Five Real-World Web Application Attacks

1. Equifax Data Breach (2017)

Threats:
- Exploited a known vulnerability in Apache Struts.
- Conducted by cybercriminals motivated by financial gain.

Vulnerabilities:
- Unpatched critical software vulnerabilities.
- Lack of robust intrusion detection and prevention systems.

Security Pillars Affected:
- Confidentiality: Exposed sensitive data of 147 million individuals.
- Integrity: Systems and data were compromised.

Risks & Impact:
- Legal: Fines, lawsuits, and congressional scrutiny.
- Financial: Settlements and reputational damage.
- Reputational: Erosion of public trust.

Remediation Measures:
- Prompt patching and regular vulnerability scanning.
- Implementing effective IDPS.

Risk Mitigation:
- Security audits, employee training, and Data Loss Prevention (DLP) solutions.

2. Yahoo Data Breaches (2013-2016)

Threats:
- State-sponsored actors using phishing and exploiting vulnerabilities.

Vulnerabilities:
- Weak password security and insufficient data protection measures.

Security Pillars Affected:
- Confidentiality: Theft of personal data, including security questions and passwords.
- Integrity: User and system data compromised.

Risks & Impact:

- Legal: Regulatory investigations and lawsuits.
- Financial: Security upgrades and settlement costs.
- Reputational: Loss of user trust and diminished brand value.

Remediation Measures:
- Strong password policies, data encryption, and intrusion response systems.

Risk Mitigation:
- User education, regular security assessments, and a comprehensive incident response plan.

3. Target Data Breach (2013)

Threats:
- POS systems compromised by organized cybercriminals.
- Attackers accessed the network via vulnerabilities in the HVAC system.

Vulnerabilities:
- Poor network segmentation.
- Weak access control mechanisms.

Security Pillars Affected:
- Confidentiality: Exposed millions of customers' payment data.
- Integrity: POS systems and customer trust compromised.

Risks & Impact:
- Legal: Regulatory fines and lawsuits.
- Financial: Settlements and enhanced security investments.
- Reputational: Erosion of customer loyalty and brand image.

Remediation Measures:
- Improved network segmentation and robust access controls.
- Compliance with PCI DSS standards.

Risk Mitigation:
- Leveraging threat intelligence, audits, and vendor risk management programs.

4. Marriott Data Breach (2018)

Threats:
- Unauthorized access to the Starwood guest reservation system.

Vulnerabilities:
- Unpatched vulnerabilities in the Starwood system.
- Insufficient security monitoring and timely detection.

Security Pillars Affected:
- Confidentiality: Compromised personal information of 500 million guests.
- Integrity: Reservation systems undermined.

Risks & Impact:
- Legal: Regulatory actions and lawsuits.
- Financial: Security upgrade costs and settlements.
- Reputational: Loss of customer trust and loyalty.

Remediation Measures:
- Patch management, IDPS implementation, and SIEM solutions.

Risk Mitigation:
- Vendor risk management, DLP solutions, and employee training.

5. Ashley Madison Data Breach (2015)

Threats:
- Hacktivists aimed to expose user data.
- Extortion attempts against the company.

Vulnerabilities:
- Weak data encryption and overall poor security practices.

Security Pillars Affected:
- Confidentiality: Exposure of sensitive user data, including credit card information.
- Integrity: Systems and data compromised.

Risks & Impact:
- Legal: Investigations and lawsuits.
- Financial: Loss of revenue and settlements.
- Reputational: Significant damage leading to service shutdowns.

Remediation Measures:
- Enhanced data encryption and multi-factor authentication.

Risk Mitigation:

- Regular audits, employee training, and DLP implementation.