# 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

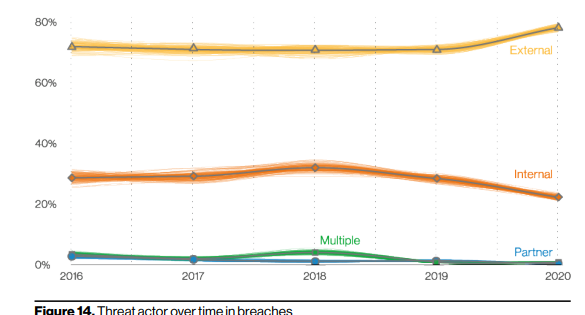
1. What is the difference between an incident and a breach?

An incident is a security event when there is a breach in the integrity, availability, and confidentiality of an information asset. This can take into the form of a denial of service of impersonation where the user is denied access from their own machine/network.

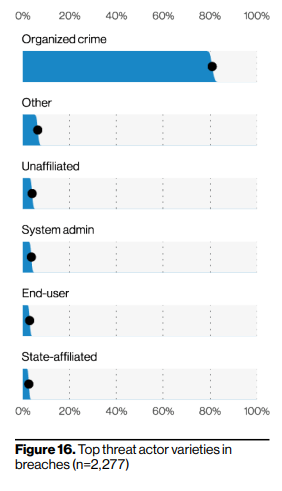
A breach involves an incident that results in the confirmation of a disclosure of data to an unauthorized party that has been leaked, hacked or released.

1. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?

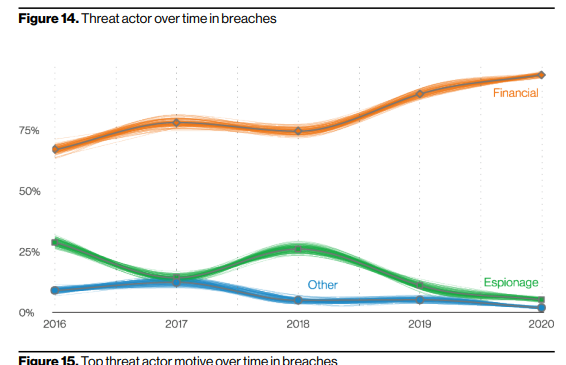
Based on Figure 14 graph from the Verizon DataBreach report, this illustrates the percentage of perpetrated breaches conducted by internal & external actors. As conveyed in the graph, external actors are the vast majority in the 80% territory, while internal actors are involved in around 20% of these breaches.



1. What percentage of breaches were perpetrated by organized crime?   
   As displayed in the Figure 16 graph, organized crime perpetrated 80% of breaches



1. What percentage of breaches were financially motivated?   
   As per Figure 15 graph, financially motivated breaches were the most common form of attacks as it represents a total percentage of 75+% of top threat actors motives in breaches



1. Define the following (Additional research may be required outside of the report):   
     
   Denial of Service:

Denial of Service (DDoS) is type of attack in an attempt to make an online service unavailable by utilizing a network of compromised systems to overflow sites with connection requests.

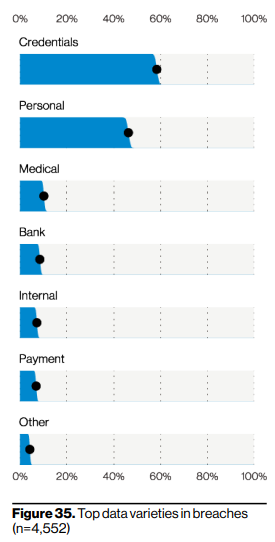
Command and Control:   
Command and Control (C&C) involves the adversary aiming to communicate a system that is compromised and controlling it. This method involves a number of techniques in order to have the systems under their control within a victim network such as phishing emails, security holes in browser plugins, and via other infected software.

Backdoor:  
In the Cyber Security industry, backdoor is a reference to any sort of method by unauthorized/authorized users are able to get around security measures and retrieve root access on a software application, computer system, or network.

Keylogger:  
Keylogger is a type spyware that cybercriminals utilize to be able to monitor and record users keystrokes on their keyboard. This type of spyware once installed on your system can completely compromise of data sensitive information as cybercriminals may now be able to retrieve private data such as passwords, credit cards numbers, social security, etc.

1. What remains one of the most sought-after data types for hackers?

As per Figure 35 graph, credentials are the most sought-after data types for hackers as it represents a total percentage of 55 – 60% in top data varies in breaches



1. What was the percentage of breaches involving phishing?

As per Verison Data Breach Report 2021, phishing remains as one of the largest forms of methods to breach private data, as it currently consists of 36% of total breaches, which is an increase of 25% from 2020.

**References**

Wragg, P, 2021, *Is it an Incident or a Breach? Defining the Difference,* Integrity 360. <https://insights.integrity360.com/incident-or-breach>

Verizon, 2021, *Data Breach Investigation Report (DBIR),* Retrieved March 13th, 2022

ACSC, 2020, *Denial of Service,* Australian Cyber Security Centre, Retrieved March 14th, 2022, <https://www.cyber.gov.au/acsc/view-all-content/threats/denial-service>