📅 Insider Threat Simulation Log Day 2: Unattended & Unlocked Workstations
Date of Entry: 6/17/2025
Observer: Michael Warner
Location: Multiple Departmental Devices @ Pharmacy
Classification: Internal Security Simulation

🧾 Incident Overview

A significant and repeated lapse in endpoint security practices was observed during a routine walkthrough. Across several departments, including data entry, management, and production, multiple employees left active computer sessions unlocked and unattended. These workstations were accessible to anyone passing by and, in some cases, were left idle for long periods. This was not an isolated event but a pattern of negligent behavior observed multiple times throughout the day.

⚠️ Risk Assessment

This pattern points to a cultural or policy failure rather than individual forgetfulness, likely stemming from a lack of enforced screen timeout policies, minimal user security training, or no disciplinary structure for such offenses. This behavior introduces critical risks to the organization. The primary concerns are:

- Privilege Abuse: A malicious insider could use another user's active session to modify or exfiltrate sensitive data.
- Session Hijacking: External vendors or unauthorized staff could gain system access simply by walking by an unattended terminal.
- Non-repudiation Compromise: If a malicious act is performed using another person's login, it becomes difficult to ensure accountability.

🕵️ Speculative Insider Perspective

From an adversarial viewpoint, these unlocked workstations offer a low-effort, high-reward opportunity. An insider could easily take control of another user's session to access privileged information, such as HR dashboards or company databases. By using an existing logged-in session, any malicious actions become difficult to attribute correctly, effectively framing the legitimate user for the activity. The widespread nature of this issue means an attacker could choose a target based on the level of access they desire.

🛡️ Initial Thoughts & Actions

My actions consisted of observing and discreetly documenting these security lapses across the different departments. The goal was to understand the scope of the problem without altering the environment. The analysis suggests these repeated offenses are a systemic issue, not a series of isolated mistakes.

✅ Recommendations (Mitigation Actions)

To address this vulnerability, the following actions are recommended:

- Enforce automatic screen locks on all workstations after 3–5 minutes of inactivity.
- Launch security awareness campaigns that emphasize the importance of workstation responsibility.
- Incorporate workstation security checks into routine audits and walkthroughs.
- Log repeated offenses to identify patterns and address them at a departmental level.

🟠 Severity Rating

High. The behavior is described as a "significant and repeated lapse" that happens across multiple departments. The concluding thought, "If it’s not respected, everything else is already compromised," underscores the critical nature of this vulnerability.

End of Entry