Data Breach

Published On: 26-12-2023

Why is in news?

In October, Resecurity, a US company, informed the world about the **availability of Indians' personal data on the dark web**.

It would have been easy to ignore this amid the deluge of bad news filling our news feeds but for the size and sensitivity of data. The seller of the data set was providing verifiable, **sensitive information of 55 per cent of the Indian population** — roughly around 815 million (81.5 crore) citizens.

This included **personally identifiable information** like name, phone number, Aadhaar number, passport number and address. All for a paltry sum of $80,000. On December 18, we learnt that Delhi police had arrested four individuals in this matter.

PII:

Personally Identifiable Information (PII) is information that when **used alone or with other relevant data, can identify an individual.**

PII may be direct identifiers like **passport information or quasi-identifiers** that can be combined with other information to successfully recognise an individual.

Thieves who have stolen names, Aadhaar numbers and passport information can **use that information not only to sign up for new accounts in the victim's name, but also** to commit tax identity theft, online-banking theft and other financially motivated scams.

We are already seeing a **rise in cyber frauds**, with people losing their life savings, taking on debt and suffering shame and stigma for having been scammed.

As **per the World Bank**, "India is one of the fastest growing economies of the world and is poised to continue on this path, with aspirations to reach high middle income status by 2047".

Our mobile phone usage, enhanced banking access and the ever-growing market size that generates enormous amounts of data not only makes us attractive to companies but also to bad actors.

No country is safe from data breaches. Eg, the Biden administration has issued multiple Executive Orders to modernise and implement stronger cybersecurity standards in the federal government.

Threats Arising from the Leaked Information:

Increased Cyberattacks: India has witnessed a significant rise in disruptive cyberattacks, leading to heightened risks of digital identity theft and cyber-enabled financial crimes.

Vulnerability to Identity Theft: With India ranking fourth globally in malware detection, the leaked information poses a serious threat, enabling threat actors to carry out various malicious activities, including online-banking theft

and tax frauds.

Impact of Unrest in West Asia: Recent disturbances in West Asia have exposed personally identifiable data, exacerbating the risk of identity theft and other cyber threats.

Safeguarding Personal Information for Users:

Check for Personal Data Leaks: Users are advised to ascertain whether their information has been compromised in the data breach.

Exercise Caution with Emails and Accounts: Vigilance is crucial, especially when dealing with emails from unknown sources, as stolen information may be used for phishing campaigns and brute force attacks.

Implement Two-Factor Authentication: To enhance security, users should enable two-factor authentication for all their online accounts and promptly report any suspicious activity to the authorities.

Be Mindful of Security Upgrades: Regularly updating security measures and staying informed about emerging threats is essential for safeguarding personal information.

Previous Instances of Data Breach:

Aadhaar data leaks were also reported in **2018, 2019, and 2022**, with three instances of large-scale leaks being reported, including one in which farmer's data stored on the PM Kisan website was made available on the dark web.

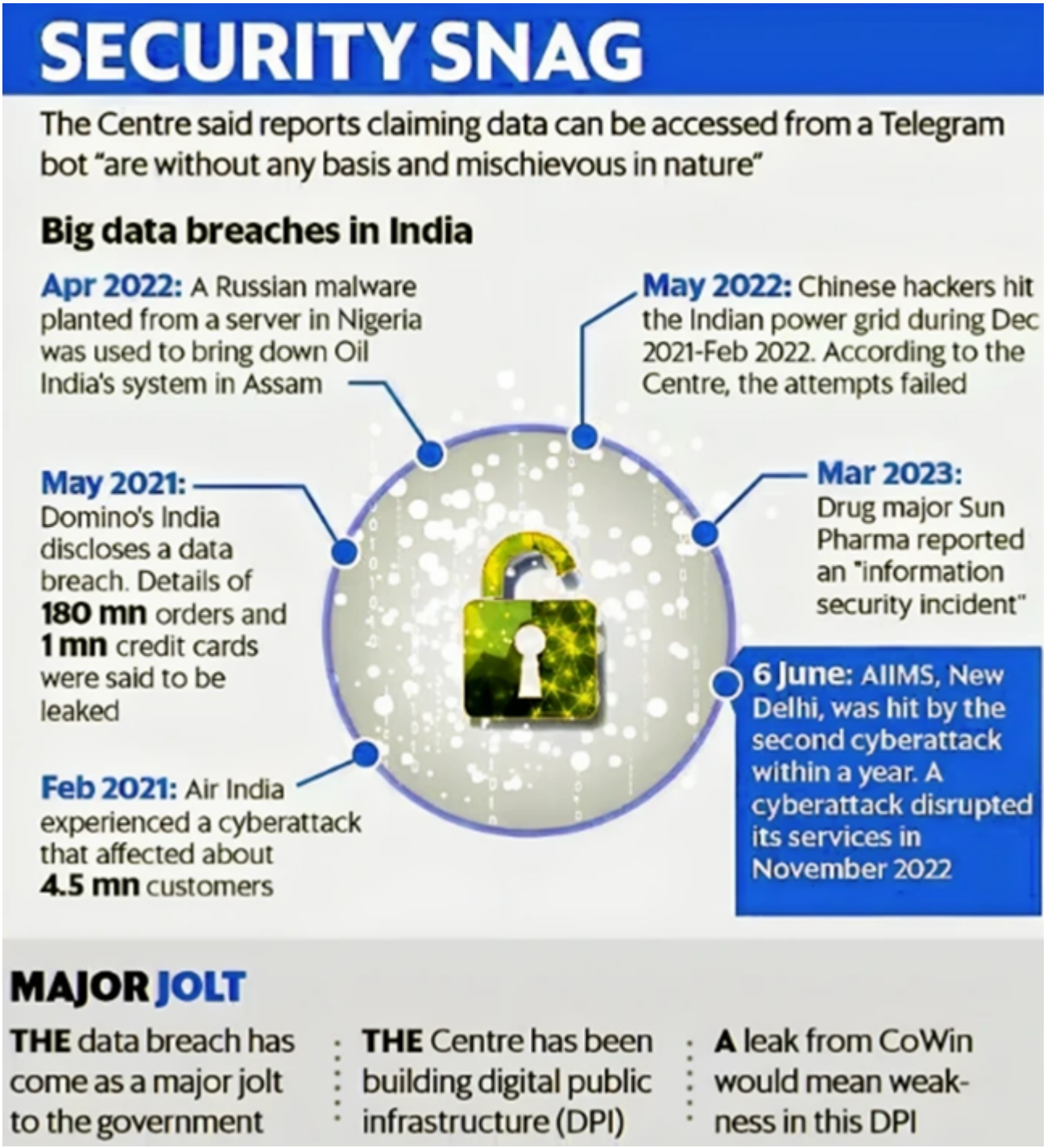
Earlier in 2023, reports emerged that a bot on the messaging platform Telegram was returning personal data of Indian citizens who registered with the Covid-19 vaccine intelligence network **(CoWIN) portal**.

Provisions Related to Data Governance in India:

IT amendment Act,2008:

Existing Privacy Provisions India has some privacy provisions in place under the IT (Amendment) Act, 2008.

However, these provisions are largely specific to certain situations, such as restrictions on publishing the names of juveniles and rape victims in the media.



Justice K. S. Puttaswamy (Retd) vs Union of India 2017:

In August 2017, a nine-judge bench of the Supreme Court in Justice K. S. Puttaswamy (Retd) Vs Union of India unanimously held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under Article 21.

B.N. Srikrishna Committee 2017:

Government appointed a committee of experts for Data protection under the chairmanship of Justice B N Srikrishna in August 2017, that submitted its report in July 2018 along with a draft Data Protection Bill.

The Report has a wide range of recommendations to strengthen privacy law in India including restrictions on processing and collection of data, Data Protection Authority, right to be forgotten, data localisation etc.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021:

IT Rules (2021) mandate social media platforms to exercise greater diligence with respect to the content on their platforms.

‘Digital India Act’, 2023 to replace IT act,2000:

?IT Act was originally designed only to protect e-commerce transactions and define cybercrime offenses, it?did not deal with the nuances of the current cybersecurity landscape?adequately nor did it address data privacy rights.

The new Digital India Act envisages to act as catalysts for the Indian economy by enabling more innovation, more startups, and at the same time protecting the citizens of India in terms of safety, trust, and accountability.

Way ahead:

Make the **prevention, detection, assessment, and remediation** of cyber incidents a **top priority**.

Recognise the **importance of digital infrastructure** as essential to national and economic security of the population.

Make the **state digital infrastructure trustworthy** by increasing transparency and accountability.

A **cyber security board** should be established with government and private sector participants that has the authority to convene, following a significant cyber incident, to analyse what happened and make concrete recommendations for improving cybersecurity.

Adopt a zero-trust architecture, and mandate a standardised playbook for responding to cybersecurity vulnerabilities and incidents.

Urgently **execute a plan** for defending and modernising state networks and updating its incident response policy.

Put **people at the centre of all policies**. Informing them immediately, helping them protect themselves and remediate fallout from cyber incidents should be the government’s responsibility.

We want a Digital India. Just not the Digital India we are living in at the moment.