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?

    a. **The difference between the two is one (Incident) leads to the violation of policies placed by an organization's sensitive data. While the other (Security Breach) is access to unauthorized data by the security incident. So usually they can be interrelated, as the Security Incident can cause the Security Breach.**

2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?

    a. **For outside actors, there were 69% of security breaches.**
    b. **For inside actors, there were 34% of security breaches.**

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

    a. **There were 39% perpetrated by the organized criminal groups.**

4. What percentage of breaches were financially motivated?
    a. **There were 71% of breaches that were financially motivated.**

5. Define the following:

    Denial of Service: A DoS is where the attack is on services that disrupt the normal functions and prevents anyone from accessing. Example of a bank website going down, preventing clients from accessing their accounts.

    Command and Control: An attacker or hacker has full control of the compromised computer or network to collect data or even shut down the company's network.

    Backdoor: It's a method used by attackers/hackers to get access to the company's computers or networks by getting around normal security measures and gain high-level user access.

    Keylogger: It's a type of monitoring software designed to record keystrokes made by a user to gain access to data by the attacker or hacker.

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?

    It takes minutes for the attacker to get the data, once the computer or network is compromised.

7. When it comes to phishing, which industry has the highest click rates?

    Financial institutions and Webmail are the two highest click rates.