# 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? **Answer: -** An incident is a security event that compromises the integrity, confidentiality or availability of an information asset.

And

A breach is an incident that results in the confirmed disclosure not just potential exposure of data to an unauthorized party.

1. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?   
   **Answer: -**
2. The percentage of breaches were 69% perpetrated by outsiders actors.
3. The percentage were 34% perpetrated by internal actors.
4. What percentage of breaches were perpetrated by organized criminal groups?   
   **Answer: -** The percentage of breaches were 39% perpetrated by organized criminal groups.
5. What percentage of breaches were financially motivated?   
   **Answer: -** The financially motivated breaches were 71%.
6. Define the following:   
   **Answer: -**  
   **Denial of Service:**

In cyber world, an attack intended to compromise the availability

of networks and systems, or in in other words an attack targeting an IP address or network/systems connected to one and this includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.

**Command and Control:**

Command and Control server that is computer controlled by an attacker to send commands to systems compromised by malware. An example of command is exercise of authority based upon certain knowledge to attain an objective and the control process of verifying and correcting activity such that the objective or goal of command is accomplished.  
 **Backdoor:** An easy “entrance” in a machine that is more vulnerable to malware & hackers due to security malfunctions or invulnerability. **Keylogger:** Keylogger is a type of malware that can track everything on user system and keylogger is a small program which runs in background without letting know of user and it can save all keystrokes by the keyboard.

1. 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?   
   **Answer: -** It measured in minutes.
2. When it comes to phishing, which industry has the highest click rates?  
   **Answer: -** Education industry is the highest click rates in phishing.