📅 Insider Threat Simulation Log Day 9: Badge-Controlled Door
Date of Entry: 6/24/2025
Observer: Michael Warner
Location: Internal Delivery Area
Classification: Internal Security Simulation

🗒️ Incident Overview

During the ninth day of my insider threat simulation, I focused on physical security measures in the pharmacy's rear access area. Although the main back door (used for stock deliveries) is reliably locked, I observed that the secondary interior door, which provides access to the secured pharmaceutical storage area, is frequently propped open.

This door is normally controlled by a badge scanner, but it appears that for convenience or habit, staff leave it open during delivery hours or extended periods of activity. While external delivery personnel (e.g., FedEx, Amazon) rarely enter this inner zone, the unsecured door allows potential unauthorized access without the need for a badge.

Given that pharmaceuticals—including controlled substances—are stored in this area, the bypass of the door's access control poses a critical risk.

⚠️ Risk Assessment

- Leaving the badge-controlled door propped open presents several security risks:
- Unauthorized access to medications or sensitive areas by malicious insiders or opportunistic outsiders
- Potential for inventory theft, tampering, or contamination
- Violation of physical access protocols that may impact compliance with regulatory standards (e.g., DEA, HIPAA)

Lack of access logs for individuals entering the pharmaceutical zone when the door remains unmonitored

🕵️ Speculative Insider Perspective

- As a malicious insider or a curious third-party delivery contractor, I could:
- Wait for the door to be left open and enter undetected
- Steal or tamper with pharmaceutical stock, especially if left unattended
- Plant unauthorized devices (e.g., RFID cloners, USB drops) in the pharmacy
- Bypass badge logging, making it harder to trace my presence

These actions would require no technical skill, only awareness of timing and habits.

🛡️ Initial Thoughts & Actions

I did not interact with the door or tamper with physical equipment. My observations were made through passive monitoring of staff and delivery routines throughout the day. No alerts or security personnel were present to monitor access during observed times.

✅ Recommendations (Low-Impact Suggestions)

- Install automatic door closers or timed locking mechanisms for badge-controlled doors
- Educate staff on the importance of maintaining access controls—even during routine deliveries
- Conduct regular checks to ensure badge-controlled doors are not being bypassed
- Place "Do Not Prop Open" signage on sensitive internal access points
- Review camera placement and consider adding one to monitor that interior door

🟠 Severity Rating

High — The ability to enter a restricted pharmaceutical area without credentials represents a serious physical security flaw that could be exploited with minimal effort.

- End of Entry