### **Discussion Questions for the Equifax Data Breach (2017)**

Answer the following questions based on the information provided about the Equifax data breach. You are encouraged to use diagrams and charts to illustrate your ideas.

**1. What happened in the Equifax data breach of 2017?**

* A) Hackers stole credit card information through phishing attacks.
* B) Attackers exploited an unpatched Apache Struts vulnerability, leading to the exposure of sensitive personal data of over 147 million consumers.
* C) Equifax’s mobile app was compromised, leading to data leakage.
* D) A server misconfiguration allowed public access to financial data.

**Answer: B) Attackers exploited an unpatched Apache Struts vulnerability, leading to the exposure of sensitive personal data of over 147 million consumers.**

**2. What are two effective security mechanisms to prevent breaches like the Equifax incident?**

* A) Implement automated patch management systems and conduct regular vulnerability assessments.
* B) Disable security updates to avoid system downtime.
* C) Allow unrestricted access to all servers for convenience.
* D) Reduce the use of encryption to speed up data access.

**Answer: A) Implement automated patch management systems and conduct regular vulnerability assessments.**

**3. As a security consultant for Equifax, how would you advise the company to improve its patch management processes?**

* A) Implement an automated patch management system, conduct frequent security audits, and establish a clear process for applying critical updates as soon as they are released.
* B) Only patch systems once a year to reduce disruptions.
* C) Avoid installing security patches to prevent system crashes.
* D) Only focus on external threats, ignoring internal systems.

**Answer: A) Implement an automated patch management system, conduct frequent security audits, and establish a clear process for applying critical updates as soon as they are released.**

**4. How could Equifax have better handled its public communication and crisis management after the breach?**

* A) Establish a clear and transparent communication strategy, secure the breach notification website, and provide timely updates to consumers with concrete action steps.
* B) Avoid informing the public to prevent panic.
* C) Provide minimal information to reduce the spread of misinformation.
* D) Blame consumers for the breach.

**Answer: A) Establish a clear and transparent communication strategy, secure the breach notification website, and provide timely updates to consumers with concrete action steps.**

**5. How can large organizations effectively conduct security audits?**

* A) Use automated tools like Nessus, Qualys, and manual penetration testing to regularly assess vulnerabilities, and ensure that third-party vendors are also included in audits.
* B) Perform security audits only when required by regulations.
* C) Disable logging to reduce storage costs during audits.
* D) Only audit systems that have experienced recent breaches.

**Answer: A) Use automated tools like Nessus, Qualys, and manual penetration testing to regularly assess vulnerabilities, and ensure that third-party vendors are also included in audits.**

**6. As the CIO of Equifax, what measures would you implement to enhance security while maintaining operational efficiency?**

* A) Implement a patch management process that applies updates during off-peak hours and use network segmentation to reduce the impact of potential breaches.
* B) Disable security features to speed up business operations.
* C) Only apply patches to critical systems, ignoring secondary ones.
* D) Allow unrestricted access to all employees for efficiency.

**Answer: A) Implement a patch management process that applies updates during off-peak hours and use network segmentation to reduce the impact of potential breaches.**

**7. What steps should organizations take to protect sensitive data and ensure compliance with data privacy regulations like GDPR?**

* A) Encrypt all sensitive data, implement strong access controls, and ensure regular compliance audits with privacy regulations.
* B) Only focus on data encryption without monitoring.
* C) Store all sensitive data in plaintext for easy access.
* D) Ignore data privacy regulations to avoid compliance costs.

**Answer: A) Encrypt all sensitive data, implement strong access controls, and ensure regular compliance audits with privacy regulations.**

**8. What steps would you take to improve vulnerability management to prevent incidents like the Equifax breach?**

* A) Use automated vulnerability scanning tools, prioritize patching high-risk vulnerabilities, and establish a dedicated security team to continuously monitor threats.
* B) Only focus on vulnerabilities once a year.
* C) Ignore low-priority vulnerabilities to focus on operational tasks.
* D) Allow outdated software to continue running until a breach occurs.

**Answer: A) Use automated vulnerability scanning tools, prioritize patching high-risk vulnerabilities, and establish a dedicated security team to continuously monitor threats.**

**9. What IT weaknesses were present in Equifax’s systems that enabled the breach?**

* A) Unpatched Apache Struts vulnerability, weak incident response, and lack of strong encryption for sensitive data.
* B) Too many firewalls blocking external access.
* C) Lack of antivirus software on all systems.
* D) Excessive monitoring of internal systems leading to false positives.

**Answer: A) Unpatched Apache Struts vulnerability, weak incident response, and lack of strong encryption for sensitive data.**

**10. As the CIO of Equifax, how would you improve overall IT security and protect sensitive consumer data?**

* A) Implement automated patch management, enforce strong encryption, conduct regular security audits, and improve employee training on security best practices.
* B) Disable all security measures for faster data access.
* C) Store customer data in plaintext to avoid encryption overhead.
* D) Only focus on securing external threats and ignore internal vulnerabilities.

**Answer: A) Implement automated patch management, enforce strong encryption, conduct regular security audits, and improve employee training on security best practices.**