Handling the Data Privacy

Group 5

Ankit Sharma, M08
Ajay Kumar Sharma, M05
Prashant Kumar Pasi, M27
Gopal Krishna Gautam, M37
Rajat Mishra, M32

Data Privacy v/s Data Security

Data Privacy

comprised of the policies and processes that dictate how your business collects, shares, and uses data

Data Security

Mechanisms in place that protect the company's data feom being accessed maliciously

Why Data Privacy?

- A breach of data may create a bad reputation for the organization
- Protects the privacy of your customers
- Improves your brand value with data privacy policies in place
- Supports the ethical code of practice in org
- Data privacy regulations give you an edge over your peers

Privacy breaches around the world

Facebook

Affected 87 mn Facebook Accounts and data used by Cambridge Analytica

Twitter

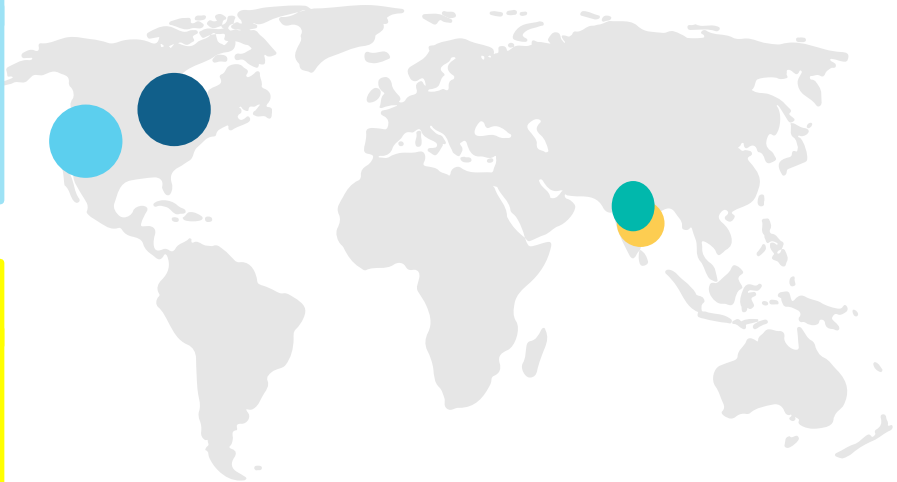
A glitch unmasked all user passwords to the internal network

Debit Card data breach

3.2 million debit cards from major Indian banks were compromised

Aadhaar

Data leak exposed World's largest biometric database



Privacy breaches around the world

Figure 1. Number of breaches reported in 2020

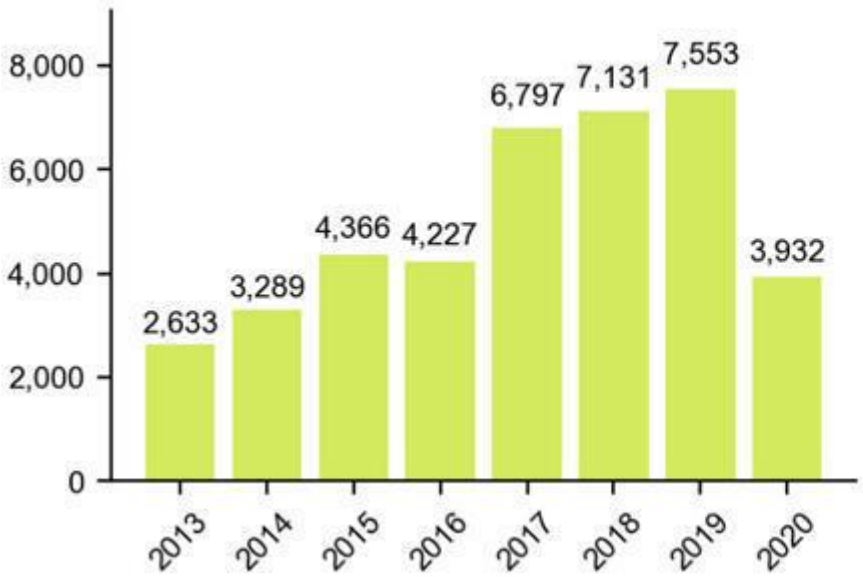
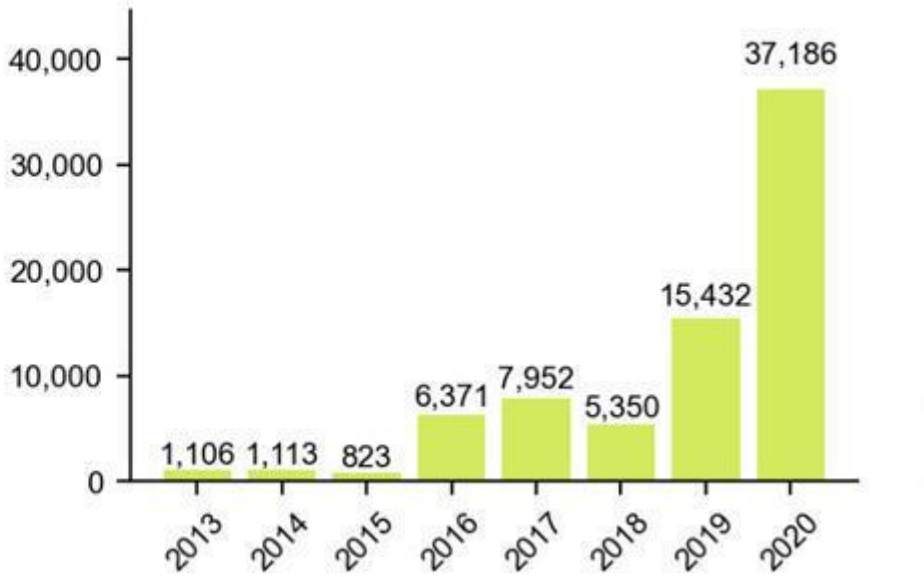
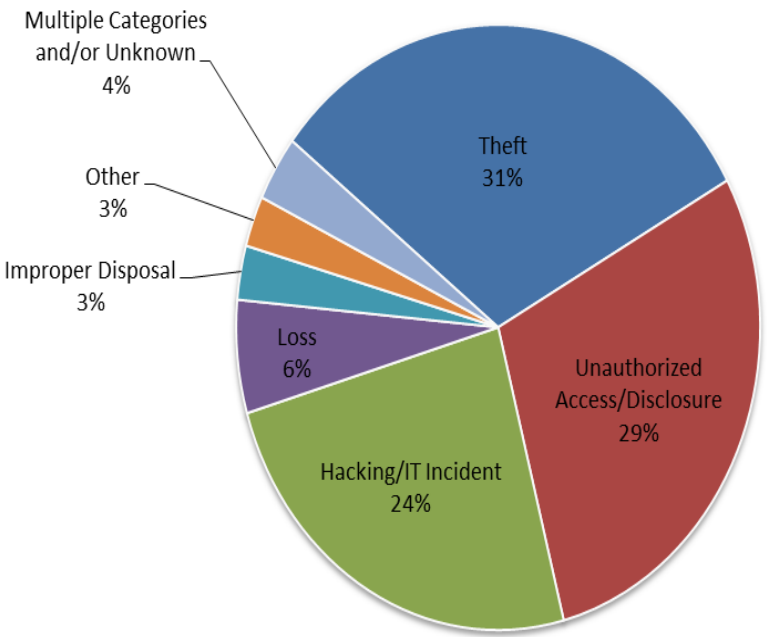


Figure 2: Number of records lost (in millions) reported in 2020

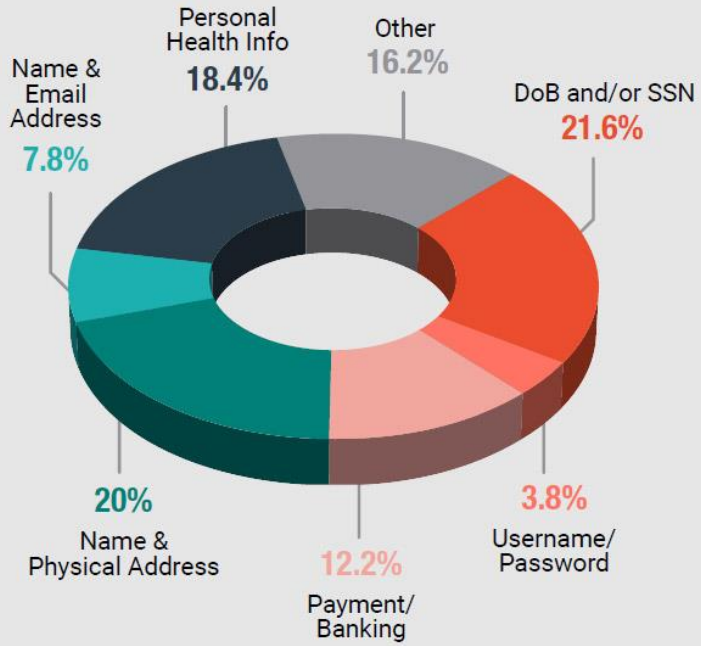


Causes of Breaches



Breach Types

Types of Data Exposed in Every Breach



Data Privacy Risks

1. Collecting and Storing Too Much Personal Information
2. Lack of Transparency Regarding Data Collection and Use
3. Using Personal Data for an Unauthorized Purpose
4. Insufficient Processes for Deleting Personal Data
5. Vulnerable Applications and Insufficient Data Security
6. Insufficient Responses Around Personal Data Loss

Sensitive Personal Data

- Some personal data is considered sensitive, as it could cause harm to the individual if leaked or misused

Physical or mental Health

Political or Religious Beleifs

Racial or Ethnic origin

Sexual Orientation

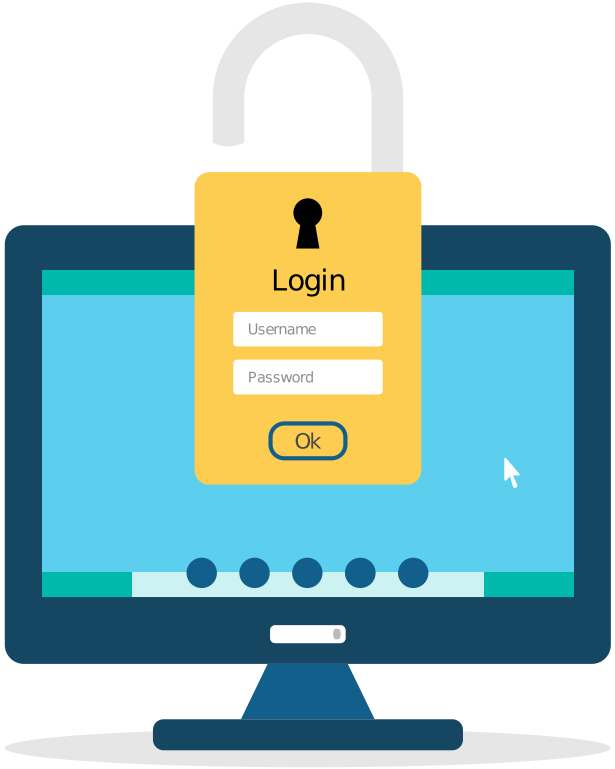
Criminal offences and court proceedings

Voice recordings & biometrics

When can personal data be processed?

1	2	3	4	5	6
Consent	**Legitimate interest**	**Legal obligation**	**Vital interest**	**Public Interest**	**Contractual necessity**
of the individual to the processing of their personal data.	of the organisation or the third parties engaged.	for which the organisation is obliged to process personal data	of individuals, where processing is necessary to protect their lives	specific to organisations carrying out tasks in the public interest.	processing is needed in order to enter into or perform a contract.

Levels of Data Privacy Regulation in an Org



Data Collection

how and when businesses can collect data about consumers

Data Breach

what organisations must do in the event of a data breach

Data access

how internal access of information should be handled

Data Storage

how data must be stored in order to keep it safe

Ensuring Data Privacy

- Establish a data privacy policy
- Implement data privacy and cyber security frameworks
- Notify purpose and seek consent
- Notify data breaches

- Conduct internal audits on a regular basis
- Embed data privacy into your systems
- Communicate your data protection policies
- Keep record of compliance activities

Ensuring Data Privacy

build the data privacy policies and procedures based onnwhat exactly data privacy policy needs to address.

Establish a data privacy policy

evaluate your internal controls against the best practices, identify the gaps, and implement new policies and procedures

Implement data privacy and cyber security frameworks

provide users with clear information explaining why, what and how you're intending to process their info

Notify purpose and seek consent

Describing the estimated impact and possible effects and procedures taken by organisation to remediate the incident

Notify data breaches

Ensuring Data Privacy

Regularly auditing the compliance processes to spot possible issues and prevent disasters like a major data breach from happening.	**Conduct internal audits on regular basis**
embed data privacy into the design and overall lifecycle of any technology, business process, product, or service	**Embed data privacy into systems**
to the customers & employees to ensure they are familiar with how you process and protect personal data	**Communicate your data protection policies**
demonstrate that you take that risk seriously and are actively working to mitigate it	**Keeping record of compliance activities**

REGULATIONS AROUND THE WORLD

Regulation Framework in The EU:

- The General Data Protection Regulation (GDPR) was enacted in 2018 to protect the rights of citizens in the EU when it comes to data collection and privacy.
- It gives customers the right to know what data is being collected and sets requirements for how and when businesses must report breaches
- GDPR is one of the toughest data privacy regulations to comply with
- in 2019, British Airways was fined $228 million and Marriott International was fined over $124 million for exposing millions of records of personal data

REGULATIONS AROUND THE WORLD

Regulation Framework in The US:

- The CCPA regulations govern compliance with the California Consumer Privacy Act.
- Requires businesses to make disclosures to consumers about any personal information collected and the purposes for which the personal information is used.
- Requires businesses to make disclosures to consumers about any personal information collected and the purposes for which the personal information is used.
- Prohibits a business from selling the personal information of a consumer under 16 years of age.

REGULATIONS AROUND THE WORLD

Regulation Framework in India:

- Until now, the personal data of India's population of 1.4 billion people has been protected by the IT Act 2000.
- The IT Act and India's Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011, are now relatively dated.
- The Indian Personal Data Protection Bill (PDPB) is a proposal that came from the Srikrishna Committee to modernize the laws that govern personal data in India.
- The bill proposes to create independent public authority called the Data Protection Authority of India (DPA) that will oversee the implementation of the protections provided under the bill and is therefore a key part of the proposed regulatory framework.

CONCLUSION

- Data breach, a cybercrime, or a security threat can cause harmful and negative consequences to any org
- Consumers trust org with their sensitive data and in case of data theft, it leads to a complete break of trust
- Complying with the rules of data privacy protection will save the business reputation and also avoid the huge penalties and fines charged to those who do not comply with data privacy laws
- Therefore, to collect, store, process and discard data in ways that are compliant with regulations, the org need to have strong information security policies and practices that protect your clients' data from malicious or unauthorized use.

THANK YOU