# 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.” **(Verizon Data Breach Pg. 2)**

A breach is “an incident that results in the confirmed disclosure - not just potential exposure - of data to an unauthorized party.” **(Verizon Data Breach Pg. 2)**

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

Outside actors perpetrated 69% of breaches and Internal actors perpetrated breaches by 39%.**(Verizon Data Breach Pg. 5)**

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

Organized criminal groups perpetrated 39% of the breaches. **(Verizon Data Breach Pg. 2)**

1. What percentage of breaches were financially motivated?

Financially motivated perpetrated breaches were at 71%. **(Verizon Data Breach Pg. 2)**

1. Define the following:   
     
   Denial of Service:

(DoS) ”Any attack intended to compromise the availability of networks and systems. This includes both networks and application attacks designed to overwhelm systems, resulting in performance degradation and interruption of service.” **(Verizon Data Breach Pg. 25)**

Command and Control:

“A command - and - control (C&C) server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.” (<https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server>)   
Backdoor:

“Backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.” (<https://www.imperva.com/learn/application-security/backdoor-shell-attack/>)

Keylogger:

“Keyloggers are activity - monitoring software programs that give hackers access to personal data. The passwords and credit card numbers you type, the web pages you visit - all by logging your keyboard strokes. The software is installed on your computer, and records everything you type.”

1. 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?

The initial compromise of an asset is measured in “Minutes.” **(Verizon Data Breach Pg. 19)**

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

Education has the highest number of click rates of 4.93%. **(Verizon Data Breach Pg. 32)**