**The Cost of Data Breaches Exercise**

**Learning Goal: Understanding the cost of data breaches.**

**Please review The IBM Data Breach Report (**[**How much does a data breach cost in 2022?**](https://www.ibm.com/security/data-breach)**) and answer the following questions.**

1. Data breaches in which three industries involve the highest average cost?

A: Healthcare, Financial and Pharmaceutical.

1. What factor contributes most to the cost of a data breach?

A: “DevSecOps approach”, breaches at organizations with a DevSecOps approach in place had an average cost that was USD 249,000 less than the average cost of a data breach of USD 4.45 million.

1. What is the average time required for an organisation to contain a data breach?

A: 277 days, or just over nine months.

1. Identify common threats and indicate which have the highest average cost?

A: Destructive attack, Ransomware, Attack on the business partner supply chain, Attack on the software supply chain.

The one that has the highest average cost is “Destructive attack”.

1. What is the impact of incident response strategies on the cost of a data breach?

A: Incident response strategies focus on reducing the duration of a data breach, reducing their impact.

“Organizations with both an IR team and IR plan testing identified breaches 54 days faster than those with neither.” Is a direct quote from the report.

Meaning that organizations that implement incident response strategies, will considerably minimise the cost of a data breach, taking less time to identify and contain them.

1. Which strategies can help reduce the cost of data breaches?

A: 1- Build security into every stage of software development and deployment—and test regularly (Application testing or penetration testing).

2 - Modernize data protection across hybrid cloud (and seek data security and compliance technologies).

3 - Use security AI and automation to increase speed and accuracy (implement threat detection and response tools).

4 - Strengthen resiliency by knowing your attack surface and practicing IR (incident response).