# Cybersecurity Threat Landscape (Part 3 - Verizon)

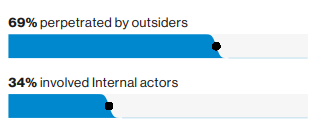
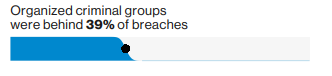
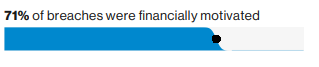
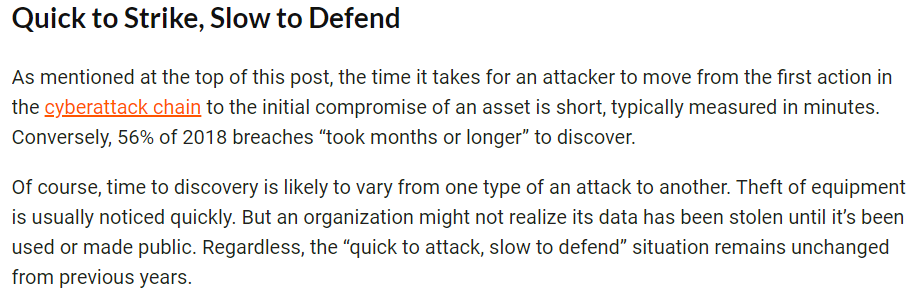
In this part, you should primarily use the *Verizon Data Breaches Investigation Report* plus independent research to answer the below questions.

1. What is the difference between an incident and a breach?  
     
   Think of a security incident as a pesky cold that may sideline you for a couple days, but clears up fairly quickly. It’s any event that violates an organization’s security or privacy policies around sensitive information like Social Security numbers or confidential medical records. This can be anything from a misplaced drive to missing paper files.

A data breach, on the other hand, is like the nastiest flu bug ever — a whopper of a virus that will knock you off your feet. The folks at ID Experts define it as a security incident that meets specific legal definitions per state and federal laws.

Specifically, data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies and media.

[What's the Difference Between a Breach and Security Incident?](https://www.spartantec.com/2016/12/07/whats-the-difference-between-a-breach-and-security-incident/)   
  
Incident vs. breaches We talk a lot about incidents and breaches and we use the following definitions:   
  
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?   
   
2. What percentage of breaches were perpetrated by organized criminal groups?   
   
3. What percentage of breaches were financially motivated?   
   
4. Define the following:   
     
     
   [Denial of Service](https://en.wikipedia.org/wiki/Denial-of-service_attack)  
   In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.   
   [Command and Control [C&C]](https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server):  
   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. ... It can be used to disseminate **commands** that can steal data, spread malware, disrupt web services, and more.   
   [Backdoor](https://www.sitelock.com/blog/what-is-a-backdoor-attack/):  
   A **backdoor attack** is a type of malware that gives cybercriminals unauthorized access to a website. Cybercriminals install the malware through unsecured points of entry, such as outdated plug-ins or input fields.[Keystroke Logging](https://en.wikipedia.org/wiki/Keystroke_logging):  
   **Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a [keyboard](https://en.wikipedia.org/wiki/Keyboard_(computing)), typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A **keylogger** can be either [software](https://en.wikipedia.org/wiki/Software) or [hardware](https://en.wikipedia.org/wiki/Computer_hardware).
5. 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?   
     
     
   [Key Takeaways from the 2019 Verizon DBIR](https://www.beyondtrust.com/blog/entry/key-takeaways-from-the-2019-verizon-dbir)
6. When it comes to phishing, which industry has the highest click rates? Education   
   