ROLE OF PCS : DATA PRIVACY REGULATIONS

CS Anushanethri V

AGENDA

- Introduction to Data Privacy Laws
  - Indian Laws
  - International Laws
- Data protection policies and procedures
  - Key Elements
- Data flow maps to track the movement of data and identify potential risks
  - Data Flow maps
  - DPIA
- Data Breach
  - Data Breach Investigation and Mitigation
  - Preventing data breach
- Summary – Role of PCS in Data Privacy

UN INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (ICCPR)

Article 17 of ICCPR:

1.No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2.Everyone has the right to the protection of the law against such interference or attacks.

CHANCE TO WIN INR 1,00,000/-

WHAT IS PERSONAL INFORMATION AND WHY IS ITS PROTECTION IMPORTANT?

WHAT IS PERSONAL INFORMATION?

Any information that can be used to identify a person:

Examples:

- Basic information, like a person's name or phone number
- Identification details
- Biometric data
- Location tags
- Online or real-world behavior
- Health records, etc.

WHY IS PERSONAL INFORMATION PROTECTION IMPORTANT?

- Universal Human Right
- Prevents from fraudulent activities, hacking, phishing, and identity theft.
- Possible damages to the business and the image of the Individual & the Company.

INTRODUCTION TO DATA PRIVACY LAWS

INDIAN DATA PROTECTION REQUIREMENTS

- Information Technology Act, 2000
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules');
- Information Technology (The Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013 ('CERT-In Rules');
- Consumer Protection Act, 2019 ('CPA') and Consumer Protection (E-Commerce) Rules, 2020;
- Rules made by the Reserve Bank of India ('RBI'); Telecom Regulatory Authority of India ('TRAI');
- Rules imposed by the Insurance Regulatory and Development Authority of India; Securities and Exchange Board of India ('SEBI'); Pension Fund Regulatory and Development Authority;
- Various decisions of Indian courts; and
- Unified Licence Agreements issued pursuant to the National Telecom Policy, 2012 by the Department of Telecommunications ('DOT').

THE IT ACT

IT Act:

body corporates that handle sensitive personal data or information are liable:

- to pay damages for any loss caused by their negligence in implementing and maintaining reasonable security practices and procedures

Prescribes criminal penalties for persons that disclose personal information:

- without the consent of the person to whom the data relates,
- where such disclosure is in breach of a contract or
- results in wrongful loss or gain

SPDI RULES

SPDI Rules:

- Applicable to Natural Person
- body corporates that process sensitive personal data
- All territories of India and applies to offences that occur outside India, if the offences involve electronic resources in India
- Every organization should have privacy policy
- Every organization should obtain consent when collecting or transferring sensitive personal data or information. Minor – Consent from Guardian mandatory

SPDI RULES

Data transfers:

Export of sensitive personal data or information within or outside India is permissible, provided that:

- same standards of data protection required in India are adhered
- transfer is necessary for the performance of a lawful contract
- consented to by the provider of the information

Data protection officer appointment

CASE LAW

Supreme Court of India ('the Supreme Court') in Justice K S Puttaswamy and Anr v. Union of India and Ors [Writ Petition (Civil) No. 494 of 2012

Supreme Court unanimously held that the right to privacy was an intrinsic element of the promise of the right to life and personal liberty protected under Article 21 of the Constitution, and that it included, at its core, a negative obligation to not violate the right to privacy and a positive right to take all actions necessary to protect the right to privacy.

The Supreme Court went on to clarify that any law that encroached upon the right to privacy would be subject to constitutional scrutiny, and would have to meet the three-fold requirement for:

- legality;
- necessity; and
- proportionality.

DIGITAL PERSONAL DATA PROTECTION

APPROVED BY LOK SABHA ON 7TH AUGUST 2023

Applies to the processing of digital personal data within India

- collected online
- collected offline and is digitized
- processing of personal data outside India

Consent

- lawful purpose only
- notice should contain details and the purpose
- Consent - withdrawn at any point in time
- Minor - consent will be provided by the parent or the legal guardian

CONTINUED….

Obligations of Data Fiduciaries

- to ensure the accuracy and completeness of data
- build reasonable security safeguards to prevent a data breach
- inform the Data Protection Board of India and affected persons in the event of a breach
- erase personal data as soon as the purpose has been met

Transfer of personal data outside India

- allows transfer of personal data outside India, except restricted countries.

INTERNATIONAL DATA PROTECTION REQUIREMENTS

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR)

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, COMMONLY KNOWN AS HIPAA.

US CITIZENS AND HEALTHCARE ORGANIZATION ALL OVER THE WORLD.

INTERNATIONAL DATA PROTECTION REQUIREMENTS

1. Privacy Rule

The HIPAA Privacy Rule establishes standards to protect individuals' electronic medical records and personal health information and how it can be used and not disclosed.

2. Security Rule

The HIPAA Security Rule establishes standards to protect individuals' electronic personal health information with right safeguards must be in place to ensure appropriate protection (see below).

3. Transaction Rule

The HIPAA Transaction Rule address the safety, accuracy and security of medical records in transactions and PHI

4. Identifiers Rule

The HIPAA Identifiers Rule ensures unique identifiers.

5. Enforcement Rule

The HIPAA Rule addresses the authority's power to enforce penalties for violations and set the breach reporting requirements.

SUMMARY ON COMPLIANCES

- Notice and Consent is mandatory
- Purpose to be lawful
- Data Transfers are governed
- Personal data to be protected by all means
- Data breach to be reported

BRAINSTORMING

- Which transactions will require consent?
- How will the consent be obtained?
- How can we provide option to opt out from consent?
- How can the Company ensure that the Consent is multi-linguistic?
- What is the data security assessment exercise?
- Destruction of Personal records and maintaining records for destruction?

DATA PROTECTION POLICIES AND PROCEDURES

IS THERE ANY DIFFERENCE BETWEEN DATA PROTECTION POLICY AND A PRIVACY POLICY?

- **A privacy policy** is a document that explains to customers how the organization collects and processes their data. It is made available to the public by organizations required to comply with privacy regulations.

- **A data protection policy** is an internal document created for the purpose of establishing data protection policies within the organization. It is made available to company employees, as well as third parties, responsible for handling or processing sensitive data.

KEY ELEMENTS – DATA PRIVACY POLICY

- Types of Data Collected
- How You Use the Data
- Data Storage and Security
- Opt-Out Procedures
- Company Contact Info

KEY ELEMENTS – DATA PROTECTION POLICY

Scope

- types of personal data collected, purpose processes, and storage

Definitions

- clear definitions for key terms and concepts

Statute

- Details of the Data protection statute complied with

Lawful Processing of Data

- clearly outline the lawful bases

CONTINUED…

Roles and Responsibilities

- assignment of roles and responsibilities

Data Breach - Procedures

- well-defined process in place

Rights of Data Subjects

- rights to individuals in relation to their personal data

Security and Record Keeping

- policy should detail the security measures

Contact Information

- contact information for supervisory authorities

DATA FLOW MAPS AND IDENTIFY POTENTIAL RISKS

DATA FLOW MAPS

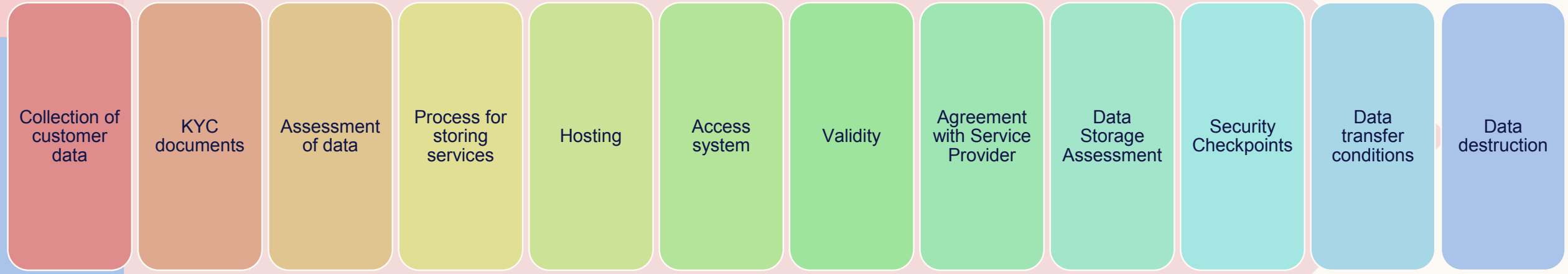
Data mapping - system of cataloging what data you collect, how it's used, where it's stored, and how it travels throughout your organization and beyond.

Creation of Data mapping:

1) identify the personal data collected, used, shared, and stored, define the data processing activities and their legal basis
2) map the data flows
3) data lifecycle
4) document the data controllers
5) processors involved
6) any data that can directly or indirectly identify a person
7) how to use personal data
8) legal grounds
9) who is responsible
10) for deciding and carrying out the data processing activities and what

CASE STUDY

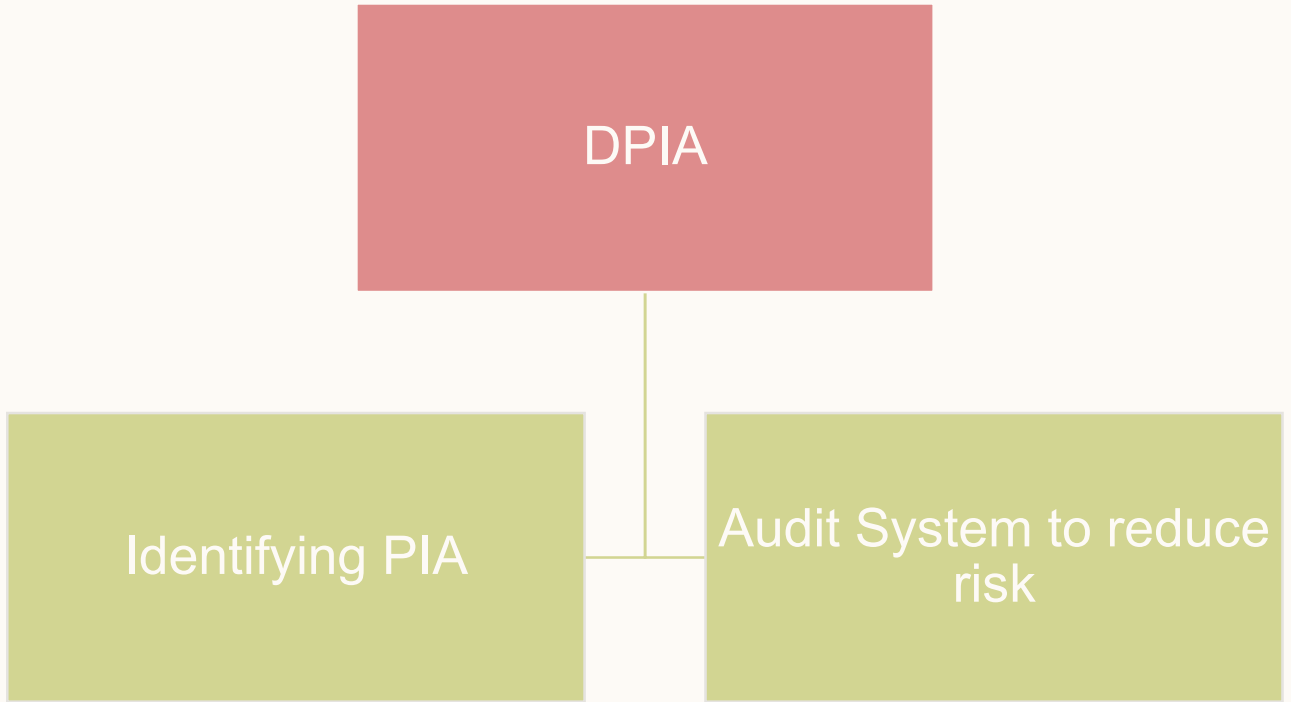
Create a Data Flow Maps for Collection of KYC data by the Bank



DPIA - DATA PROTECTION IMPACT ASSESSMENT

DPIA - DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment (DPIA) is a process that systematically identifies and minimizes risks related to personal data processing.



DPIA - CHECKLIST

Data Protection Impact Assessment (DPIA) is a process that systematically identifies and minimizes risks related to personal data processing.

Contents of the DPIA checklist:

1) Identify the need for a DPIA
2) Describe the processing
    1) Nature
    2) Scope
    3) Context
3) Consultation process
4) Assess necessity and proportionality
5) Identify and assess risks
6) Identify measures to reduce risk
7) Sign off and record outcomes

DATA BREACH

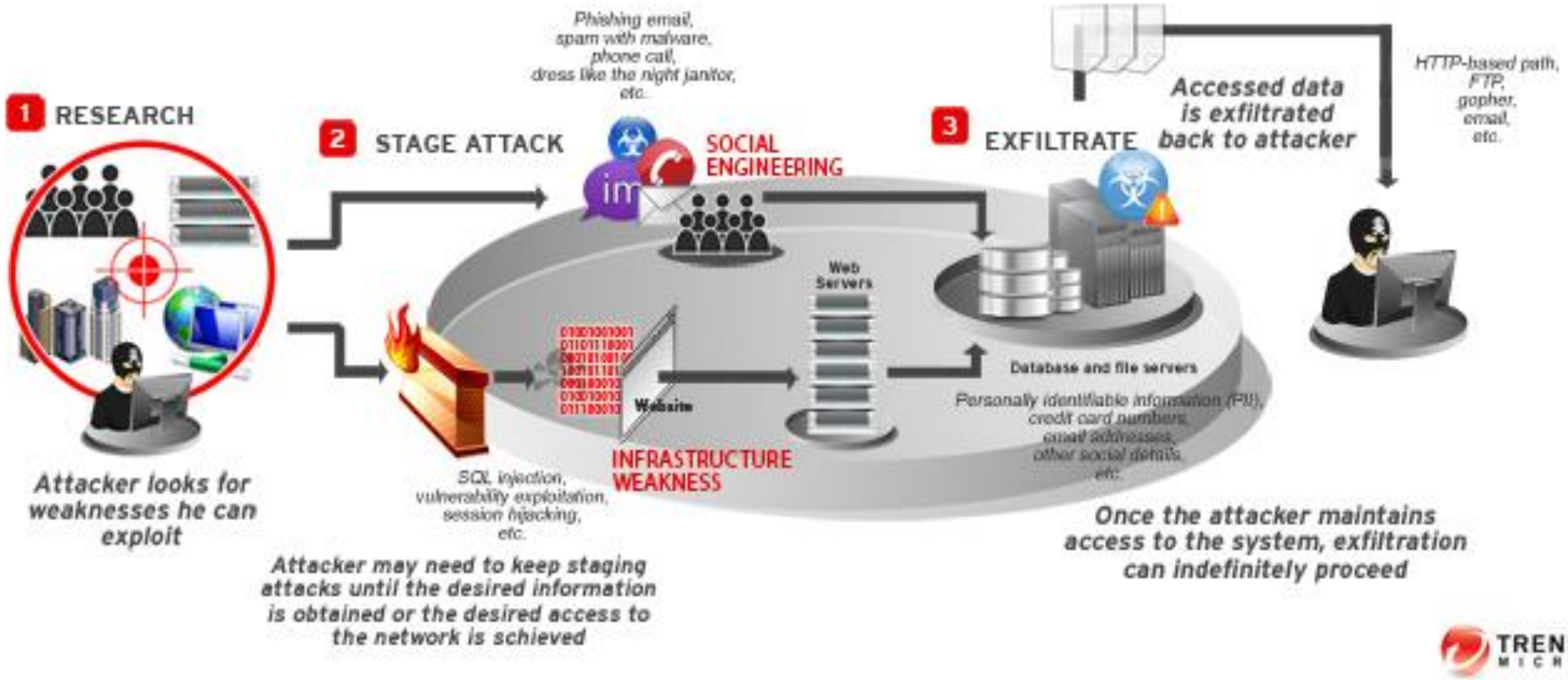
DATA BREACH

A data breach is an event that results in exposing confidential, sensitive, or other protected information to an unauthorized person.

How Data Breach Happens?

- Malicious attacks, which involve cybercriminals or insiders
- Human error, such as careless employees or contractors
- Systems glitches, including business process failures

DATA BREACH


1 RESEARCH
Attacker looks for weaknesses he can exploit
2 STAGE ATTACK
Phishing email, spam with malware, phone call, dress like the night janitor, etc.
SOCIAL ENGINEERING
SQL injection, vulnerability exploitation, session hijacking, etc.
Website
Web Servers
INFRASTRUCTURE WEAKNESS
Attacker may need to keep staging attacks until the desired information is obtained or the desired access to the network is schieved
3 EXFILTRATE
Accessed data is exfiltrated back to attacker
HTTP-based path, FTP, gopher, email, etc.
Database and file servers
Personally identifiable information (PII), credit card numbers, email addresses, other social details, etc.
Once the attacker maintains access to the system, exfiltration can indefinitely proceed
TREND MICRO
MALICIOUS DATA BREACH DIAGRAM

EXAMPLES OF DATA BREACHES

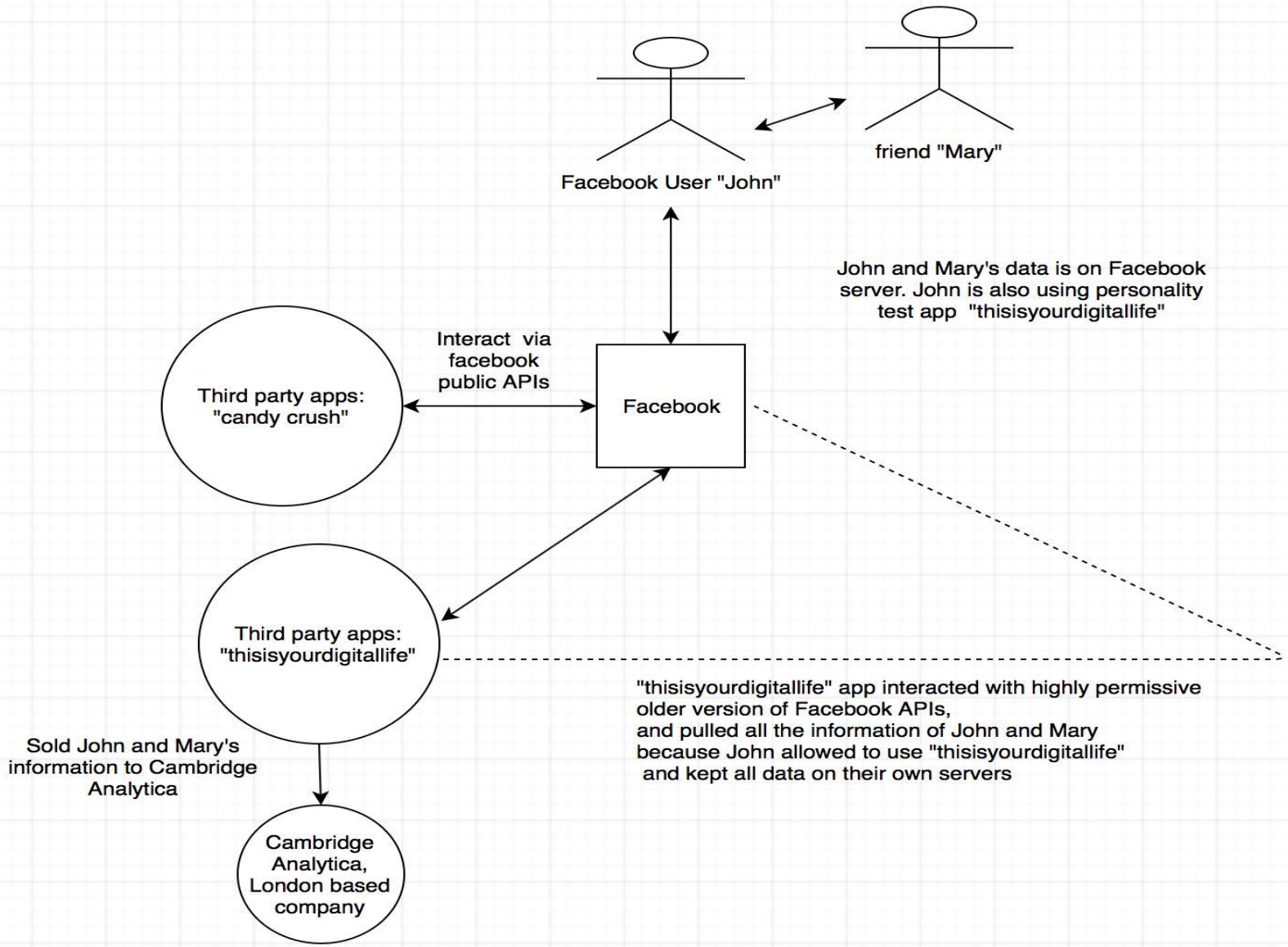
Yahoo: The popular email service, Yahoo, disclosed two data breaches in 2016, which affected all three billion of its user accounts.

Twitter: January 2022. The company reported that a bug exposed the phone numbers of 5.4 million users to potential hackers.

Facebook: April 03, 2021. The company confirmed that a data leak exposed the personal information of 533 million users, including phone numbers, names, and email addresses.

Samsung: July 2022. The company accidentally leaked the personal data of an undisclosed number of users through its

FACEBOOK – DATA BREACH



DATA BREACH INVESTIGATION AND MITIGATION CHECKLIST

- Establish a data breach response team
- Notify appropriate personnel and agencies
- Collect and preserve evidence
- Identify the cause of the breach
- Containment and eradication of the breach
- Mitigation of damage caused by the breach
- Post-mortem analysis

PREVENTING A DATA BREACH

Take care of the basics

- Install firewalls
- Install antivirus
- Install encryption software
- Use a VPN or Zero Trust Network
- Use strong passwords

Promote employee awareness

- Educate employees
- Communicate
- Encourage accountability

Update your starters and leavers process

- Set up new starters
- Process leavers
- Review returned devices

Manage ongoing maintenance and planning

- Stay up to date
- Prepare
- Make copies

DATA PRIVACY AND DATA SECURITY

DATA PRIVACY VS DATA SECURITY

Data Security	Data Privacy
Block all external unknown links embedded in email	Filter website links to only visit those that have a data use agreement where I explicitly consent to the terms
Use a strong password to unlock my laptop hard drive	Password protect specific folders where sensitive data is located, leaving other business data alone and open to free use
Don't give my name, credit card number & CVV code to a stranger	Provide my credit card details to trusted e-commerce systems where data protection is moderated, and standards of use are transparent
Encrypt my document before mailing it on a USB stick	Mask sensitive data that is not necessary to the recipient in my file before mailing it on a USB stick, sharing non-sensitive details
Apply 2-factor authentication *(e.g., password + fingerprint)* to bank login	Apply 2-factor authentication, while not storing any more personal data than required in my online account to limit improper use risks.

SUMMARY – ROLE OF PCS IN DATA PRIVACY

- Interpreting the law
- Support in drafting Data Privacy Policy, Data Protection Policy
- Consents
- Creation of Data Flow and analysis of Risk
- DPIA
- Investigating Data Privacy Breach – Audit and post Audit reviews
- Support in prevention of breach

QUESTIONS?

THANK YOU

CS Anushanethri V

Email id: anushanethri88@gmail.com