# 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.

A breach is 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 percent of breaches were perpetrated by outside actors and 34 percent of breaches were perpetrated by internal actors

1. What percentage of breaches were perpetrated by organized criminal groups?   
   39 percent
2. What percentage of breaches were financially motivated?   
   71 percent
3. 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 command-and-control [C&C] server is a computer controlled by an [attacker](https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf) or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.  
   Backdoor: A 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.Keylogger: A keylogger monitors each keystroke of the user. The malware keeps track of the keystroke and saves the user’s information locally – later the hacker requires physical access to retrieve the stored user information. It also works the other way where the hacker can gain instant access to the user data through the Internet.
4. 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
5. When it comes to phishing, which industry has the highest click rates?  
   Education