INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

EDUCATION SECTOR UNDER SIEGE: CYBER ATTACK CHALLENGES

AUTHOR - SOWNDHARYAA K M, LLM STUDENT AT SCHOOL OF EXCELLENCE IN LAW, THE TAMILNADU DR. AMBEDKAR LAW UNIVERSITY.

BEST CITATION - SOWNDHARYAA K M, EDUCATION SECTOR UNDER SIEGE: CYBER ATTACK CHALLENGES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (3) OF 2024, PG. 63-68, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT:

" Where there is data online, there is cyber risk."

In recent years, the education sector has increasingly become a target for cyber attacks, exposing vulnerabilities in schools, colleges, and universities. These attacks include ransomware incidents that disrupt academic operations and data breaches that compromise sensitive student information. As educational institutions embrace digital technologies for remote learning and administrative tasks, the risks linked to insufficient cybersecurity measures have intensified. This paper explores the nature and prevalence of cyber threats in the education sector, assesses their potential impacts on students, faculty, and institutional integrity, and presents strategies to enhance cybersecurity resilience. By adopting a proactive stance on digital security, educational institutions can better protect their environments and uphold trust within their communities.

Keywords: cyber attacks, education sector, cybersecurity

INTRODUCTION:

The Education sector has emerged as the most targeted business for cyber attacks, accounting for more than 7 lakhs detected threats in April-June 2023. According to SEQRITE Labs' malware analysis study, the large number of attacks highlights educational institutions' growing vulnerability to Cyber attacks, the manufacturing industry came in second with 3.29 lakh threats, followed by professional services with 3.28 lakh threats. Students in India have returned to school as the COVID outbreak has subsided. The Indian education industry, like other developed economies, has been the target of malicious cyber security attacks. According to some projections, India would be the top target of cyber threats to educational institutions and online platforms in 2022, followed by the United States, the United Kingdom, Indonesia, and Brazil.The education sector was found to be the worst hit globally, with 79% of higher education organizations surveyed and 80% of lower education organizations surveyed reporting that they were victims of ransomware attacks[192]. Due to the increasing number of cyberattacks, the University Grants Commission (UGC), which is the leading education regulator in India has advised colleges, institutions and universities to enhance their cyber security systems.

EDTECH:

Edtech which refers to new technological implementations in the classroom.The pandemic resulted in numerous significant reforms in the Indian education sector. During the pandemic, the education industry used technology to transform physical classes into virtual ones. With the support of cloud-based technologies, e-learning became a reality. Virtual learning has become the norm in both public and private institutions, with millions of

[192]Puja mahendru, July 13, 2023, The State of Ransomware in Financial Services 2023, available at: https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 3 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

students using these platforms on a daily basis. Several Edtech startups also used modern technology such as Audio Recording/Video Recording (AR/VR) to instruct the students. While such digital transformation alleviated the access problem, threat actors began looking for weak links for hostile cyber attacks. Notably, students' personal data relating to teaching, learning, progress, and other associated information was stored on digital platforms.

As a result, threat actors are using these tools as launching pads to obtain student data. Student tracking software, in particular, provides a clear path for actors to gather personally identifiable information (PII) from students.An example in point is the data breach reported by one of India's leading Edtech Organisations. According to claims, customer data was compromised by one of the company's vendors who were in charge of the Customer Relations Management (CRM) system. This data breach, which occurred in 2020, exposed student names and classes, as well as email addresses and phone numbers of parents and teachers. Similarly, numerous ransomware and malware assaults have been carried out against different colleges in India during the last two years.[193]

REASONS AND COMMON CYBER THREATS TARGETING EDUCATION SECTOR:

It wouldn't be inaccurate to state that cyber attacks are growing more common in the education industry as more and more breaches in higher education and schools are made public. Because of emerging technologies, we face growing challenges from hackers who are rapidly creating sophisticated ways to perpetrate cybercrimes. As a result, cyber security for the educational sector becomes essential.

There are four primary reasons why cybercriminals target educational institutions. Because educational venues differ widely in terms of size, purpose, and stature, there can be a wide range of reasons why attacks occur. For example, schools or school districts might not be concerned about a hazard that is common at prestigious institutions and colleges.

Distributed Denial of Service or DDoS attacks -- It is common in schools and colleges with perpetrators as young as 9. As per a study conducted by the National Cyber Crime Unit, the average age of DDoS attackers was 15 years. These attacks may be motivated by retaliation for a teacher's poor handling of a particular situation at school or by a dislike of that instructor in particular. A DDoS attack usually affects an organization's network in order to reduce productivity.

Data theft -- For cybercriminals, confidential data is the most precious resource. One of the industry's most frequently targeted by data theft is education. To steal sensitive data, including bank account information, home addresses, and contact details of parents, students, and instructors, they break into protected networks and systems of educational establishments. Once they have access to this data, they either use it as leverage to demand ransom from victims or sell it to other parties.

Financial gain -- Since private educational institutions manage thousands of students' money, financial gain is a major motivator for cybercrimes. In the post-pandemic period, parents and students are increasingly using online portals to pay tuition fee to the increased digitization of education. In order to secure these portals and stop cybercrime, educational institutions must collaborate with cyber-security experts.

Espionage -- The other motive of cyber criminals who want to meddle in school networks is espionage. There are a lot of universities and colleges home to priceless research work and Intellectual Property. The educational networks are often hacked by cyber criminals for the purpose of stealing research work. And then they sell this for a lot of money in the black market.

[193] Diwakar Dayal, Cyber Risks in the Education Sector: Why Cybersecurity Needs to Be Top of the Class, Jan 19,2022, available at: https://www.digitalfirstmagazine.com/cyber-risks-in-the-education-sector-why-cybersecurity-needs-to-be-top-of-the-class/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER THREATS TARGETING THE GLOBAL EDUCATION SECTOR:

The report titled 'cyber threats targeting the global education sector' was compiled by the threat research and information analytics division of the Singapore based CloudSEK which manages digital risks to companies though artificial intelligence. The report reveals that globally, the education sector saw 20percent more digital threats in the first 3 months of 2022, as compared to the same period in 2021. The reasons for this were the adoption of digital methods in remote learning during the covid pandemic. By 2025, CloudSEK data says, the global education and training market is expected to reach $7.3 trillion, a growth rate which has doubled from 2019 to 2025. A significant section of the growth is in the education sector especially in developing countries. This growth, in turn, has attracted several cybercriminals.

Over 58 percent of the threats in Asia and pacific were found in India or India-based educational institutions followed by Indonesia which accounted for 10 percent of the attacks. This included attacks on BYJU's, IIM Kozhikode and TamilNadu's Directorate of Technical Education. Apart from India, globally, the US attracted the highest number of such threats accounting for 86 per cent of threats in North America. "These include Ransomware attacks on prestigious institutions such as Howard University and University of California. In addition high risk API vulnerabilities were uncovered in Coursera, the report said.[194]

Among the steps that the company has outlined for institutions to adopt to stop such attacks, is the not clicking on suspicious emails, messages and links; not downloading or installing unverified apps; using strong passwords and enabling multi-factor authentication (MFA).

EDUCATION SECTOR ATTACKS:

- ✓ **University of California, San Francisco**

AnNetWalkerRansomware attack in June 2020 involving the University of California, San Francisco (UCSF) medical school let cybercriminals encrypt data stored on the school's servers, where the cyber criminals demanded $1.14 million. The criminals agreed to accept $1,140,895 paid via 116.4 bitcoins when the negotiations concluded. In exchange, UCSF received decryption software to unlock its data.

- ✓ **Michigan State University**

A cyber attack involving NetWalkerransomware targeted Michigan State University in May 2020. A blame game followed. The university's IT department alleged that attackers gained access when IT employees in the physics department failed to install a patch for a virtual private network (VPN). However, the department's IT team said it was not to blame, indicating that it lacked resources and direction from the central IT department. The attackers demanded $1 million. Shortly after the breach became public knowledge, the university announced it would not pay the attacker's ransom.

In response to the attack, the university has centralized IT resources. It also instituted additional protections, including supporting VPNs via the university's central IT department, employing multi-factor authentication, and restricting user access.

- ✓ **Illuminate Education, New York City, New York**

In January 2022, cybercriminals targeted the school management platform Illuminate Education and gained access to a database containing personal information on more than 820,000 current and former NYC students. The attack took the New York public school system's online grading and attendance system offline for several weeks. The ransomware demanded was not reported but was not paid by the university. Almost 8,20,000 people were affected in this attack.

[194] Indian education sector biggest target of cyber threats: Report, 1 May 2022, available at: https://www.deccanherald.com/india/indian-education-sector-biggest-target-of-cyber-threats-report-1105555.html

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

✓ **Broward County Public Schools, Florida**

An attack on March 7, 2021, exposed the personal information of approximately 50,000 students and employees of the Broward County public school system, including names, dates of birth, Social Security numbers, and healthcare-related information.

The perpetrators demanded a ransom of $40 million to relinquish control of the school system's data, which officials declined to pay. The district did not release details regarding the attack to protect "the integrity of our data security."

✓ **Howard University, Washington, D.C.**

A ransomware attack forced Howard University to cancel online and hybrid classes in September 2021. The university's response included shutting down its campus Wi-Fi. Days after the attack, online and hybrid classes remained canceled, and the university's Wi-Fi was still offline. Later The University upgraded its cloud-based security, deployed upgraded routers and connectors, and installed a new wireless network.

PAKISTANI ATTACK:

The Pakistan-based group (dubbed as APT36) is using a malicious file titled "Revision of Officers posting policy" to lure the Indian Army into compromising their systems. The file is disguised as a legitimate document, but it contains embedded malware designed to exploit vulnerabilities.
A group from Pakistan that is well known has been found to be responsible for a new series of cyber attacks, as revealed by Indian security researches.These attacks targeted the Indian Army and the education sector. A group called Transparent Tri be from Pakistan has been attacking the government and military of India since 2013. A report by Seqrite, a company from Pune called Quick Heal Technologies, has confirmed this.

Furthermore, the cyber-security team has also observed an alarming increase in the targeting of the education sector by the same threat actor. Since May 2022, Transparent Tribe has been focusing on infiltrating prestigious educational institutions such as the Indian Institutes of Technology (IITs), National Institutes of Technology (NITs), and business schools.The subdivision of the Transparent Tribe, known as SideCopy, has also been identified targeting an Indian defenceOrganisation. Their modus operandi involves testing a domain hosting malicious file, potentially to serve as a phishing page said the researchers.

APT36 has cleverly utilised malicious PPAM files masquerading as "Officers posting policy revised final". A PPAM file is an add-in file used by Microsoft PowerPoint.Seqrite recommended some preventive measures such as exercising caution while opening email attachments or downloading files, especially if they are unsolicited or from untrusted sources."Regularly update security software, operating systems, and applications to protect against known vulnerabilities. It is also important to implement robust email filtering and web security solutions to detect and block malicious content," the team advised.[195]

INDIAN LEGISLATION:

➢ **National Cybersecurity Policy, 2021:**

The Indian government has developed the National Cybersecurity Policy in order to create a strong security framework. Additionally, the government is actively considering a comprehensive National Cyber Security Strategy for 2021. The All India Council for Technical Education (AICTE), the highest authority for technical education, has developed a strategy for institutions across the country in accordance with existing policy. According to AICTE norms, students and teachers should utilise their own accounts and

[195] Jun 24, 2023, Pak-Based Hackers Target Indian Army, Education Sector In New Cyber Attack, available at: https://zeenews.india.com/technology/pak-based-hackers-target-indian-army-education-sector-in-new-cyber-attack-2626212.html

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 3 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

practise cyber sanitization as directed by their respective institutes. It is recommended that students and faculty adhere to needed account management policies and do not tamper with their own requirements. Students are advised to notify institutes in the event of any misconfiguration. Furthermore, students and professors should not use any form of user account circumventing tactics and should adhere to all rules of Information Technology Act, 2000 and all applicable laws.

Similarly, the Ministry of Home Affairs is implementing a cybersecurity education scheme for school students of classes 6 to 11 and above with an aim to deal with cybercrimes. Schools are organising workshops, seminars, and interactive sessions under this programme in their bid to spread awareness.

- **The Digital Personal Data Protection Act of 2023 (DPDP):**

On August 11, 2023, the Indian Central Government passed the Digital Personal Data Protection Act (DPDP). The act was enacted following principles from the EU's General Data Protection Regulation (GDPR) and aims to protect data principles and restrict the activities of data fiduciaries.

- **Information Technology Act, 2000:**

- **Sec.43** of the Act deals with the unauthorized access, denial of service, spreading virus, malware, etc.
- **Section 43A** of the IT Act, Indian businesses and organisations must have "reasonable security practices and procedures" to protect sensitive information from being compromised, damaged, exposed, or misused.
- **Section 72A** of the IT Act, any intermediaries or persons that disclose personal data without the owner's consent with ill intention and causing damages are punishable with imprisonment which extend up to three years, a fine of up to Rs500,000, or both.
- **Sec.66C and 66D** deals with the punishment for identity theft and cheating by impersonation.
- **Section 70B** deals with CERT-IN (Indian Computer Emergency Response Team) which was brought by Indian government and respond to any cyber attacks immediately. And many nodal agencies area appointed to protect critical information infrastructure.

INTERNATIONAL CONVENTIONS:

- **Universal Declaration of Human Rights (UDHR)**[196]and **International Covenant ofCivil and Political Rights (ICCPR**)[197] says about right to privacy where no one shall shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
- **Budapest Convention**, also known as cyber convention has provisions from Article 3 to 8 relating to concepts of illegal access, denial of access, data interference, system interference, computer fraud and computer forgery to prevent the crimes through which many of the cyber crimes being committed.

CONCLUSION:

In order to protect the data, services and users in education organisations it is vital that we develop a comprehensive and coherent strategy. With the evolving threats environment and with resource constraints, it is necessary for authorities to understand their risks in line with existing government guidance.The threat posed by cybercriminals, especially those who are skilled in launching cyber attacks, is becoming even more evident as the digital footprint of education institutions grows to meet both

[196] Universal Declaration of Human Rights (UDHR), 1948, Article 12
[197] International Covenants on Civil and Political Rights (ICCPR), 1966, Article 17

faceto face and distance learning needs. Protecting against ransomware or any other form of cyber attack means having access to and supported by a 24/7 expert team is necessary. With the rise of cybercrime, cybersecurity courses are becoming increasingly popular in university curricula and cybersecurity jobs are in high demand. With accredited degree programs, one can learn how to protect data and build a career in cybersecurity through courses that focus on concepts that give you authority to build secure systems.

REFERENCES:

STATUTES:

- Information Technology Act, 2000
- Digital Personal Data Protection Act, 2023

CONVENTION:

- Universal Declaration of Human Rights (UDHR)
- International Covenant ofCivil and Political Rights (ICCPR)
- Budapest Convention

WEBSITES:

- www.digitalfirstmagazine.com
- www.zeenews.india.com
- www.deccanherald.com
- www.ptinews.com
- www.arcticwolf.com
- www.telegraphindia.com