**Report on 5 Real-World Web Application Attacks**

**1. Equifax Data Breach (2017)**

Threats and Vulnerabilities:

Threats: SQL Injection, unpatched software vulnerabilities.

Vulnerabilities: Failure to patch a known vulnerability in Apache Struts.

Affected Security Pillars: Confidentiality (exposure of sensitive personal data), Integrity (data tampering), Availability (service disruption).

Risk Analysis:

Impact: The breach exposed personal information of approximately 147 million people, leading to significant legal repercussions, including lawsuits and regulatory fines. Financially, Equifax faced costs exceeding $4 billion, including settlements and security upgrades. Reputational damage was severe, eroding consumer trust.

Remediation Measures:

* Regularly update and patch software.
* Implement a robust vulnerability management program.
* Conduct regular security audits and penetration testing.

Risk Mitigation Strategies:

* Adopt a proactive security posture with continuous monitoring.
* Educate employees on security best practices.
* Implement multi-factor authentication for sensitive data access.

Sources:

* Federal Trade Commission (FTC) report on Equifax breach.
* "Equifax Data Breach: What Happened and What to Do" - Security Magazine.

**2. Yahoo Data Breach (2013-2014)**

Threats and Vulnerabilities:

Threats: Credential stuffing, phishing attacks.

Vulnerabilities: Weak password policies and inadequate encryption.

Affected Security Pillars: Confidentiality (user data exposure), Integrity (data manipulation), Availability (service disruption).

Risk Analysis:

Impact: The breach affected all 3 billion Yahoo accounts, leading to a $350 million reduction in Verizon's acquisition price. Legal consequences included multiple lawsuits and regulatory scrutiny. The breach severely damaged Yahoo's reputation, leading to loss of user trust.

Remediation Measures:

* Enforce strong password policies and implement two-factor authentication.
* Encrypt sensitive data both in transit and at rest.

Risk Mitigation Strategies:

* Regularly review and update security policies.
* Conduct user awareness training on phishing and social engineering.

Sources:

* "Yahoo Confirms 3 Billion Accounts Hacked in 2013" - The New York Times.
* Verizon's acquisition report on Yahoo.

**3. Target Data Breach (2013)**

Threats and Vulnerabilities:

Threats: Malware, network intrusion.

Vulnerabilities: Compromised third-party vendor access.

Affected Security Pillars: Confidentiality (credit card data theft), Integrity (data manipulation), Availability (service disruption).

Risk Analysis:

Impact: The breach affected 40 million credit and debit card accounts, costing Target over $162 million in settlements and legal fees. The incident led to a significant loss of customer trust and a decline in sales.

Remediation Measures:

* Implement strict access controls for third-party vendors.
* Use advanced threat detection systems to monitor network traffic.

Risk Mitigation Strategies:

* Conduct regular security assessments of third-party vendors.
* Invest in employee training on cybersecurity awareness.

Sources:

* "Target Data Breach: What Happened and What to Do" - Krebs on Security.
* Target's financial reports post-breach.

**4. Facebook Cambridge Analytica Scandal (2018)**

Threats and Vulnerabilities:

Threats: Data harvesting, unauthorized data sharing.

Vulnerabilities: Inadequate data privacy controls and user consent mechanisms.

Affected Security Pillars: Confidentiality (user data exposure), Integrity (manipulation of user data), Availability (service disruption).

Risk Analysis:

Impact: The scandal affected over 87 million users, leading to a $5 billion fine from the FTC. Facebook faced intense scrutiny and criticism, resulting in reputational damage and loss of user trust.

Remediation Measures:

* Strengthen data privacy policies and user consent mechanisms.
* Regularly audit third-party applications for compliance.

Risk Mitigation Strategies:

* Enhance transparency in data usage and sharing practices.
* Implement robust data governance frameworks.

Sources:

* "The Cambridge Analytica Scandal: What Happened?" - BBC News.
* FTC report on Facebook's data privacy violations.

**5. Capital One Data Breach (2019)**

Threats and Vulnerabilities:

Threats: Misconfigured web application firewall, insider threats.

Vulnerabilities: Inadequate security controls for cloud services.

Affected Security Pillars: Confidentiality (exposure of sensitive financial data), Integrity (data manipulation), Availability (service disruption).

Risk Analysis:

Impact: The breach exposed personal information of over 100 million customers, leading to a $80 million fine and significant legal costs. The reputational damage was substantial, affecting customer trust

Remediation Measures

* Implement Strict Access Controls: Ensure that permissions are limited to the least privilege necessary for users and applications to perform their functions.
* Regular Security Audits: Conduct frequent audits of security configurations and practices to identify and rectify vulnerabilities.
* Enhance Cloud Security Configurations: Utilize cloud-specific security services and ensure proper configuration of firewalls and other security appliances.

Risk Mitigation Strategies

* Continuous Monitoring: Establish a system for real-time monitoring of network traffic and security alerts to detect anomalies promptly.
* Employee Training: Provide regular training sessions for employees on recognizing phishing attempts and understanding security protocols.
* Comprehensive Incident Response Plan: Develop and maintain an incident response plan that outlines procedures for responding to security breaches effectively.

Sources:

* (https://www.infosecinstitute.com/resources/news/lessons-learned-the-capital-one-breach/)
* [What We Can Learn from the Capital One Hack](https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/)
* [Preventing The Capital One Breach](https://ejj.io/blog/capital-one)
* [Cloud Security: Lessons Learned from the Capital One Data Breach](https://www.bitsight.com/blog/cloud-security-lessons-learned-from-capital-one-data-breach)