# 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 which has the potential to result in disclosure of data through compromisation of the CIA triad.  
   A breach is an incident wherein the potential disclosure of data is realised.  
   A simple analogy is that of driving a car and almost crashing vs actually crashing ie, incident vs accident.
2. **What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?**  
   Per the summary of findings within the Verizon report, 69% of breaches were external actors, whilst 34% involved internal actors.
3. **What percentage of breaches were perpetrated by organized criminal groups?**  
   The statistics suggest 39% of breaches were instigated by organised criminal groups.
4. **What percentage of breaches were financially motivated?**   
   Around 71% of breaches were classed to be financially motivated.
5. **Define the following:   
   Denial of Service:**  
   Typically the goal is to disrupt services being provided by a host on the internet. This is commonly achieved by overloading the host or resource with endless false requests, slowing services, preventing access and often causing the service to come to a halt.  
    **Command and Control:**  
   Also known as C2 or C&C, Command and Control is an attack usually looking to create a network of infected hosts which can then be leveraged for nefarious uses.  
   Often the attacker will start with a single infected device, which will then report to the attacker’s server which provides the next command, such as installation of software and assimilating other hosts on the network.  
     
    **Backdoor:**Backdoor attacks are usually discreet attacks with the goal of attaining high levels of access within a host.  
   Backdoors are usually created by malware (typically Trojans) or as a feature of specific software/hardware configurations. Some backdoors genuinely have a purpose, but if it is not sufficiently protected it becomes an exploitable vulnerability. **Keylogger:**One of the older tricks in the book, keyloggers basically just watch what you are doing, harvesting keystrokes and information which is then sent back to the actor. With a little time and patience, a successfully deployed keylogger can easily provide the keys to the castle on almost any system.  
   Commonly classed as Spyware, keyloggers can be deployed both digitally via malware and physically via hardware - though the latter obviously requires physical access.
6. **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?**   
   According to the section discussing breach timelines, the initial compromise of an asset is typically measured in minutes.
7. **When it comes to phishing, which industry has the highest click rates?**  
   The education industry exhibits the highest click rate in regards to Phishing, at 4.93%

Great work overall