# 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 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.**

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

What percentage were perpetrated by internal actors? **34%**

1. What percentage of breaches were perpetrated by organized criminal groups?   
   **39%**
2. What percentage of breaches were financially motivated?   
   **71%**
3. Define the following:   
     
   Denial of Service: **Any attack intended to compromise the availability of networks and systems. This includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.**  
   Command and Control **The set of tools and techniques (malware) that attackers use to maintain communication with compromised devices following initial exploitation.**  
   Backdoor: **An undocumented way of gaining access to a computer system. A malware type that negates normal authentication procedures to access a system giving perpetrators the ability to remotely issue system commands and update additional malware.**Keylogger: **Activity-monitoring software programs that record everything you type and send this log file to a server so that it can be exploited.**
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?   
   **Minutes**
5. When it comes to phishing, which industry has the highest click rates?  
   **Education with 4.93%**