ITAD Chain of Custody Case Studies – Challenges & Common Excuses

Published on Oct 17th, 2011
http://www.itassetmanagement.net/2011/10/17/itad-chain-custody-case-studies/
By Kyle Marks at Retire-IT.

In his previous article Kyle explored the value of process in IT Asset Disposal – in this article Kyle explores some real life scenarios to illustrate chain-of-custody challenges.

When outsourcing IT asset disposal (ITAD) to a qualified vendor, it is critical to establish a system of checks and balances. An unbroken chain-of-custody is necessary to shield your organization from malicious insiders and downstream liability. Establishing chain-of-custody is far easier said than done.

The "Switch-a-Roo "

The switch-a-roo is a common tactic used to trick someone by switching two things around. An IT manager at a healthcare organization used a switch-a-roo to take retired laptops for personal use. The organization thought it had a foolproof process to track the equipment it sent to the ITAD vendor. Asset tags were verified and if one was not available then serial numbers would be matched.

One IT manager who knew this tracking process simply manipulated the disposal inventory to conceal his crime. Just before a pickup of equipment, he would alter the disposal inventory by switching an asset tag number – an asset tag ID associated with a laptop would be swapped with an asset tag associated with a low-value asset (e.g. a laptop docking station). Since low-value items were routinely omitted and did not pose a security risk, the loss of one was rarely investigated. Ultimately, the switch-a-roo scam was uncovered when the organization implemented a systematic validation of both asset tags and serial numbers.

The "Déjà Vu "

We have all experienced the feeling that we've seen something before. While performing a periodic audit of a financial service firm's disposal process, an asset manager was

surprised to see the same server show up on two different disposal project reports. The server had been decommissioned, retired from the fixed asset system, earmarked for disposal, and placed on the disposal inventory with several dozen other assets. The lot of equipment was then transported to the disposal vendor for processing.
It turns out that this particular server was not physically sent to the disposal vendor as planned. It had been "pulled off the disposal pile" at the last minute (someone wanted to harvest memory). The disposal inventory, however, was not updated to reflect the exclusion. Ultimately, the server was physically sent to the vendor the following month, as part of different disposal project. Strangely, the disposal vendor reported receiving the specific server on both projects. On the first project, the disposal vendor ignored the omission. On the second project, the vendor disregarded the duplicate to avoid the risk of embarrassment.

Preventing problems associated with ITAD chain-of-custody requires a proven process and independent verification. Situations like the "Switch-a-Roo" and the "Déjà Vu" show us that even diligent organizations are susceptible to mischievous insiders and irresponsible vendors.

By far, insider crimes are the biggest threat. Crimes committed by insiders often go undetected. When a loss is detected, an insider can often escape responsibility by denying any knowledge. If caught red-handed, insiders tend to dismiss the importance and downplay the risk. An excellent example of such excuse-making is someone we refer to as "Ms. Robin Hood."

Excuses, Excuses, Excuses

During a disposal project for a large bank, a chain-of-custody audit revealed three computers were untracked. An IT director (a.k.a. "Ms. Robin Hood") was suspected of taking them. When first questioned about the missing systems, she denied any knowledge. Then she blamed the disposal vendor for taking an inaccurate inventory. Then she accused a truck driver of stealing the systems en route to the recycling facility. Ultimately, she admitted to her involvement when confronted with evidence. As a 12-year veteran of the bank, she explained how she would never intentionally harm the bank. She further explained how her daughter's elementary school really needed the computers. She believed that there was no risk to the bank because she made certain the hard drives were wiped. Furthermore, since the bank had historically donated computers, her actions were consistent with the bank's long-standing policy.

The Ms. Robin Hood situation is an example of the common excuses we hear insiders use to justify ITAD theft. "What is the big deal?" excuses typically fall into the following categories:

- Entitlement – "In the past, the company gave us old computers."

- Environment – “It is better the old computers get reused rather than dispose of them.”
- Harmless – “There wasn’t any important data on the drive.”
- Victimless – “The computers were going to be recycled anyway.”

Tolerating these types of excuses is essentially turning a blind-eye to employee theft.

In Conclusion

At some point, every organization must confront challenges associated with IT asset disposal. Of course, it is imperative to work with qualified disposal vendors. However, it is even more important to recognize that while you can outsource recycling, but you cannot outsource responsibility. If an asset is found in the wrong place or found with data, your organization pays the price. Organizations must adopt a formal ITAD policy to minimize conflicts-of-interest and document accountability. For an ITAD policy to be effective, chain-of-custody controls must be established and should be monitored by an independent 3rd party.

Photo Credit