📅 Insider Threat Simulation Log Day 12: Recycled PCs Still Contained Company Data
Date of Entry: 6/27/2025
Observer: Michael Warner
Location: Off-Site
Classification: Internal Security Simulation

🗒️ Incident Overview

On the twelfth day of my insider threat simulation, I reviewed several mini desktop computers that had been offered to employees as part of a hardware cleanout. The organization had recently made a supply of old workstations available for staff to take home before the remainder were scheduled for recycling.

While many employees selected monitors or accessories, I chose five mini desktop systems — mostly identical models — with the intention of combining parts to restore at least one functional device. Ultimately, I was able to power on two of the five systems, and to my surprise, both still contained company data.

Despite informal claims that the devices had been “wiped by IT,” the recovered systems contained internal documents, user profiles, and visible traces of business operations. No formal record of sanitization or data clearance was included with the devices.

⚠️ Risk Assessment

- Releasing old devices without secure data destruction introduces the following risks:
- Uncontrolled leakage of company data into employee or public hands
- Loss of regulatory compliance for sensitive data disposal procedures
- Exposure of user credentials, business communications, or protected health data
- Lack of audit trail for who received which device and what data remained
- Reputational damage if data were mishandled, shared, or exploited

🕵️ Speculative Insider Perspective

As a malicious insider, I could have:

- Cloned and reviewed disk contents for sensitive files, credentials, or cached emails
- Recovered deleted files using forensic tools or system logs
- Sold, published, or traded company data with no traceable breach
- Used the data to gain additional context for future insider actions

Because the devices were given away with no wipe confirmation or tracking, I would not appear suspicious for taking one — or for what I later accessed on it.

🛡️ Initial Thoughts & Actions

No data was exfiltrated or tampered with during my simulation. I conducted only passive file and system inspection to validate the presence of residual company data. When I powered the PCs on I confirmed a company domain login for Windows. I then restarted the PCs and performed a system wipe within BIOS settings. The intent was to document the outcome of receiving unsanitized hardware through an informal internal handout process.

✅ Recommendations (Low-Impact Suggestions)

- Enforce a standard device sanitization protocol before any employee distribution
- Require formal documentation or certification of data destruction (per NIST SP 800-88)
- Avoid distributing devices without logging serial numbers or recipients
- Discourage informal tech giveaways unless systems are confirmed to be data-free
- Consider issuing standardized IT surplus policies for device disposal and handoff

🟠 Severity Rating

High — Multiple unverified systems were handed out to employees, two of which contained internal data. This represents a clear breakdown in data lifecycle controls and opens the door to silent insider access or future leaks.

- End of Entry