Case Study: Home Depot Data Breach (Part A)

Introduction

The Home Depot data breach occurred in 2014, compromising the personal and financial information of over 56 million customers. Hackers gained access to the company's payment systems through a third-party vendor, exploiting weak security practices. The breach exposed sensitive data, including credit and debit card details, leading to significant financial losses and reputational damage for the company.

Root Cause

The Home Depot data breach had several causes:

- **Vulnerabilities in outdated systems**: Outdated systems often lack the latest security updates, making them more susceptible to attacks.
- **Stolen credentials**: Hackers used stolen credentials from a third-party vendor to access the network.
- **Unpatched zero-day vulnerabilities in Windows systems**: The attackers exploited unpatched vulnerabilities in Windows systems that were unknown to Microsoft at the time.
- **Lack of regular vulnerability scanning**: Home Depot did not regularly scan their systems for vulnerabilities, allowing the attack to go unnoticed.
- **Poor system configurations**: No network segregation; Home Depot's network was not adequately segmented, allowing the attackers to move laterally within the system.
- **Outdated Windows XP systems on POS terminals**: The Point of Sale (POS) terminals ran outdated Windows XP, which lacked modern security features.

Actions Taken

Question 1: List six key actions the company took to address the situation, based on insights from the previous video and additional online research.

1. **Launched an Immediate Investigation** - On September 2, 2014, Home Depot bega n investigating the breach to determine the scope and impact. This included engagin g internal teams and outside cybersecurity experts.
2. **Public Disclosure and Customer support** - On September 8, 2014, they issued a pr ess release acknowledging the breach. They also apologized to customers and offer ed free credit monitoring and identity protection services to those affected.

3. **Replaced and Upgraded POS Systems** - Home Depot transitioned away from Windows XP POS terminals, upgrading to more secure systems and encrypting payment card data (point to point encryption).
4. **Enhanced Security Controls** - HD implemented stronger endpoint protection and ensured network threat protection features were properly enabled. They also introduced more robust network segmentation to isolate POS systems from the broader corporate network.
5. **Restricted third party vendor access** - They limited vendor credentials using the principle of least privilege, reducing the external attack surface. They strengthened the oversight and monitoring of third party connections.
6. **Financial compensation and settlements** - They paid $19.5 m in customer settlements, they paid over $134m to banks and credit card companies to cover fraud charges all totaling nearly $200m.

Summary Statement

Home Depot addressed the 2014 PoS breach by investigating the incident, publicly disclosing it and offering free credit monitoring, upgrading outdated PoS systems with modern encryption, enhancing security controls and network segmentation, restricting vendor access with least privilege, and compensating customers and banks with settlements totaling nearly $200 million.

The student effectively addressed all six key actions outlined in the rubric: investigation, public disclosure, offering credit monitoring, upgrading security, restricting vendor access, and financial settlements. This comprehensive coverage justifies awarding the maximum points.

To further enhance your response, consider providing more details on how each action specifically mitigated risks or prevented future breaches. Including insights from additional research or case studies could also strengthen your analysis.

Score: 12/12 (100%)

Detailed Breakdown:

Analysis: The student response accurately identifies and explains six key actions taken by Home Depot following the 2014 data breach. The actions include launching an investigation, public disclosure, upgrading POS systems, enhancing security controls, restricting third-party access, and financial settlements.

Evaluation: The student's response meets the highest rubric criteria by providing a clear and detailed explanation of six key actions. Each action is well-articulated and aligns with the rubric's requirements.

Explanation: The student effectively addressed all six key actions outlined in the rubric: investigation, public disclosure, offering credit monitoring, upgrading security, restricting vendor access, and financial settlements. This comprehensive coverage justifies awarding the maximum points.

Guidance: To further enhance your response, consider providing more details on how each action specifically mitigated risks or prevented future breaches. Including insights from additional research or case studies could also strengthen your analysis.