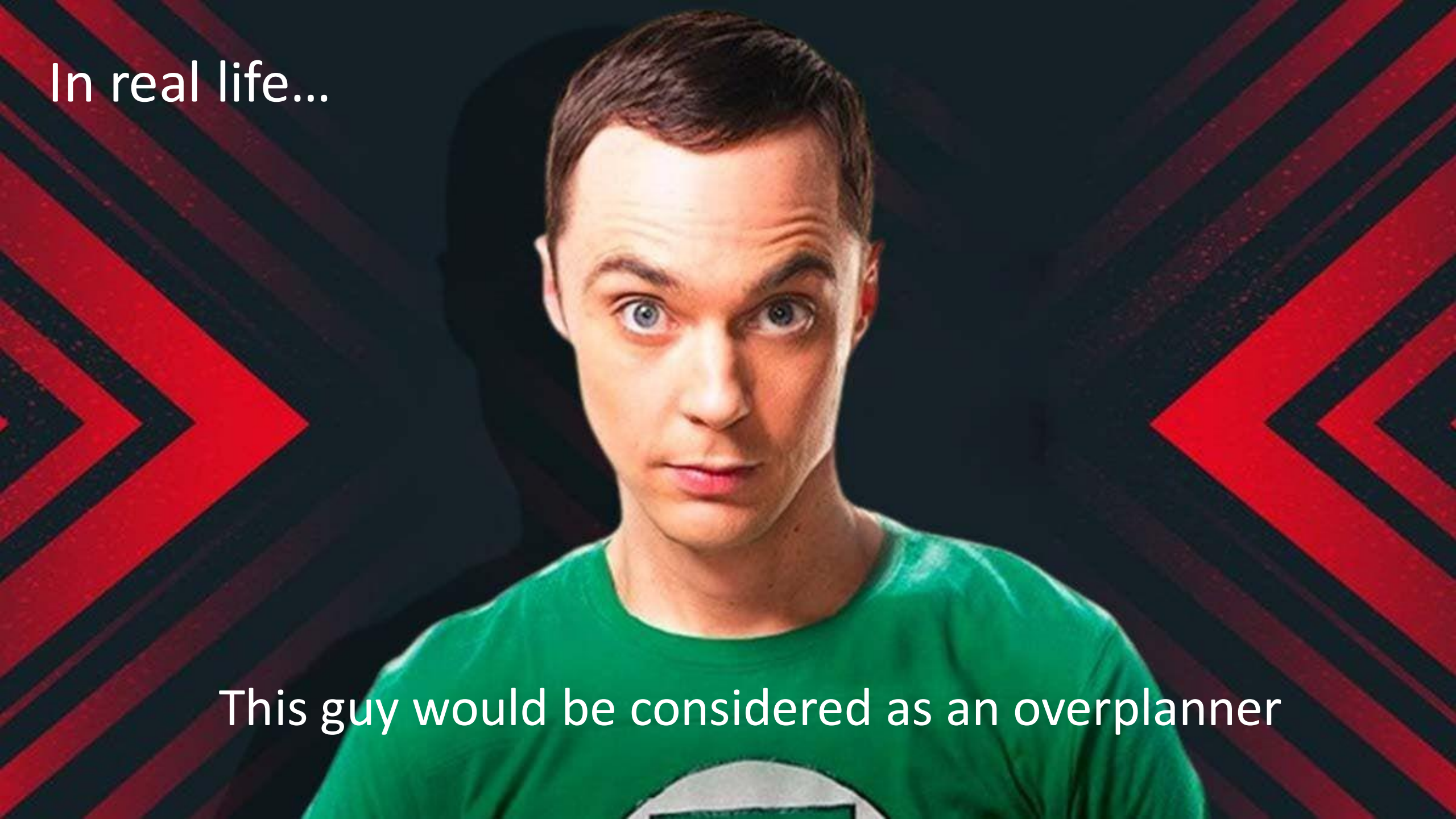
NEVERHACK

YOUR CYBER PERFORMANCE PARTNER

In real life…



This guy would be considered as an overplanner

In real life… man with no plan also have their issues…

Man with a plan usually avoid this…

1. Lack of Direction: Without a plan, organization might feel lost and unsure of the next steps or how to achieve its goals.

2. Inefficiency: Time and resources may be wasted on unproductive activities due to the absence of a clear path.

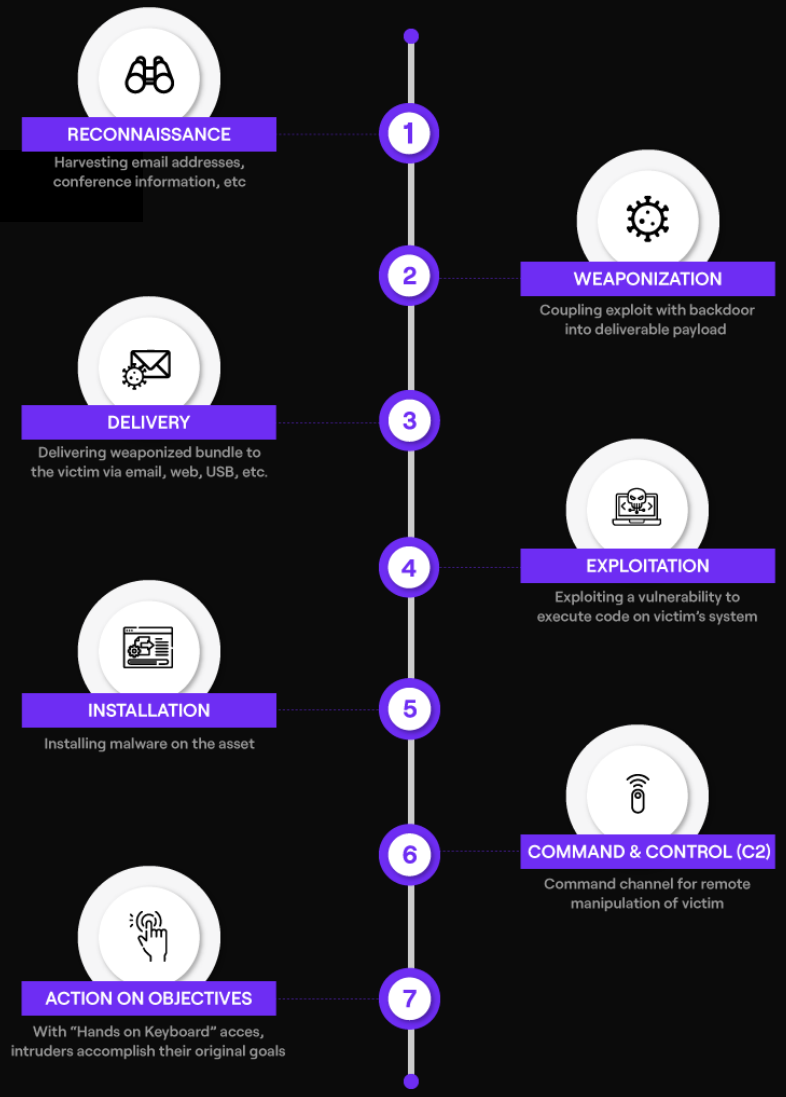
3. Missed Opportunities: organizations might miss out on beneficial opportunities because they weren't prepared.

4. Increased Stress: The uncertainty and lack of control leads to higher stress and anxiety levels.

5. Poor Decision Making: Decisions made without a plan tend to be reactive rather than proactive, often resulting in poor outcomes.

6. Low Morale: In a cybercrisis situation, employees may feel abandoned and uncertain about their roles and the organization's.

CyberKillchain



Reconnaissance: Attackers gather information about their target, identifying vulnerabilities and potential entry points.

Delivery: Transmission of the malware to the target, often via phishing emails or exploiting software vulnerabilities.

Exploitation: Execution of the malware on the target system, exploiting the vulnerabilities.

Installation: Establishment of the malware on the target system, creating a foothold for the attacker.

Command and Control (C2): Establishment of a communication channel with the compromised system for remote control.

Actions on Objectives: Achievement of the attacker's goals, such as data theft, system disruption, or further network infiltration.

2017, WANACRY

Reconnaissance: Attackers targeted systems running outdated versions of Windows.

Weaponization: They developed the WannaCry ransomware using the EternalBlue exploit.

Delivery: The ransomware was disseminated through phishing emails and malicious downloads.

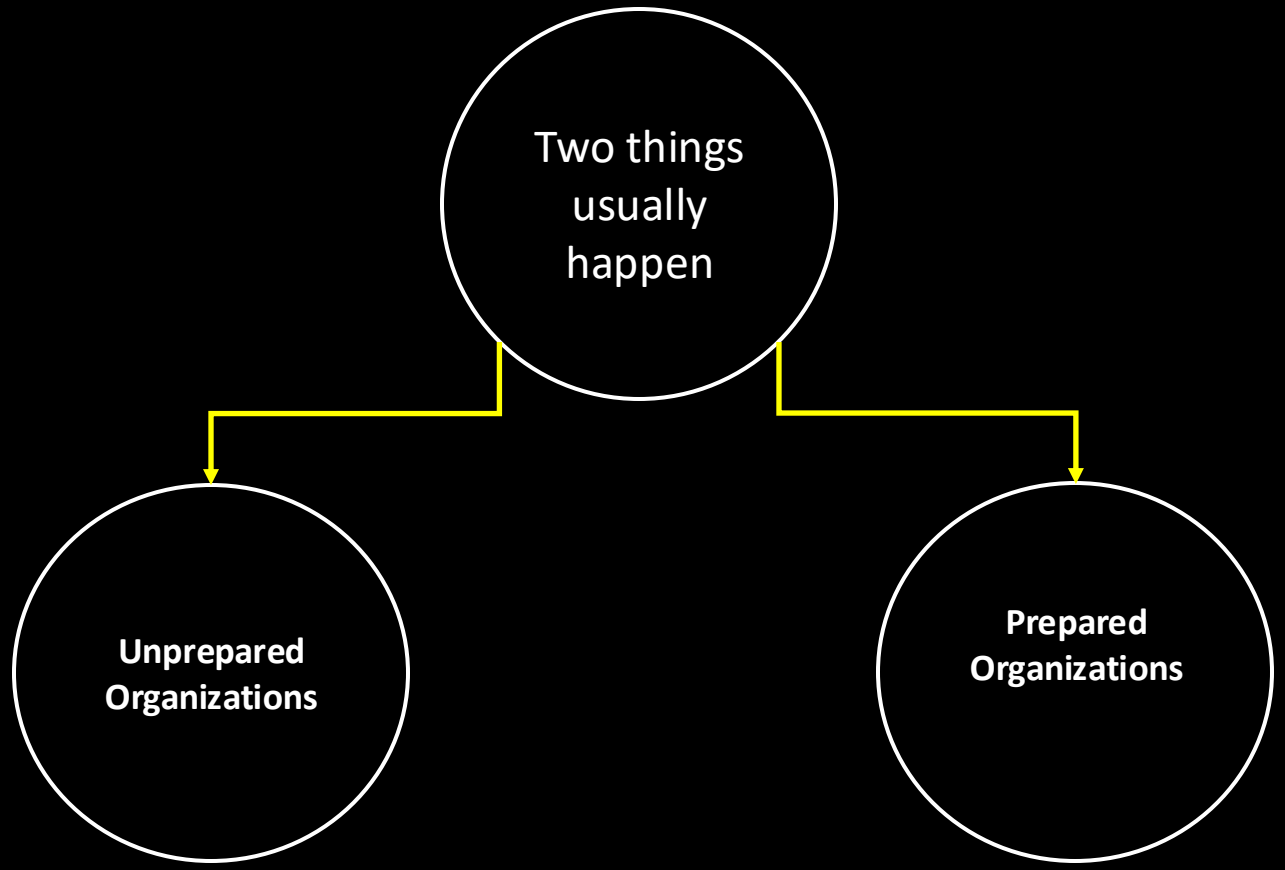
Exploitation: EternalBlue was employed to exploit a vulnerability in the SMB protocol.

Installation: The ransomware encrypted files on the infected systems.

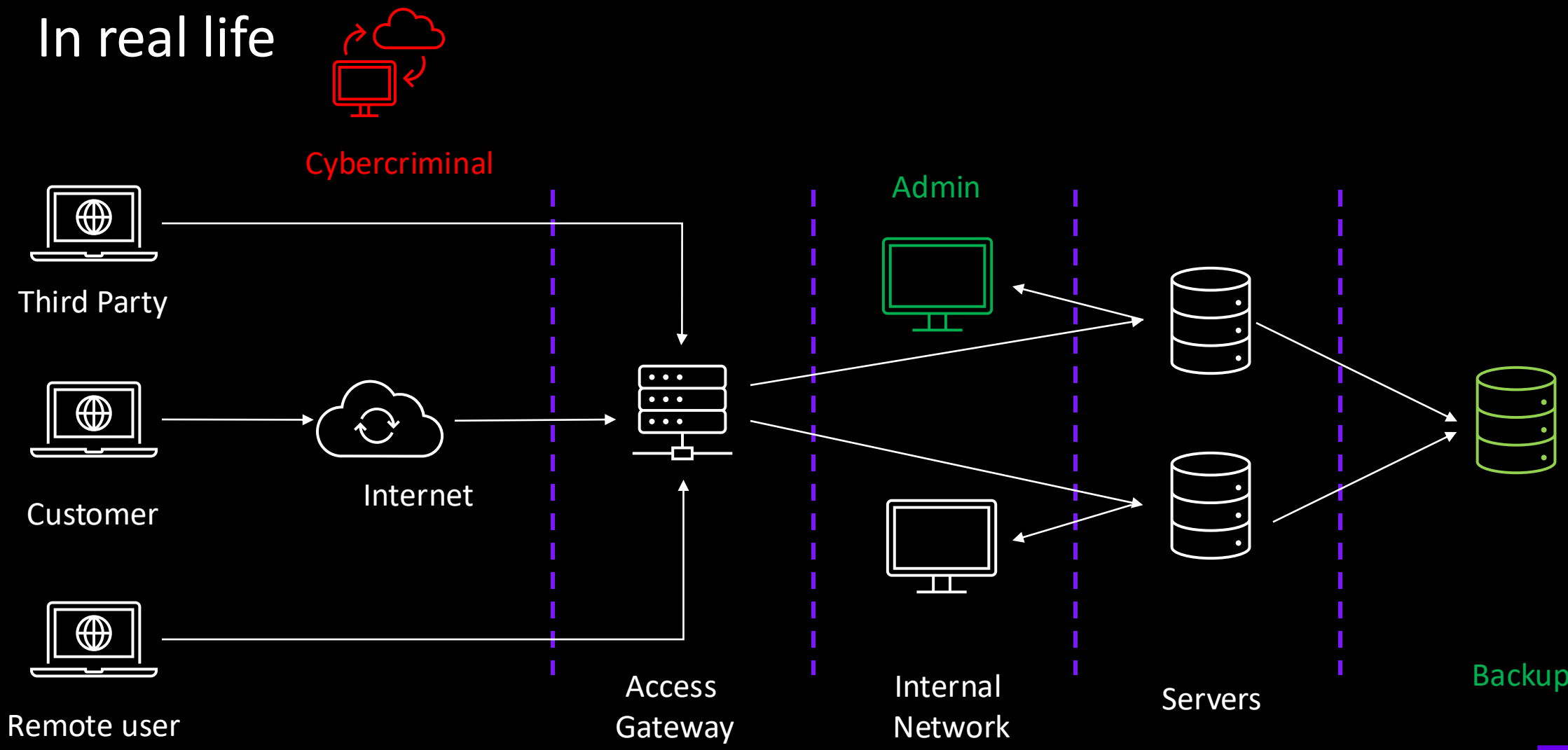
Command and Control: It connected to an external server to report new infections.

Actions on Objectives: Attackers demanded ransom payments to decrypt the encrypted files.

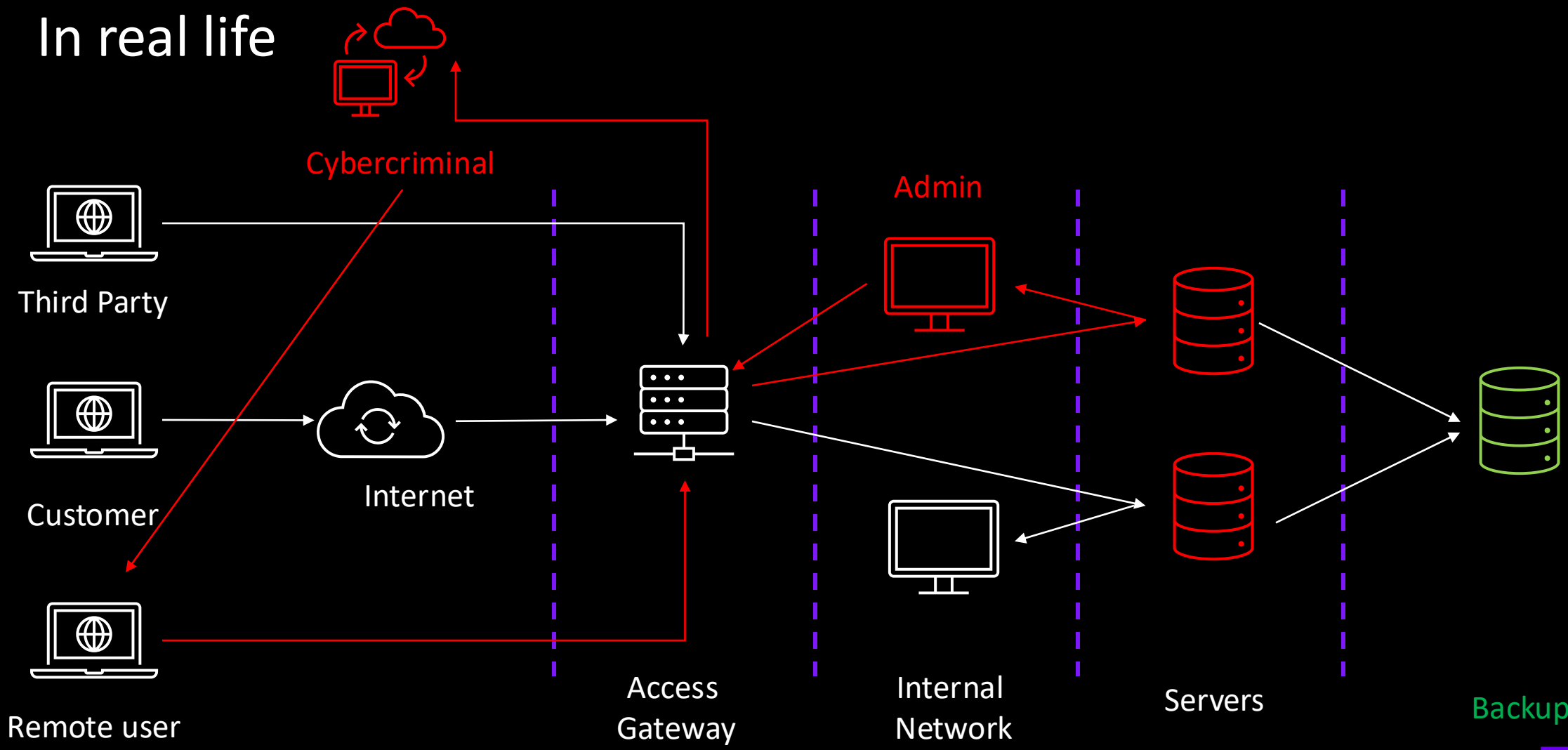
In real life


Two things usually happen
Unprepared Organizations
Prepared Organizations

In real life

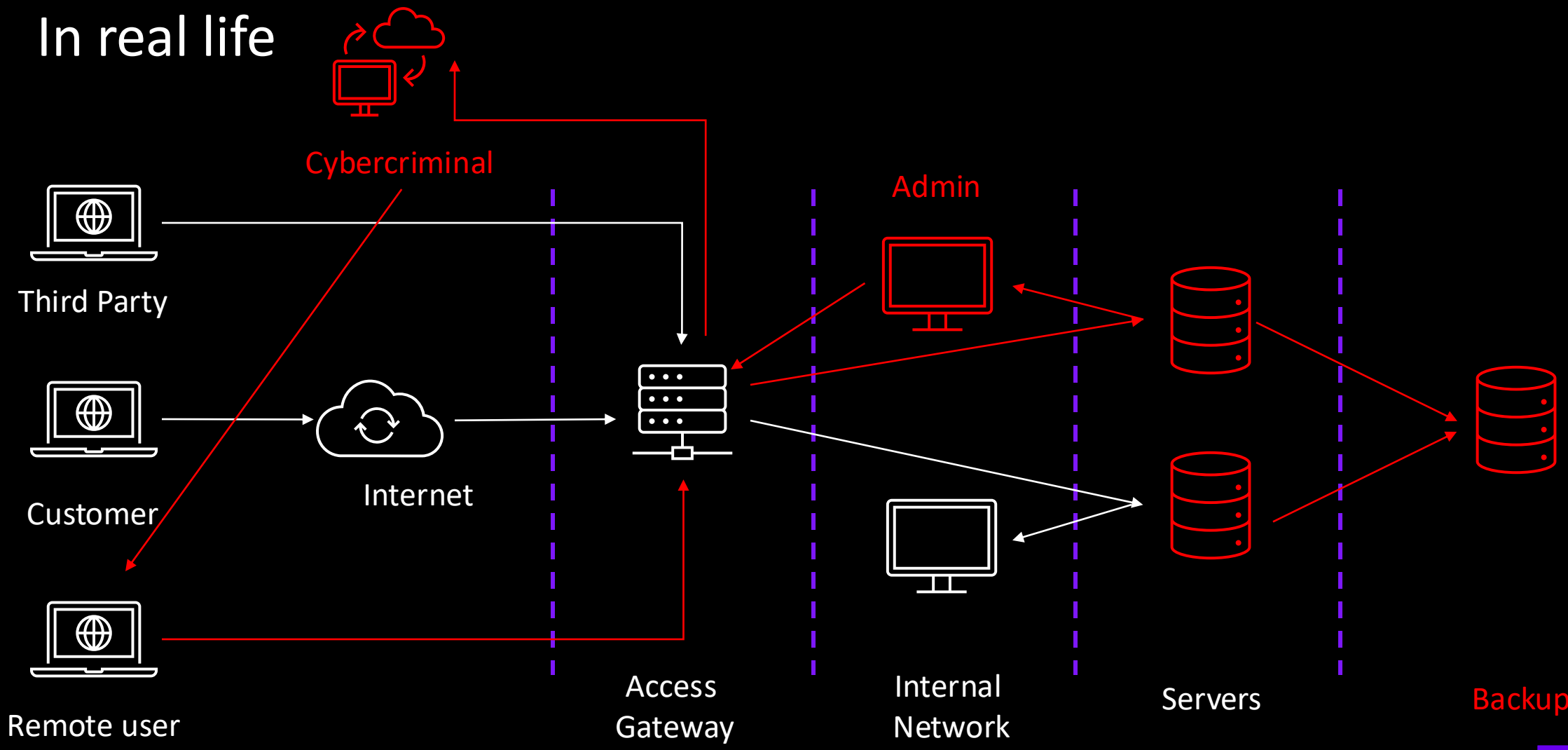

Cybercriminal
Admin
Third Party
Customer
Internet
Remote user
Access Gateway
Internal Network
Servers
Backup

In real life



Bad case scenario

In real life



Worst case scenario

NEVERHACK

PARTENAIRE DE VOTRE PERFORMANCE CYBER