# 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 is a security event that compromises the CIA of an information asset whereas a breach is a confirmed leak of data to an unauthorized party.

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

69% from external actors and 34% from internal actors.

1. What percentage of breaches were perpetrated by organized criminal groups?   
   39% of breaches were from organized criminal groups.
2. What percentage of breaches were financially motivated?   
   71% of breaches were financially motivated.
3. Define the following:   
     
   Denial of Service: an attack that is meant to disrupt the availability of a network or system.  
   Command and Control: An attack that allows the attacker to take full control of the victims system and network.  
   Backdoor: A method of bypassing firewalls and other protections to gain access to a system and/or network.Keylogger: a type of software that monitors keystrokes of users to gain sensitive information or passwords.
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 attacks are measured in Minutes.
5. When it comes to phishing, which industry has the highest click rates?  
   Education had the highest click rate at 4.93%