# 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 compromises the integrity, confidentiality or availability of an asset while a breach results in a disclosure 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 outside actors. 34% perpetrated by 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:** A type of attack in which the perpetrator makes a machine or network unavailable to it’s users either temporarily or permanently   
    **Command and Control:** A computer controlled by a cybercriminal which is used to send commands to systems compromised by malware or other methods to control the system   
    **Backdoor**: A form of malware that negates usual authentication procedures to access a system **Keylogger:** A form of monitoring software that is designed to record every keystroke performed by the user
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**