# 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 integrity, confidentiality, or availability of an information asset. While a breach is an incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.**
2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?   
   **69% perpetrated by outsiders and 34% by involved internal actors**
3. What percentage of breaches were perpetrated by organized criminal groups?   
   **39%**
4. What percentage of breaches were financially motivated?   
   **71%**
5. Define the following:   
     
   Denial of Service: **Any attack intended to compromise the availability of networks and systems.**  
   Command and Control: **C2 is often used by attackers to retain communications with compromised systems within a target network.** (OPTIV)  
   Backdoor: **A malicious program that listens for commands on a certain TCP or UDP port, it is an undocumented way of gaining access to a computer system.** (NIST)Keylogger: **A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys** (NIST)
6. 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**
7. When it comes to phishing, which industry has the highest click rates?  
   **Education**