📅 Insider Threat Simulation Log Day 14: IT Oversees Its Own Compliance
Date of Entry: 6/29/2025
Observer: Michael Warner
Location: Organization-Wide (Leadership Escalation Attempt)
Classification: Internal Security Simulation

🧾 Incident Overview

On the final day of my insider threat simulation, I followed up on my formal business proposal submitted to the CEO, in which I recommended the creation of an Information Security Officer (ISO) role. The goal of this role was to oversee cybersecurity, monitor internal compliance, and serve as a check-and-balance against internal oversights — several of which I had previously documented.

After receiving no direct response, I formally requested a brief 15-minute meeting to discuss the proposal further. Instead of hearing back from the CEO, I was contacted by Human Resources, who informed me that they had been asked to respond on behalf of the CEO.

The message relayed was as follows:

- All cybersecurity and compliance matters are currently handled by a third-party IT provider.
- The CEO contacted this IT provider to ask whether we were “in compliance.”
- The response was deemed sufficient to the pharmacy and no further internal oversight was considered necessary.

In effect, the CEO decided to delegate the responsibility for validating compliance to the same group tasked with maintaining it, without external review or independent verification. My proposal to establish an internal ISO role — intended to reinforce best practices and close accountability gaps — was ultimately rejected.

⚠️ Risk Assessment

- Relying on an external IT provider to self-certify compliance introduces significant strategic risks:
- Lack of independent oversight or internal auditing
- Conflict of interest, as IT assesses its own work and controls the narrative
- No internal resource available to validate, challenge, or escalate overlooked risks
- Missed opportunity to embed a culture of security accountability inside the organization
- Ongoing issues may persist unchecked simply because no one is assigned to track them internally

🕵️ Speculative Insider Perspective

As a malicious insider, I could:

- Rely on the lack of local oversight to exploit known vulnerabilities indefinitely
- Take advantage of IT's broad trust to bypass internal checks
- Exploit the absence of a security-focused leader to push phishing, privilege escalation, or data theft schemes without resistance
- Know that no one on the inside is watching — which increases confidence to act

Without a dedicated ISO or internal security advocate, oversight becomes a matter of trust, not verification.

🛡️ Initial Thoughts & Actions

No technical action or testing occurred. This entry reflects the organizational outcome of my attempt to escalate legitimate concerns through a formal proposal. I acted in good faith, documented key risk indicators, and provided clear recommendations. Despite this, the leadership chose to defer cybersecurity entirely to an external vendor — with no internal security governance or transparency mechanism.

✅ Recommendations (Low-Impact Suggestions)

- Re-evaluate the need for an internal ISO, CISO, or compliance liaison
- Perform periodic external cybersecurity audits not conducted by the same IT vendor
- Establish an internal risk register to track IT recommendations and response timelines
- Create a security committee that includes non-IT staff, compliance officers, and leadership
- Foster a culture of shared accountability where cybersecurity is not solely delegated away

🟠 Severity Rating

High — The rejection of internal cybersecurity oversight leaves the organization vulnerable to undetected misconfigurations, compliance drift, and insider threats. Outsourcing risk does not eliminate it — it simply obscures it.

- End of Final Entry