# 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?
   From the report:
   - Incident: “A security event that compromises the integrity, confidentiality or availability of an information asset.”
   - Breach: “An incident that results in the confirmed disclosure—not just potential exposure—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 outside actors and 34% by internal actors

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: This is an attack that seeks to shut down a machine and/or a network. For a machine, it does this by sending the machine something that will cause a crash. For a network, it does this by bombarding the network with packets.

   Command and Control: From the webpage, https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server: “A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.”

   Backdoor: From the webpage,

https://www.imperva.com/learn/application-security/backdoor-shell-attack/#:~:text=A%20backdoor%20is%20a%20malware,system%20commands%20and%20update%20malware: “A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.”

Keylogger: This is a program that runs on a PC and logs a user’s keystrokes. The data is then stored for later access by an attacker or simply sent to an attacker’s remote machine.

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
   **Note:** the report doesn’t state click rates for actual phishing attacks; it reports on click rates for phishing tests.