1)   Although India had 40,000 job openings for cybersecurity professionals as of May 2023, 30% of these vacancies could not be filled due to huge skill shortage, reported TeamLease Digital, a subsidiary of TeamLease Services.

The demand for cybersecurity professionals has far exceeded supply, causing many businesses to struggle to recruit qualified personnel. Cyber Security skill sets that are in high demand include data privacy, cloud security, AI security, and network security. Soft skills such as problem-solving, communication, teamwork, and collaboration were also most sought after. The top job roles include IT auditor, Information Security analyst, Network/IT Security Engineer/Specialist, Security Testing/Penetration Tester, and Computer Forensics analyst, according to an analysis conducted by TeamLease Digital.

Sunil Chemmankotil, Chief Executive Officer, TeamLease Digital, said, as India Inc. embraced digital infrastructures, the heightened vulnerability to cyber threats necessitates proactive measures. The prevalence of malware attacks, social engineering tactics, and other sophisticated cyber threats require a comprehensive approach to safeguarding our digital frontiers, he added.

For instance, enterprises in the country have experienced over 2000 attacks every week in Q1 2023, marking an 18% increase compared to the previous year. The healthcare industry was a prime target, with 7.7% of attacks directed towards it, found TeamLease Digital.

2)

Nearly 60% of healthcare organisations globally have suffered a cyberattack in the past 12 months, [the *Economic Times* has reported](https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms), citing a new study by Sophos, a UK-based cybersecurity firm.

This includes India’s top institutions such as the All India Institute of Medical Sciences (AIIMS) and the Indian Council of Medical Research (ICMR), the newspaper reported.

Of these, cybercriminals were able to successfully encrypt data in nearly 75% of ransomware attacks – the highest rate of encryption in the past three years, the business daily reported.

This is a significant increase from the 61% data encryptions carried out last year, *ET* reported, citing the cybersecurity firm’s study.

In comparison, only 24% of healthcare organisations were able to disrupt a ransomware attack before the attackers encrypted their data. This, per the report, has fallen from 34% in 2022. This is also the lowest rate of disruption reported by the sector over the past three years, it added.

Last year, on November 30, the website of the Indian Council of Medical Research (ICMR) faced around 6,000 hacking attempts in 24 hours.

This happened a week after five servers of the All India Institute of Medical Sciences (AIIMS) [had been hacked](https://thewire.in/government/aiims-servers-cyberattack-ransomware-rajya-sabha) by ransomware. An estimated 1.3 terabytes of data was encrypted. The hackers had made it impossible for AIIMS to access its own data.

On October 31, 2023, in a massive data breach, information of over 81.5 crore Indians with the ICMR [were sold](https://www.financialexpress.com/healthcare/news-healthcare/questions-abound-but-icmr-still-silent-on-the-data-leak/3293107/) on the dark web.

Outdated software, legacy systems, and inadequate investments in cybersecurity has worsened the situation, Raj Sivaraju, president APAC, Arete, a cyber risk management firm, [told](https://www.hindustantimes.com/technology/why-is-healthcare-sector-a-new-target-for-cyberattacks-experts-insights-101698758038809.html) *Hindustan Times*.

As India moves towards digitising the healthcare sector, it has increasingly become important to secure the online systems.

India [was ranked](https://www.deccanchronicle.com/nation/in-other-news/310823/india-faces-3rd-most-cyber-threats-report.html) the third-worst country, following the US and Brazil, for cybersecurity risk events in the first half of 2023, according to Trend Micro’s 2023 report.

**The cyber threat landscape**

What’s even more concerning is that Indian firms cannot prevent almost half of cyber attacks, said a [report](https://www.deccanherald.com/business/indian-firms-cannot-prevent-almost-half-of-cyber-attacks-report-2753970) by Columbia-based cybersecurity company Tenable.

The report is based on an online study of 825 IT and cybersecurity professionals, of which 69 were Indians.

“In today’s threat landscape, by the time organisations react to cyberattacks, the battle is half lost,” Tenable India country manager Kartik Shahani told news agency PTI.

This is due to the lack of coordination between the IT and cybersecurity teams, a challenge acknowledged by 43% of Indian organisations, per the report.

The misalignment in goals between IT and security teams in organisations results in a palpable lack of synchronisation, making it challenging to work cohesively toward a shared goal, Shahani said.

As many as 78% of Indian respondents believe their organisations could better defend against cyber attacks with more resources dedicated to preventive cybersecurity. However, only seven in 10 (71%) organisations say their IT teams are more concerned with uptime than patching and remediation, the report said.

3)

The higher education institutions have become a huge target because of the large amounts of personal data, medical records, and advanced project research papers they store in their system databases.

We will take a more in-depth look at some key reasons why universities are being avidly targeted by cybercriminals.

* Universities, unlike their industrial counterparts, adopt a more open and transparent take on their infrastructure. These colleges and universities make sure that their sites can be connected to easily and without trouble by students and parents. This has unknowingly thrown the door wide open to cybercriminals.
* Many leading global universities were early adopters of digital tools and internet access. Their systems hold valuable troves of knowledge and research materials that go way back. This makes them attractive targets for data theft. The situation is exacerbated by the fact that, unlike corporate networks, educational networks aren't always the most advanced or up-to-date. Therefore, they don’t end up being a good match against the advanced and highly sophisticated tools of the modern cyber-criminal.
* Another reason why universities fall prey to cyber attacks is the limited talent in their cybersecurity or IT departments. Most technology graduates are lured away by handsome remuneration packages offered by companies like Apple and Microsoft. Thus, educational institutions, whose pockets aren't always as deep as the corporate bigwigs’, aren't necessarily able to attract the best talent who can keep their cybersecurity infrastructure robust and relevant all the time.

Common Cybersecurity Attack Trends

Now we’re going to take a look at some forms of cybersecurity attacks that pose potential risks to institutions of higher learning and ways to mitigate them.

* **Phishing -**This is one of the most common forms of cybersecurity threats we face today yet it’s not always easy to [identify a phishing attack](https://www.cm-alliance.com/cybersecurity-blog/how-to-identify-a-phishing-scam). Phishing attacks are a type of social engineering attack. To put it simply, when a cybercriminal takes up a false identity to scam or trick someone into soliciting sensitive/important information or installing some sort of virus/malware on their system through malicious downloads, it is known as phishing. These cybercriminals often use popular topics or extremely attractive propositions to lure users into clicking strange links or downloading dangerous files.
* **Ransomware -**After cybercriminals have managed to get your vital information or gained access to your crucial files, they then hold this information for ransom for outrageous financial demands. This is usually the aim of [ransomware attacks](https://www.cm-alliance.com/ransomware). So students who are innocently looking for help writing an essay or are in need of online writing assistance often fall prey to phishing attacks which can then lead to larger ransomware attacks on the network they were using.
* **Evolving Attacks -**As technologies become updated and evolved, so do cybersecurity attacks. One worthy of mentioning is fileless malware, which has been on the rise lately. This does not require the user to download any file or install any code. Instead, it uses the tools built into the system to initiate and perform these attacks. It makes legitimate programs execute dangerous attacks while your programs continue to run in the background. This form of attack is hard to detect as it leaves no footprint and is a nagging headache for most antiviruses

Solutions

While there’s no denying that the threat of cyber-attacks is imminent and almost every business and institution is likely to get attacked at some point in their existence, here are a few steps universities and schools can take to ensure greater protection from cyber threats and more resilience in case of an incident.

* [**Cybersecurity training**](https://www.cm-alliance.com/cyber-security-training-courses): Staff and students alike should be given relevant cyber awareness training. They need to be helped in understanding that they play an important role in organisational cybersecurity and often they can be the ones preventing a phishing attempt or a ransomware attack from having any significant impact on the organisation.
* **Make sure all systems are updated regularly**. Operating systems, browsers, and applications should always be up-to-date as each update fixes vulnerabilities and protects against new threats. This is a simple good practice that can make a world of difference when it comes to cyber safety of educational institutions.
* **Be Prepared**. While creating awareness and instilling the importance of good security habits is imperative, unfortunately, this may not be enough. Your school or university could still come under attack and it’s important to be prepared for that eventuality. Make sure you have a good [incident response plan](https://www.cm-alliance.com/cyber-incident-response-plan-template) or [ransomware response checklist](https://www.cm-alliance.com/ransomware-response-checklist) that your team can refer to in case of an incident. When a crisis hits, it becomes difficult to think straight so visual workflows and pre-vetted response plans can really help to cut the chaos and take the right steps.

4)

## Trojans

A Trojan program — like its namesake horse found in Greek mythology — pretends to be innocuous, but it is in fact malicious. A Trojan can’t spread by itself like a virus or worm, but instead must be executed by its victim, often through social engineering tactics such as phishing. Trojans rely on social engineering to spread, which puts the burden of defense on users. Unfortunately, in 2023, 7[4% of all breaches](https://www.verizon.com/business/resources/reports/dbir/) involved the human element, making Trojans especially dangerous to organizations.

***The King of Malware:***
Emotet — a Trojan spread primarily through phishing — first appeared in 2014. Since then, it has surged in and out of prominence multiple times, thanks to its modular structure and ability to serve as a delivery program for other forms of malware. According to CISA, “Emotet is difficult to combat because of its ‘worm-like’ features that enable network-wide infections.” This is likely why it’s gained a reputation in cybersecurity circles as the “king of malware.

### Ransomware

Arguably the most common form of malware, ransomware attacks encrypt a device’s data and hold it for ransom. If the ransom isn’t paid by a certain deadline, the threat actor threatens to permanently delete the data or — in [**double extortion models**](https://arcticwolf.com/resources/blog/dangers-of-double-and-triple-extortion/) — release the valuable data on the dark web.
Ransomware gangs, as well as individual actors, are continuing to see the payoff in attacking high-value targets like supply chains and critical infrastructure. The ransomware-as-a-service (RaaS) model is becoming a preferred method for threat actors, with many cybercriminals relying on specialized services and offerings to conduct intrusions, and we expect those offerings to expand and evolve in 2024 to bypass security controls.

See [***Arctic Wolf’s 2024 Cybersecurity Predictions***](https://arcticwolf.com/arctic-wolf-labs-2024-predictions/)

Fighting ransomware takes a holistic response. A managed detection and response (MDR) solution can help organizations monitor their environment and act in case of an immediate threat. In addition, security awareness training can help users spot social engineering tactics that may lead to a ransomware attack. If an incident occurs, having a strong incident response plan and solution can be the difference between stopping a threat and having to pay a hefty ransom.

***Maybe the House DOESN’T Always Win***
*All it took was one phone call to a third-party IT helpdesk by a member of the ransomware gang Scattered Spider (using ransomware from ALPHV and BlackCat) and suddenly MGM Resorts had 100 ESXi hypervisors encrypted and was unable to continue basic functions such as checking in guests, running casino operations, and more.*

*MGM Resorts lost $100 million due to canceled bookings, in addition to “$10 million in one-time expenses in the third quarter related to the cybersecurity issue, which consisted of technology consulting services, legal fees and expenses of other third-party advisors,” per their filing.*

### ILOVEYOU, worm, 2000

The ILOVEYOU worm was used to disguise itself as a love letter, received via email. Reports say that it infected more than 45 million people in the 2000s, causing more than USD 15 billion in damages.

ILOVEYOU is also considered as one of the first cases of [social engineering](https://gatefy.com/blog/social-engineering-what-it-and-how-it-works/) used in malware attacks. Once executed, it had the ability to self-replicate using the victim’s email.

Also see [*10 real and famous cases of social engineering*](https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/).

5)

DES:

Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security**.**Data encryption standard (DES) has been found vulnerable to very powerful attacks therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and [decryption](https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/), with minor differences. The key length is **56 bits**.

**The basic idea is shown below:**

We have mentioned that DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security**.**Data encryption standard (DES) has been found vulnerable to very powerful attacks therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of **64 bits** each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and [decryption](https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/), with minor differences. The key length is **56 bits**.

**The basic idea is shown below:**

We have mentioned that DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

[Advanced Encryption Standard (AES)](https://www.geeksforgeeks.org/aes-full-form/) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

* AES is a block cipher.
* The key size can be 128/192/256 bits.
* Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

**Working of the cipher :**
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

**RSA algorithm** is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and the Private key is kept private.

**An example of asymmetric cryptography:**

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client’s public key and sends the encrypted data.
3. The client receives this data and decrypts it.

Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

**The idea!** The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is a multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.