### Meghana D Duttargi

(241059042)

1st Assignment

### 1. Twitter Data Breach (2022)

Incident Details:

In 2022, Twitter experienced a breach where hackers exploited an API vulnerability to access and exfiltrate data of over 5.4 million users, including email addresses and phone numbers. The data was later sold on dark web marketplaces.

Threats and Vulnerabilities:

* Threats: API exploitation by malicious actors.
* Vulnerabilities: Insufficient rate-limiting and API validation.
* Affected Security Pillars: Confidentiality (user data exposed).

Risk Analysis:

* Legal: Potential non-compliance with data privacy regulations.
* Financial: Loss from lawsuits and settlements.
* Reputational: Erosion of user trust in platform security.

Remediation Measures:

* Conduct regular API security assessments.
* Enforce strict rate-limiting on APIs.
* Validate API inputs and outputs effectively.

Risk Mitigation Strategies:

* Implement OAuth 2.0 for API authentication.
* Monitor API usage for abnormal patterns.
* Educate developers on secure API design

### 2. Colonial Pipeline Ransomware Attack (2021)

Incident Details:

The Colonial Pipeline attack occurred in May 2021, where ransomware deployed by the DarkSide group caused significant disruptions in fuel supplies across the U.S. East Coast. The attackers demanded and received a $4.4 million ransom.

Threats and Vulnerabilities:

* Threats: Ransomware delivered via phishing emails.
* Vulnerabilities: Weak endpoint protection and insufficient network segmentation.
* Affected Security Pillars: Availability (pipeline shutdown), Integrity (tampered data).

Risk Analysis:

* Legal: Regulatory scrutiny over cybersecurity measures.
* Financial: Ransom payments and operational losses.
* Reputational: Public backlash due to service disruption.

Remediation Measures:

* Deploy advanced anti-phishing tools.
* Use network segmentation to limit lateral movement.
* Back up critical data regularly.

Risk Mitigation Strategies:

* Train employees to recognize phishing attempts.
* Implement an incident response plan.
* Employ real-time monitoring for ransomware signatures.

### 3. Uber Data Breach (2016)

Incident Details:

In 2016, attackers exploited a misconfigured cloud storage service to steal data of 57 million Uber riders and drivers. Uber paid $100,000 in "bug bounty" to conceal the breach.

Threats and Vulnerabilities:

* Threats: Exploitation of cloud misconfiguration.
* Vulnerabilities: Lack of access control policies.
* Affected Security Pillars: Confidentiality (sensitive data exposed).

Risk Analysis:

* Legal: Fines for violating privacy laws.
* Financial: Remediation costs and lawsuits.
* Reputational: Trust erosion among users.

Remediation Measures:

* Conduct regular cloud security reviews.
* Apply the principle of least privilege to cloud resources.
* Use encryption for sensitive data.

Risk Mitigation Strategies:

* Monitor cloud configurations continuously.
* Deploy automated tools for access control.
* Educate employees on cloud security best practices.

### 4. Yahoo Data Breach (2013-2014)

Incident Details:

Yahoo disclosed breaches in 2013 and 2014 that affected all 3 billion user accounts. Hackers exploited weak security measures to access account credentials and sensitive data.

Threats and Vulnerabilities:

* Threats: State-sponsored hacking groups.
* Vulnerabilities: Poor encryption and lack of MFA.
* Affected Security Pillars: Confidentiality (account credentials exposed).

Risk Analysis:

* Legal: Settlements totaling $117 million.
* Financial: Long-term revenue decline.
* Reputational: Loss of user trust and market share.

Remediation Measures:

* Implement MFA for all accounts.
* Enhance password encryption techniques.
* Regularly update security protocols.

Risk Mitigation Strategies:

* Monitor user accounts for unauthorized access.
* Employ AI-based anomaly detection systems.
* Provide transparency about security practices.

### 5. Facebook-Cambridge Analytica Scandal (2018)

Incident Details:

In 2018, Facebook revealed that Cambridge Analytica had harvested data from over 87 million users without consent through a third-party app. The data was used to influence political campaigns.

Threats and Vulnerabilities:

* Threats: Data misuse by third parties.
* Vulnerabilities: Weak third-party app permissions.
* Affected Security Pillars: Confidentiality (user data exposed).

Risk Analysis:

* Legal: Fines exceeding $5 billion.
* Financial: Share price decline.
* Reputational: Loss of user confidence in data security.

Remediation Measures:

* Enforce stricter controls on third-party app data access.
* Provide users with granular data-sharing permissions.
* Conduct periodic audits of third-party apps.

Risk Mitigation Strategies:

* Educate users on privacy settings.
* Develop transparency reports on data-sharing practices.
* Invest in ethical data governance frameworks.