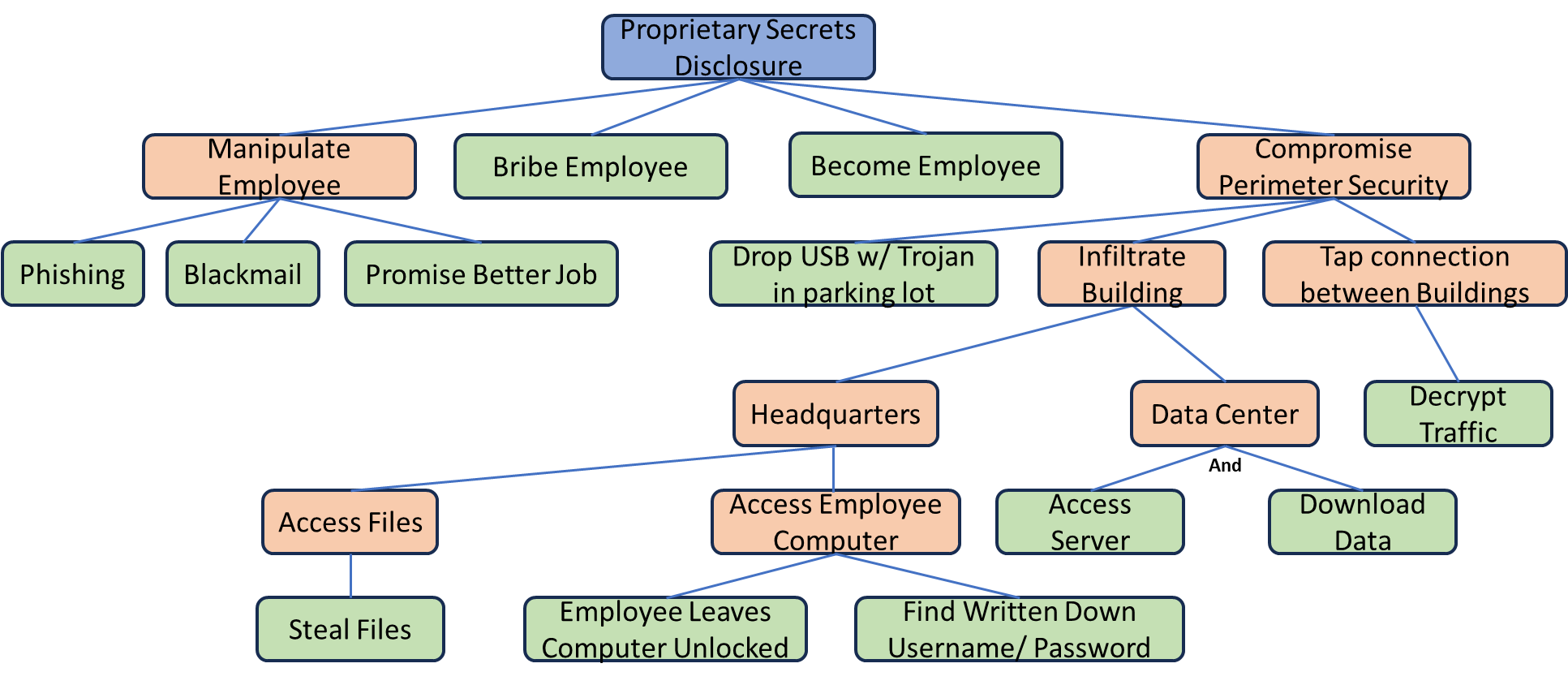
Task 1

P1: Simplicity and Necessity. One example of this being followed is the system to enter my building at work. It is a simple system where the only thing someone needs to do is hold their assigned badge up to a reader on the door. This reader then confirms that the badge is authorized entry to the building and unlocks the door if it is.

P6: Least Privilege. Another example from work. We recently had an organization wide scrub of all our access rights. There were a few rights that everyone was expected to have or maintain, but for the rest, additional justification and explicit approval from leadership was required for each type of access.

Task 2



Task 3

The entity will be my work building:

-Security Policy: No one is permitted to enter unless they are explicitly authorized or have the necessary clearances and need to enter and are escorted by an authorized person.

-Security Violation: An unescorted, unauthorized person enters the building.

-Vulnerability: The door that I enter through does not close automatically when the climate control system is running. This results in it being left open regularly.

-Threat: Existence of a person who wishes to access computer systems, damage property, or harm employees.

-Attack: An intruder enters through the unclosed door with the intent to cause harm.

Task 4

For cyber attacks on the healthcare industry, attacker motives were dominated (98%) by the prospect of financial gain. The main patterns of these attacks were system intrusion, basic web application attacks, and miscellaneous errors. A major issue for this sector was ransomware, and a possible mitigation strategy for this is to maintain and utilize frequent data backups, to allow critical information to be restored in the event of an attack.