# 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. **An incident is a security event that affects the CIA triad with respect to an information asset. This is a compromise of the confidentiality, integrity, or availability of that asset.**

**A breach is an incident that results in a confirmed disclosure of data to an unauthorized entity.**

1. What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?   
   1. **21% internal 79% external**
2. What percentage of breaches were perpetrated by organized crime?
   1. **80%**
3. What percentage of breaches were financially motivated?
   1. **70%**
4. Define the following (Additional research may be required outside of the report):   
     
   Denial of Service: **This is an attack that can be carried out in almost any way with any tool. Denial of service prevents those who wish to access something from being able to do so. This can include; flooding a web server with requests so legitimate users cannot use the server’s hosted content, cutting fiber lines thereby removing network connection for geographic locations, and redirecting network traffic to prevent it from reaching the proper destination. This type of attack can generally be carried out by even low sophistication actors.**

Command and Control: **This is an infrastructure and design model. Instead of packing everything you expect your malware to do into one package, you can program it to reach out to a server (Command server) when it is installed or during other predetermined situations. The server your malware reaches out to is the control server. Your control server can send out commands, or your malware can reach out to the server and ask for instructions, updates, changes, etc.. This allows more sophisticated attacks by allowing smaller and more discrete malware design when gaining a foothold while still allowing for a greater set of options to be available if/when needed.**   
Backdoor: **A backdoor is a method or means to bypass security that is normally in place. Often, in the legal (opposed to illicit) context, this is used to allow access to devices that need to be recovered in the instance someone forgot their credentials or for designers to get into a device or software that is not available to consumers.**

**For attackers (illicit), this can be planted, after access is gained, to a device or software to maintain control or availability of access. For instance, if you break into a computer system, you may install a backdoor by changing registry keys, setting up remote shell access, or weakening security to allow you to compromise the system if your original method is found or fails operating.**

Keylogger: **This can be a hardware device or software program.The intent of keyloggers is to capture the keystrokes made by the person inputting data into a computing device. These can range from legal and beneficial uses to malicious uses. Keyloggers are sold openly on the consumer market and are prebuilt into software in some cases.**

**For legal uses, in programing interfaces this can be used to record a command log history or to provide a record of changes made and commands put in. This can also be used by parents or even businesses who want to monitor what those under their purview are doing.**

**Some illicit uses include capturing passwords or sensitive information typed in by a target, spying on the activity of targets by examining what they search for or create (Espionage, corporate or otherwise), and some devices can even replay or send commands as if it was the user entering them allowing further attacks.**

1. What remains one of the most sought-after data types for hackers?
   1. **Credentials**
2. What was the percentage of breaches involving phishing?
   1. **36%**