Cybersecurity Threat Landscape (Part 3 - Verizon)

In this part, you should primarily use the *Verizon Data Breaches Investigation Report* plus independent research to answer the below questions.

---

1. What is the difference between an incident and a breach? An incident is an event that compromises all three sides of the CIA triad of an information asset. A breach is when an incident results in confirmed disclosure of data to an unauthorized party

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors? 69% by outsiders and 34% internal

3. What percentage of breaches were perpetrated by organized criminal groups? 39%

4. What percentage of breaches were financially motivated? 71%

5. Define the following:

   Denial of Service: an interruption in an authorized user's access to a computer network, typically caused with malicious intent. (oxford dictionaries)

   Command and Control: also known as C2 or C&C. When bad actors use a central server to covertly distribute malware to people's machines, execute commands to the malicious program, and take control of a device. (howtogeek.com)

   Backdoor: any method by which authorized and unauthorized users are able to get around normal security measures. (malwarebytes.com)

   Keylogger: spyware that can record and steal consecutive keystrokes that the user enters on a device. (malwarebytes.com)

6. The time from an attacker's first action to the initial compromise of an asset is typically measured in which one? Seconds, minutes, hours, days? minutes

7. When it comes to phishing, which industry has the highest click rates? Education (4.93%)