# 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 violates a company’s security policies and puts data at risk, whereas a breach is a security incident in which it is known that data was compromised.

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

69% of breaches were perpetrated by outside actors, while 34% involved inside actors.

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

It was determined that 39% of breaches involved organized crime.

1. What percentage of breaches were financially motivated?

71% of breaches were financially motivated.

1. Define the following:   
     
   Denial of Service:

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network. These attacks are usually accomplish this by flooding the target with so much traffic that it overburdens the server.  
Command and Control :

Command and Control is a type of malware that sends commands to systems that are already compromised by malware and tries to receive stolen data, such as credit card information.  
Backdoor:

Backdoor is malware that circumvents traditional authentication processes to gain access to a system or network. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.

Keylogger:

A keylogger is a type of software that is used to record keystrokes made by a user. They can be used to record credit card numbers and passwords typed into different websites.

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 time between the first action and the initial compromise is typically measured in minutes. However, the time to discovery is more likely to be measured in months.

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

Education has the highest click rate, which highlights the lack of security awareness in the industry.