**Course:** Networks and Systems Security

**Name:** Ana Berjano(33821542)

**Group members:**

-Ana Berjano (33821542)

-Maksymilian Zarzycki (33800519)

-kyle easy (3382815601)

**Activity:** analyse the following scenarios. For each one, identify

the primary principle of the CIA Triad being violated: Confidentiality,

Integrity, or Availability.

**A) 2017 Equifax Data Breach — Student Response (expanded)**

**1) Primary Impact:** **Confidentiality**.

**2) Justification (why):**

* Attackers got in through an unpatched Apache Struts bug (CVE-2017-5638) on a public-facing site and stayed long enough to steal data .
* What they took was highly sensitive personal information for 147 million people overall (names, dates of birth, addresses, social security numbers, plus some driver’s licence and credit card data).
* UK angle: about 13.8 million UK consumers were impacted because UK data was outsourced to Equifax Inc’s US servers for processing. Stolen UK data included names, dates of birth, phone numbers, Equifax membership logins, partial card data, and addresses.
* Service posture: Equifax’s systems mostly kept running; there wasn’t evidence of widespread record tampering during the breach window, so this wasn’t an availability or integrity event first.
* Governance/oversight failures(it could have been prevented): Equifax didn’t treat the parent relationship as outsourcing, so oversight of how UK data was protected in the US was weak. There were known security weaknesses at the parnet that weren’t addressed, and patching,assurance fell short.
* Detection/notification issues (UK ): Equifax Ltd learned UK data was accessed 6 weeks after the US partner discovered the hack and was reportedly told minutes before the public announcement, so it struggled with complaints and contacting customers promptly, and early public statements under-reported UK impact.
* Overall, the main harm was unauthorised disclosure of personal data at massive scale, a direct hit to Confidentiality.

**3) Secondary Impacts:**

* **Integrity (indirect):** Stolen personal information fuels identity theft and synthetic identities, which then pollute credit records(wrong data tied to victims, disputes/corrections later). Compromised login details also raise account takeover risks.
* **Availability (minor):** Some customer portals were taken offline temporarily during incident response and support demand spiked. These were short-term remediation effects, not the core impact.