📅 Insider Threat Simulation Log Day 1: Unsecured Server Room Access

Date of Entry: 6/16/2025
Observer: Michael Warner
Location: On-Site Server Room @ Pharmacy
Classification: Internal Security Simulation

🧾 Incident Overview

On the first day of my insider threat simulation, I identified an immediate and high-priority physical security lapse. At approximately 9:28 AM, I discovered the facility's primary server room door was left unlocked. No personnel were present inside. There was no access control system visible at the door — no badge reader, no surveillance camera, and no logging mechanism to indicate who had entered or exited.

Based on daily shift routines, the server room likely remained unsecured for approximately 8 hours. A return inspection the following morning revealed the door had been re-secured.

⚠️ Risk Assessment

Prolonged physical access to core infrastructure without monitoring introduces serious risk, including:

- Unauthorized access to sensitive systems
- Potential hardware tampering or malware introduction
- Exposure of unencrypted credentials or sensitive files
- Tailgating risk, enabling external threat actors to exploit lax security

This suggests either; a failure in enforcing physical access policy or a disregard for standard operational protocols. Either scenario creates exploitable gaps for malicious insiders.

🕵️ Speculative Insider Perspective

From an adversarial viewpoint, this was a rare opportunity. Without surveillance or access logging, I could have:

- Deployed a USB-based keylogger or rogue device
- Cloned access credentials from active or idle terminals
- Installed a backdoor with minimal detection risk

The absence of monitoring mechanisms meant low deterrence and zero attribution.

🛡️ Initial Thoughts & Actions

This is the first observed instance of the server room being unsecured. I conducted only visual verification and took no further action to alter the environment.
No one was observed in or near the server room during my discovery. Documentation of the incident was done discreetly for the purposes of this simulation.

✅ Recommendations (Low-Impact Suggestions)

- Conduct an immediate audit of server room access logs (if any exist)
- Install badge-swipe or biometric entry with automated logging
- Place a security camera covering all server room entry points
- Implement random spot checks by security or supervisory staff across shifts

🟠 Severity Rating

Moderate to High, depending on audit results and whether any unauthorized access occurred.

- End of Entry