# 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?

* Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.
* Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

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

* 69% perpetrated by outsiders
* 34% involved Internal actors

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

* Organized criminal groups were behind 39% of breaches

1. What percentage of breaches were financially motivated?

* 71% of breaches were financially motivated

1. Define the following:   
     
   Denial of Service: Any attack intended to compromise the availability of networks and systems. This includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.  
   Command and Control: 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.  
   Backdoor: 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.Keylogger: Activity-monitoring software programs that give hackers access to your personal data. The passwords and credit card numbers you type, the web pages you visit,
2. 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 from the attacker’s first action in an event chain to the initial compromise of an asset is typically measured in minutes. Conversely, the time to discovery is more likely to be months.

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

* Social with nearly 80% of active braches resulting from phishing.