



CYBER SECURITY: WHY IS IT IMPORTANT FOR EDUCATIONAL INSTITUTIONS?

Increasing threats from cyberattacks have become a grave matter of concern for educational institutions across the country. **Namrata Hazarika** from **Elets News Network (ENN)** highlights the importance of cybersecurity in the education sector.

After the Covid 19 pandemic, there has been an immense growth in the use of e-learning platforms, which has further accelerated cyberattacks in the education sector. A report from the security research firm CheckPoint stated, India's education sector has witnessed an average of 5,196 attacks weekly per organisation in July. For this reason, educational institutions should not overlook the threats from cyberattacks.

As educational institutions are focusing on online learning, there is tremendous data and personal information that are being shared

by parents, students and teachers. This information is prone to be mishandled by cybercriminals. So, educational institutions need to be well prepared for handling any types of cyberattacks and malicious activities online.

Hersh Shah, CEO, Institute of Risk Management, India Affiliate said, "This mirrors cyber-attack patterns in South Asia where the education sector was the most targeted by malicious players. These figures highlight the risk the Indian education sector is facing in cyberspace and the need for qualified risk managers to play their part."



"This high incidence can be attributed to the increased dependence of educational institutions on digital infrastructure, further aggravated by their vulnerability to attacks due to inadequate cybersecurity provisions. The consequences of a cyber-attack can be crippling, causing disruptions to learning, opening opportunities for fraud, and more worryingly, posing a threat to the safety of students. For instance, laptop or phone cameras that are used for classes can be accessed by hackers, as has been the case many

“Cyberattacks were never restricted to just one sector. Recently, it has been witnessed how top universities and schools across the globe suffered ransomware attacks and had to hand over big sums to the attackers.”



HIMANSHU TYAGI
CEO
Digikull

“Any industry that has gone digital is aware of the possible hiccups. The rate of cyberattacks has grown multifold over the years and increased due to the pandemic



“The consequences of a cyber-attack can be crippling, causing disruptions to learning, opening opportunities for fraud, and more worryingly, posing a threat to student safety.”



HERSH SHAH
CEO
Institute of Risk Management
India Affiliate

times since last year with hackers accessing Zoom classes.” he added.

Prioritizing Cyber Security in Educational Institutions

To maintain the safety of young children, it is imperative that we prioritise cybersecurity in educational institutions and spread awareness. Going forward, the educational institutions will continue with e-learning, creating vibrant learning and teaching cultures in the classroom.

Further, pointing out his views, Himanshu Tyagi, CEO, Digikull, said, “Cyberattacks were never restricted to just one sector. Recently, it has been witnessed how top universities and schools across the globe suffered ransomware attacks and had to hand over big sums to the attackers. Similarly, malware attacks are more frequent than one can think.”

“Any industry that has gone digital is aware of the possible hiccups. The rate of cyberattacks has grown multifold over the years and increased due to the pandemic,” he added.

There are dangers like data breaches, ransomware attacks, data theft, widespread disruption, espionage including others, which is impacting the education sector adversely. Also, it seems that Indian educational institutions lack the necessary infrastructure and know-how to ward off cybersecurity threats.

“In a traditional brick-and-mortar model, online dangers would be minimised. However, as this scenario has morphed greatly since the pandemic began, the need to close off these gaps in digital security has been exacerbated. It is also true that shoring up defences against such risks requires a certain level of investment, both financially and in terms of personnel,” added Shah.

He also added that the situation is now changing rapidly as institutions are beginning to understand the permanence of the hybrid education model, and are slowly refitting their capabilities to adapt. “Recently,

“ Yes, on cybersecurity, most from the education fraternity are genuinely less aware or selectively unaware. ”



SUDHANSU M NAYAK
Head Cybersecurity &
Cyber Forensics
CMS IT Services

“ With education moving online, children also have become more vulnerable to cyberattacks. ”



SANJAY TYAGI
Chairman
St. Froebel School

the University Grants Commission (UGC) also instructed all Higher Education Institutions (HEIs) to facilitate and encourage cybersecurity awareness as part of their curriculum. By throwing the spotlight onto this critical issue, the UGC has helped to foster awareness of this risk to business and management education, and we will see a change, both in how early we teach cybersecurity as well as in how educational institutions deploy protective resources,” he said.

Spreading Awareness Among Youth

The question is: ‘How do we spread awareness of cyber security currently?’ Commenting in this context, Sudhansu M Nayak – Head Cybersecurity & Cyber Forensics, CMS IT Services, said, “Yes, on cybersecurity, most from the education fraternity are genuinely less aware or selectively unaware. In absence of stringent legal, regulatory, or statutory compliances in action, decision-makers from the education fraternity work with progressively diminishing cybersecurity priorities and gravitate towards assigning low funds and resources towards securing data. In many areas, there is genuine lack of awareness between students, faculty, and the administration.”

Nayak mentioned that the introduction of cybersecurity courses in school, college, and university curriculum and cybersecurity training delivery to students, faculty, and administrative staff can greatly

increase cybersecurity awareness across the spectrum. Promoting students to run voluntary cybersecurity clubs in their cities, towns, and villages will increase traction among youth.

He also suggested that nodal national agencies like the National Association of Software and Service Companies (Nasscom) or Indian Computer Emergency Response Team CERT-In can conduct an educational simulation of Model Vulnerability Assessments and Penetration Testing M-VAPT or Cybersecurity breach and incident response exercises in controlled environments. This has the potential to generate immense interest in cybersecurity among school-going children. To create a minimum cybersecurity safeguards baseline in all institutions, the Ministry of Electronics and Information Technology (MeiTY) and Ministry of Education (MoE) should come together with the decision-makers in the education sector and create a set of controls, policies, and compliance guidelines.

Minimising Cyber Risks

Sanjay Tyagi, Chairman, St. Froebel School, said, “With education moving online, children also have become more vulnerable to cyberattacks. With many educational institutions holding a wealth of personal and financial data about their students, staff and administrators, cybersecurity is a major issue. The primary issue is lack of awareness !”

“With the shift to online learning, schools and educational institutions must create safe and robust cyberspace for both their students and staff. Threats can be minimised by giving training to all using the Internet in safety measures. Multi-factor authentication is another way to secure apps and websites. It is a cost-effective measure and helps to prevent unauthorised access. Cybersecurity campaigns and workshops should be conducted,” he added.

Shah also said, “The first step should be to formulate a cyber risk policy that lays down a cyber-security framework with the procedures to follow in case of a cyber-attack. The second step involves facilitating and encouraging risk intelligence through continuous training of various stakeholders, including educationists, institutional staff and employees, and students.”

“The United Nations had earlier warned that the increase in screen time during the pandemic could also result in a surge of harmful online activities targeted at children. Other than potential exposure to harmful or violent content, the internet can also be used by malicious players for sexual exploitation, grooming and cyberbullying,” Shah also added.

Experts believe that it is also the responsibility of educationists to teach students responsible online behaviour. Since most students now spend the majority of their time online, whether for educational, social, or recreational purposes, they must be taught about harmful online behaviour that can put them at risk. Without trained risk officers, inadequate and ineffective training of faculty and ignorance of security measures are some issues that make educational institutions vulnerable to cyber attacks.

Monitoring the current scenario is certainly the utmost priority for educationists. Increased investment and resources are the need of the hour to reduce the risk of cyberattacks.