# 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?  **Incident: a security event that attacks the CIA triad of an asset**

**Breach: Gained access to an asset**

1. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?   
   **69% by outside actors**

**34% by internal actors**

1. What percentage of breaches were perpetrated by organized criminal groups?   
   **39% by organized criminal groups**
2. What percentage of breaches were financially motivated?   
   **71% were financially motivated**
3. Define the following:   
     
   Denial of Service: **DoS attack is meant to shut down machines or networks**  
   Command and Control **C&C server is a computer controlled by the by an attacker to send commands to systems compromised to malware and receive stolen data from a target network**  
   Backdoor: **Method by which authorized and unauthorized users are able to get around normal security measures and gain Root access on a computer system.**Keylogger: **monitoring software that’s designed to record valuable info**
4. 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?   
   **Typically measured in minutes**
5. When it comes to phishing, which industry has the highest click rates?  
   **Manufacturing industries**