| **Equifax** | |
| --- | --- |
| **Question** | **Response** |
| 1. What types of data were affected? | 1. Personal information (including Social Security numbers, birth dates, addresses, and in some cases, drivers' license numbers) 2. Credit card data |
| 1. What happened? | Several security lapses that allowed attackers to enter supposedly secure systems and exfiltrate terabytes of data:   1. Application vulnerability that allowed the attacker's access was unpatched. 2. Inadequate system segmentation made lateral movement easy for the attackers. |
| 1. Who was responsible? | The first incursion was achieved by relatively inexperienced hackers who were using a readily available hacking kit that had been updated to take advantage of the Struts vulnerability, which was only a few days old at that point and easy to exploit.  Eventually, unable to get much further beyond their initial success, they sold their foothold to more skilled attackers, who used various techniques associated with Chinese state-backed hackers to gain access to confidential data. |
| 1. Were any escalation(s) stopped - how? | Yes; Renewed public-key certificate |
| 1. Was the Business Continuity Plan instigated? | No |
| 1. Was the ICO notified? | Yes: <https://www.bbc.com/news/uk-england-essex-45574163> |
| 1. Were affected individuals notified? | Yes |
| 1. What were the social, legal and ethical implications of the decisions made? | No; Equifax was slow to report the breach. |
| 1. If you had been the ISM for the organisation you selected what mitigations would you have put in place to stop any reoccurrences? | Among other cybersecurity controls, the following should be implemented:   * Vulnerability management * Patch management * Data Loss Prevention (DLP) solution * Key management |