# 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 an event that compromises the integrity, confidentiality, or availability of an information asset and a breach is an incident that results in the confirmed disclosure of data.

1. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?   
     
   69% of breaches were performed by outside actors and 34% were performed by internal actors.
2. What percentage of breaches were perpetrated by organized criminal groups?

39% of breaches were performed by organized criminal groups.

1. What percentage of breaches were financially motivated?   
     
   71% of breaches were financially motivated.
2. Define the following:   
     
   Denial of Service:   
   This is an attack intended to compromise system and network availability; including application and network attacks designed to overwhelm systems and degrade and interrupt service.  
   Command and Control   
   This is the result of an attack where an attacker infects a computer for the purpose of retaining communication and executing commands or installing malware to issue commands from within the compromised network.  
   Backdoor:  
   Backdoor is a method by which both authorized and unauthorized users can get around normal security measures and gain high-level user access on a computer system, network, or software application, allowing them to then steal data and install malware or hijack devices (<https://www.malwarebytes.com/backdoor/>**)**Keylogger:   
   Software that records every keystroke on a device. This allows an attacker to gain access to passwords and confidential information.
3. 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; the time from an attacker’s first action to the initial compromise of an asset is measured in minutes.
4. When it comes to phishing, which industry has the highest click rates?

Education is the industry with the highest phishing related click rates.