# Security 101 Homework: Cybersecurity Threat Landscape

# Part 3: *Verizon Data Breaches Investigation Report*

In this part, 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?**The difference between an incident and a breach is that an incident compromises the CIA triad, whereas the breach is confirmed disclosure of the data or information to unauthorized actors/parties.
2. **What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?**The majority of the breaches are perpetrated by outside actors. In 2020, approximately 80% were perpetrated by outside actors, while approximately 20% were perpetrated by internal actors.
3. **What percentage of breaches were perpetrated by organized crime?**Over 80% of breaches that were perpetrated by threat actors were done by organized crime.
4. **What percentage of breaches were financially motivated?**Over 90% of the breaches done by threat actors were financially motivated.
5. **Define the following (Additional research may be required outside of the report):   
     
   Denial of Service:**A denial of service, usually a “distributed denial of service” (DDoS) is an attack by a malicious actor that sends multiple requests or inquiries repeatedly to a point that it overwhelms the internet-based service, website, or similar so that no one else can access it.

**Command and Control:**The Department of Defense’s definition is: "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called C2.” Wikipedia also describes it as a military system. A more simplified definition is a "set of organizational and technical attributes and processes ... [that] employs human, physical, and information resources to solve problems and accomplish missions" to achieve the goals of an organization or enterprise according to a 2015 definition by military scientists Marius Vassiliou, David S. Alberts, and Jonathan R. Agre. The best definition found to summarize this is “Command and control is the process through which an attacker establishes a connection with a compromised asset that they have taken control of in a target network,” found on cyber-security-insiders.com article “The Hunter’s Den: Command and Control.”  
 **Backdoor:**Also known as “Trojan” viruses for a computer, but can be any method that malicious or legitimate actor(s) can get around standard security measures set in place and gain access to (possibly higher level) computer system(s), network(s), or software applications of an organization or individual.  **Keylogger:**A piece of spyware that is used by threat actors to record and steal keystrokes or things that are typed on a keyboard by the user that is being attacked/recorded without the user’s knowledge. This is often used to steal information or login credentials with usernames/ passwords.

1. **What remains one of the most sought-after data types for hackers?**Banking data remained the top most sought-after data type for jackets over the past 3 years that the report covered. Declining slightly YoY from 2019 to 2020, but still significantly higher than the next highest, bins and bank identification number(s).
2. **What was the percentage of breaches involving phishing?**  
   Over 35% of breaches involved phishing.