8th Tech talk on employee benefits

Venue Webinar session

Date 9th Nov 2023

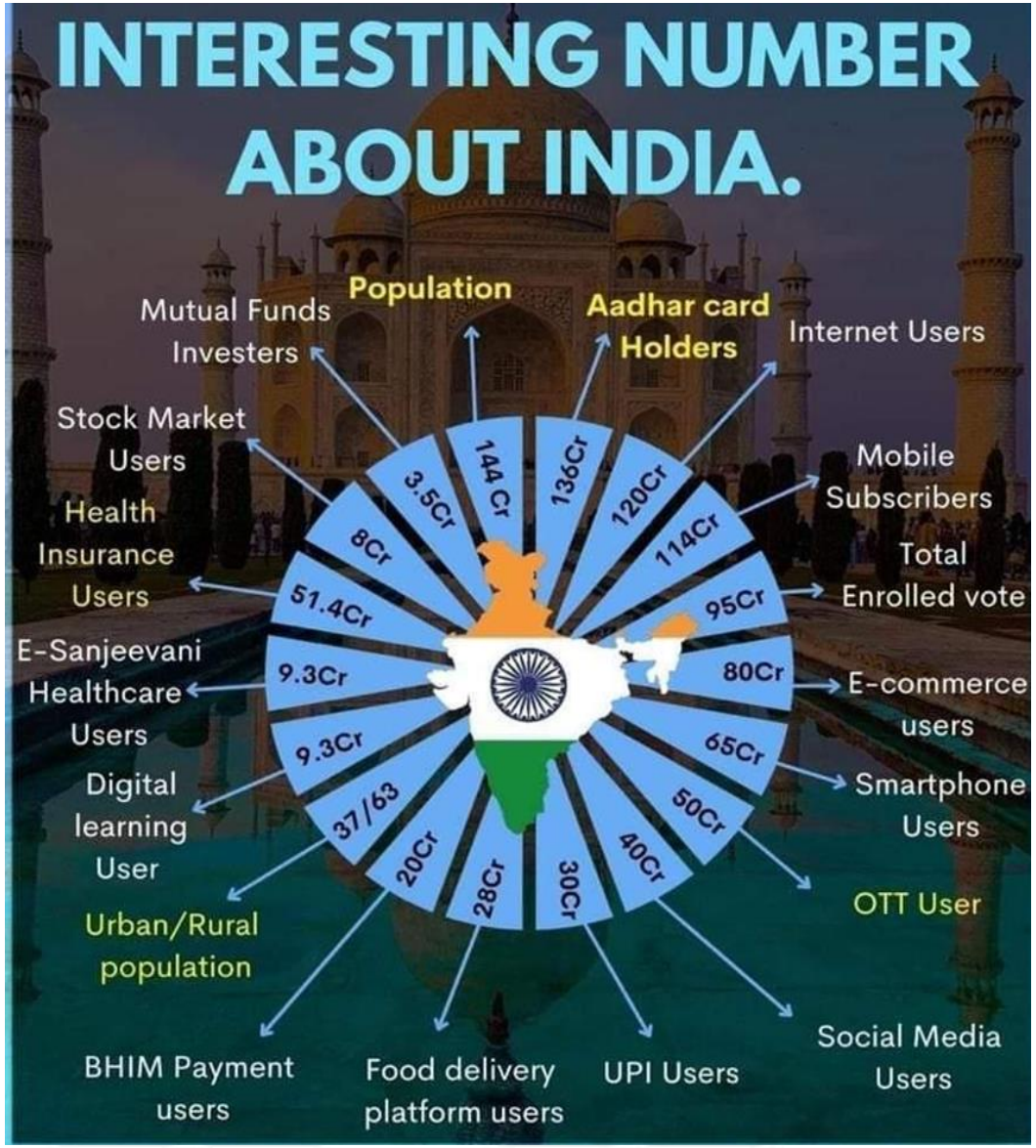
Data Protection & Data security

G S Krishnan

Consultant & advisor BFSI segment

Institute of Actuaries of India

DATA REVOLUTION



DATA BREACH IN 2023

7th most cyber breached nation globally

2200 cyber attacks per day

255 mio data affected by Phishing

Average cost of data breach is **17.9 crore** in 2023

No. of hacked accounts dropped from **65** per min to **16** per min in 2023

Biggest data breach **81.5 crore** personal details leaked from ICMR

Financial frauds account for **75%** of cyber crime -- UPI / internet banking

India's low ranking (17 out of 20) in the MIT Technology Review Cyber Defence Index 2022/23 is indicative of its inadequate cybersecurity preparedness.

TOP TEN DATA BREACH

Institute of Actuaries of India

Cyber attack on AIIMS --Cert in— Improper network segmentation	Mochhatua data breach on govt app Public distribution system	Zivame data breach -- women's wear – 1.5 mio customer data compromised	Cyberabad police case facts Data leak 66.9 crore data	Rentomojo cyber attack Furniture rental app
Sun pharma cyber attack Ransome ware attack on health data	Bharat pay financial trust breach Application breach	Railyatri data breach Booking site	Cloudsek data breach PW compromised	CoWin portal for vaccination purpose Bot on messaging platform leaked personal info

OWASP **TOP TEN DATA VULNERABILITIES**

Institute of Actuaries of India

- Broken Access Control
- Cryptographic Failure
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable Outdated Component
- Software & Data Integrity Failure
- Identification & Authentication Failure
- Security Logging & Monitoring Failure
- Server Side Request Forgery

  SSRF

TOP CYBER CRIMES

Institute of Actuaries of India

PHISHING

Deceive people to reveal info

DENIAL OF SERVICE ATTACK

Malicious targeted attack

TROJAN HORSE

Malware disguised as legitimate prog direct to fake website

RANSOMWARE

Malware used to deny access to files

MALWARE

Malicious software file or code delivered over network explore, steal , destruct.

MAN IN THE MIDDLE

Eavesdropping two party negotiating

SOCIAL ENGINEERING

Scams appeal to emotion - disclose info - PW theft

SPYWARE

Malicious software gathers data and shares with third party.

BUSINESS EMAIL COMPORMISE

Trick to share info, transfer funds.

WHAT IS DATA PROTECTION?

Institute of Actuaries of India

Data protection is the process of protecting sensitive information from damage, loss, or corruption.

As the amount of data being created and stored has increased at an unprecedented rate, making data protection increasingly important.

Data protection measures prevents frauds & cyber crimes.

WHAT IS DATA PROTECTION? TYPES

Institute of Actuaries of India

A comprehensive approach to data protection that includes encryption, backup and disaster recovery planning, access control, network security, and physical security can help ensure the security and confidentiality of sensitive information.

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two. Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to the data.

DATA SECURITY

- Data security is the practice of protecting digital information from unauthorized access, corruption or theft throughout its entire lifecycle.
- It covers the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.
- Robust data security strategies protect an organization’s information assets against cybercriminal activities, guard against insider threats and human error, which is the leading causes of data breaches today.
- Data security involves deploying tools and technologies that enhance the organization’s visibility into where its critical data resides and how it is used.
- Tools should be able to apply protections such as data masking , encryption and automate reporting to streamline audits and adhering to regulatory requirements. Redaction of sensitive information.

HOW TO PROTECT DATA & ENSURE SECURITY

- Application security & patching
- Automated compliance reporting
- Physical security of server & user devices Hyper convergence
- Access management & control
- Data encryption -- Data erasure
- Data masking -- Data resiliency -- disaster recovery as a service
- Data discovery & classification tool
- Data & file activity monitoring
- Vulnerability assessment and risk analysis tools
- Employee education
- Network & endpoint security monitoring and control

DATA SECURITY INITIATIVES & PROG

- **Digital public infrastructure:** India has established a digital public infrastructure (DPI), known as India Stack. This DPI ensures secure and privacy-respecting digital access to public and private services.
- **Computer Emergency Response Team (CERT-In):** It is the national nodal agency that deals with cybersecurity threats in India. It responds to cybersecurity incidents and strengthens India's response to cybersecurity threats.
- **Regulatory measures:** DPDP act 2023 effective date is still pending, India relies on regulations within the Information Technology (IT) Act of 2000 and sector-specific regulations for data privacy and protection.
- **National cybersecurity policy:** India has a national cybersecurity policy that provides a framework for securing cyberspace in the country. It aims to create a cyber-secure environment that allows the robust growth of the IT and digital sectors.
- **Public-private partnerships:** India works with private sector companies to enhance cybersecurity capabilities. The government has established institutions to ensure the continuity of India Stack's operations, acting as a catalyst in developing India's cybersecurity ecosystem.

DIGITAL PERSONAL DATA PROTECTION ACT 2023

Institute of Actuaries of India

In India, data protection got a legal cover when in 2017 data privacy was declared as a fundamental right. Entities covered data principal, data fiduciary, regulatory offices, data protection board of India.

Sync with KYC, PMLA, protection of privacy guidelines.

The DPDP Act applies to the processing of digital personal data within India, whether collected in digital or non-digital form that has been digitized.

Covers processing of DPD outside India if this is related to offering of goods & services to data principal within India.

DPDP Act 2023

The DPDP Act was enacted on 11th August 2023 and recognizes the right of individuals to protect their personal data while allowing its processing for lawful purposes

Act's provisions aimed at safeguarding personal data while allowing lawful processing

DPDP ACT 2023 – VS – GDPR

Particulars	DPDP Act	GDPR
Geography covered	India 7 principles of GDPR not fully covered	EU (all countries) 7 Principles of GDPR fully covered lawfulness, fairness, purpose limitation, accuracy, storage limitation, accountability , integrity & confidential
Coverage	Digitised data	Online and Offline data
Segmentation of data	No additional demarcation	More segments based on racial, ethical data
Consent manager Penalties	Consent managers is a role prescribed Breach of duty by DP 10000 per day Obligation failure by DF fine up to Rs 250 cr	No such role prescribed Heavy penalties and legal implications

DPDP ACT 2023 – KEY TENETS

Institute of Actuaries of India

Data collection

- Consent and consent withdrawals for DP right to correction of PD/ Notice and Parent /Guardian consent for DF .

DPDP ACT 2023 – 4 IMMEDIATE STEPS

Institute of Actuaries of India

- Where do you stand in terms of data privacy ?
- Where does “personal data “ sit and with whom
- Do you use external service providers
- Define first level measures including : Designing draft versions of documents , design consent mechanisms, appoint the right people

CYBER SECURITY

- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information.
- Extorting money from users via ransomware; or interrupting normal business processes.
- 5 types of cyber security -- application, network, cloud, critical infrastructure, IoT .
- The six pillars of cybersecurity are governance, risk management, compliance, education and training, incident management, and technical controls
- Cyber security products & services – antivirus, endpoint security, identity & access management, incident response management, firewall , one time password / otp gateway, VPN.

Institute of Actuaries of India

Thank you