# 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?
   1. According to 2021 DBIR, an incident is “a security event that compromises the integrity, confidentiality or availability of an information asset” while a breach is more serious, and described as “an incident that results in confirmed disclosure - not just potential exposure - of data to an unauthorized party” (pg 4).
2. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?
   1. Figure 14 on page 12 shows that about 20% of breaches were perpetrated by internal actors in 2020, and about 80% of breaches were perpetrated by internal actors.
3. What percentage of breaches were perpetrated by organized crime?
   1. On page 12, Figure 16 shows that about 80% of breaches were perpetrated by organized crime in 2020.
4. What percentage of breaches were financially motivated?
   1. Financially motivated breaches were the most common in 2020, with about 90% of the breaches (Figure 14).
5. Define the following (Additional research may be required outside of the report):   
     
   Denial of Service: cisa,gov defines Denial of Service attacks as when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor… which is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users” (https://www.cisa.gov/uscert/ncas/tips/ST04-015).

Command and Control: Command and Control attack starts by infecting the victim computer and then “the infected machine sends a signal to the attacker’s server looking for its next instruction. The infected computer will carry out the commands from the attacker’s C2 server and may install additional software. The attacker now has complete control of the victim’s computer and can execute any code” (https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained).  
Backdoor: In a backdoor attack, the threat actor is able to “install the malware through unsecured points of entry, such as outdated plug-ins or input fields. Once they enter through the back door, they have access to all your company’s data, including customers’ personal identifiable information” (https://www.sitelock.com/blog/what-is-a-backdoor-attack/).  
Keylogger: “A keylogger (or keystroke logger) is a type of software or hardware used to track and record what someone types on their keyboard… Malicious actors can also use them to capture your personal and financial information, PIN codes and account numbers, credit card numbers, usernames, passwords, and other sensitive data” (https://us.norton.com/internetsecurity-malware-what-is-a-keylogger.html).

1. What remains one of the most sought-after data types for hackers?
   1. In almost all of the “Data Compromised” sections of the Summaries, Credentials were the highest percentage of compromised data. For example, in Public Administration, “the most frequently stolen data type is Credentials, which are then used to further the attacker’s presence in the victim’s network and systems” (pg 85).
2. What was the percentage of breaches involving phishing?
   1. Figure 73 on page 50 shows that about 80% of Social Engineering breaches involved Phishing.