# 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 CIA of information

A **breach** is an incident that involves data being disclosed to an unauthorized party

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

About 69% of breaches are from external sources, 34% are from internal actors

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

About 39% of breaches were perpetrated by organized criminal groups

1. What percentage of breaches were financially motivated?

About 71% of breaches were financially motivated

1. Define the following:   
     
   **Denial of Service**: An attack focused on making a machine or service inaccessible to users  
    **Command and Control** : this is a type of attack where the attacker can send commands to systems already infected by malware to receive data  
    **Backdoor**: Malware that negates normal authentication procedures to access data

**Keylogger**: A keylogger is a program that tracks hardware button clicks and sends them back to attackers

1. The time from an attacker’s first action to the initial compromise of an asset is typically measured in which one?

**MINUTES**

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

**Education** has the highest phishing click rate

Source used for this activity:

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf