Exploring Cyber Threats and Digital Risks

to Indian Educational Institutions

CyberPeace

CyberPeace is the world's first non-profit civil society organisation and think tank of cyber and policy experts with the vision of pioneering CyberPeace initiatives to build collective resilience against cybercrimes, global threats of cyber warfare. Key areas of CyberPeace Foundation work are in Technology Governance, Policy Review and Advocacy, Capacity and Capability creation and building through partnerships with various government organisations, academic institutions and civil society entities.

Title: **Exploring Cyber Threats and Digital Risks in Indian Educational Institutions**

Editor: **Maj Vineet Kumar**

ISBN Digital: 978-93-340-8660-7

ISBN Print: 978-93-340-8890-8

Published by: CyberPeace, Plot No. B-55, Harmu Housing Colony, Ranchi
Jharkhand, Pin- 834002

https://www.cyberpeace.org/

TABLE OF
Contents

SECTION 1

Introduction

> My message to the companies that think they haven't been attacked is - you aren't looking hard enough.
>
> —— James Snook

In today's fast-paced digital world, it is next to impossible to be immune to cybercrime. Any entity that collects or shares user information can easily be the next victim. In this context, CyberPeace has studied the cyber threats and digital risks faced by Indian educational institutions as they expand their digital infrastructure to include online learning platforms, digital student records, and virtual administrative systems.

What is the Context of this Study?

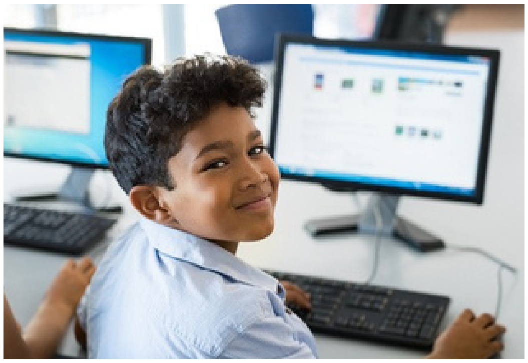
Cybercrime is diversifying into different sectors such as education and health, with large-scale implications on human safety, security, and well-being. With increased digitisation, educational institutions such as schools and universities world- over have become prime targets of cyber attacks due to their extensive collection of personal records and lack of cyber-risk awareness. There is an unprecedented increase in the scale and number of cyber-attacks globally and institutions must practice digital hygiene to address their safety and security needs.

Technology is valuable and unavoidable in modern learning environments. Rapid digitisation of educational institutions makes learning more interactive, accessible, and personalized to each student's unique learning pace and style. However, the integration of technology brings unique security and safety challenges which educational institutions may often be ill-equipped to tackle, making them susceptible to cybercrime targets.

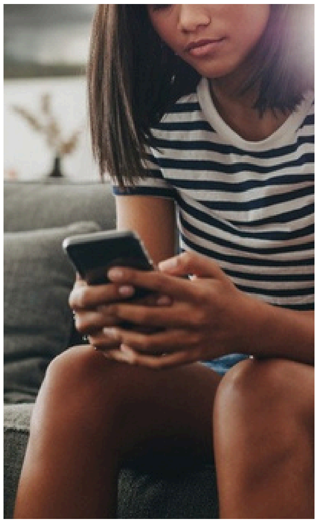
A cursory glance at news reports on cyberattacks on educational institutions reveals that they have been on the rise over the last few years, particularly since the beginning of the pandemic. What makes educational institutions susceptible to cyber-attacks and threats? Why do cybercriminals attack organisations that largely cater to students, both children and young adults, for their learning and development?

Educational Institutions and Issues Surrounding Digitisation

Educational institutions vary widely based on factors such as the level of education offered, class sizes, student-teacher ratios, geographic location, socio-economic context, degree of digitization, type of infrastructure, and the presence or absence of digital safety policies. Given India's size and diversity, multiple typologies of educational institutions can be developed by examining different combinations of these characteristics.



The increased adoption of technology by schools and colleges over the last few years due to pandemic-induced lockdowns has resulted in schools, colleges, and universities introducing digital, remote, or online learning. Higher educational institutions, too, have become increasingly digitised, and not just as a result of the pandemic. They are increasingly technologically connected with the provision of WiFi support, online learning platforms, digital libraries, virtual classes, and video conferencing facilities. For ease of administrative support and scaling up of educational institutions, there has been an increase in the amount of data stored by educational institutions, such as personally identifiable information (PII) of students, teachers, and staff. Such information, depending on the region under consideration, includes student records, financial information, unique identification numbers, grades, and health records.



Volumes of such information can be a goldmine for cybercriminals, making educational institutions prime targets for cyber attacks. Apart from the large volume of data they manage, Higher Education Institutions (HEIs) networks are often open in design, decentralised, and have a large number of users. HEIs also contain repositories of confidential cutting-edge research data. Such research conducted by universities consists of valuable intellectual property that can be sold by cyber criminals on the dark web for millions of dollars. Such data can even be encrypted (which prevents victims from accessing their files or systems) as part of a ransomware attack and threatened to be destroyed or uploaded on the dark web if the institution fails to make exorbitant payments for the same.

Although the pandemic gave a huge impetus to cyber attackers to intercept networks of educational institutions, such attacks began much before the pandemic.

In a pre-Covid-19 case, the University of Calgary in Canada paid $20,000 in response to a cyberattack on its computer systems that encrypted staff and faculty emails. In the aftermath of this attack, an associate professor of the university's Computer Science department shared that while incidents of ransomware go back to the '80s, the attacks have become increasingly sophisticated such that once the files are encrypted, it is next to impossible to decrypt it.

The specific factors that characterise the networks of educational institutions, along with the intensity of threats, render their vulnerabilities quite different from that of other organisations. Unlike the websites of major companies and governments, university and school websites often lack adequate cybersafety and security mechanisms, making them easy to penetrate. The primary reason for the slow adoption of cybersecurity measures is insufficient funding. As a result, there is little, if any, investment in cyber solutions and a resulting use of outdated technology. According to a cybersecurity assessment of K-12 (kindergarten through grade 12) schools in the US of the year 2021-2022, an average K-12 school district dedicates eight percent or less of their IT budget to cybersecurity while one in five respondents shared that their cybersecurity spending amounts to less than one percent of their IT budget. Apart from these reasons, there are many more that render educational networks vulnerable and susceptible to cyber attacks. We shall consider these factors in detail in this report.

The Global Nature of Cyberthreats to Educational Institutions

To gain an aerial understanding of the issue, let us consider some statistics. In a study conducted in the quarter from April to June 2023 in India by malware analysis lab SEQRITE, the education sector emerged as the most targeted one for cyberattacks, followed by the manufacturing and professional services industries. The education sector accounted for over seven lakh detected threats while manufacturing, which stood second, reported a much lower number of 3.29 lakh.

In March 2023, the Cybercrime Wing of the Chennai police detained a suspect based on a complaint by the School Education Department that said that the personal details of school students were sold by an individual to third parties. Details such as names and contact information of private and government school students from 20 districts were allegedly sold by the individual for which the latter received online payments. Not only did this sale violate the privacy of the students, but it also put their safety and security at risk, according to the complainant.

Over the past several years, this has become a global issue, with the fallout being faced by multiple nations. For example, in the US, K-12 schools have reported significant educational impact as a result of cybersecurity related incidents over the past few years. Further, according to the European Repository of Cyber Incidents, the sectors most targeted by cybercrime in 2023 in the order of number of incidents were critical infrastructure (comprising energy, telecommunications, transport and health), followed by state institutions and political systems, education, corporate targets, media and others.

Cyber attacks can cause severe financial losses for affected schools and colleges from the downtime and resources required to recover from them. A report by IBM and Ponemon Institute found that in 2020 the education sector faced a loss of $3.9 million for data breaches. Another study by CheckPoint (that provides cybersecurity solutions to governments and corporations globally) found that the average number of weekly cyber attacks per academic organisation in July and August 2020 increased by 24 percent, while the overall increase in the number of cyber attacks in all sectors in Europe was only nine percent. Verizon's 2022 Data Breach Investigations Report revealed that the educational services sector experienced 1,241 incidents in 2021, with 282 involving confirmed data disclosure. Of that number, 75 percent were from external sources, while the rest came from insiders. A whopping 95 percent of these tracks had a financial motive. As we shall see through this report, prevention of attacks against the cyber defences of digital educational systems will prove to be more effective than a reactive stance.

Loss of $3.9 Million for Data Breaches

24% increase ↗

average number of weekly cyber attacks per academic organisation in July and August 2020

1,241 incidents in 2021 ⚠

Verizon's 2022 Data Breach Investigations Report - Educational services sector

Purpose of the Study

Given the scale, intensity and frequency of cyber attacks against educational institutions, we believe that the time is ripe for an exploration not just into what is happening, but to also reveal the magnitude of the issue and how it impacts the stakeholders involved. This is the crux of the purpose of this timely and relevant research report. Here, we will aim to understand why such incidents occur, what the specific risks and challenges are, and how these can be overcome. We shall also consider the stakeholders in this matrix and how cyber threats and incidents can and do affect them. Since the issue is global and devoid of boundaries, we shall discuss cases and solutions from different parts of the globe. At the same time, some specific issues particular to the Indian context will also be shared.

This research report will be of interest to anyone who is directly connected to the cyber safety of educational institutions, such as educators, management of educational institutions at all levels, cyber security professionals, students, parents and the government. This report will also be beneficial for cyber safety researchers and others who work directly and indirectly with stakeholders in schools and colleges such as counsellors, journalists and civil society.

SECTION 2

Significance of the Study, Research Objectives and Methodology

> ❞ If it’s known, it’s manageable. If it’s well-known, it’s actionable.
>
> —— Bradley B Dalina

It is within the context and background shared in the previous section that we set out to explore the impact of cyber threats and attacks against educational institutions. A deeper and better understanding of the specific vulnerabilities of educational institutions allows for solutions to be prescribed towards protecting not just sensitive data but also the privacy of students, teachers and staff. This serves as a significant undertaking as recovering from cyber attacks may not be fully possible either financially, emotionally or otherwise. Cyber attacks leave a trail of destruction whose effects cannot be undone. One’s best bet as governments, institutional management and other stakeholders is to find ways to protect the privacy of the personal information of stakeholders, the intellectual property of HEIs and the integrity of institutional data systems.

Objectives

Through this exploratory study, we aim:

01 To identify the types and gravity of cyber threats in Indian educational institutions

02 To evaluate how well-prepared Indian educational institutions are to manage cyber threats and where their weaknesses lie

03 To investigate how cyber threats affect the universities' education and management activities

04 To suggest ways and strategies to strengthen cybersecurity in Indian educational institutions

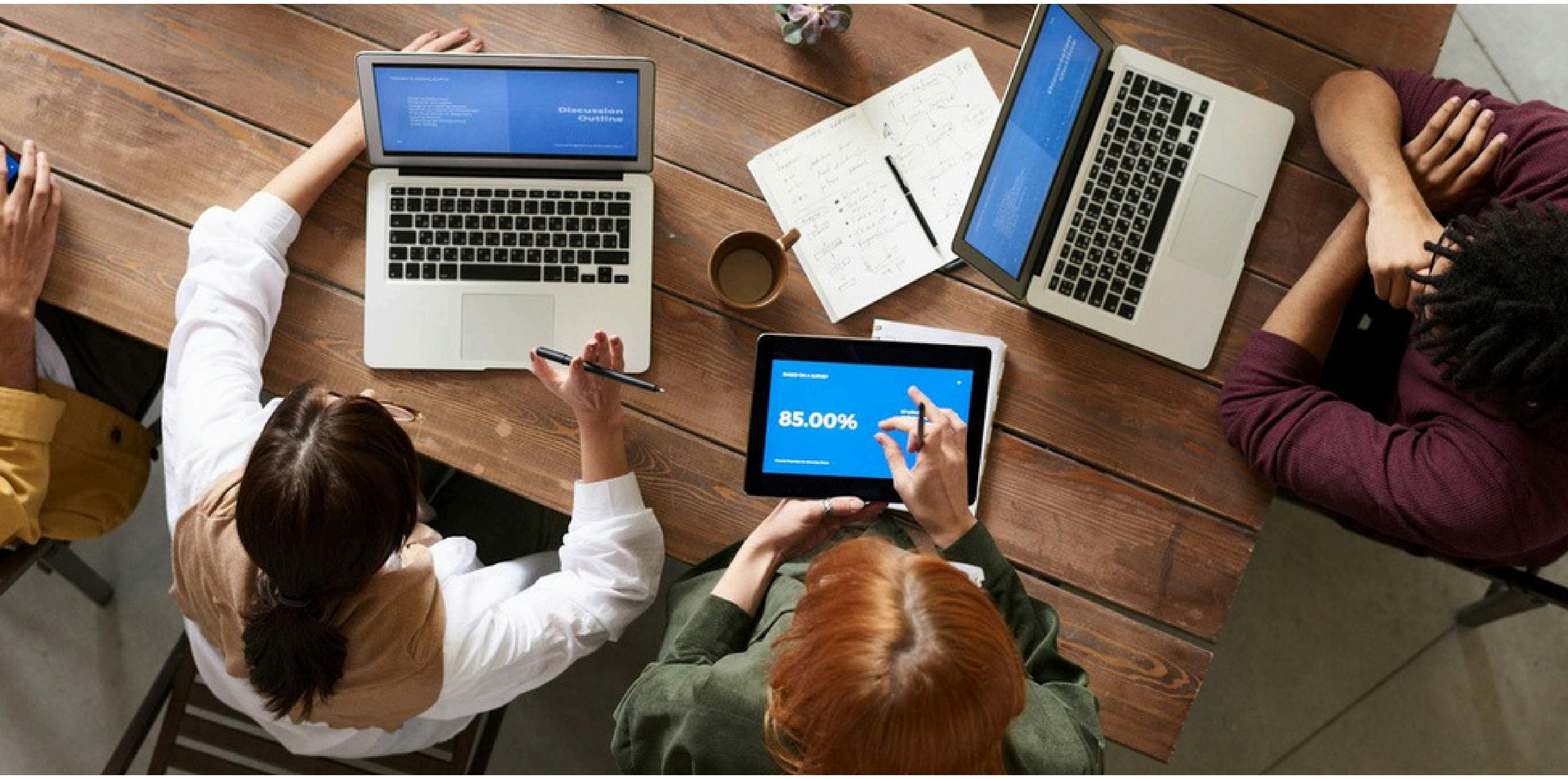
The hypothesis we are setting out to test is that incidents of cyber threats in educational institutions are increasing, with limited knowledge within institutions to protect themselves.

Methodology

This report draws insights from a comprehensive review of media reports, academic studies, and industry articles to assess the scale of the issue, identify key stakeholders, and explore effective solutions and best practices for safeguarding privacy, data, and intellectual property.

The research is conducted under CyberPeace's e-Kawach project, an initiative aimed at strengthening cybersecurity infrastructure through a nationwide deployment of public network and threat intelligence sensors. These sensors are designed to monitor internet traffic and analyze real-time cyber threats targeting specific locations and organizations.

The study examines cyber incidents and trends over a nine-month period (July 2023 – April 2024), providing data-driven insights into emerging risks and mitigation strategies.



SECTION 3

Global Overview of Cyber Threats in Educational Institutions

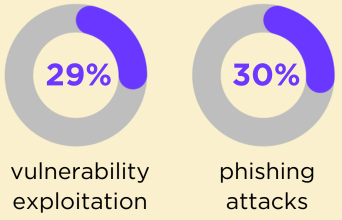
The Magnitude of the Issue

How big is the issue surrounding cyber safety of schools, colleges and universities? Was this a problem only during the peak of the pandemic-induced lockdowns or is it something one must continue to be cautious about? As mentioned briefly earlier, cyber threats, risks and attacks against educational institutions existed prior to the pandemic but became a very real issue ever since Covid-19. However, we will not be able to wish it away. The continual adoption of technology will only make this issue more real henceforth and stakeholders will find it in their interest to take it very seriously and give it the priority it now demands.

To understand the urgency of this, let us consider some statistics. Based on its survey of 1610 IT and security professionals from over 100 countries, cybersecurity company Netwrix found that 69 percent organisations in the education sector had suffered a cyberattack in the 12 months preceding the survey in 2023.

Phishing and user account compromise were the most common attack paths faced by these organisations, according to the report. It further found that three out of four attacks (or 75 percent) in the education sector were associated with a compromised on-premises user or admin account, compared to 48 percent for other sectors. According to an article by Forbes, in 2021 and 2022, education and research institutions faced the highest attack volumes each month in comparison to other industries. For K-12 schools, the threats came primarily from vulnerability exploitation (29 percent) and phishing attacks (30 percent) (Gurinaviciute, 2024).

3 out of 4 attacks
in the education sector were associated with a compromised on-premises user or admin account

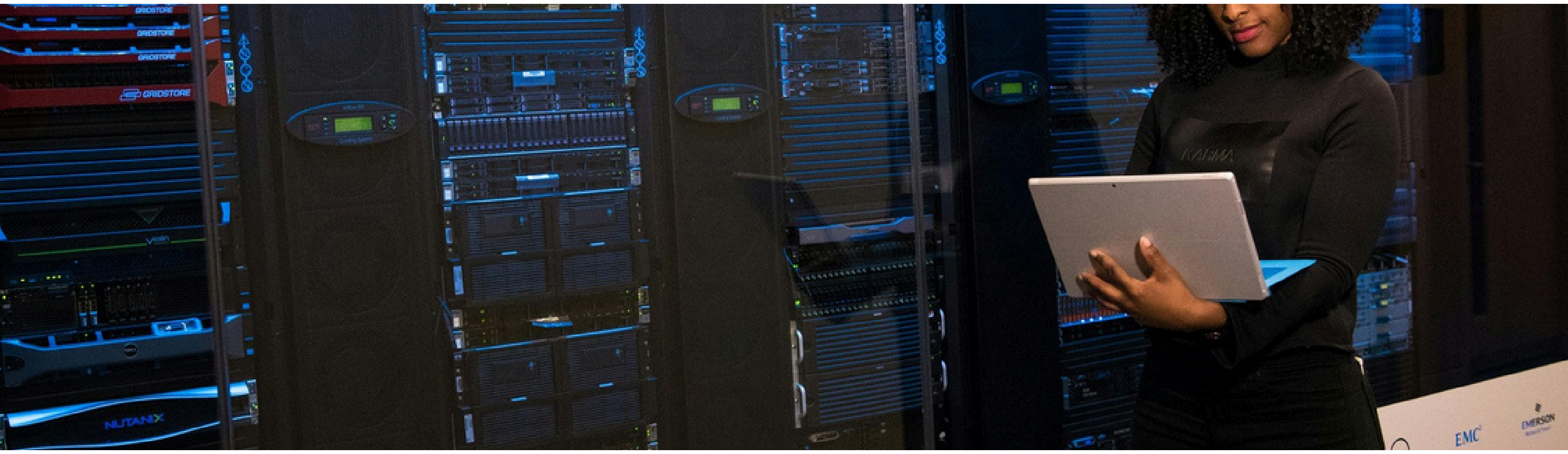


In fact, according to a report from 2017 on cyber threats to small and medium businesses, 96 percent IT decision-makers believe their organisations are susceptible to external cyberattacks and 71 percent say they are not prepared to cope with them. If businesses were in a state like this, the education sector would not be in a much better place. Why is this so? Primarily because the information possessed by educational organisations grows per year and there's an increase in the adoption of technology. Thus, it isn't viable any longer to safeguard this volume of sensitive information in servers that don't have requisite protections.

Downtime costs of over $53 billion

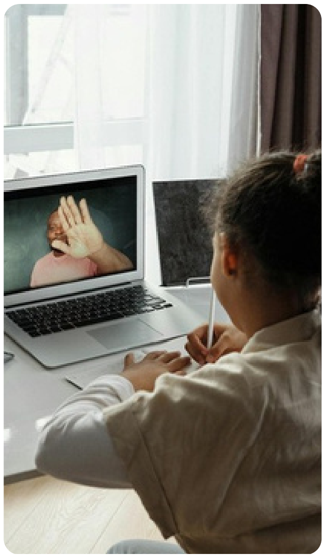
Caused by ransomware incidents in schools and higher education institutions globally from 2018 to mid-September 2023

According to the IBM Report on the Cost of Data Breaches from 2023, critical infrastructure organisations (which includes the education sector), incurred data breach costs that were USD 1.26 million higher than the average cost for organisations in other industries (indicating a 28.6 percent difference). Infosecurity Magazine found that in 2023, 29 percent of attacks on educational institutions exploited vulnerabilities and 30 percent involved phishing campaigns that targeted K-12 schools. Further, ransomware incidents in schools and higher education institutions globally from 2018 to mid-September 2023 led to the breach of over 6.7 million personal records causing downtime costs of over $53 billion.



Why Educational Institutions are Vulnerable to Cyber Attacks[1]

As a precursor to examining the specific threats that educational institutions' networks are often exposed to and at risk for, it is important to first consider in detail the factors that render them vulnerable in the first place. This not only provides context to our understanding of said threats, it further provides perspective into appropriate responses by all parties involved towards preventing and where required, addressing these issues. Some specific issues faced by educational institutions globally that make them particularly vulnerable are shared below.



1. New learning technologies and endpoints

Covid-19 induced lockdowns saw many schools and colleges turning to online remote learning to keep the learning process going. This led to an increase in attack surfaces through new endpoints (a communication network node) to education networks. Such endpoints are often unvetted personal devices using unvetted connections. The increase in endpoints combined with the simultaneous rapid adoption of new technologies to facilitate online learning led to increase in size and complexity of networks without corresponding increase in cybersecurity measures to protect networks and users. Education systems continue to fail to monitor and protect their networks due to improper cybersecurity practices.

2. Budget constraints

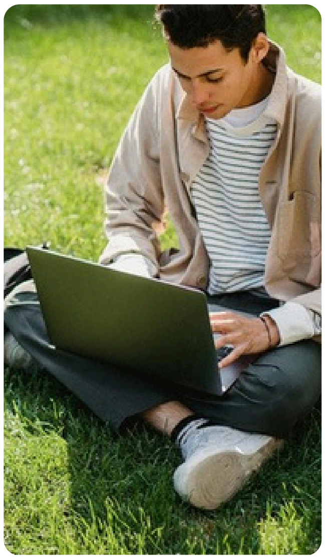
Budgetary constraints play a major role in making schools and universities vulnerable to cyber attacks. Schools, while having low cybersecurity spending, contain personal data that criminals can use to perform identity theft or sell on the dark web. Universities provide them this opportunity along with easy access to ingenious and original research of high quality that can be stolen.

[1] See https://www.upguard.com/blog/education-sector-cyber-attacks and https://www.forbes.com/sites/forbestechcouncil/2024/03/11/what-cybersecurity-threats-does-the-education-sector-face/?sh=2589415b4b90

3. Lack of training and awareness of cybersecurity

Given that schools and universities thrive on values such as collaboration and learning, and the fact that there is a lack of training and awareness on cyber risks leading to decreased exercise of caution in the use of devices and institutional networks, staff, students and institutional mechanisms of educational institutions tend to be at greater risk than other sectors and industries.

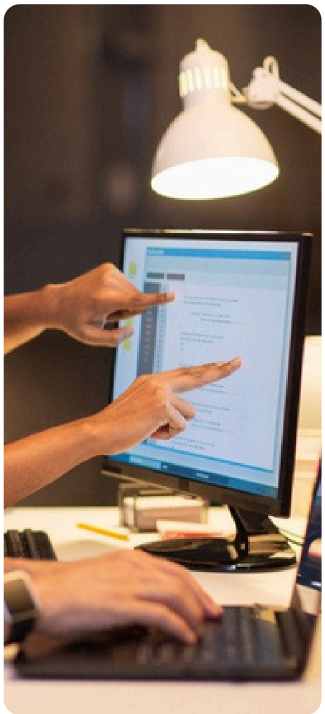
Discussions on issues surrounding cyber security are lacking or altogether absent in educational institutions in general. Additionally, the fact that such networks are storehouses with information on many young people makes them especially of interest to cyber abusers.



4. Use of outdated computing hardware and software

Limited investments into technology and a lack of focus on cybersecurity translates into the use of outdated software and hardware, also known as legacy systems in technological parlance. Such systems are not necessarily obsolete so they continue to work despite being outdated.

Various enterprises often continue to use them if they are critical to their daily functions as they are cost-effective in the short term. Such systems, however, are extremely vulnerable to cyber attacks such as increased risk of unauthorised access and compromise by hackers as outdated hardware is not supported by software developers.

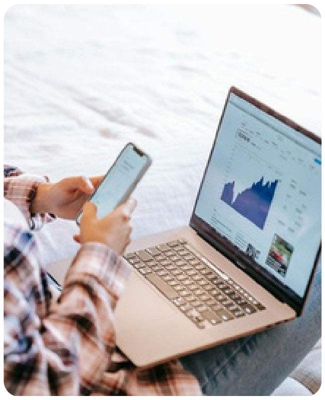


5. Structural issues

An additional issue that plagues large universities is that given that such institutions are large and are segregated into different departments that function autonomously, department heads or others such figures could direct the installation of software or hardware that is required by their department, independent of any central authority. Such a structural issue could make it harder to defend the university as a whole from cyber attacks as an IT professional could find it difficult to identify the source of a cyber attack or maintain adequate controls of and monitor network activities if they don't have full knowledge of all systems in place. This will therefore make it all the more difficult to remediate any issue that might come up as well. Thus, a lack of standardised protocols and procedures, information security policies and cybersecurity practices can lead to increased security gaps and to higher incidence of cybercrime in such institutions.

6. Lack of technical resources

Educational institutions may, more often than not, be devoid of dedicated and full-time resources or a cybersecurity department that can perform activities such as regularly monitoring access, protecting the network and implementing security measures to protect sensitive data. These factors play a major role in increasing its vulnerability to attacks.



7. Use of personal devices

The fact that students and staff in educational institutions make use of their personal devices such as smartphones, laptops and USB drives for projects and assignments presents a large vulnerability to the safety of the network. Such devices could carry malware that can then affect the organisation's network as a whole, leading to potential large-scale ransomware attacks and data breaches.

SECTION 4

Types of Cyber Threats in Educational Institutions

As we've seen, cyber threats and risks are becoming increasingly common and posing worrisome risks for students, teachers, staff and the institution itself. Here we shall consider specific threats in some detail and understand the nature of the risks.

Major Cyber Threats in Educational Institutions[2]

Social engineering (particularly phishing and ransomware)

In the context of cybersecurity, social engineering refers to the process by which cyber criminals trick people into divulging personal or private information that is then used in a cyber attack. It is a manipulation technique that exploits human error to gain private information or access text messages or emails infected with links that direct the user to malicious websites or phone calls by a cybercriminal impersonating tech support or other authorities requesting personal information. Social engineering attacks, including phishing and ransomware, pose the most significant threat to the education sector.

Such attacks are popular as they save the cyber criminal the effort of exploiting network security vulnerabilities as manipulated users hand over credentials to the criminals unwittingly.

Social engineering attacks have two possible goals:

a. Sabotage: to disrupt or corrupt data to cause harm or inconvenience
b. Theft: to obtain valuables like information, access, or money

Attacks use a believable premise to create a sense of urgency and heightened emotions through persuasion (fear, excitement, curiosity, anger or, sadness) to mislead victims and gain trust.

[2] See https://www.upguard.com/blog/cyber-threats-education, https://www.aicte-india.org/sites/default/files/cyber/AICTE%20Cyber%20Security%20Strategy%20for%20Higher%20Education%20Institutes.pdf and https://preyproject.com/blog/cyber-security-threats-it-professionals-in-education-face

- **Phishing:** It is used to gather sensitive or private information like login credentials, bank account details, credit card numbers etc. by criminals who masquerade as a trusted source. Phishing emails or messages are embedded with malicious codes that, when clicked, direct victims to a webpage that is a replica of the website the sender claims to represent. Such fake pages are often difficult to distinguish from the real one. When an unsuspecting victim submits their information, it is sent to a hacker who then uses it to log into the legitimate website. Phishing emails, messages and calls often create a sense of urgency to urge the victim to divulge information quickly. Phishing attempts are often successful despite not being sophisticated in its approach. Phishing takes various forms including spear phishing (an email spoofing attack targeting an organisation or individual), smishing (phishing performed over SMS), vishing or voice phishing (conducted over phone; can be paired with voice deep fakes)

- **Ransomware:** It is a type of malicious software (or malware) that is designed to deny access to a computer system or data until the user pays a ransom amount to the cyber attacker. It can be circulated through phishing emails, malvertising (malicious advertising that inserts a malicious code within digital ads), by visiting infected websites or when an attacker exploits a system's vulnerabilities. It can cause downtime (a period of time when a website is nonfunctional as a result of malfunctions), data leaks, intellectual property theft, and data breaches. Ransom demands can range from a few hundred to hundreds of thousands of dollars.

- **Malware:** Cyber criminals use malicious software (or malware) against educational institutions to gain unauthorised access to their internal systems and bypass information security defences.

Distributed Denial of Service (DDoS)

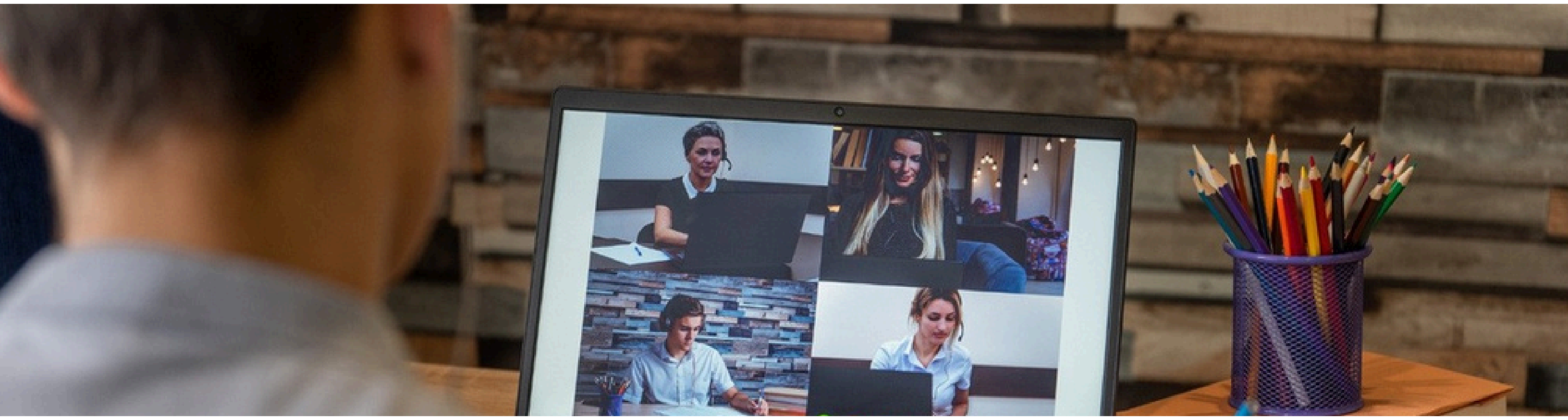
DDoS attacks lead to denial of access for users to various websites and force a server to overload. The motivation for such an attack is to simply cause disruptions to users' day-to-day operations, thus affecting productivity. Such an attack impacts students or teachers trying to access learning resources or submit time-sensitive assignments online. Such attacks are typically easier to carry out compared to others. DDoS attacks are relatively easy to carry out if the target network is insufficiently protected. Hence amateur cybercriminals including an institution's students and teachers might carry out DDoS attacks in an attempt to simply get a day off or to protest something they were unhappy about.

Cyber espionage

Higher education institutions like universities that perform cutting-edge research are particularly susceptible to spyware, insider threat and other forms of cyber espionage. Spyware refers to any software downloaded to a user's device without authorisation. It is therefore, an unwanted software or a malicious software (or malware) designed to expose sensitive information, steal internet usage data or gain access to or damage a commuting device. An insider threat is one that comes from negligent or malicious insiders such as staff, third party vendors, former staff etc. who have inside information about sensitive data, computer systems or cybersecurity practices. The threat can involve fraud, theft of intellectual property or commercially valuable information or misconfiguration that leads to data leaks.

Video conferencing disruptions

Cyberattacks on educational institutions can severely disrupt video conferencing—a critical tool for remote learning. DDoS attacks can overload servers, making platforms like Zoom, Google Meet, or Microsoft Teams inaccessible, while ransomware attacks can lock educators and students out of essential systems. Zoombombing, where unauthorized users hijack online classes, can lead to harassment, data breaches, and a loss of academic continuity. Additionally, phishing attacks targeting school administrators may compromise login credentials, allowing attackers to disrupt sessions or access sensitive student data. These disruptions not only hinder learning but also expose vulnerabilities in the digital infrastructure of educational institutions



Data Thefts

Data thefts affect educational institutions at all levels since they contain different types of data that are of interest to cybercriminals. It includes personal information of staff and students and information on research conducted by the institution. Criminals can use such information to sell it to a third party or use it to extort money from the institution. Theft of university research, which is often scientific, medical, or engineering focused, occurs as it can give the attacker (which could be a professional organisation) an unfair competitive advantage over valuable research without investing time and money into it. Cyber criminals can also conduct such data theft to sell such research on the dark web. Such a form of attack can, unfortunately, go unnoticed for a long time, increasing the vulnerability of unprotected networks. For example, hackers struck the University of California, Berkeley network for several months, during which at least 160,000 medical records were allegedly stolen.

SQL Injection

SQL injection or SQLI is a type of attack that employs malicious code to manipulate backend databases to access information that was not intended for display. This includes items such as private customer details, user lists and sensitive company data. A successful SQLI attack can cause deletion of information, unauthorised viewing of user lists or administrative access to a database.

Eavesdropping attack

An eavesdropping breach, snooping or sniffing is a network security attack in which a cybercriminal tries to steal information that smartphones, computers and other digital devices send or receive. It capitalises on unsecured network transmissions to access data being transmitted. It is challenging to detect such an attack as it does not cause abnormal data transmissions. An attacker can install network monitors (such as sniffers) on a server or computer to perform an eavesdropping attack to intercept data as it gets transmitted.

AI-powered attacks

AI makes cyber attacks such as identity theft, password cracking and denial-of-service attacks more powerful, efficient and automated. It can be used for anything from injuring people, stealing, causing emotional harm and even to affect national security, shut down organisations and cut power supplies to entire regions.[3]

One must note that the types of major cyber threats putlined above are not separate and exclusive in a strict sense; there are overlaps among them. Therefore, the table above is presented to portray a variety of threats and must not be considered as existing in separate and distinct types.

Deep Dive into Cyber Threats in Educational Institutions

So far, we've taken a broad look at the issues of cyber attacks affecting universities and schools. We've seen the reasons that render educational institutions vulnerable, the specific challenges that they face and the prominent cyber attacks that affect them. The impact of such attacks are significant given its scale and frequency are felt not just by institutional and third party actors but by students, teachers and staff, making such issues worthy of further examination and study. There are some patterns that are relatively consistent along with new and upcoming trends observed in India and globally. We shall take a look at them here.

Data and research on cyber crimes against educational institutions is mainly available from the US. So let us consider some statistics from the nation that situates the issue a little better. In December 2021, a vendor for Chicago Public Schools was a victim of a ransomware attack which compromised the personal information of over 500,000 students and staff members. A few months prior to that, in February 2021, a chain of schools in Massachusetts was a victim of a DDoS attack that disrupted teaching and learning on the district's web- based systems. It affected emails, learning platforms and video conferencing services during a time when they were crucial, given classes were conducted remotely owing to the pandemic.

500,000
personal information compromised

A vendor for Chicago Public Schools was a victim of a ransomware attack

[3] AICTE Cybersecurity Strategy for Higher Education Institutes, p. 11. See also India Cyber Threat Report 2023, p.12, 68, 69, 71, 72. See also The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation, p.10.

A similar incident had taken place in September 2020 to a chain of schools in Miami. According to officials from Connecticut, a school district had to shut down for a few days as a result of a cyber incident. The school district was reinfected a few days later owing to another attack. Officials said that the follow-up attack was a result of the failure of the school district's cybersecurity insurance company to provide sufficient recovery response. This shows that stakeholders external to the institution too have crucial roles to play in the protection of educational systems. Cyber attacks and threats to educational institutions also follow different patterns. A study by the US GAO found among affected schools that wealthier, larger and suburban school districts had higher likelihood of reporting breaches.

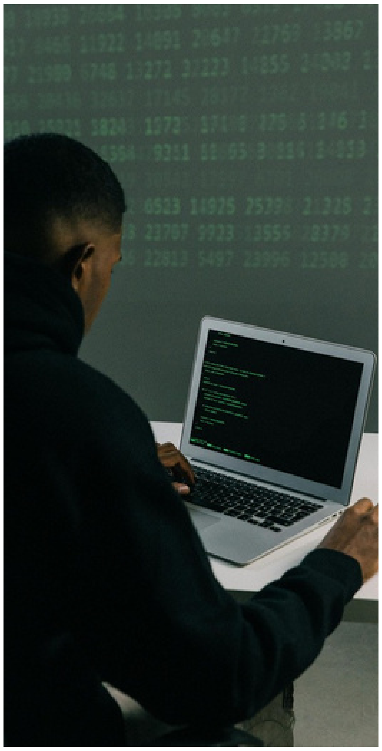
What evidence and reports are available on the state of cyber crimes against educational institutions in India?

10,000
cyberattacks

CERT-In | 2022

As per a report by the Indian Computer Emergency Response Team (CERT-In), the education sector in India has witnessed a significant rise in cyberattacks in recent years. The organisation reported over 10,000 cyberattacks against educational institutions in the year 2022, which primarily involved cases of phishing, malware, and ransomware. These have resulted in data breaches, financial losses, and disruptions to educational activities.

In terms of attack vectors, over 50 percent of detections were associated with removable media and network drives and about 25 percent attacks resulted from clicking on malicious links in emails and websites, according to the India Cyberthreat Report 2023. Cybercriminals creating malware and ransomware attacks have been continually evolving in their methodologies and employing sophisticated techniques to evade traditional signature-based detection. Common threats like phishing and account compromise pose a continuing challenge in educational institutions. Account compromise is a dominant threat as the schools, colleges and universities manage a variety of accounts for staff, students, teachers, alumni and third-party contractors. The malware most prevalent in the education sector was one named W32.Neshta.C8. The trait of this particular malware is that it self-extracts data and executes a dropped binary (indicates an intrusion or malicious activity) and establishes autorun at Windows startup. The education sector comprised about four out of every 10 detections of malware.



Key Insights from Project eKawach:

In a recent study conducted by the Research Wing of CyberPeace, in collaboration with SAKEC CyberPeace Center of Excellence (CCoE) and Autobot Infosec Private Limited, a simulation of educational institutions' networks was performed to gather valuable intelligence on state and non-state actors.

This research is part of the e-Kawach project, an initiative by CyberPeace to deploy a comprehensive public network and threat intelligence sensors across the country. The aim is to capture internet traffic and analyze real-time cyber attacks targeting specific locations or organizations. The study covers the period from July 2023 to April 2024.

217,886 cyberattacks

July 2023 to April 2024

Over the specified period, the deployed network recorded a substantial 217,886 attack events originating from different IP addresses worldwide. A pattern analysis of the attack shows that apart from India, most attacks originated from IP addresses from countries such as the USA, China, Germany, the Republic of Korea, Brazil, the Netherlands, Russia, France, Vietnam, Singapore, and Hong Kong.

However, attribution regarding cyberattacks is complex. There may be some cases where either the actor from another country exploits the resources of that accused country to leave a footprint leading back to the same or they use VPN, proxy technology to mask their real origin. In such a type of provision, it is extremely difficult to make a proper attribution.

Additionally, the analysis identified 8,337 unique usernames and 54,784 unique passwords used in brute force attacks, indicating the extensive use of automated scripts or tools by threat actors. The most frequently used username in the attack is “root” with more than 200,000 attempts and other common user names include “admin”, “test”, “user”, “oracle”, “ubuntu”, “guest”, “ftpuser”, “pi”, “support”. Common passwords such as “123456”, “password” were attempted more than 3,500 and 2,500 times, respectively and the other common passwords include "1234", "12345", "12345678", "admin", "123", "root", "test", "raspberry", "admin123", "123456789", "1234567", "qwerty". This underscores the importance of robust security measures such as multi-factor authentication, network segmentation, and intrusion detection/prevention systems to prevent unauthorized access to critical infrastructure.

217,886
cyberattacks

Total number of attacks

8,337
usernames

Unique usernames used for brute forcing

54,784
passwords

Unique passwords used for brute forcing

"root"
200,000+ attempts

Most common username in attacks include

"123456"
3,500+ attempts

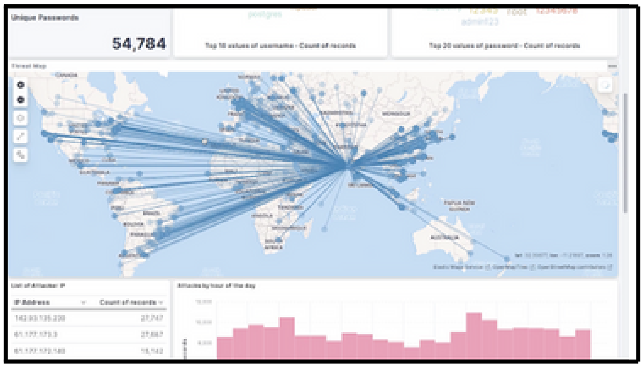
Most common passwords include

"password"
2,500+ attempts

Most common passwords include

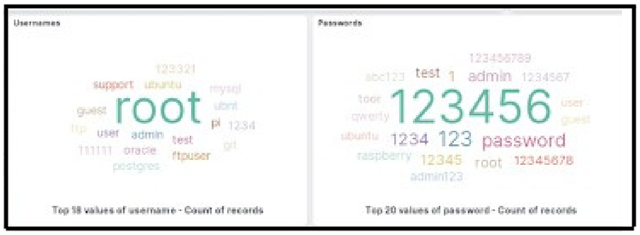
Top Attackers by Country:

The United States, China, Germany, Republic of Korea, Brazil, Netherlands, Russia, France, Vietnam, India, Singapore, Hong Kong.



List of Attacker IP

IP Address	Count of records
142.93.135.220	27,747
61.177.173.3	27,687
61.177.172.140	15,142



Key Insights from Threat Landscape Analysis:

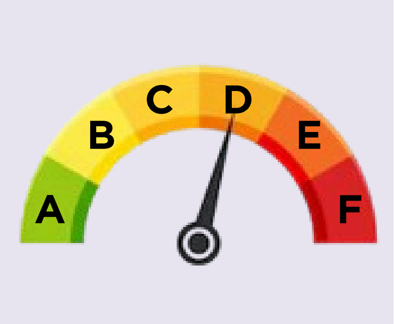
Research conducted by the USI - CyberPeace Centre of Excellence (CCoE) and Resecurity has revealed the presence of several breached databases belonging to some of the Public, Private, Government universities and its associates available on the internet. The investigation highlights the significant cybersecurity threats in the education sector in India.

Disclaimer:

This research is intended solely to identify and mitigate potential cybersecurity risks and is not meant to harm individuals or place blame on any entity. The information provided is based on data available at the time of the research and may evolve as new information emerges.

Risk Rating:

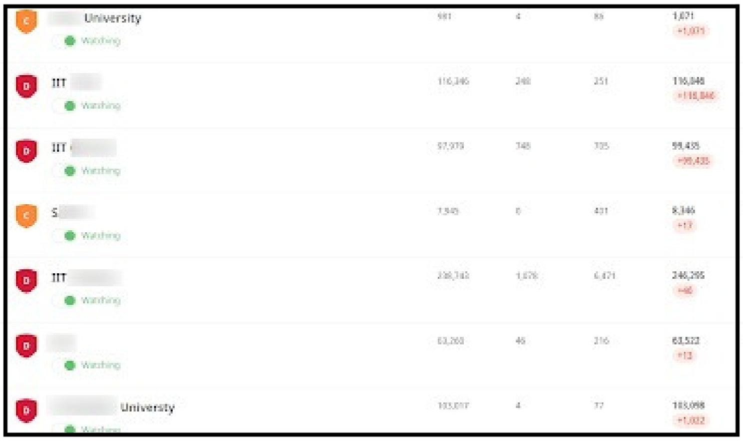
Most of the institutions are in the risk rating of **D** and very few in C as indicated in the below picture. A **D** rating indicates that Risk has detected numerous problems that could compromise security posture. Please review the risk indicators identified below and act upon them immediately.



Risk ratings descend from **A** to **F** as the severity and number of threat indicators increases. Companies with a **D** or **F** rating are 5.4 times more likely to be victims of data breaches than those with an **A** or **B** rating.

Risk Findings :

The total risk findings for the institutions are explained using the pie chart for factors such as data breaches, dark web leaks, botnet activity, and phishing & domain squattings. The data breaches and botnet activities occur at a higher rate compared to the dark web leaks and phishing & domain squatting.



C	[redacted] University ● Watching	981	4	86	1,071 +1,071
D	IIT [redacted] ● Watching	116,346	248	251	116,846 +116,846
D	IIT [redacted] ● Watching	97,979	748	735	99,435 +99,435
C	S[redacted] ● Watching	7,945	0	431	8,346 +17
D	IIT [redacted] ● Watching	238,743	1,078	6,471	246,295 +46
D	[redacted] ● Watching	63,260	46	216	63,522 +13
D	[redacted] University ● Watching	103,017	4	77	103,098 +1,022

393,518

Data Breaches

339,442

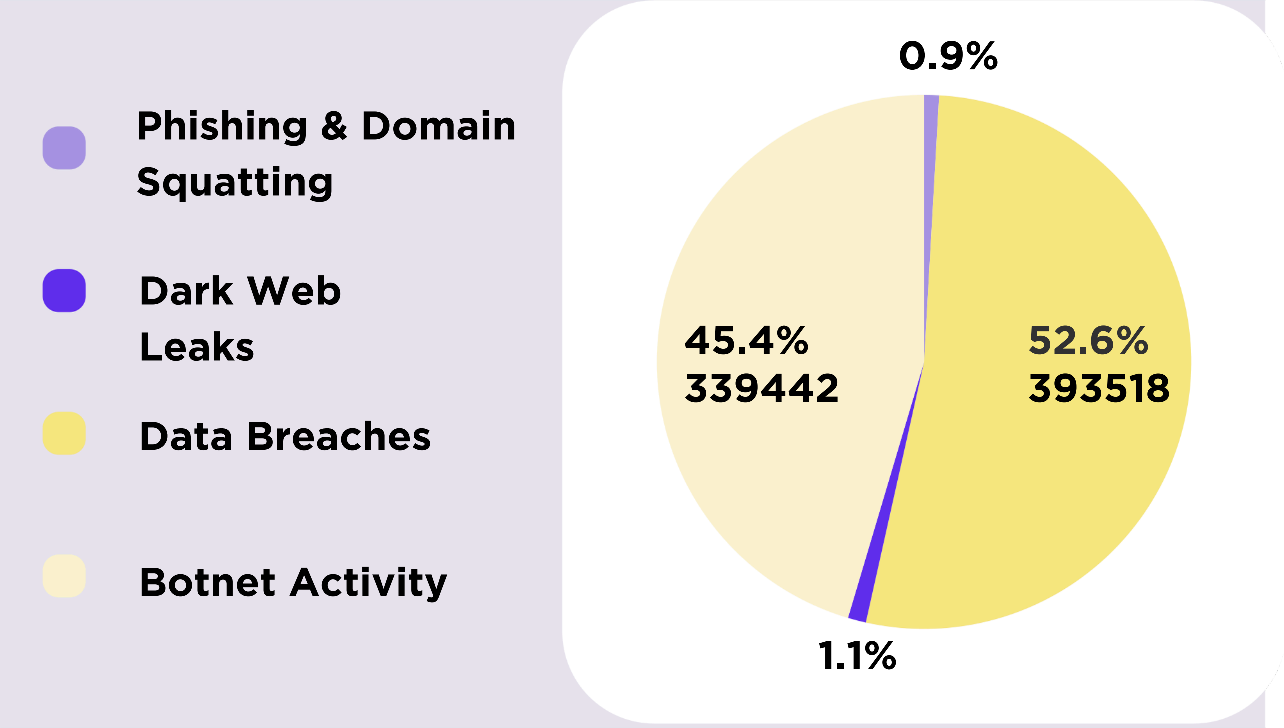
Botnet Activity

7,926

Dark Web Leaks

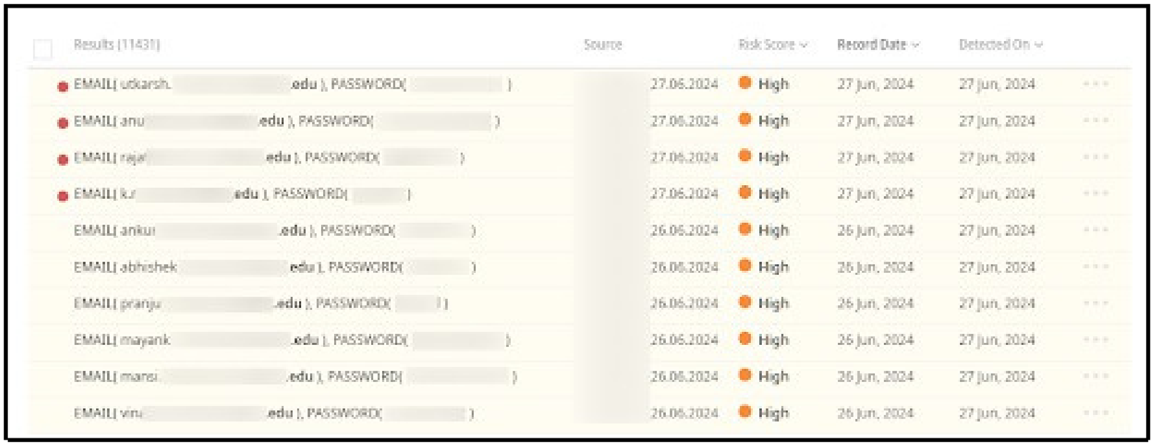
6,711

Phishing and Domain Squatting

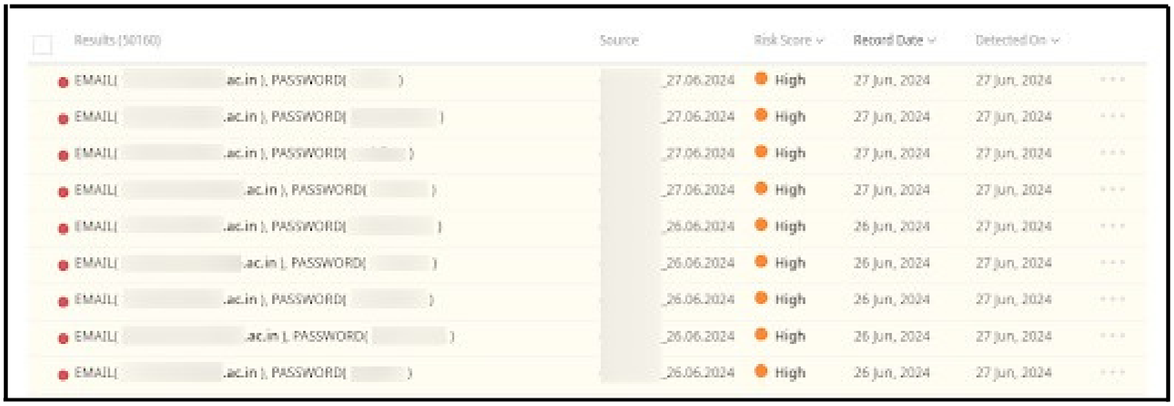


Key Indicators:

1. Multiple instances of data breaches containing credentials (email/password) in plain text.

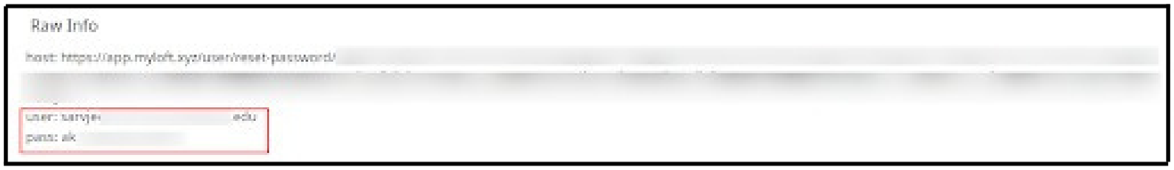


Results (11431)	Source	Risk Score	Record Date	Detected On
● EMAIL(utkarsh.[redacted].edu), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL(anu[redacted].edu), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL(raja[redacted].edu), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL(k.r[redacted].edu), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
EMAIL(ankur[redacted].edu), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
EMAIL(abhishek[redacted].edu), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
EMAIL(pranju[redacted].edu), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
EMAIL(mayank[redacted].edu), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
EMAIL(mansi[redacted].edu), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
EMAIL(viru[redacted].edu), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024



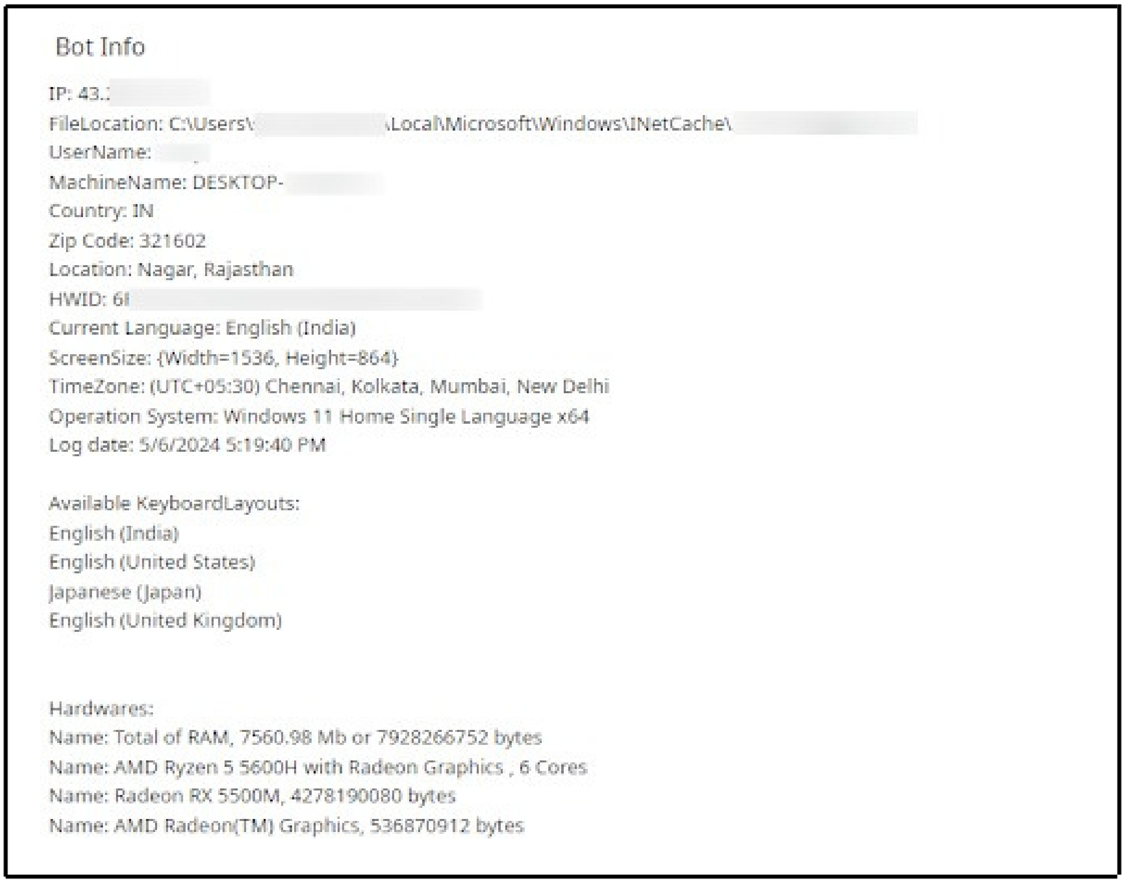
Results (50160)	Source	Risk Score	Record Date	Detected On
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
● EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted] 26.06.2024	● High	26 Jun, 2024	27 Jun, 2024

2. Botnet activity indicating network hosts compromised by malware.



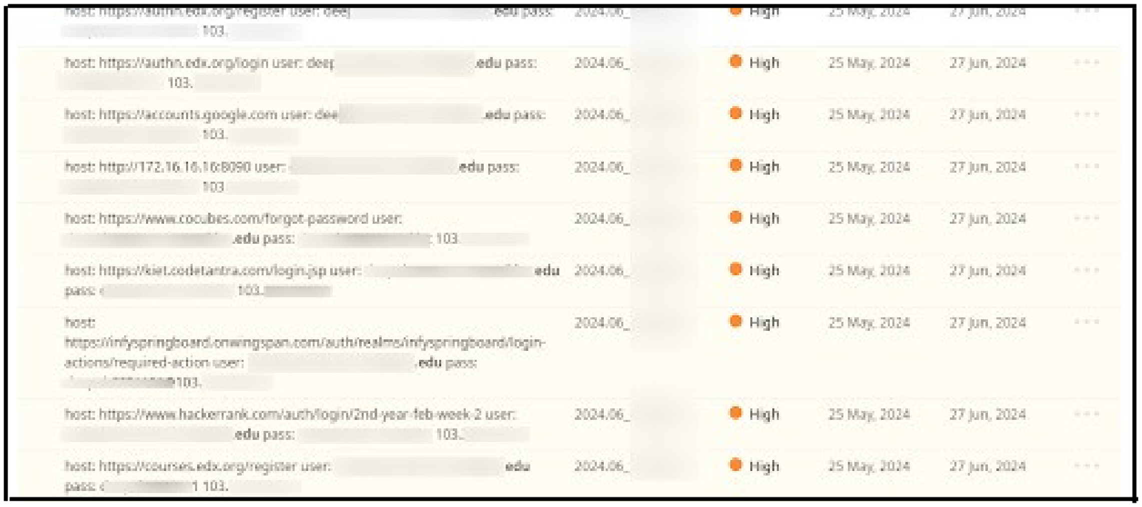
Raw Info

```
host: https://app.myloft.xyz/user/reset-password/[redacted]
[redacted]
user: sanje[redacted]edu
pass: ak[redacted]
```



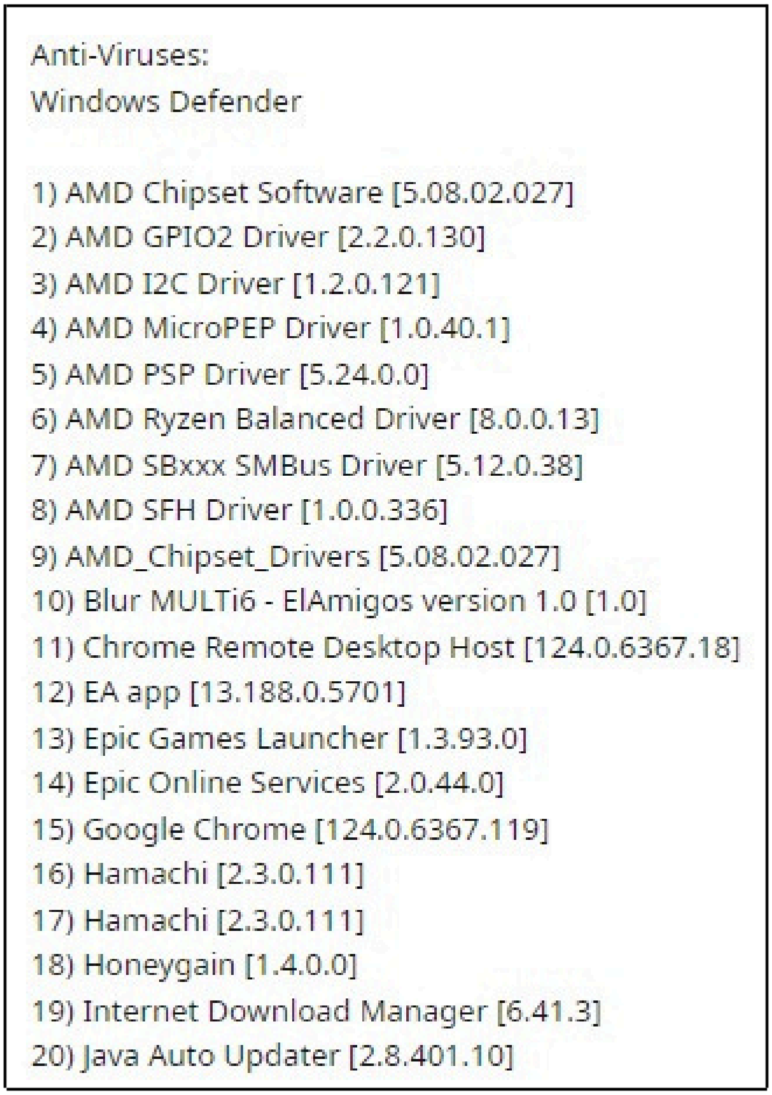
```
Bot Info
IP: 43.[redacted]
FileLocation: C:\Users\[redacted]\Local\Microsoft\Windows\INetCache\[redacted]
UserName: [redacted]
MachineName: DESKTOP-[redacted]
Country: IN
Zip Code: 321602
Location: Nagar, Rajasthan
HWID: 6[redacted]
Current Language: English (India)
ScreenSize: {Width=1536, Height=864}
TimeZone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Operation System: Windows 11 Home Single Language x64
Log date: 5/6/2024 5:19:40 PM

Available KeyboardLayouts:
English (India)
English (United States)
Japanese (Japan)
English (United Kingdom)


Hardwares:
Name: Total of RAM, 7560.98 Mb or 7928266752 bytes
Name: AMD Ryzen 5 5600H with Radeon Graphics , 6 Cores
Name: Radeon RX 5500M, 4278190080 bytes
Name: AMD Radeon(TM) Graphics, 536870912 bytes
```

3. Credentials from third-party government and non-governmental websites linked to official institutional emails.



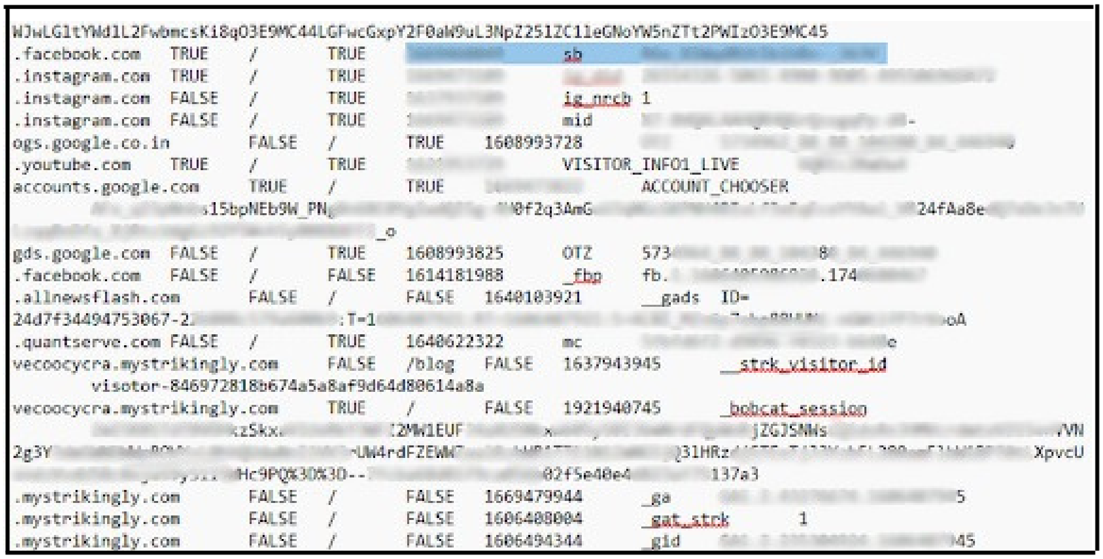
host: https://authn.edx.org/register user: deej[redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://authn.edx.org/login user: deep[redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://accounts.google.com user: dee[redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: http://172.16.16.16:8090 user: [redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://www.cocubes.com/forgot-password user: [redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://kiet.codetantra.com/login.jsp user: [redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://infyspringboard.onwingspan.com/auth/realms/infyspringboard/login-actions/required-action user: [redacted].edu pass: [redacted]103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://www.hackerrank.com/auth/login/2nd-year-feb-week-2 user: [redacted].edu pass: [redacted] 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···
host: https://courses.edx.org/register user: [redacted].edu pass: [redacted]1 103.[redacted]	2024.06_[redacted]	● High	25 May, 2024	27 Jun, 2024	···

4. Details of software applications, drivers installed on compromised hosts.

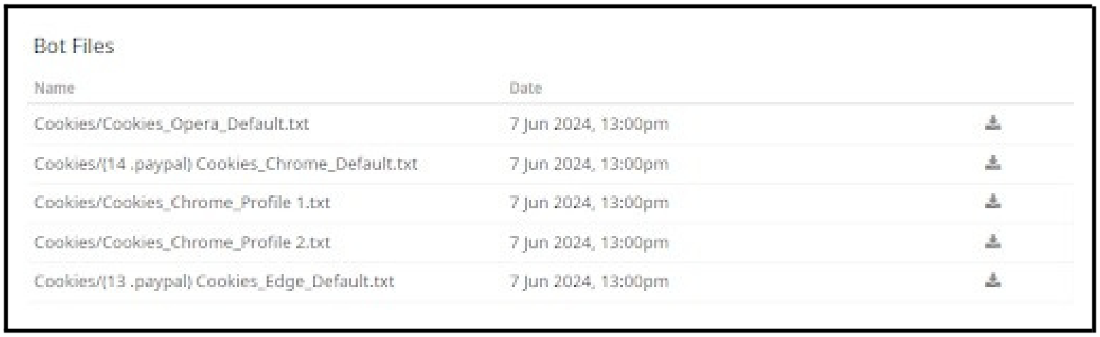


```
Anti-Viruses:
Windows Defender

1) AMD Chipset Software [5.08.02.027]
2) AMD GPIO2 Driver [2.2.0.130]
3) AMD I2C Driver [1.2.0.121]
4) AMD MicroPEP Driver [1.0.40.1]
5) AMD PSP Driver [5.24.0.0]
6) AMD Ryzen Balanced Driver [8.0.0.13]
7) AMD SBxxx SMBus Driver [5.12.0.38]
8) AMD SFH Driver [1.0.0.336]
9) AMD_Chipset_Drivers [5.08.02.027]
10) Blur MULTi6 - ElAmigos version 1.0 [1.0]
11) Chrome Remote Desktop Host [124.0.6367.18]
12) EA app [13.188.0.5701]
13) Epic Games Launcher [1.3.93.0]
14) Epic Online Services [2.0.44.0]
15) Google Chrome [124.0.6367.119]
16) Hamachi [2.3.0.111]
17) Hamachi [2.3.0.111]
18) Honeygain [1.4.0.0]
19) Internet Download Manager [6.41.3]
20) Java Auto Updater [2.8.401.10]
```

5. Sensitive cookie data exfiltrated from various browsers.



```
WJwLG1tYWd1L2FwbmcsKi8qO3E9MC44LGFwcGxpY2F0aW9uL3NpZ251ZC1leGNoYW5nZTt2PWIzO3E9MC45
.facebook.com   TRUE    /       TRUE    [redacted]      sb      [redacted]
.instagram.com  TRUE    /       TRUE    [redacted]      [redacted]      [redacted]
.instagram.com  FALSE   /       TRUE    [redacted]      ig_nrcb 1
.instagram.com  FALSE   /       TRUE    [redacted]      mid     [redacted]-
ogs.google.co.in        FALSE   /       TRUE    1608993728      [redacted]
.youtube.com    TRUE    /       TRUE    [redacted]      VISITOR_INFO1_LIVE      [redacted]
accounts.google.com     TRUE    /       TRUE    [redacted]      ACCOUNT_CHOOSER
        [redacted]s15bpNEb9W_PN[redacted]0f2q3AmG[redacted]24fAa8e[redacted]
[redacted]_o
gds.google.com  FALSE   /       TRUE    1608993825      OTZ     573[redacted]8[redacted]
.facebook.com   FALSE   /       FALSE   1614181988      _fbp    fb.[redacted].174[redacted]
.allnewsflash.com       FALSE   /       FALSE   1640103921      __gads  ID=
24d7f34494753067-2[redacted]:T=1[redacted]oA
.quantserve.com FALSE   /       TRUE    1640622322      mc      [redacted]e
vecoocycra.mystrikingly.com     FALSE   /blog   FALSE   1637943945      __strk_visitor_id
        visotor-846972818b674a5a8af9d64d80614a8a
vecoocycra.mystrikingly.com     TRUE    /       FALSE   1921940745      _bobcat_session
        [redacted]zSkx[redacted]2MW1EUF[redacted]x[redacted]jZGJSMWs[redacted]VN
2g3Y[redacted]UW4rdFZEWW[redacted]31HRz[redacted]XpvcU
[redacted]Hc9PQ%3D%3D--[redacted]02f5e40e4[redacted]137a3
.mystrikingly.com       FALSE   /       FALSE   1669479944      _ga     [redacted]5
.mystrikingly.com       FALSE   /       FALSE   1606408004      _gat_strk       1
.mystrikingly.com       FALSE   /       FALSE   1606494344      _gid    [redacted]45
```

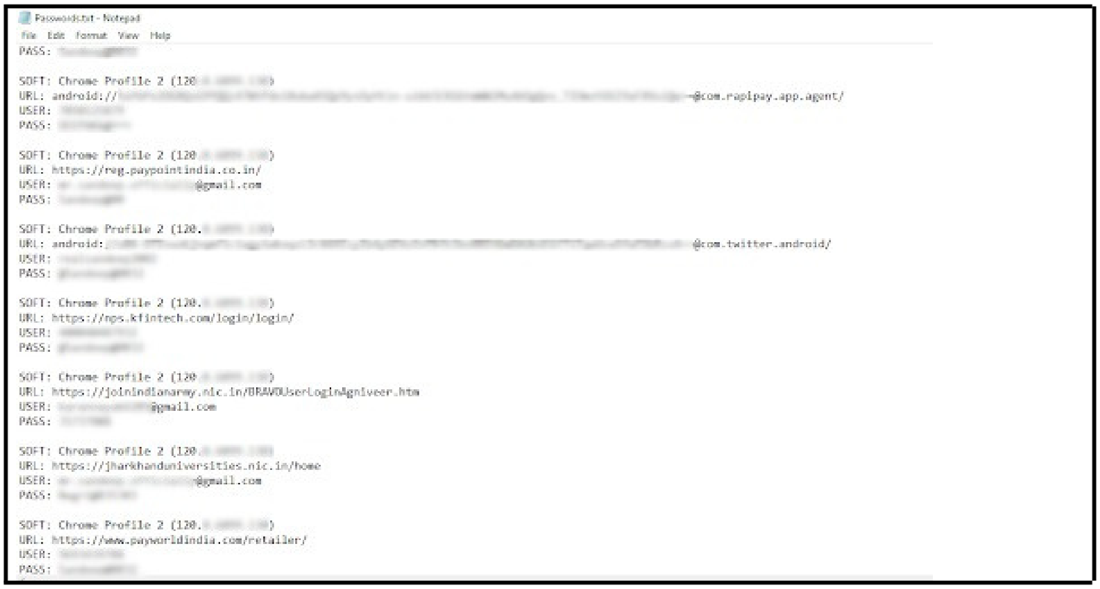


Bot Files

Name	Date	
Cookies/Cookies_Opera_Default.txt	7 Jun 2024, 13:00pm	⤓
Cookies/(14 .paypal) Cookies_Chrome_Default.txt	7 Jun 2024, 13:00pm	⤓
Cookies/Cookies_Chrome_Profile 1.txt	7 Jun 2024, 13:00pm	⤓
Cookies/Cookies_Chrome_Profile 2.txt	7 Jun 2024, 13:00pm	⤓
Cookies/(13 .paypal) Cookies_Edge_Default.txt	7 Jun 2024, 13:00pm	⤓

6. IP addresses of compromised systems.

7. Login credentials for different Android applications.

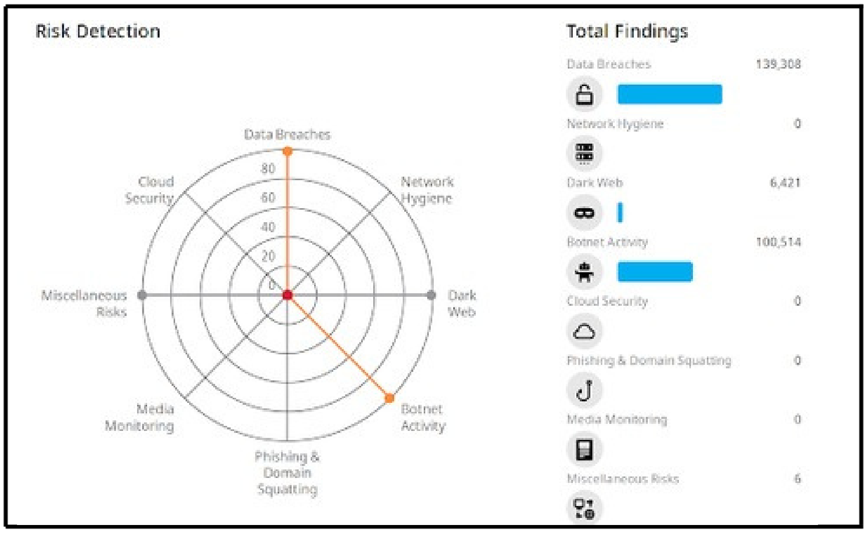


```
PASS: [redacted]

SOFT: Chrome Profile 2 (120[redacted])
URL: android://[redacted]@com.rapipay.app.agent/
USER: [redacted]
PASS: [redacted]

SOFT: Chrome Profile 2 (120[redacted])
URL: https://reg.paypointindia.co.in/
USER: [redacted]@gmail.com
PASS: [redacted]

SOFT: Chrome Profile 2 (120.[redacted])
URL: android:[redacted]@com.twitter.android/
USER: [redacted]
PASS: [redacted]

SOFT: Chrome Profile 2 (120.[redacted])
URL: https://nps.kfintech.com/login/login/
USER: [redacted]
PASS: [redacted]

SOFT: Chrome Profile 2 (120[redacted])
URL: https://joinindianarmy.nic.in/BRAVOUserLoginAgniveer.htm
USER: [redacted]@gmail.com
PASS: [redacted]

SOFT: Chrome Profile 2 (120[redacted])
URL: https://jharkhanduniversities.nic.in/home
USER: [redacted]@gmail.com
PASS: [redacted]

SOFT: Chrome Profile 2 (120.[redacted])
URL: https://www.payworldindia.com/retailer/
USER: [redacted]
PASS: [redacted]
```

Below is the sample detail of one of the top educational institutions that provides the insights about the higher rate of data breaches, botnet activity, dark web activities and phishing & domain squatting.

Risk Detection:

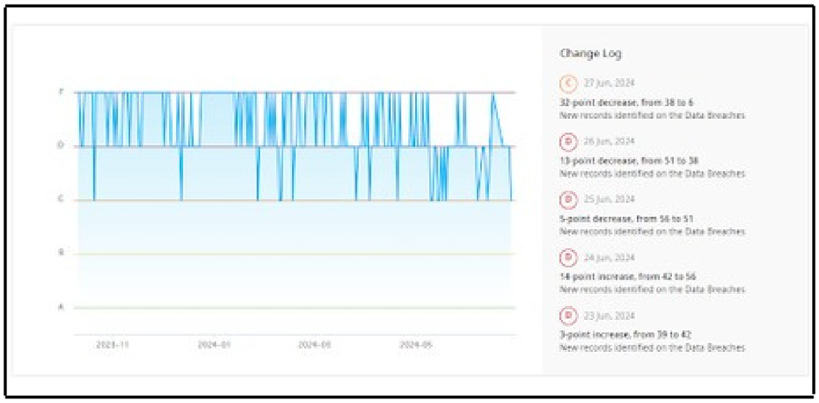
It indicates the number of data breaches, network hygiene, dark web activities, botnet activities, cloud security, phishing & domain squatting, media monitoring and miscellaneous risks. In the below example, we are able to see the highest number of data breaches and botnet activities in the sample particular domain.



Total Findings

Data Breaches	139,308
Network Hygiene	0
Dark Web	6,421
Botnet Activity	100,514
Cloud Security	0
Phishing & Domain Squatting	0
Media Monitoring	0
Miscellaneous Risks	6

Risk Changes:



Change Log

27 Jun, 2024
32-point decrease, from 38 to 6
New records identified on the Data Breaches

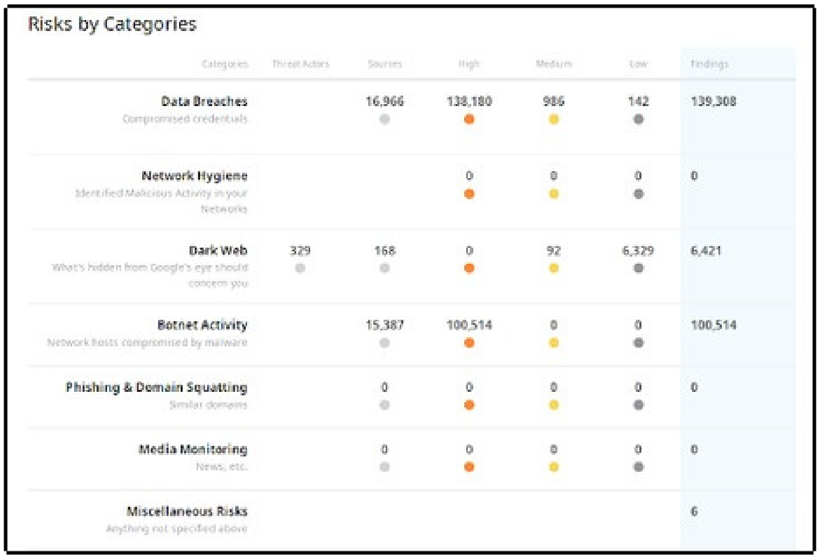
26 Jun, 2024
13-point decrease, from 51 to 38
New records identified on the Data Breaches

25 Jun, 2024
5-point decrease, from 56 to 51
New records identified on the Data Breaches

24 Jun, 2024
14-point increase, from 42 to 56
New records identified on the Data Breaches

23 Jun, 2024
3-point increase, from 39 to 42
New records identified on the Data Breaches

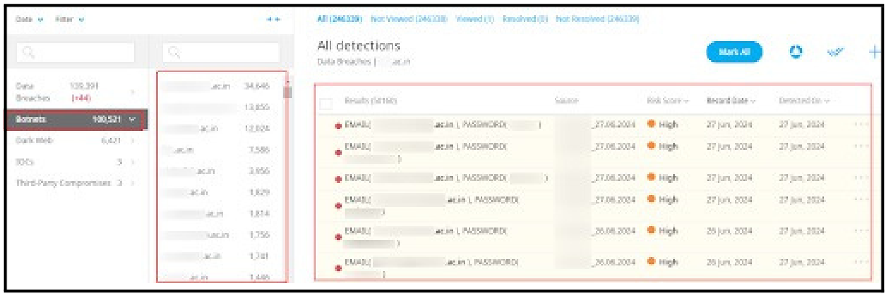
Risk by Categories:



Risks by Categories

Categories	Threat Actors	Sources	High	Medium	Low	Findings
Data Breaches Compromised credentials		16,966 ●	138,180 ●	986 ●	142 ●	139,308
Network Hygiene Identified Malicious Activity in your Networks			0 ●	0 ●	0 ●	0
Dark Web What's hidden from Google's eye should concern you	329 ●	168 ●	0 ●	92 ●	6,329 ●	6,421
Botnet Activity Network hosts compromised by malware		15,387 ●	100,514 ●	0 ●	0 ●	100,514
Phishing & Domain Squatting Similar domains		0 ●	0 ●	0 ●	0 ●	0
Media Monitoring News, etc.		0 ●	0 ●	0 ●	0 ●	0
Miscellaneous Risks Anything not specified above						6

Risk is categorized with factors such as high, medium and low, the risk is at high level for data breaches and botnet activities.



Data Breaches	139,391 (+44)
Botnets	100,521
Dark Web	6,421
IOCs	3
Third-Party Compromises	3

[redacted].ac.in	34,646
[redacted]	13,855
[redacted].ac.in	12,024
[redacted].ac.in	7,586
[redacted].ac.in	3,956
[redacted].ac.in	1,829
[redacted].ac.in	1,814
[redacted].ac.in	1,756
[redacted].ac.in	1,741
[redacted].ac.in	1,446

All detections
Data Breaches | [redacted].ac.in

Results (50150)	Source	Risk Score	Record Date	Detected On
EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted]_27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted]_27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted]_27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted]_27.06.2024	● High	27 Jun, 2024	27 Jun, 2024
EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted]_26.06.2024	● High	26 Jun, 2024	27 Jun, 2024
EMAIL([redacted].ac.in), PASSWORD([redacted])	[redacted]_26.06.2024	● High	26 Jun, 2024	27 Jun, 2024

Advanced Persistent Threats (APT) are ones that use sophisticated techniques and specific targets. Transparent Tribe is an APT group that traditionally focused on the Indian defence ecosystem but in more recent times has started targeting educational institutions and students. It targets information assets. Further, the group uses a malware called Crimson RAT consistently. Other targets of the group include government and critical infrastructure entities.

What we are witnessing in terms of patterns are tactics by various types of threat actors that range from simple to extremely sophisticated. As we shall see in the section below, educational institutions are attacked in multiple ways such as hacking into the network systems to gain sensitive information, hacking to deface websites and even get directly in touch with students. For example, in a new form of cyberattack witnessed last year, Pakistani Intelligence Operatives (PIO) targeted schools by contacting students directly to gain personal information.

In this series of cases which was reported in July 2023, school students across the nation received calls and Whatsapp messages from PIO impersonating school teachers or giving references of someone known to them and asking for One Time Passwords (OTPs) to enable them to join Whatsapp groups. The main targets of these calls and messages, according to a news article, were students residing in border regions where cross border infiltration attempts are more common. By using such a tactic, cyber criminals aimed to exploit the proximity of the areas in which these schools were located to sensitive locations to gain strategic advantage and access confidential information.

In these cases, the risks are manifold. Such attacks not only compromise national security by the leaking of sensitive data but they also lead to psychological effects such as trauma for children who get contacted in this manner and realise that they had been conned. Thus, not only are educational institutions attacked for the data and research they hold in their repository but an additional threat is to use such methods to compromise national security as a whole. Cybersecurity measures and awareness is thus paramount at both individual and institutional levels.

1000+ schools and colleges in India

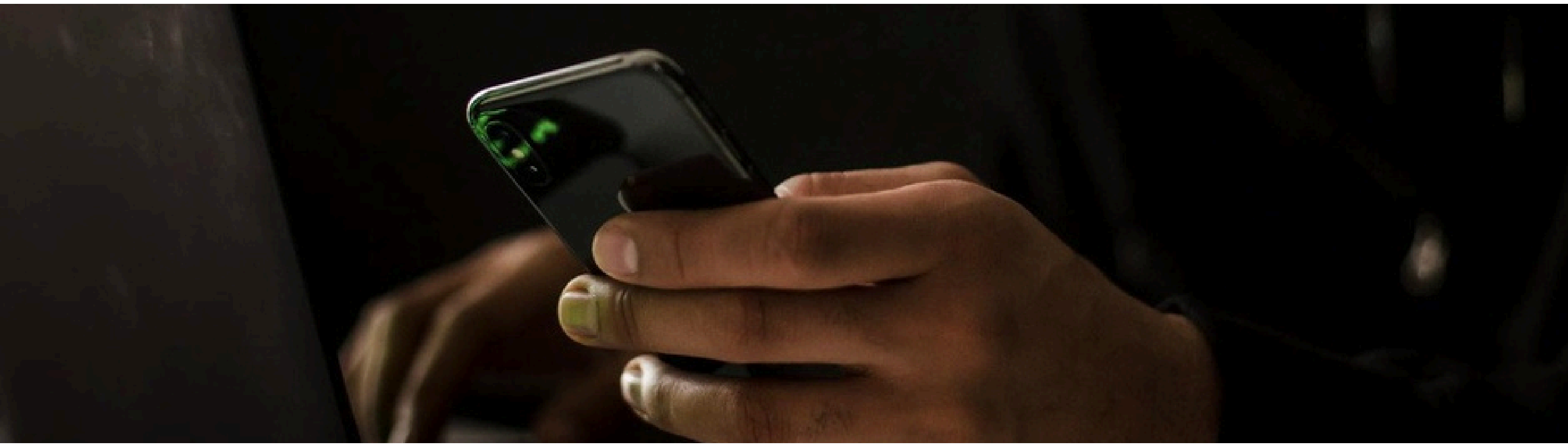
had been targeted with cyberattacks between June and September 2020

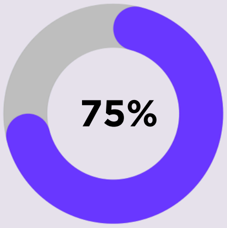
A report filed in October 2020 in which the firm Barracuda Networks conducted a research study to find that over 1000 schools and colleges in India had been targeted with cyberattacks between June and September 2020. This research report points at a mix of tactics used by the cybercriminals towards achieving their goal. Researchers found that of these cases, in 57 percent of the incidents, malicious emails were sent using compromised internal accounts. They suspect that the cybercriminals got a hold of these accounts through the dark web or social engineering. Once they got hold of these compromised accounts, they launched fresh email attacks through spear phishing. This strategy works wonders as people tend to trust accounts that seem to come from legitimate persons and domains. This creates very little suspicion with users.

Researchers also found through an analysis of these cases that about 86 percent of all business email compromise (BEC) attacks on educational institutions during this period were carried out using GMail accounts. GMail is a preferred email service since it is free, easy to register and widely used. In addition, cyber criminals used words such as ‘principal’, ‘head of department’, ‘school’ and ‘president’ to make them seem legitimate. They also used convincing subject lines to grab the attention of a target, such as, ‘new Covid guidelines’ and ‘school meeting on Covid’. Such methods could easily get unsuspecting students to click on malicious links or download attachments from the emails.

86%

of all business email compromise (BEC) attacks on educational institutions during this period were carried out using GMail accounts

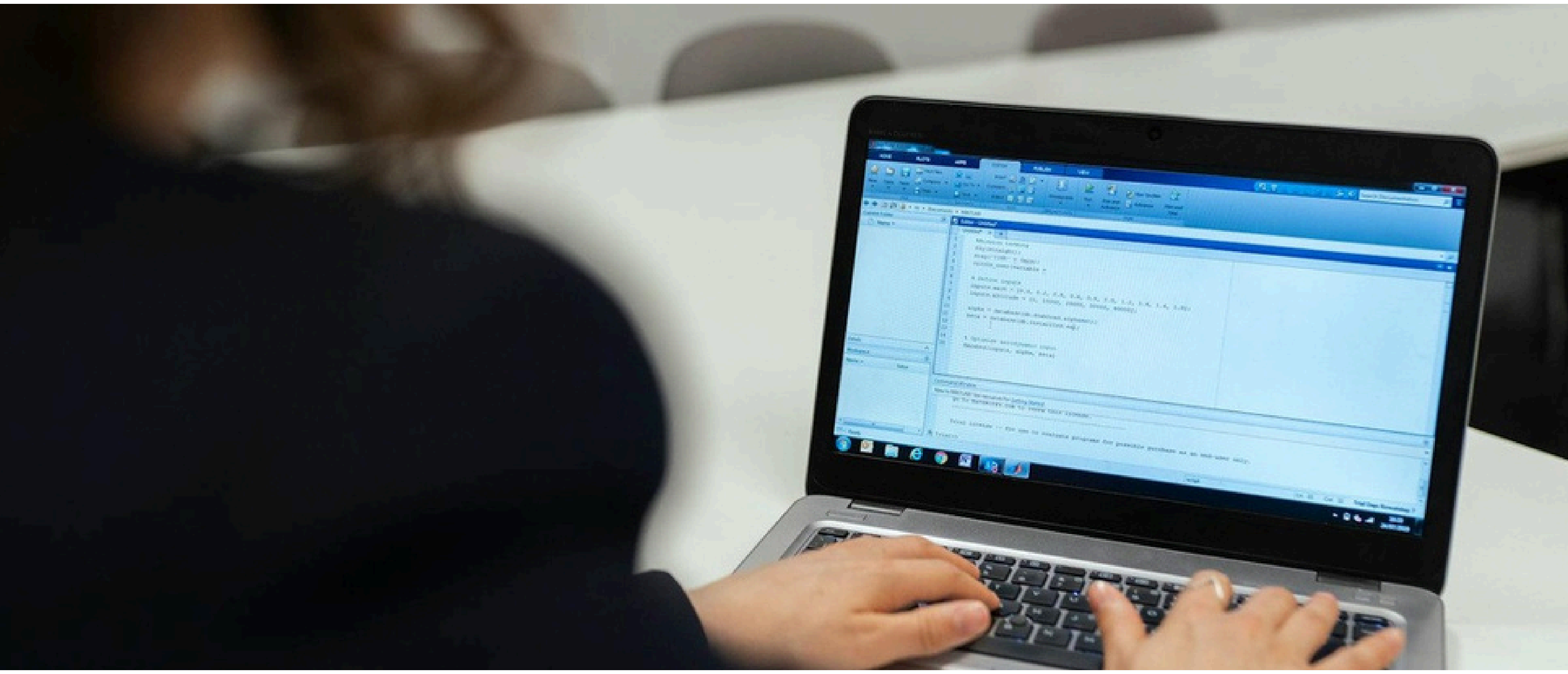




Indian organisations have faced such attacks with each breach costing an average of Rs 35 crore in damage.

In terms of evolving trends, ransomwares have emerged as the predominant among malicious cyber attacks. According to data, over 75 percent Indian organisations have faced such attacks with each breach costing an average of Rs 35 crore in damage. Other existing malwares can affect all kinds of computer systems. Thus, all systems are potentially extremely vulnerable to assaults from hostile state and non-state actors. According to experts, at this stage, most organisations in the country lack the tools to identify cyber attacks. Prevention thus becomes a far cry. An acute lack of cybersecurity professionals is another challenge. The introduction of 5G services and quantum computing poses additional risks for digital security breaches.

Given that these cases and incidents are relatively new, much is left to be examined and studied to understand the long term repercussions of such attacks. At this point authorities are still dealing with preliminary information such as motives of cyber attacks and hygiene checks to put in place to protect data and people. At the same time, reports and articles primarily are discussing ‘potential’ threats as a result. An examination of articles, reports and studies on cyber attacks in educational institutions in India points to a crucial gap- there is a dearth of research on issues surrounding how cyber attacks specifically affect educational institutions. Despite rising vulnerabilities and resultant attacks, focused research to examine specific factors is close to absent.

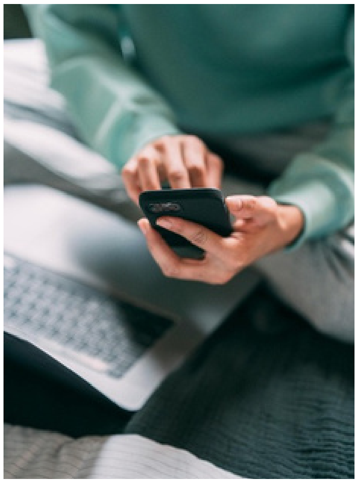


SECTION 5

Cybersecurity Challenges Faced by Educational Institutions

Understanding the specific challenges faced by educational institutions in terms of threats is key to proposing solutions at both levels, including the educational institutions and the larger stakeholder cluster that operates at the strategic policy level. This section outlines various cases of cyberattacks in India and the rest of the world. It then explores the challenges that lead to such incidents.

As discussed earlier, the unique characteristics of an educational institution influence its cybersecurity risks and the types of attacks it may face. Factors such as size, purpose, reputation, location, and student composition play a key role in shaping its threat profile. For instance, renowned universities may be targeted by advanced cyber threats, while smaller schools face different vulnerabilities. It is crucial for institutions to assess their specific risks and implement tailored security measures. For example, a small rural school is less likely to be targeted by ransomware attacks, as attackers typically seek victims with the financial capacity to pay substantial ransoms for stolen or encrypted data. Understanding these distinctions allows educational institutions to develop appropriate cybersecurity strategies based on their individual risk landscape.



Let us consider some notable cyberattacks against schools and colleges from recent times and examine the various types of threats and risks they might face

Cyberattack Incidents in University/Educational Institutions

Attack on computer systems

In April 2021, the University of Hertfordshire experienced a crippling attack that affected all of its computer systems including cloud-based resources. It took about five days for its services and classes to be restored.

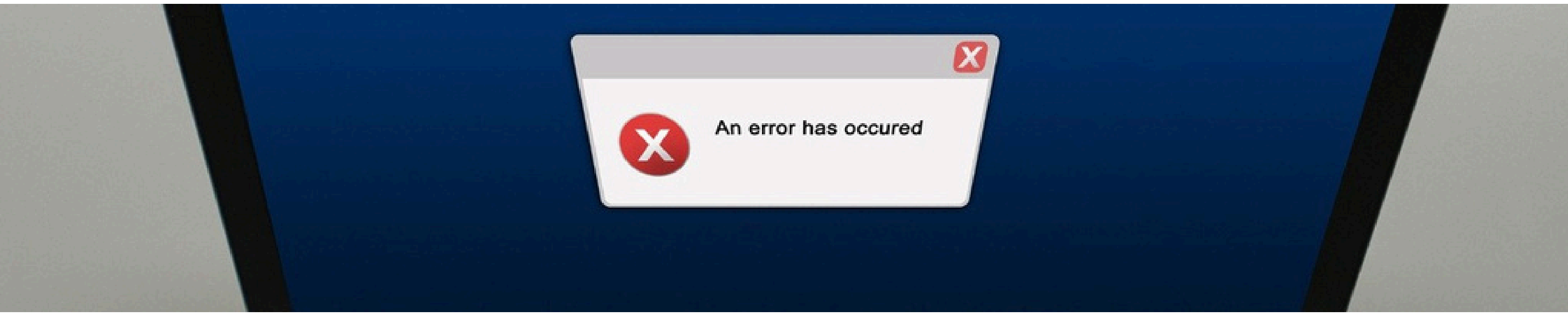
Ransomware attacks

In September 2021, a ransomware attack against Howard University forced it to cancel online and hybrid classes and the university's WiFi remained offline for many days. Even prestigious institutions like the University of California, Los Angeles, have not been immune to cyber attacks. In a December 2020 attack of the university's network, hackers exploited a vulnerability in third-party software to insert ransomware and extract personal data. Apart from the university, this attack affected government agencies and businesses. About 300 organisations were affected as a result of this attack. The data stolen during this attack was then used to send mass mails and threatened to be posted online, blackmailing individuals and companies to pay the attackers. Further, a ransomware attack against a web hosting service provider for the education sector called Finalsite led to websites of about 5000 schools and colleges going offline. Some institutions that have faced similar attacks are Michigan State University and the University of California, San Francisco.

Leakage of private and sensitive data

Compare this to a couple of cases from India. In 2021, an unsecured server at Salesken.ai had put student data from popular learning e-portal Byju's at risk. According to a report by Techcrunch, the server had been unprotected for a few days. Data found on the server comprised student names and classes, email IDs and phone numbers of parents and teachers. It also contained log chats between parents and staff and teacher's comments provided to their students. Copies of emails with codes to reset user accounts and internal Salesken.ai data were also found on the server. Further, in 2023, a security researcher found a server-side misconfiguration with Byju's which ended up exposing sensitive data of students. Apart from names and contact details, the error exposed loan details such as payouts, links to scanned documents and transactional information related to some students.

The cases above represent some of the most common cybersecurity issues faced by educational institutions worldwide.



An error has occured

What are the challenges that lead to these incidents?

Lack of a security framework

One primary challenge with respect to cybersecurity of educational institutions is the lack of a security framework that focuses on higher educational institutions. Various other organisations follow several different frameworks such as ISO27001 (an information security management system internationally recognised as best practice framework), the National Institute of Standards and Technology (NIST), COBIT or Control Objectives for Information and Related Technologies (an IT governance framework for businesses wanting to implement, monitor and improve IT management best practices) and Information Technology Infrastructure Library (ITIL) (a framework designed to standardise the selection, planning, delivery, maintenance and overall lifecycle of IT services within a business). Such frameworks do not generally support the cybersecurity of universities and colleges as they are aimed at commercial organisations and are difficult to implement and not cost effective. Most educational institutions in India at this point do not have a clearly defined cybersecurity framework.

General challenges

Multiple factors contribute to tainting the cybersecurity of educational institutions. Let us consider a few here. The attack surface in education, for one, is quite wide and deep, given that education is a growing sector and hence has associated challenges.

→ **Lack of cybersecurity awareness among stakeholders:** Cybersecurity awareness among different stakeholders, including students, parents, teachers, and staff is generally limited given this is a relatively new concern as technology's role in the education sector is on the rise. The last few years have seen an explosion in the usage of technological offerings, owing apart from the pandemic, to more investments in technology due to the plethora of benefits they bring to the table. But since the use of technology is a relatively new addition in educational institutions and education it is also a rapidly advancing and dynamic field, none of the actors in educational institutions are adequately equipped to deal with or train others on the issues arising therefrom.

Cyber Security Awareness among Female University Students

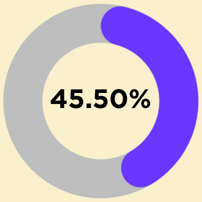
A recent study conducted by a university in Vadodara, supported by CyberPeace, explored the cybersecurity awareness level among female students. The study also aimed to enhance cybersecurity awareness among the selected female students and enlighten them about the hazards and challenges prevailing in cyberspace.

The study was conducted in three phases. The findings of the study revealed that half of the respondents were from the 17-19 age group. The survey results indicated that 43% of the students were not well aware of cybercrime. 40.72% of the students do not install antivirus software on their personal PC and smartphone.

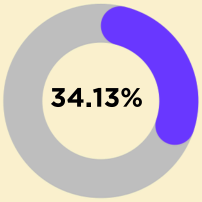
Only 23.95% knew about anti-spyware, 23.95% knew about anti-spam, 31.13% knew about cyberbullying, 25.14% knew about cyberstalking (25.14%), and security settings (22.15%) to some extent. Less than 50% of students knew about antivirus and password security management.

The findings of the study indicated that there was a significant difference in the awareness regarding general security, password security, browser security, and the use of several devices. It highlighted that as the use of several devices differs the awareness about selected security aspects also differs. Students were less aware of web browser security than general security, password security, and social media security.

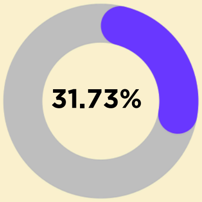
The study concluded that cyber security is highly recommendable to the students in the university and encourages more females to participate in the awareness programmes, seminars, and workshops to minimize the adverse effects of breaches.



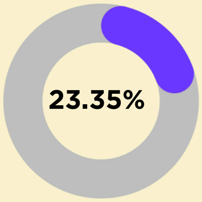
of students didn't know about phishing



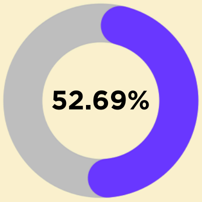
of students didn't know about social engineering



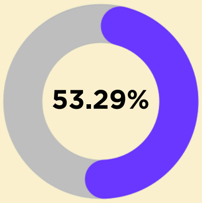
of students didn't know about firewall



of students didn't know about identity theft



of students knew about 2-step verification



of students knew about software update

- **Different user accounts:** Educational institutions generally handle a variety of accounts for staff, third-party contractors, educators, students and alumni, having a high turnover rate. Since there is a continuous arrival of newcomers into this network, keeping all users secure administratively is a challenge and this requires effective systems and training on security for all users.

- **Shared devices:** Another challenge is the fact that educational institutions provide a variety of shared devices and systems exposed to the internet to enable research and collaboration. This increases the attack surface by a huge scale.

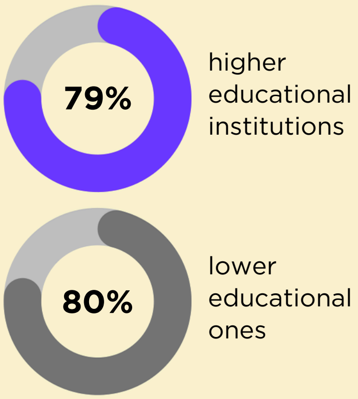
- **Financial constraints:** Restricted budgets and limited strategic oversight lead to inability of investing in tools and processes to mitigate risks.

- **Non-Reporting of Cases:** Despite incidents occurring within educational institutes, little to no reporting enables further threats and cyber attacks. There is a need for smallest to gravest, any type of incidents that affect universities and educational institutions and their functioning to be reported.

Rampant social engineering attacks (particularly phishing, DDoS and ransomware)

Social engineering, consisting of phishing and ransomware, and Distributed Denial of Service (DDoS) attacks, are particularly dangerous threats to the education sector. Ransomware affected 79 percent higher educational institutions and 80 percent lower educational ones in a quarter of 2023, in India. Between 2018 and 2023, ransomware attacks on schools cost over $53 billion in downtime alone. Further, over 6.7 million individual records were breached during the period. This figure, one must note, is based on only reported cases. Again, DDoS attacks, which can be purchased for about $10, allows attackers to throw off a school entirely. The incidents mentioned under section 2 above are examples of ransomware attacks.

Affected by ransomware
quarter of 2023



Schools and universities in the US suffered much damage due to ransomware during the Covid-19 pandemic. According to a cybersecurity firm Emsisoft, ransomware affected 62 School districts and campuses of 26 colleges and universities in 2021. It further found that ransomware incidents disrupted learning at more than 1000 schools in the US in 2021 (Jimenez and Lyngaas, 2021). In an unfortunate case, a 150 year-old Lincoln College in the US shut down in 2022 owing to several reasons, one of them being a cyber attack that it could not recover from.

Affected by ransomware
according to Emsisoft | 2021

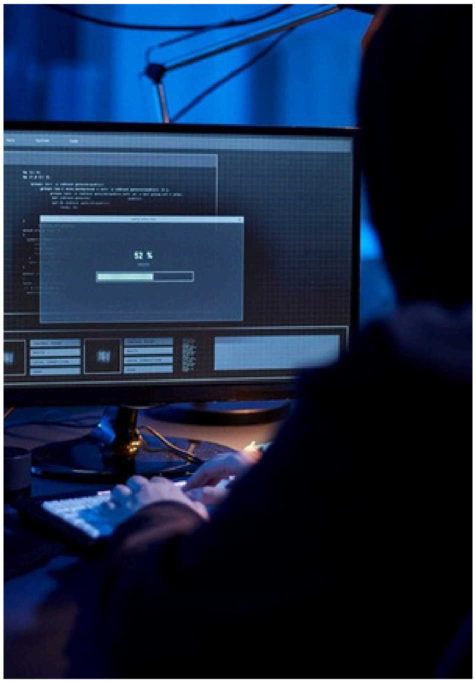
62
school districts

26
colleges and universities

A cyber attack in December 2021 disrupted the college's admission activities, hindering access to all institutional data which affected the enrollment process for Fall 2022 as systems required for recruitment, retention and fundraising were all unusable owing to the attack. As with other related issues though, it is almost impossible to know the precise number of such attacks as many of these go unreported.

Insider threats and human error

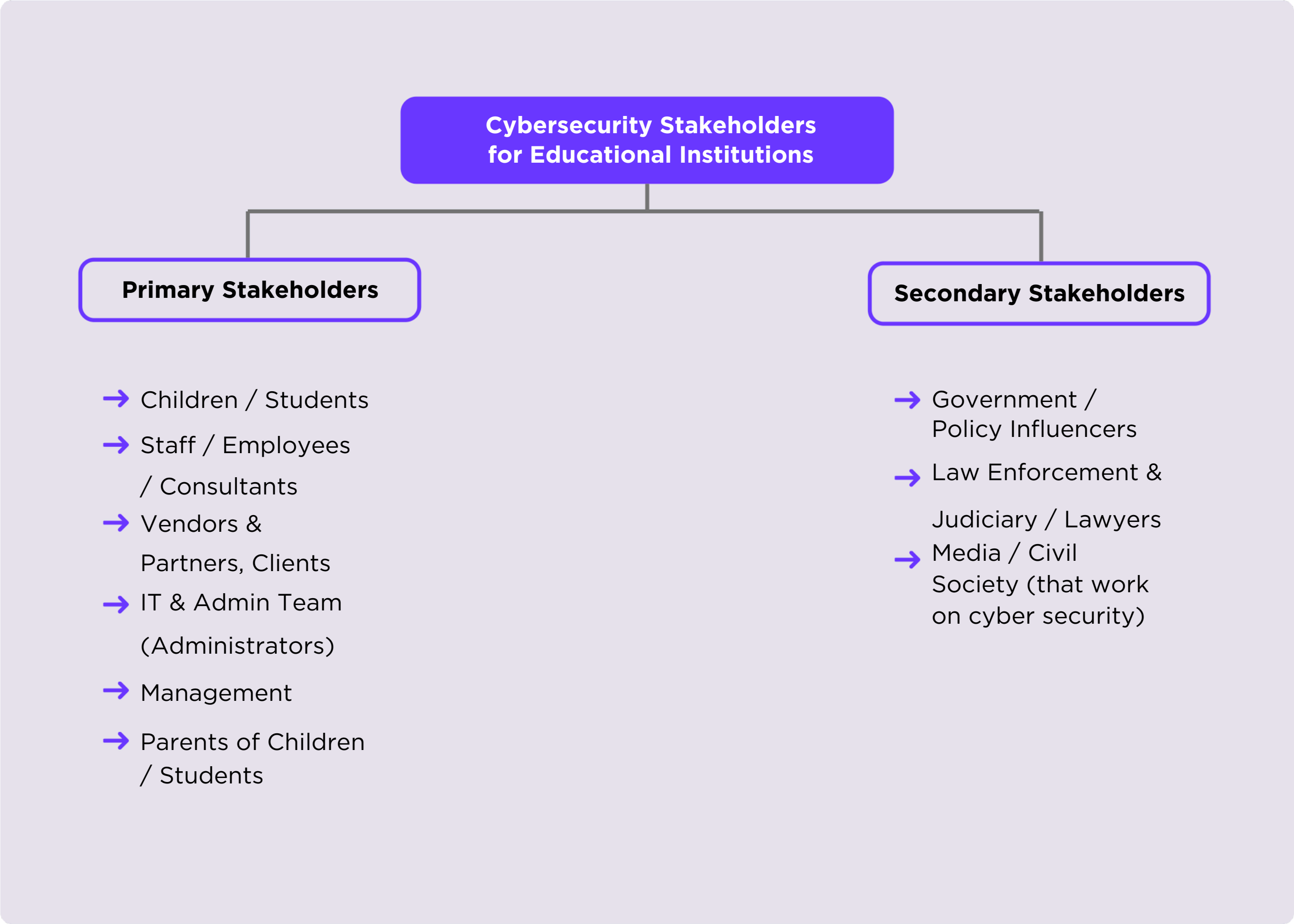
Apart from threats and attacks that are a result of malicious intent of threat actors external to an organisation, educational institutions face threats from within. Inside threats are potential and actual malicious attacks and threats performed on a computer system or network by an individual authorised to access the system. There is often less security against inside attacks as most organisations focus on defending against external attacks. Insider threats can range from injecting Trojan viruses to stealing sensitive data from a network or a system. Attackers may affect system availability by overloading the network or computer processing capacity or computer storage, resulting in system crashes. Apart from intentional acts by inside threat actors, human error also leads to multiple incidents that compromise educational institutions at large.



SECTION 6

Mapping the Stakeholders

In an ecosystem of current and persistent patterns and evolving trends in cybercrimes against educational institutions, who are the primary stakeholders involved? Below, we represent the stakeholders before moving into the responses by government agencies, followed by steps taken by educational institutions themselves.



Cybersecurity Stakeholders for Educational Institutions

Primary Stakeholders

- Children / Students
- Staff / Employees / Consultants
- Vendors & Partners, Clients
- IT & Admin Team (Administrators)
- Management
- Parents of Children / Students

Secondary Stakeholders

- Government / Policy Influencers
- Law Enforcement & Judiciary / Lawyers
- Media / Civil Society (that work on cyber security)

SECTION 7

Cyber Threat Response and Mechanisms for Prevention

Existing Cyber Security Measures by Indian Government Agencies

The government and other bodies in India have come up with various measures to address the issue of cybersecurity in schools and colleges. Although these steps have been well-meaning, there is room for improved implementation. The following is a compilation of some prominent initiatives.

Cybersecurity Strategy for Higher Educational Institutes by the All India Council for Technical Education (AICTE)

The All India Council for Technical Education (AICTE), a statutory body under the Ministry of Education, has published a document titled, 'Cybersecurity Strategy for Higher Education Institutes'. It articulates its mission in aiming to enhance the overall cybersecurity posture of higher education in India. Its goals are four-fold, namely, to:

- Create dynamic cybersecurity policies for students and institutes
- Translate policy statements into an action plan
- Raise national awareness about risks in cyberspace
- Create nationwide students and faculty cybersecurity experts

The document lays out important guidelines that university management, IT professionals and staff can and must follow. It also provides definitions of various types of external and insider threats that educational institutions can be exposed to.

Handbook for Adolescents and Students on Cyber Safety by the Ministry of Home Affairs (MHA)

The Ministry of Home Affairs (MHA) had drafted a Handbook for Adolescents and Students on Cyber Safety. It discusses cyber threats & frauds and steps to take in case one becomes a victim of cyber abuse in a child-friendly manner.

Training programmes on cyber security by AICTE

Another initiative by AICTE includes training programmes on cyber security as a part of Faculty Development Programmes in different universities and institutes in the country. Webinars on cyber hygiene, cyber security and prevention of cybercrimes have also been conducted for faculty and students of different technical institutes and universities.

Other government initiatives

Other government initiatives to strengthen cybersecurity in education include:

- The emphasis on the importance of cybersecurity education and integration of cybersecurity concepts into school curricula in the National Policy on Education (NEP) 2020 and the Cyber Safety and Hygiene Awareness Network (CSHAN) which raises cybersecurity awareness among students, teachers and parents through workshops, training programs and online resources.

- The Cyber Surakshit Bharat Mission which aims to enhance India's cybersecurity capabilities in different sectors including education 'Cyber Jagrookta Diwas', (an initiative by the MHA) which is to be observed on the first Wednesday of every month in all schools, colleges, universities, Panchayati Raj Institutions (PRI) and municipalities with the involvement of states and union territory (UT) administration and police authorities. The primary purpose of the initiative is to create awareness for the prevention of cybercrime amongst school and college students through workshops, seminars, interactive sessions, case studies, quiz competitions and creative sessions. While the initiative itself sounds useful and relevant, it remains to be seen as to how it is, if at all, being implemented by states and UTs.

- In 2022, the Indian Computer Emergency Response Team (CERT-In), India's cybersecurity agency, introduced a set of guidelines for organisations to comply with if they are digitally connected. According to the guidelines, every cyberattack incident must be reported within hours of identification.

- Apart from these, all Indian States have their own cyber command and control centres.

The Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act, 2023, was enacted in an environment of increasing digitisation of personal data and the resultant need to safeguard individual privacy in a rapidly evolving digital landscape. The Act mandates businesses to adopt responsible data protection and governance practices, given the importance of data privacy and security. Since the scope of the Act is broad- covering any entity involved in collecting, storing, using or transferring digital personal data, educational institutions also come within its ambit. Although all educational institutions may not fall within the category of businesses, the fact that they collect and store information about children and young adults renders them responsible for the protection of the data they collect. It is thus important for educational institutions to follow practices in keeping with the Act, to the extent possible.

SECTION 8

Global Best Practices and Strategies for Educational Institutions in the Face of Increased Threats[4]

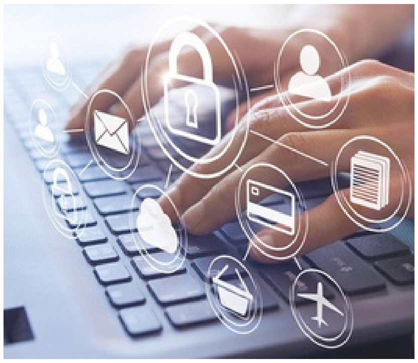
The risks and threats faced by educational institutions are real and ubiquitous; yet, the best practices and strategies to counter attacks are mostly simple and known. Vigilance and a privacy/security-conscious culture are pivotal among all stakeholders to create digitally safe and protected spaces for staff, students, and teachers. This section includes some of the global regulations and best practices that protect universities and educational institutions from cyber threats and attacks.

Government Regulations and Laws That Protect Universities

Several government regulations and laws pertaining to cyber security are applied to protect schools and universities. They apply to concerns such as protecting and preventing personal data breaches, measures, and technical protocols by organisations to ensure ongoing compliance with laws and regulations and entering into legal contracts with third-party actors before appointing them with data processing tasks, among many others.

In India, the Digital Personal Data Protection Act of 2023 is the primary law that deals with personal data protection. It has borrowed the broad definition of data protection from the EU's General Data Protection Regulation (GDPR), which is the toughest privacy and security law in the world, with specific requirements regarding collecting, storing, and processing personal data. The Australian government has developed mitigation strategies in the form of the Strategies to Mitigate Cyber Security Incidents, with the most effective being the Essential Eight which covers strategies surrounding application control, patch applications, multi-factor authentications, patch operating systems, restricted administrative privileges, restricted Microsoft Office macros, user application hardening and regular backups. The US government's NIST Cybersecurity Framework 2.0 provides guidance to industry, government agencies, and other organisations (regardless of size or sector) to manage cybersecurity risks.

[4] See https://www.isphere.net/k-12-cybersecurity-best-practices/ and https://preyproject.com/blog/cyber-security-threats-it-professionals-in-education-face



New Zealand strongly considers cybersecurity in relation with general privacy and hence, the main information cybersecurity obligations are those outlined in the Information Privacy Principle 5 (IPP 5) under the Privacy Act of 2020. IPP 5 requires that reasonable security safeguards are in place to prevent the loss, misuse, or disclosure of personal information. The Act does not, however, address the criminal law on hacking and other cybercrimes.

Although existing regulations and laws do not address the specific requirements and needs of cybersecurity related issues of educational institutions, we propose the following checklist based on information at hand and case examples from different parts of the world.

Educational Institution's Checklist to adopt best practices and increase preparedness towards combating cyber threats

- ✓ **Having an incident response plan:** Such a plan outlines procedures to identify, respond to and recover from cyber threats. When a threat is detected, this plan indicates the immediate steps to contain and eradicate the issue and minimise damage.

- ✓ **Access control implementation:** This limits access to certain systems and data to authorised individuals only. This must be role-based, ensuring permissions are assigned based on a user's role in the institution.

- ✓ **Having a strong security policy:** This must address specific needs such as student data privacy, intellectual property protection, the use of educational technology tools, etc. It may include guidelines on using personal devices, securing home networks and protecting sensitive data when studying or teaching from home (for remote educational requirements). It must establish procedures for reporting and responding to cyber threats. Finally, it must be tailored to the roles and responsibilities of different stakeholders such as students, educators and administrators.

- ✓ **Maintaining data backups:** This is mandatory to protect critical data such as student records, grades, lesson plans and research data. Regular backups enable a recent copy of data to be restored even if the original data is compromised or lost. Ensuring regular and secure backups is paramount for educational institutions.

- ✓ **Regular software updates:** All relevant systems must use updated softwares. This includes everything from the operating systems on school-owned devices, softwares used for virtual meetings, the learning management systems used to administer courses and individual applications used by students and teachers.

- ✓ **Multi-factor authentication:** Unlike passwords, which can be cracked or stolen, two factor or multifactor authentication requires users to provide at least two forms of evidence to verify their identity. This can be used to secure access to all digital platforms and makes it significantly harder for cybercriminals to gain unauthorised access.

- ✓ **Using anti-malware software:** This can be installed on school-owned devices and servers to provide real-time protection, to scan incoming files, emails and downloads for potential threats and to prevent their execution.

- ✓ **Awareness and training:** There is no replacement for this. It is a requirement at all educational institutions irrespective of their location, size and other factors. Cybersecurity awareness and training equips students, teachers and staff with knowledge and skills to recognise and avoid potential and common threats. Training can include aspects such as identifying suspicious emails, the importance of strong and unique passwords and recognising the signs of a potential system breach. This must be extended to remote education systems as well where training can additionally include aspects such as practices for securing home networks, using approved software and platforms and ensuring data privacy.

- ✓ **Using the services of a security service provider:** Where funding permits, educational institutions can employ the services of a security provider to help set up robust firewalls, monitor network traffic for unusual activities, implement intrusion detection and prevention systems and ensure regular software updates and data backups.

- ✓ **Fostering a cyber-aware culture:** Staying informed about evolving cybersecurity threats and encouraging students, staff and educators to report suspicious activity at the earliest, along with clear reporting processes for cybersecurity incidents are all crucial endeavours towards preventing cyberattacks.

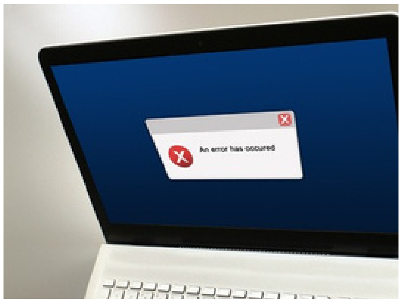
- ✓ **Conducting regular security assessments:** Periodic cybersecurity assessments must be conducted to identify vulnerabilities and weaknesses in an institution's network and systems. Where possible, external security professionals can be invited to conduct penetration testing on the instituion's infrastructure and applications to identify areas for improvement.

It is possible to implement several best practices and measures to safeguard the integrity of educational institutions' data systems. These ensure that schools and universities are not caught unaware and unprepared should they be faced with a threat or risk common to such institutions the world over.

What are Educational Institutions Doing? Response to Cyber Threats

Literature, articles and news reports on responses of educational institutions in India to cyber threats is extremely sparse, pointing to inadequate reporting and exploration of the topic. The lack of data on the incidents, frequency and specific responses to them pose major challenges for all concerned stakeholders since this affects effective policy making in the field. Although large-scale studies have shown the vulnerability of educational institutions, micro-level information is largely absent.

In cases where third party vendors are involved, universities are often left completely helpless and hapless in case of technical glitches, as was the case with Mumbai Universitie's Institute of Open and Distance Learning. The universities was forced to call off and postpone exams which affected about one lakh students. Based on a news article, it is it is known that when candidates clicked on the link to take the exam, they were faced with an error message.



University officials claimed that according to the third party exam partner, the server had crashed, resulting in the error. The reason for the same was being pegged as a cyber attack. Apart from demanding a high-level enquiry against the software vendor, the university had no other response. This points to the consequences of institutions' complete dependence on third party vendors. Not only did the students face much inconvenience, the well-known university had to face reputational damage for the same.

In the case of a man-in-the-middle attack against a Mumbai school, it was the timely information provided by the school to the Central Cyber Police Station and the latter's quick interventions with multiple banks that enabled the recovery of the amount that had been transferred by the school to fraudsters, mistaking them for the company they were in touch with. This case points to a crucial reminder-coordination between law enforcement and other stakeholders at the earliest is paramount in countering and responding to cyber attacks.

70 schools

in Bangalore received hoax bomb threats via emails

December 2023

In December 2023, about 70 schools in Bangalore received hoax bomb threats via emails. This sent parents, school authorities and students into a panic and parents rushed to schools to pick up their wards. Although it was found later to be a hoax, the panic and fear remained for a while before things returned to normalcy. The fact that this isn't an isolated incident is worrisome. In cases like this, schools and other authorities find themselves in a fix and are unable to take any action in such an emergency situation other than sending students back home. As an aftermath though, some schools with the wherewithal have beefed up their physical security measures.

In cases where school websites were hacked by groups with political and religious motives, reports do not discuss their responses to the attacks. The case of the hacking of the AIIMS networks was not followed up with official information on how the issue was handled. Although it was alleged that a huge ransom was demanded, there is no official statement on whether the amount was paid. All that was reported was that it took about two weeks before the computer systems could come back online.

While much is not known in terms of how schools and universities are specifically responding to cyber attacks, what is clear is that there is much left to be desired. Given the statistics on attacks against educational institutions and the parallel lack of news reports and articles on actual cases, it is clear that most cases go unreported to the media and cyber crime officials. This trend needs to be overcome and the stigma around reportage must be done away with in order to enable authorities, journalists, researchers, policy makers and other stakeholders to find solutions specific to the issues faced by educational institutions in India.

SECTION 9

Impact on Educational Institutions

Cyber attacks have several short and long-term consequences on different stakeholders within educational institutions and others who are indirectly connected to them. Apart from its impact on the operations of the organisation and educational institutes, it affects students, their families and teaching and non teaching staff of such institutions. In this section we shall examine them in some detail.

Impact on the learning process

A report by the US Government Accountability Office (GAO) in which researchers interviewed school districts and other stakeholders, local and state officials informed that the loss of learning resulting from a cyberattack ranged from three days to three weeks and recovery from such attack could take anywhere between two to nine months.

Financial loss

The report by the US GAO revealed that officials from US schools reported monetary losses to school districts ranging from $50,000 to $1 million. These costs included expenses towards replacement of computer hardware and increased cybersecurity measures to prevent attacks in the future. The recovery time, on average, ranged from two to nine months.

Data security breaches

Cyberattacks against schools further result in breaches in the personal and confidential information of students, teachers and staff members. Such data breaches compromised information such as students' grades, social security numbers and bullying reports. Such data breaches can cause much emotional, physical and financial harm to students and staff. Financial losses can include unauthorised charges and stolen funds. Finally, data security breaches can result in cyber bullying, identity theft and harassment.

It further needs to be realised that apart from intentional data breaches, some are accidental as well. In other words, data breaches happen for a variety of reasons and there are multiple actors and motives in this realm. In fact, in some cases the intent for a breach can be unknown actors which include, apart from cybercriminals, school staff and students. In fact, a study in the US on schools showed that staff was often responsible for accidental breaches (21 out of 25) while students were primarily responsible for many intentional breaches (27 out of 52). Breaches by students were conducted often to change grades in the system.

Impact on reputation of institutional management

Cyberattacks affect the reputation of the university, college or school that become victims of it. As an aftermath of such attacks, the leaders of educational institutions face scrutiny from internal stakeholders like students and staff and external ones like public officials. Cyberattacks can impact the trust of staff, students and their families on the management's commitment to protect them, thereby impacting the retention of staff and students and new admissions. Further, such attacks draw negative media attention.

Impact on the safety of students

Apart from financial losses, disruptions to institution's operations and reputation, one major impact of cyberattacks is the harm it causes to students, who may be minors as well as young adults. Educational institutions are entrusted to safeguard students and cyberattacks can compromise this role. For example, the CCTV camera footage of several schools in the US was live streamed online for about an hour as a result of a breach before the feed was taken offline after authorities were alerted. Such breaches can cause much harm to the privacy of students leading to much distress and concern among students and their families. This can have a negative impact on the psyche, mental health and sense of personal safety of students.

SECTION 10

Recommendations for Strengthening Cybersecurity

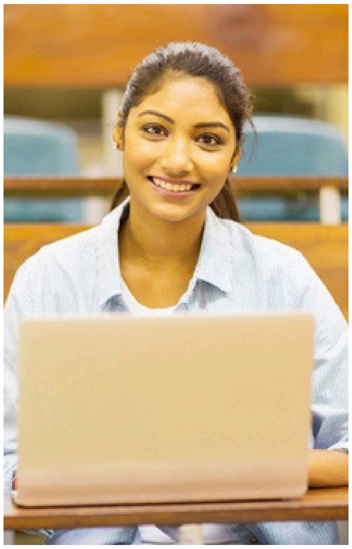
Educational institutions will continue to depend on technology for its operations in the future. As a result, the digital footprint of schools, colleges and universities will grow. In order to prevent and survive a cyberattack, educational institutions require access to security solutions customised to their needs. They need to also be able to adapt to the changing needs of the organisation. For maximum effectiveness, organisations need 24/7 support of experts to keep their systems protected. The challenge is to find the right resources to deliver these requirements.

We have already taken a look at the persistent challenges faced by educational institutions in protecting their data and network integrity. These recommendations are thus aligned to the most prominent challenges. Let us quickly recap them for our benefit. The major issues educational institutions confront in protecting the integrity of their computer systems are the lack of budget and resources (staff and software), cultural issues such as the ‘bring your own device’ norm in institutions and the lack of policies for using the network along with its implementation, given the user population is large and dynamic in nature. Institutions yet need to make it their priority to find solutions given how high the stakes are. Importantly, educational institutions must focus on preventing cyberattacks against its networks rather than reacting or responding desperately to issues once a breach has occurred, as that can prove very expensive.

In this context a simple solution that educational institutions can practise is to share information with students, staff and teachers about what they need to look out for, how to protect the network at all access points and tips for practising good cyber hygiene through training and awareness sessions and takeaway handbooks. A second cost- effective method that IT professionals can employ is to use a multi-factor authentication (MFA) tool that is user-friendly. This can go a long way in preventing unauthorised access. Priority must be given to ensure that such tools are user friendly so that all stakeholders are able to use a platform self-sufficiently. This can ensure that educational institutions are able to save on overheads without compromising their network security. In the face of increasing frequency and potential severity of cyberattacks to educational institutes, it is crucial for IT professionals to find solutions that are effective while being relatively simple to implement and cost effective to reduce the human error factor and protect the network from unauthorised access.

Higher educational institutions especially need to establish policies and control measures to protect their cyber systems. They must follow security frameworks that provide better information security experiences by laying out the policies, tools and procedures that can enhance and maintain a secured information system. Additionally, for a more robust information security management system, it is important to perform risk management which refers to- confidentiality (confirms that only authorised persons have access to information), integrity (determines the accuracy with which data is processed) and availability (ensures that authorised persons are able to access the data upon request) of data related to the critical assets of colleges and universities. Assets of organisations are generally divided into primary and support ones. Primary assets consist of all the processes and activities specific to the organisation. In this case higher educational institutions' support assets consist of hardware, software, network, staff and website. Risk management comprises three processes- risk estimation, risk mitigation and risk assessment. A robust risk management following these processes can result in reduced financial losses and reputational damage.

Universities are complex organisations that require appropriate information systems to carry out their varied activities. University information systems are heterogeneous in that it consists of different applications, platforms, academic systems and cloud applications, all of which are necessary for the processes of teaching, learning and the conduct of research activities. In this context, several researchers believe that efficient management of the IT infrastructure of universities requires the implementation of IT governance (ITG). ITG refers to a set of relational structures, processes and mechanisms that support the institution's management to effectively manage its IT resources. An effective and robust ITG can thus act as a guide for the implementation of the institution's cyber security control system.



With this overview, we shall look at specific strategies that different stakeholders in an educational institutional matrix can follow to ensure that computer networks and systems are as safe as possible, in the following section.

Recommendations : Stakeholder Wise

	Recommendation
01 Staff, students and other institutional stakeholders	✓ Attend training and awareness sessions on common breach attempts and how to respond to them ✓ Use strong and unique passwords for different applications ✓ Use Virtual Private Networks (VPNs) and avoid unsecured networks ✓ Exercise caution when downloading files and email attachments from unsolicited sources ✓ Pay attention to ensure that one does not inadvertently download files from organisations or individuals impersonating others ✓ Users must not open attachments or URL links from unsolicited emails ✓ Users must use only secure web browsers
02 Network administrators and cybersecurity personnel	✓ Establish and regularly update the institution's information security policy and incident response plan ✓ Ensure effective implementation by making sure all stakeholders follow the best practices laid out in the policy and plan ✓ Conduct tests of the organisation's and individual's knowledge of and preparedness for cyber attacks by performing controlled social engineering experiments and attacks ✓ Enforce multi-factor authentication for access to sensitive resources

Recommendation

- Oversee privileged access management and ensure authentication is required for sensitive data
- Maintain a firewall
- Monitor network activity for suspicious or malicious activity Audit third-party vendors to understand their risk profiles
- Use encryption and offline data backups wherever necessary Regularly update security software, operating systems and other applications to protect against known vulnerabilities
- Robust email filtering and web security solutions to detect and block malicious content must be implemented
- Regularly check data and code/scripts integrity
- All accounts should have strong and unique passwords
- Have an account lockout policy
- Have a proper Remote Desktop Protocol logging and configuration
- Have a spam-proof email validation system

03

Management of educational institutions

- Invest in cybersecurity to minimise known and emerging threats in cyberspace
- Create and implement an efficient IT governance system
- Commission risk assessments specific to the organisation's requirements and act on its findings. They help identify the most likely risks and the ones that can cause most damage.
- Promote cybersecurity awareness training and awareness for all stakeholders including IT personnel, staff and students
- Implement/authorise a trusted cybersecurity framework to manage the institution's cloud security (International researchers identify the five functions of a security framework as- identification, protection, detection, response and recovery).

Recommendation

- Ensure background verification of all hired staff, including temporary and permanent staff, is conducted to check for any legal violations, especially in the area of child protection and safety, and other related areas

04

Staff of Educational Institutions

- Follow standardised cybersecurity protocols and procedures
- Communicate and collaborate with IT personnel regarding IT framework responsibilities and accountability

05

Government agencies

- The **Indian Computer Emergency Response Team (CERT-In)** must commission in-depth research to understand risks and threats to educational institutions in India. Existing knowledge base for cyber threats is minimal in India. Investments into this would be necessary to prepare preventive strategies.
- **CERT-In** must also ensure that its guidelines are implemented by all organisations across sectors and that any threats and incidents are mandatorily reported to it to add to the public knowledge on evolving trends in this area.
- The **DPDP Act** must be examined in detail to create guidelines based on it specific to educational institutions of various sizes and purposes in order to find implementable solutions

  The National Cyber Security Coordinator (who coordinates with different agencies at the national level on cybersecurity issues) must create a separate structure for educational institutions since they pose a major risk on cybersecurity related matters and do not have any specific agency overseeing such matters with respect to issues specific to them.
- The **Cyber Swachhta Kendra** (Botnet Cleaning and Malware Analysis Centre) must institute a separate team to specifically examine threats and risks to educational institutions. They must provide free tools tailored to suit their specific needs and training for educational institutes to counter the menace of malware.
- The National Cyber Coordination Centre must conduct training sessions for stakeholders within the education ecosystem to ensure preparedness to prevent cyber threats and to reduce the human error factor.

06

Parents of school, college and university students

Recommendation

- ✓ As much as possible, parents of students must attempt to have a mediation strategy to discuss and communicate with their children about their online interactions and educate them about potential cybersecurity threats. Avoiding restrictive measures can be a good enabler for creating safe spaces.

Some of the strategic systemic Policy level recommendation for the Government agencies includes the following -

More organisations in the private sector, including universities, could be encouraged to sign the Digital Geneva Declaration with the aim to protect users and customers from cyber breaches, to collaborate with like-minded intergovernmental and state frameworks.

Increased funding to educational institutions to ensure that students, data and institutions are all safe from the harms caused by cyber attacks.

International cooperation to keep digital spaces secure since most cyberattacks originate from beyond borders. Although India has signed cybersecurity treaties with countries such as the US, UK, Russia, South Korea and the EU. Other multinational frameworks such as the 12U2 (India, Israel, UAE, US) and Quad (India, Australia, Japan & USA) have undertaken efforts to enhance cooperation in cyber incident responses, technology collaboration, capacity building and improved cyber resilience. What is lacking though is a global framework to prevent and counter cyber issues.

Schools and universities should have counsellors for students' welfare to help them in cases of data breach or cyber abuse resulting from a compromised network at the school, college or university level.

Training for all stakeholders in the education ecosystem must be robust, periodic and mandatory. Government agencies, civil society and other organisations must proactively design programs for training all stakeholders effectively.

All educational institutions must form steering committees that consist of senior management, the Chief Information Officer and other departmental representatives that report to the head of the institution. This committee must provide oversight of all cybersecurity related initiatives of the institution. They must prepare strategic plans for preventing, detecting and remediating cybersecurity issues and develop KPIs aligned with said strategic plans for monitoring and accountability purposes.

Technological countermeasures to address AI-based cyber threats must be made freely available to educational institutions, especially those that are in rural areas, smaller-sized institutions and those lacking the wherewithal to fund expensive tools and equipment.

In summary, educational institutions must implement comprehensive cybersecurity measures to protect the privacy and data of students and staff and to protect the integrity of the institution's network along with the intellectual property held therein. Some methods to achieve this include strict access control mechanisms, restricting access to sensitive data to authorised personnel by encrypting sensitive data. Regular monitoring checks of network systems for vulnerabilities and prompt response to any issue are paramount. Finally, to reduce internal issues related to human error and foul play by internal actors, it is important to periodically educate staff, students and parents about cybersecurity threats and best practices to minimise risks and conduct background checks of all staff and faculty hired.

We have seen through this report that cyberattacks have been on the rise in educational institutions. Yet, studies in the field of cybersecurity in educational institutions have been extremely limited. At the same time, existing studies do not sufficiently cover issues related to the implementation of cybersecurity policies and efficiency analyses of existing cybersecurity frameworks. This is especially abysmal in the case of examination of cybersecurity issues in the Indian context.

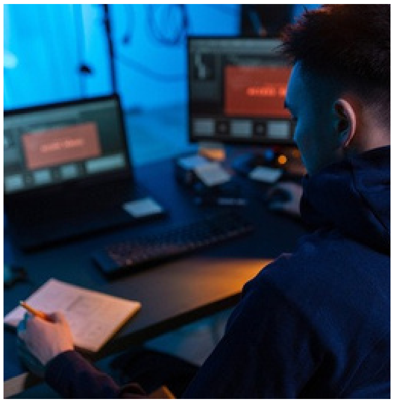
The ISO27001 standard mentioned earlier in the report, apart from the technical aspects covered, also discusses specific controls for human resource management, legal constraints and organisational management. As a research study at a university (Itradat A et. al. as cited in Alexei, A. 2021) recognises, this is due to the fact that cyber security depends more on the human factor than the technology used, and security threats coming from within the institution can be far greater than external ones. Another academic research study on the cyber security threat analysis in higher educational institutions found that personnel represent the most abstract category of vulnerabilities and that attacks based on human behaviour represent 90 percent of all cyber attacks. Research into human error and other forms of insider threats and risks within universities can be crucial in providing a glimpse into specific internal issues related to educational institutions that can then be employed to make changes and additions to the security system.

Finally, more micro level studies are required to understand how different regions and institutions of different sizes and resources are being affected. The impact on stakeholders, both in the short and long-term, and how those can be mitigated are all relevant. Data on threat actors, victims, attack vectors, incidents are all crucial going forward to enable India to carve its own response to this increasing menace.

SECTION 11

Summary of Key Findings and Conclusion

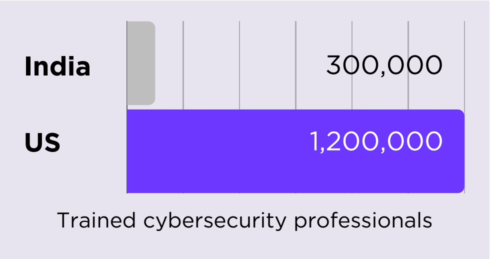
This research report set out to examine cyber risks, threats and incidents in Indian schools, colleges and universities with the aim of understanding its impact and suggesting remedial measures and solutions to prevent and combat them. As we've seen, cyber risks and threats abound in educational institutions globally and also in the case of India. In fact, schools and colleges are amongst the top sectors facing threats and incidents in recent times. However, educational institutions face specific challenges with respect to countering cyber incidents and preventing them. These include lack of sufficient funding, lack of awareness among all stakeholders, among others. Additionally, apart from the large volume of data they manage, Higher Education Institutions' (HEIs) networks are often open in design, decentralised and have a large number of users, rendering them vulnerable to cyber attacks. As a matter of fact, experts believe that educational institutions are more than twice as vulnerable than organisations in other sectors to business email compromise attacks.



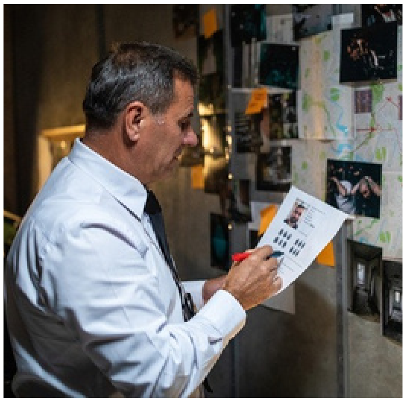
At the same time, cyber criminals have diversified their focus to target multiple sectors, with an ever increasing threat landscape. While cyber threats are persistent, they are constantly evolving in their nature. Safeguarding people, organisations and data are now paramount. Schools and colleges are particularly vulnerable to hacking, malware, ransomware, among other persistent threats. Two reasons causing successful ransomware attacks were exploitation of vulnerabilities and compromised credentials.

A nation like India, as other developing nations, finds itself at a critical juncture in this regard since they are growing steadily in power, influence and knowledge, with resources, information and data that can be a boon for cyber criminals. At the same time, nations like India are only catching up with respect to cyber safety measures and awareness. Limited funding and limited knowledge are limiting factors. Simultaneously, India faces wide disparities with levels of education, literacy and resources to counter these rising issues in the area of cybersecurity. These are all factors that cybercriminals use to their advantage, rendering an urgency to counter cyber threats and attacks.

Another major challenge that India faces in this realm is the dearth of trained cybersecurity professionals in the nation. According to a report, India is projected to have about three lakh professionals in the sector in comparison to 1.2 million in the US.



We have also seen that human error plays a key part in cyber incidents at educational institutions. Both the lack of awareness and accidents on the part of students, teachers and staff can compromise a network. It is hence essential that all stakeholders in educational institutions are provided periodical and engaging training and awareness on good cyber hygiene practices, motives and methods of cyber attackers and means by which they can keep themselves, their data and intellectual property safe and protected. Effective training can mitigate the effects of a lack in funding and resources that are common challenges faced by educational institutions.



A major challenge faced in terms of a way forward is the lack of micro data and case study knowledge about cyber security incidents in schools and colleges in India. Although there is macro level data to suggest that incidents are increasing, reportage of cases needs to improve. Not only will this provide data that researchers, policy makers and government agencies can use towards finding specific solutions, it will also enable individuals, students and their families to find ways to keep themselves protected.

Available data points to the fact that educational institutions in India are far from equipped to prevent or respond to cyber attacks. These have caused much panic, uncertainty and fear among students, parents and others and affected the reputation of well-known educational institutions. It is important for all stakeholders to implement guidelines provided by government agencies and recommendations in this report towards being better prepared to face such issues in the future.

Finally, organisations, including educational institutions, need to be proactive and follow a comprehensive approach to cybersecurity. Especially given the risk to students which includes psychological harm and trauma, this becomes a key responsibility for institutions.

SECTION 12

Annexure

How Cyberthreats Affect Educational Institutes: An Examination of Select Case Studies

As we have seen, cybercriminals employ different forms of tactics to dupe people and institutions. In this section we shall examine some recent cases to understand a range of incidents and threats that are common to schools, colleges and other institutions in India.

CASE STUDY 01

Man-in-the-Middle attack: A case of misspelt email IDs

In a case from an international school in Mumbai, a simple ploy of replacing the letter ‘u’ with ‘v’ led to the school transferring over Rs 87 lakh to fraudsters. Hearteningly though, much of the amount was successfully recovered by the Mumbai police. Let us understand the case a little better.

The school was in conversation with a vendor based in the UAE named Europhone Acoustics for some construction work in the school. Cyber criminals managed to gain access to the email conversations between the two and created an email ID similar to the one from which the company’s had communicated with the school. To mimic the original ID arul@eurosystems.com, the fraudsters created a similar one i.e. arul@evrosystems.com. The criminals then emailed the school from the latter ID asking the school to deposit an amount of Rs 87 lakh to a specific bank account, which the school did. They had also created a second fake email ID to mimic a CCed email ID by the original company which was abhay@eurosystems and created one abha.y@eurosystems to further trick the school. Later, when the original company communicated the cost to the school, they said that the amount was already transferred. This led them to investigate the issue and the case of the fake IDs was revealed. The school registered the crime with the Central Cyber Police Station which got into action immediately and contacted the banks and other intermediaries to recover almost the entire amount that the school had transferred.

As is clear from this case, even simple tactics can lead to a huge loss. Attention must be paid each time one communicates via email and other means to organisations or individuals.

Database compromised, sensitive information leaked from a private university

An alleged cyberattack on the Jaypee University of Engineering and Technology this year has led to the university's database getting compromised and sensitive information such as names, email IDs and contact numbers getting leaked. Responsibility for the attack was claimed by a threat actor on Telegram and the motive was said to be retaliation for Indian aggression along the border. The hacker's location, origin and the border in question is not known. The university's website appeared to be operational and no immediate signs of a cyberattack were discernible. This indicates that the attack is characterised by a leak without any defacement.

In another case from late last year, a Noida school's website was hacked by an unknown group that called themselves 'Bangladeshi.' The group left several messages on the website along with a flag of Bangladesh. According to a report by the organisation Group-IB, the group has attacked multiple sectors in India. They are known to be driven primarily by a religious and political motive.

We see therefore that in contrast to the previous case, in this one the hackers goal was to deface the school website.

CASE STUDY 02

Pakistan-based group using malware to acquire sensitive information from top universities

CASE STUDY 03

A Pakistan-based group called Transparent Tribe has been conducting cyberattacks against the education sector, along with the Indian Army. The motive of these sophisticated attacks is to deceive unsuspecting victims to gain sensitive information. The group is believed to have originated in 2013. Their attacks against top institutions such as the IITs and NITs began circa May 2022 and peaked in early 2023. Their modus operandi is to use malicious files disguised as a legitimate document. These files contain embedded malware that can exploit vulnerabilities.

A primary preventive measure would be to exercise caution when downloading files and email attachments from unsolicited sources. As we have seen in the above case, attention to detail is paramount to ensure that one does not inadvertently download files from organisations or individuals impersonating others. Other protective measures include regularly updating security software, operating systems and other applications to protect against known vulnerabilities. Robust email filtering and web security solutions to detect and block malicious content must be implemented.

Ransomware attack on All India Institute of Medical Sciences

CASE STUDY 04

In November 2023, the e-services of the All India Institute of Medical Sciences were down due to a suspected ransomware attack. AIIMS' Local Area Network (LAN) comprises over 6500 computers across its institute, hospital, centres and other departments. Preliminary findings into the case indicated that at least five of the institute's servers that hosted data of over three crore patients were compromised. It took over two weeks for the system to come back online. According to reports, hackers had demanded about Rs 200 crore in cryptocurrency from the hospital.

It was suspected that a malware may have been injected remotely by tricking the user to download it by clicking on a seemingly safe web link sent via an email. This could've then spread throughout the network by exploiting vulnerabilities. In cases like these, ransomware incidents can be accompanied by theft of sensitive data which can then be capitalised on with further malicious motives.

Key Terms and Definitions

Attack surface or attack vectors: An organisation's attack surface is the totality of all vulnerabilities, pathways and methods, also called attack vectors, that can be used by cybercriminals to gain unauthorised access to its network or sensitive data or, alternately, to carry out a cyber attack. As organisations adopt hybrid work models and cloud services, their networks and associated attack surfaces become larger and more complex. Digital attack surfaces include weak passwords, misconfiguration, software, operating system & firmware vulnerabilities, among many others.

Cybersecurity incident: An incident related to cybersecurity that actually or potentially jeopardises a system or the information contained in it.

Dark web: It refers to a hidden part of the internet that is not indexed by regular search engines. It is accessed through specialised web browsers such as Tor. Given this characteristic, it hosts both legal and illegal activities. An advantage of the dark web is that it provides anonymity but at the same time, as a flip side, it poses risks of scams and illegal content.

Deep fake: A deep fake is an artificial image or video that is generated by a special form of machine learning called 'deep' learning, from which it receives its name. Although initially considered harmless, deep fakes are now misused to malign famous and high-profile people such as politicians, actors and others to reduce their popularity in general or prior to important events such as elections.

Encryption and decryption: Encryption is the process which converts a readable message into an unreadable form to prevent unauthorised parties from accessing it. Although it has been used traditionally to protect sensitive information, cybercriminals are now using it to prevent data owner's from accessing their own information. This happiness when encryption keys are lost or destroyed. Criminals can use it to gain access to sensitive data and to perform ransomware attacks. Decryption, on the other hand, is the process of converting an encrypted message back to its original readable format.

Endpoint: These are physical devices that connect to and exchange information with a computer network. Examples of endpoints include mobile devices, desktop computers, virtual machines, embedded devices and servers.

Phishing: Phishing is a practice of sending fraudulent communications that appear to come from reputable sources to different users. It can be done through various methods including email and instant messaging. The goal of a phishing attack is to steal sensitive data like credit card or login details or to install malware on the victim's machine. This happens when a victim unwittingly clicks on links shared in phishing messages.

Key Terms and Definitions

ITG: IT governance (ITG) refers to a set of relational structures, processes and mechanisms that support the institution's management to effectively manage its IT resources. An effective and robust ITG can thus act as a guide for the implementation of the institution's cyber security control system.

Malware: Malicious software or malware is any intrusive software developed by cybercriminals to steal data or to damage or destroy computer systems. Examples include viruses, worms, Trojan, spyware, adware and ransomware.

Principle of Least Privilege (POLP): The principle of least privilege is a criterion that a user, program or process should have only the bare minimum privileges necessary to perform its functions. It is considered a best practice in information security.

Ransomware: Ransomware is a type of malicious software, used by cyber criminals, to infect a computer system by blocking access to the stored data by encrypting the files. A ransom is then demanded from the owner in exchange for the decryption key.

Threat actors: Threats actors comprise of individuals or groups that seek to breach or undermine systems and data security by involving in direct data theft, phishing or compromising a computer system by exploiting vulnerabilities or creating malware. The purpose of data security infrastructure is to detect and contain attacks by threat actors.

References

Abi Tyas, Tunggal. (2023, April 18). What is an insider threat? Definition, examples, and mitigations. UpGuard. Retrieved April 2, 2024, from https://www.upguard.com/blog/insider-threat

Ahaskar, A. (2020, October 30). Over 1,000 Indian schools, colleges targeted in cyberattacks in Jun-Sep: Report | Mint. https://www.livemint.com/technology/tech-news/over-1-000-indian-schools-colleges-targeted-in-cyberattacks-in-jun-sep-report-11604044942722.html Accessed 20 April, 2024

AICTE Cybersecurity Strategy for Higher Education Institutes.

Alexei, Arina. 2021. Cyber Security Strategies for Higher Education Institutions, Journal of Engineering Science, Vol. XXVIII (4), pp. 74-92

Antony, A. K. (2023, February 25). Cyberattacks are rising, but there is an ideal patch. The hindu. https://www.thehindu.com/opinion/op-ed/cyberattacks-are-rising-but-there-is-an-ideal patch/article66550210.ece Accessed 20 April, 2024

Aradhya, Rohit. (2024, April 1). Cyberattacks can be devastating; Here's how AI could make them worse. Financial Express. https://www.financialexpress.com/business/digital-transformation-cyberattacks-can-be-devastating-heres-how-ai-could-make-them-worse- 3440139/ Accessed 26 April, 2024

Arctic Wolf. (2023, December 18). 8 Major cyber attacks against schools and colleges. https://arcticwolf.com/resources/blog/cyber-attacks-against-schools-and-colleges/ Accessed 6 April, 2024

As cyberattacks increase on K-12 schools, here is what's being done. (2024, March 21). U.S. GAO. https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done Accessed 4 April, 2024

A server leak put student data from Byju's at risk, says report. (2021, June 30). Moneycontrol. https://www.moneycontrol.com/news/technology/a-server-leak-put-student-data-from-byjus- at-risk-says-report-7109731.html Accessed 21 April, 2024

Australian Signals Directorate. (2017, February 1). Essential Eight Explained. www.cyber.gov.au. Retrieved May 8, 2024, from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eightexplained

Bharadwaj, KV Aditya & TR, Jahnavi. (2024, February 8). New cyber threats catch India's IT Capital, Bengaluru, unawares. The Hindu. https://www.thehindu.com/news/cities/bangalore/cyber-threats-throw-an-it-city-into- chaos/article67636818.ece Accessed 23 April, 2024

Brenneman, Richard. (2009, August 6). *Hackers Strike UC Journalism School's Computer system. Category: Extra from the Berkeley daily Planet*. https://www.berkeleydailyplanet.com/issue/2009-08-06/article/33488?headline=Hackers- Strike-UC-Journalism-School-s-Computer-System Accessed 8 April, 2024

Centre for Internet Security and Multi-State Information Sharing & Analysis Centre (MS-ISCA), K-12 Report: A Cybersecurity Assessment of the 2021-2022 Scholl Year

References

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher education Institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192 Accessed 23 April, 2024

Cybersecurity threats in educational institutions / Prey. (2024, April 30). https://preyproject.com/blog/cyber-security-threats-it-professionals-in-education-face Accessed 06 May, 2024

DeForge, J. (n.d.). *The impact of Cyber-Attacks on schools*. https://blogs.iuvotech.com/the-impact-of-cyber-attacks-on-schools Accessed 4 April, 2024

DSCI and SEQRITE. 2023. India Cyber Threat Report 2023.

Economic Times (2023, September 4). 3 out of 4 cyber attacks in education sector associated with compromised on-premises user or admin account.. *ETCIO.com.* https://ciosea.economictimes.indiatimes.com/news/security/3-out-of-4-cyber-attacks-in- educat ion-sector-associated-with-compromised-onpremises-user-or-admin-account- report/103337437 Accessed 21 April, 2024

Education sector emerges as most targeted sector for cyber attacks in April-June: Study. (2023, November 1). The Economic Times. https://economictimes.indiatimes.com/tech/technology/education-sector-emerges-as-most-targetted-sector-for-cyber-attacks-in-april-june_study/articleshow/104889132.cms?from=mdr Accessed 10 April, 2024

Express News Service. (2024, April 18). How fraudsters duped a Mumbai school of Rs 87 lakh by changing ‘U’ to ‘V’ in email, police recovers money. *The Indian Express. https://indianexpress.com/article/cities/mumbai/police-recover-rs-82-lakh-from-cyber- fraudsters-mumbai-school-9264913/ Accessed 19 April, 2024*

First Post. (2023, July 26). How Pakistan is targeting students from army schools in India to seek sensitive info. *Firstpost*. https://www.firstpost.com/explainers/how-pakistan-is-targeting- students-from-army-schools-in-india-to-seek-sensitive-info-12916342.html Accessed 23 April, 2024

Free Press Journal (2023, July 25). Pakistani intelligence operatives target school students in a new kind of cyberattack, warns Indian Army. Free Press *Journal*. https://www.freepressjournal.in/education/pakistani-intelligence-operatives-target-school-students-in-a-new-kind-of-cyberattack-warns-indian-army Accessed 20 April, 2024

Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Centre for a New American Security, Electronic Frontier Foundation, & Open AI. (2018). *The Malicious Use of Artificial intelligence: Forecasting, Prevention, and Mitigation*. Retrieved April 26, 2024, from https://arxiv.org/pdf/1802.07228 Accessed 26 April, 2024

General Data Protection Regulation (GDPR) – legal text. (2024, April 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/ Accessed 08 May, 2024

Gurinaviciute, Juta. 2024 https://www.forbes.com/sites/forbestechcouncil/2024/03/11/what-cybersecurity-threats-does-the-education-sector-face/?sh=2589415b4b90 Accessed 3 April, 2024

IBM Security. Cost of Data Breach Report 2023.

References

India Today. (2024, January 18). *Cybersecurity in education: Protecting student data in the digital world*.https://www.indiatoday.in/education-today/featurephilia/story/cybersecurity-in-education-protecting-student-data-in-the-digital-world-2490262-2024-01-18 Accessed 9 April, 2024

iSphere. (2024, April 17). *K-12 Cybersecurity Best practices to Safeguard your school*. iSphere. https://www.isphere.net/k-12-cybersecurity-best-practices/ Accessed 06 May, 2024

Jimenez, O., & Lyngaas, S. (2022, May 9). Predominantly Black college to shut down after Covid-19 and cyberattack burdens. CNN. Retrieved April 2, 2024 from https://edition.cnn.com/2022/05/09/us/lincoln-college-shutting-down-ransomware- attack/index.html

Khaitan, A. (2024, February 19). Jaypee University cyberattack: Hackers claims data access. *The Cyber Express*. https://thecyberexpress.com/jaypee-university-cyberattack-india/ Accessed 19 April, 2024

Muncaster, P. (2024, February 27). School CCTV streams end up on US website. *Infosecurity Magazine*.https://www.infosecurity-magazine.com/news/school-cctv-streams-end-up-on-us/ Accessed 8 April, 2024

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In NIST CSWP 29 [Report]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdfAccessed 08 May, 2024

New Zealand: Cybersecurity. (2022, February). www.dataguidance.com. Retrieved May 8, 2024, fromhttps://www.dataguidance.com/opinion/new-zealand-cybersecurity#:~:text=There%20is%20a%20strong%20relationship,2020%20('the%20Act'). Accessed 08 May, 2024

NordLayer. (2024, April 22). Cybersecurity in education: back to school, back to risks. NordLayer. https://nordlayer.com/blog/cybersecurity-challenges-in-education/ Accessed 27 April, 2024

Press Trust of India & Business Standard. (2023, August 11). Noida school's website hacked by group identifying as "Bangladeshi." www.business-standard.com. https://www.business-standard.com/india-news/noida-school-s-website-hacked-by-group-identifying-as- bangladeshi-report-123081100008_1.html Accessed 19 April, 2024

Privacy Act 2020 No 31 (as at 06 December 2023), Public Act 22 Information privacy principles New *Zealand Legislation* (2024, February 13). 08 – https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23342.html Accessed May, 2024

Rao, H. C. (2020, October 7). Mumbai University distance education exams hit by "cyber attack" on server. The Times India. https://timesofindia.indiatimes.com/city/mumbai/mumbai-university-distance-education- exams-hit-by-cyber-attack-on-server/articleshow/78525093.cms Accessed 23 April, 2024

Rohit KVN (2023, November 7). *Explained | What are deepfakes and how to spot them*. Deccan Herald.https://www.deccanherald.com/technology/what-are-deepfakes-heres-how-to-spot them-2760185 Accessed 23 April, 2024

Saini, N. (2023, June 26). Pakistan-based threat actors attacking IITs, Indian Army: Modus operandi, motive, and other details to know | *Mint*. https://www.livemint.com/technology/tech-news/pakistanbased-threat-actors-attacking-iits-indian-army-modus-operandi-motive-and-other-details-to-know-11687759925987.html Accessed 20 April, 2024

References

Sheldon, R., Loshin, P., & Cobb, M. (2024, February 7). encryption. security. https://www.techtarget.com/searchsecurity/definition/encryption Accessed 23 April, 2024

Sur, A. Pandey, Devesh K. (2022, December 4). *Explained | Are ransomware attacks increasing in India?* The Hindu. https://www.thehindu.com/news/national/explained-are-ransomware- attacks-increasing-in-india/article66207006.ece Accessed 20 April, 2024

Secure. (2022, August 22). Why cybersecurity needs to be a priority for the education sector. https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/ Accessed 8 April, 2024

TechCrunch. (2023, August 25). https://techcrunch.com/2023/08/25/byjus-student-data- exposed/ Accessed 21 April, 2024

The Hindu Bureau. (2022, November 30). AIIMS continues silence on media reports of ₹200- crore demand by hackers. The Hindu. https://www.thehindu.com/news/cities/Delhi/aiims- continues-silence-on-media-reports-of-200-crore-demand-by-hackers/article66201742.ece Accessed 20 April, 2024

The Hindu Bureau. (2023, March 30). Chennai’s cybercrime police detain man for selling personal data of school students. The Hindu. https://www.thehindu.com/news/cities/chennai/chennais-cybercrime-police-detain-man-for- selling-personal-data-of-school-students/article66676982.ece Accessed 21 April, 2024

The Hindu Bureau. (2023b, May 25). *Education sector worst hit as ransomware attacks rise in India: Report*. The Hindu. https://www.thehindu.com/sci-tech/technology/education-sector-worst-hit-ransomware-attacks-rise-india/article66891972.ece Accessed 20 April, 2024

The 5 biggest cyber threats for the education sector in 2024 | UpGuard. (n.d.). https://www.upguard.com/blog/cyber-threats-education Accessed 18 April, 2024

Top cybersecurity regulations in India [Updated 2024] | UpGuard (n.d.) https://www.upguard.com/blog/cybersecurity-regulations-india#:~:text=The%20Information%20Technology%2 0Act%2C%202000&text=While%20India%20does%20not%20have,critical%20information%20infrastructure%20in%20India. Accessed 08 May, 2024

United States Government Accountability Office. Sept 2020. Data Security: Recent K-12 Data Breaches Show that Students are Vulnerable to Harm, https://www.gao.gov/assets/gao-20-644.pdf Accessed 4 April, 2024

United States Government Accountability Office. Oct 2022. Critical Infrastructure Protection: Additional Federal Coordination is Needed to Enhance k-12 Cybersecurity, https://www.gao.gov/assets/730/723578.pdf Accessed 4 April, 2024

University of Calgary paid $20K in ransomware attack. (2016, June 8). CBC. https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack- 1.3620979 Accessed 8 April, 2024

U of C ransom payout better than battling hackers, expert says. (2016, June 8). CBC. https://www.cbc.ca/news/canada/calgary/university-of-calgary-cyberattack-part-of- increasing-problem-1.3621505 Accessed 8 April, 2024

References

Webroot & Wakefield Research. (2017). WebRoot Survey on IT security Concerns and Strategies of Small to Medium-Sized businesses in the US, UK, and Australia. In Webroot Survey [Report]. https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/2114/9911/0468/SMB-   MSP_Survey_US .pdf Accessed 27 April, 2024

What is an Attack Surface? | IBM. (n.d.).https://www.ibm.com/topics/attack-surface#:~:text=An%20organization's%20attack%20surface%20is,to%20carry%20out%20a%20c yberattack. Accessed 23 April, 2024

What is a Phishing attack? Definition and types. (2024, March 12). Cisco. https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html Accessed 23 April, 2024

What is Social Engineering? Definition + Attack Examples | UpGuard. (n.d.). https://www.upguard.com/blog/social-engineering Accessed 2 April, 2024

What is Social Engineering? (2023, November 1). usa.kaspersky.com. https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering Accessed 18 April, 2024

What is Spyware? | UpGuard. (n.d.). https://www.upguard.com/blog/spyware Accessed 2 April, 2024

What is the Deep and Dark Web? (2024, March 27). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/deep-web Accessed 23 April, 2024

Why is the Education Sector a Target for Cyber Attacks? | UpGuard. (n.d.-b). https://www.upguard.com/blog/education-sector-cyber-attacks Accessed 2 April, 2024

Zandt, F. (2024, March 26). The sectors most targeted by cybercrime. Statista Daily Data. https://www.statista.com/chart/31985/number-of-cyber-attacks-recorded-per-sector/?_utm_source=Statista+Newsletters&utm_campaign=1f25c39905-EMAIL_CAMPAIGN_2024_03_15_09__04_COPY_03&utm_medium=email&utm_term=0_-a4545a3122-%5BLIST_EMAIL_ID%5D Accessed 19 April, 2024

Collaborators:

CyberPeace

USI-CYBERPEACE CYBER CENTER OF EXCELLENCE

UNITED SERVICE INSTITUTION OF INDIA (Estd. 1870)

Autobot Infosec

SHAH & ANCHOR CyberPeace CENTER OF EXCELLENCE

SHAH & ANCHOR

Resecurity

www.cyberpeace.org| secretariat@cyberpeace.net| +91-9534456565

/cyberpeacefoundation /cyberpeacengo cyberpeace.org