# 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?

**An incident describes the potential exposure of the integrity, confidentiality or availability of your data. A breach defines a confirmed disclosure of your data.**

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

**69% perpetrated by outsiders and 34% involved Internal actors.**

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

**39% of breaches were perpetrated by Organized criminal groups.**

1. What percentage of breaches were financially motivated?

**71% of breaches were financially motivated**

1. Define the following:   
     
   Denial of Service:

**A DDoS attack is an attempt to make an online service unavailable by overwhelming it with traffic.**Command and Control:

**C&C servers are computers which are controlled by a cybercriminal which sends commands to systems that are compromised by malware to receive stolen data from the targeted network.**

Backdoor:

**Backdoor is a method of bypassing the authentication or encryption in a computer.**

Keylogger:

**Keylogger is a program that records every keystroke made by a computer user.**

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?

**It is measured in minutes.**

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

**The Education Industry (4.93%)**