of BYOD (Bring Your Own Device)

Bring your own device (BYOD) and connect it to the school's network; this is permitted by many educational institutions. Because these gadgets which include laptops, tablets, and smart phones frequently have insufficient security safeguards, they give hackers more avenues of entry. In addition to raising the danger of malware, phishing, and other cyber attacks, BYOD policies can be challenging to administer and safeguard.

Large and Decentralized Networks

With several departments, campuses, and networks, universities and colleges in particular frequently have big, dispersed IT systems. It can be difficult to manage security across many different systems, and a lack of consistency in security procedures might leave vulnerabilities open to attack.

Examination Systems and Grading Manipulation

In order to falsify test scores, grades, and admissions procedures, hackers also target educational institutions. Educational databases are prime candidates for manipulation and tampering because of the pressure associated with university admissions and competitive tests.

Exam systems may be compromised by attackers in order to change results or leak exam materials.

Political or Ideological Motives

Sometimes political or ideological motivations drive cyber attacks on educational institutions. Hackti vist organizations may attack educational institutions to express disapproval of particular affiliations, research endeavors, or policies. In order to make a point, these assaults may involve tampering with websites, exposing private information, or stopping services.

Opportunistic Cybercriminals

Because educational institutions are seen as simple, opportunistic targets, hackers frequently target them. Because they might not have the same strict cyber security protocols as the business or financial sectors, educational institutions are more susceptible to attacks. These alleged vulnerabilities are exploited by cybercriminals to initiate low-effort, high-reward attacks.

The requirement to strike a balance between rigorous data protection and openness for learning presents a special set of cyber security concerns for educational organizations. The education industry is a prime target for cyber attacks due to a mix of sensitive data, insufficient cyber security expenditures, and growing digitalization. To lessen the frequency and impact of attacks on educational institutions, it is imperative to increase knowledge of cyber security, invest in modern security architecture, and make sure that sufficient IT resources are devoted to this problem.

India's Cyber security Framework: Safeguarding the Nation's Digital Frontier

In order to handle the increasing risks in the digital realm, India's cyber security policy environment has undergone tremendous change. The 2013 National Cyber Security Policy (NCSP) was a significant advancement that established the framework for India's strategy for protecting cyberspace. Since then, the nation has kept up its efforts to strengthen its cyber security. The main elements of India's cyber security policy framework are outlined below:

National Cyber Security Policy (NCSP) 2013

The first comprehensive policy to protect India's cyberspace was the NCSP 2013. By concentrating on the following, it was intended to create a safe and robust cyberspace:

i. **Securing Critical Information Infrastructure (CII)**: Ensuring that vital infrastructure, such as that of the banking, telecommunications, energy, and defense industries, is protected from online attacks.
ii. **Promoting Awareness**: promoting cyber security awareness, education, and training among the public, government agencies, and corporations.
iii. **Building Capacity**: building a cyber security-focused research and development (R&D) ecosystem and a qualified workforce.
iv. **Establishing an Assurance Framework**: establishing operational, legal, and regulatory frameworks to improve cyber security and guarantee safe e-governance.

Indian Computer Emergency Response Team (CERT-In)

The Ministry of Electronics and Information Technology (MeitY) oversees CERT-In, the national nodal organization in charge of organizing responses to cyber security incidents. In addition to working with international cyber security bodies, it releases advisories and does cyber security drills. Developing plans for addressing vulnerabilities, keeping an eye on and reacting to cyber security occurrences, and encouraging cyber security best practices across industries are some of its duties.

Information Technology (IT) Act, 2000 (Amended in 2008)

Hacking, identity theft, phishing, and data breaches are all covered by the legal framework for cyber security in India, which is provided by the IT Act, 2000. Important information infrastructure protection, acknowledging the seriousness of cybercrimes, and enforcing sanctions were all covered by the 2008 amendment.

Personal Data Protection Bill

The Personal Data Protection (PDP) Bill seeks to control the collection, processing, and storage of personal data, although it has not yet been passed. It is based on the GDPR of the European Union and imposes stringent data protection requirements on businesses, with an emphasis on protecting Indian residents' privacy.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)

Cyber Swachhta Kendra is an awareness and cleanup method designed to detect and eliminate malware and Botnets. It was introduced as part of the Digital India project. The center encourages safe internet usage by offering free tools for identifying system infections.

National Critical Information Infrastructure Protection Centre (NCIIPC)

Established under the IT Act, the NCIIPC is in charge of defending India's vital information infrastructure against online threats. Defense, energy, banking, and transportation are among the vital industries that the institute focuses on.

Data Localization and Sovereignty Initiatives

In recent years, India has placed a strong emphasis on data localization, requiring businesses to keep specific types of data particularly personal data within its borders. By retaining data under Indian jurisdiction, this measure seeks to improve cyber security and protect sensitive information from foreign snooping.

Cyber security Initiatives in Banking and Financial Sector

In order to prevent cyber attacks in the banking industry, the Reserve Bank of India (RBI) has released guidelines for financial institutions that place a high emphasis on developing incident response plans, real-time monitoring, robust cyber security frameworks, and frequent audits.

Cyber security Awareness Programs

The following programs seek to raise general understanding about cyber security:

- **Information Security Education and Awareness (ISEA) Project**: This MeitY-funded initiative encourages cyber security training and education.
- **Digital India Initiative (DII)**: It incorporates cyber security components, emphasizing safe access to e-governance services and encouraging digital literacy nationwide.

International Collaboration

India works with international cyber security organizations like Interpol, the **International Telecommunication Union** (ITU), and bilateral agreements with nations like the US and Japan to share cyber security best practices, create capacity, and exchange cyber security information.

In order to handle new threats and integrate more recent technology like cloud security and block chain, India is anticipated to update its National Cyber Security Policy shortly.

In the face of a rapidly expanding digital economy, India's cyber security landscape is generally concentrated on safeguarding personal data, boosting collaboration, protecting key infrastructure, and raising public awareness.

Cyber security in Education: Key Strategies to Prevent Data Breaches

Educational institutions may successfully stop data breaches that could endanger their operations with the correct tools and tactics. They can reduce risks and guarantee the integrity of sensitive data by implementing thorough cyber security measures. Among the crucial actions are:

- Frequently updating software and computer systems.
- Making use of safe storage techniques and strong passwords.
- Multi-Factor Authentication (MFA) implementation.
- Teaching employees how to spot breach attempts and follow cyber security guidelines.
- Creating a plan for responding to cyber attacks and keeping frequent backups of your data to ensure quick recovery.

Here are some beneficial actions your organization may take to strengthen cyber security if these safeguards aren't currently in place:

Identity Access Management (IAM)

Only those who are permitted can access institutional resources as a result of Identity Access Management (IAM). IAM enables organizations to monitor who is accessing data, when they are doing so, and from where by giving them more insight into user activities. Access can also be restricted according to elements like:

- Device.
- Location.
- User roles inside the company;
- Access time.

In order to stop illegal breaches, compromised accounts, and data leaks, IAM is essential.

Privileged Access Management (PAM)

In order to lessen hostile cyber activity, Privileged Access Management (PAM) assists in monitoring, identifying, and preventing unauthorized access to sensitive resources. The following are are two important PAM practices.

- Enforcing zero-standing rights and
- limiting account access and permissions

MFA and automatic password management are two security protocols that should be supported by effective PAM software. It should also help administrators automate account management procedures, provide reports, and keep an eye on user sessions. Institutions can improve security and reduce the chance of data breaches with the help of this visibility into privileged accounts.

Password Management and Protection (PMP)

Managing many digital platforms results in a complicated array of login credentials for educational institutions. Staff may employ re-used or easily-guessable passwords to streamline the procedure, which raises the possibility of credential fraud.

Password management can be simplified using a single sign-on authentication system, which also lowers password-related problems and lets users fix login issues on their own. Crucial elements for safeguarding login credentials consist of:

- Authentication protocols.
- Password policy enforcement.
- Password synchronization.
- Security question integration.
- Self-service password resets.

Faculty and staff can log in more easily and securely with an all-in-one password management solution.

Multi-Factor Authentication (MFA)

By asking users to confirm their identity using extra steps beyond a password, like a fingerprint scan, MFA offers an extra degree of security.

- An email with a verification code.
- A push alert sent to a device that has been enrolled.
- Responding to a security query.

An even more secure option is authentication without a password. Using biometric techniques like fingerprint or facial recognition, faculty members may log in quickly, enhancing user experience and security. Government-led cyber security programs are crucial to guaranteeing a secure digital environment as the number of incidents increases worldwide, especially in India.

Next-Gen Cyber security: Innovations and Best Practices for Digital Defense

Future cyber security measures must take into account the quickly changing threat landscape brought about by new technologies and growing levels of digitalization. Among the main areas of attention are:

Security of the Fifth Generation (5G)

Protecting 5G networks from any cyber attacks is of utmost importance since these networks are being implemented all over the world. 5G technology expands the possible attack surface by increasing the number of connected devices. To protect 5G infrastructures, strong encryption, safe network slicing, and sophisticated intrusion detection technologies will be crucial.

Artificial Intelligence (AI) and Machine Learning (ML)

In order to automate threat detection and response, artificial intelligence (AI) and machine learning (ML) will be essential. However, protecting AI systems from hostile attacks such as algorithm manipulation will be essential. Strengthening AI models to guarantee data integrity and utilizing AI-driven tools to anticipate and thwart cyber attacks are examples of future actions.

Internet of Things (IOT) Security

As the number of IOT devices in homes, businesses, and communities increases, protecting these devices from vulnerabilities is essential. Future actions will concentrate on establishing secure network frameworks to stop unwanted access, guaranteeing device-level encryption, and building IOT-specific security standards.

Quantum Computing

There are advantages and disadvantages to quantum computing for cyber security. It has unmatched processing power, yet it has the potential to crack existing encryption techniques. In the future, creating cryptographic algorithms that are immune to quantum attacks will be essential to protecting private information.

Zero Trust Architecture

With increasingly distributed and cloud-based workforces, traditional perimeter-based security is becoming obsolete. Future approaches will be based on Zero Trust models, which presume that all users and devices are untrusted until they are verified. It lowers the possibility of internal intrusions by requiring continuous authentication and monitoring.

Block chain for Security

Block chain technologies decentralized and impenetrable data storage can enhance cyber security. It can be applied to transparent auditing procedures, data integrity, and supply chain security. It is possible that block chain-based security methods may be adopted more widely in the future.

Advanced Threat Intelligence Sharing

It will be more crucial for governments, businesses, and international organizations to work together on cyber security initiatives. Rapid threat identification and mitigation will be facilitated by increased real-time threat intelligence exchange. For proactive defense plans, governments are supposed to create frameworks that promote collaboration across sectors.

Biometric Authentication

Future cyber security plans will shift from using passwords to safer and easier-to-use techniques like biometrics (voice, facial, and fingerprint recognition). By lowering the possibility of credential theft, these solutions offer an extra degree of protection.

Cyber security Regulations and Compliance

Stricter cyber security laws and industry-wide compliance requirements are anticipated from governments. To lessen vulnerabilities, especially in industries like finance and healthcare, these regulations will call for frequent audits, penetration tests, and adherence to new security guidelines.

Cyber security Workforce Development

There is a rising concern about the lack of qualified cyber security personnel. Building a highly skilled workforce that can handle sophisticated cyber threats will require future investments in cyber security education, training courses, and certifications.

The goal of these proactive steps is to offer more robust and resilient defenses against the ever-changing nature of cyber threats in the digital realm.

II. CONCLUSION

Securing sensitive information is crucial for higher education institutions in an era where digital revolution is driving education. These institutions are becoming prime candidates for cyber attacks due to their growing reliance on technology and the internet. A strong information security plan is necessary to protect against these weaknesses.

Adopting thorough security regulations, providing frequent training for employees and students, and putting cutting-edge technical solutions into practice are all crucial requirements. Fostering a culture of security awareness requires cooperation between administration, academics, and IT departments. Institutions must also constantly evaluate and update their security procedures to remain ahead of new threats.

Higher education institutions can preserve stakeholder trust, safeguard their data, and make sure their educational missions are upheld by placing a high priority on information security. Proactive security measures will not only protect the present but also enable institutions to flourish in the future by fostering innovation.

III. REFERENCES

(2023). Recent Advances in Cyber Security Laws and Practices in India. Advances in human and social aspects of technology book series, 220-241. doi: 10.4018/978-1-6684-8133-2.ch012

1. Adharsh, C., S., Vijayalakshmi. (2022). 3. Prevention of Data Breach by Machine Learning Techniques. doi: 10.1109/icacite53722.2022.9823523
2. Ayça, Atabey., C, Robinson., Anna, Čermáková., Andra, Siibak., Natalia, Kucirkova. (2024). Ethics in EdTech: Consolidating Standards For Responsible Data Handling And Usercentric Design. doi: 10.31265/usps.283

3. Deepthy, Jose. (2024). Data Privacy and Security Concerns in AI-Integrated Educational Platforms. 2, doi: 10.46632/rmc/5/2/19
4. Haydar, Teymourlouei., Vareva, E., Harris. (2022). 2. Preventing Data Breaches: Utilizing Log Analysis and Machine Learning for Insider Attack Detection. doi: 10.1109/csci58124.2022.00181
5. Ms, Roopesh. (2024). Cyber security solutions and practices: firewalls, intrusion detection/prevention, encryption, multi-factor authentication. 4(3):37-52. doi: 10.69593/ajbais.v4i3.90
6. Nokuthaba, Siphambili. (2024).Exploring Cyber security Implications in Higher Education. Proceedings of the ... European conference on information warfare and security, doi: 10.34190/eccws.23.1.2306
7. Shipra, Varshney., Dheeraj, Munjal., Orijit, Bhattacharya., Shagun, Saboo., Nikunj, Aggarwal. (2020). Big Data Privacy Breach Prevention Strategies. doi: 10.1109/ISSSC50941.2020.9358878
8. Sunita, Mane, Saware. (2024).Personal Data Protection In Digital Age: Issues And Challenges. doi: 10.59646/data protection/127
9. Yatu, Rani, Sarthak, Jain. (2023). 2. Cyber Warfare by Chinese hackers: The AIIMS Story. International journal of science and research, doi: 10.21275/sr23217131720.