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

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

* **What Happened?** A former employee got unauthorized access due to a misconfigured web firewall.
* **What Was Vulnerable?** The setup of the web firewall was faulty.
* **What Was Affected?**
  + **Confidentiality**: Sensitive data like Social Security Numbers (SSNs) and bank info were leaked.
  + **Integrity**: There was a risk of data being tampered with.
  + **Availability**: No major disruption in services.
* **Impact:**
  + **Legal**: The company was fined $80 million.
  + **Financial**: They had to spend a lot on legal issues and fixing the problem.
  + **Reputation**: Customers lost trust in Capital One.
* **How Could It Have Been Prevented?**
  + Better security settings for the firewall.
  + Regular security checks and tests.
* **Strategies to Avoid Future Risks:**
  + Keep a close watch on cloud services.
  + Train employees to handle security better.

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

* **What Happened?** Hackers exploited a vulnerability in Equifax’s software because it wasn’t patched in time.
* **What Was Vulnerable?** The company didn't update their software promptly.
* **What Was Affected?**
  + **Confidentiality**: Over 140 million people’s personal information was exposed.
  + **Integrity**: There was a risk that this data could be altered.
  + **Availability**: Services were not disrupted.
* **Impact:**
  + **Legal**: Equifax faced huge lawsuits and fines.
  + **Financial**: The breach cost them over $700 million.
  + **Reputation**: People lost confidence in Equifax.
* **How Could It Have Been Prevented?**
  + Regularly update and patch software.
  + Have a system to quickly spot vulnerabilities.
* **Strategies to Avoid Future Risks:**
  + Improve systems for detecting and responding to issues fast.
  + Do regular software checks.

**3. SolarWinds Supply Chain Attack (2020)**

* **What Happened?** Hackers inserted malicious code into SolarWinds’ software, which many organizations used.
* **What Was Vulnerable?** The supply chain security was weak.
* **What Was Affected?**
  + **Confidentiality**: Sensitive data from governments and companies was accessed.
  + **Integrity**: The software itself was compromised.
  + **Availability**: It could have disrupted important services.
* **Impact:**
  + **Legal**: There could be regulatory actions against them.
  + **Financial**: A lot of money was spent on fixing the damage.
  + **Reputation**: Trust in SolarWinds’ security was shaken.
* **How Could It Have Been Prevented?**
  + Stronger security checks on the supply chain.
  + Thorough reviews of third-party vendors.
* **Strategies to Avoid Future Risks:**
  + Have stricter code review processes.
  + Use systems that detect unusual activities.

**4. Uber Data Breach (2016)**

* **What Happened?** Hackers used stolen passwords to access Uber’s system.
* **What Was Vulnerable?** Poor password management.
* **What Was Affected?**
  + **Confidentiality**: Personal data of 57 million users and drivers was exposed.
  + **Integrity**: There was a risk of data being altered.
  + **Availability**: Services were not disrupted.
* **Impact:**
  + **Legal**: Uber was fined and faced regulatory scrutiny.
  + **Financial**: The breach cost them over $148 million.
  + **Reputation**: Users lost trust in Uber.
* **How Could It Have Been Prevented?**
  + Enforcing stronger password rules.
  + Using multi-factor authentication.
* **Strategies to Avoid Future Risks:**
  + Regularly check access controls.
  + Train staff on password security.

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

* **What Happened?** Hackers, believed to be state-sponsored, stole data from Yahoo.
* **What Was Vulnerable?** Weak encryption and poor security protocols.
* **What Was Affected?**
  + **Confidentiality**: Data from 3 billion accounts was stolen.
  + **Integrity**: The data could have been tampered with.
  + **Availability**: There was no service outage.
* **Impact:**
  + **Legal**: Yahoo faced lawsuits and regulatory fines.
  + **Financial**: They had to sell their business at a reduced price.
  + **Reputation**: Trust in Yahoo's security was severely damaged.
* **How Could It Have Been Prevented?**
  + Upgrading encryption methods.
  + Regular security reviews.
* **Strategies to Avoid Future Risks:**
  + Improve processes for account recovery.
  + Use real-time systems to detect anomalies.