ITAD Chain of Custody

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

What has more value, an armored bank truck, or a van delivering old computers to a disposal vendor? An armored truck may hold millions of dollars. An old computer on the other hand, if lost, may mean millions in liability.

Every old computer does not need to be transported in an armored vehicle. However, the process of tracking of old computers certainly does deserve serious attention.

Experts tell us that “chain-of-custody” is critical for effective IT asset disposal (ITAD) but chain-of-custody is really just the sign off or evidence that effective, well thought through processes have been implemented. Serious thought and attention must go into the creation of those processes to ensure that they are as foolproof as possible, as the lack of rigorous and proven processes to support chain-of-custody can produce massive liability.

What Is Chain-of-Custody Really Worth?

Chain-of-custody is unimpeachable evidence that an ITAD vendor has physical possession of a particular asset. This evidence is the foundation for indemnification. Suppose an asset is found in a dump, or sold on eBay with data. Chain-of-custody will enable you to hold the disposal vendor accountable.

Logic dictates that the value of chain-of-custody depends on the likelihood of a situation happening, the level of compensation to which you are entitled, and the probability of collecting damages. So, how valuable is this indemnification? Try to think of a time that a disposal vendor has been held accountable for a data breach or illegal dumping… Having trouble thinking of any examples? You’re not alone.

Indemnification is about as valuable as an insurance policy that never paid out. Excluding the remote possibility that disposal vendors don’t make mistakes, the absence of any

memorable examples of vendor accountability illustrates the dubious “value” of chain-of-custody.

Value of Process

Of course, many organizations continue to pay a heavy price when their equipment is found in the wrong place or found with data. An effective chain-of-custody process reduces the chance of this situation happening to your organization in two ways. First, an effective process produces superior chain-of-custody evidence. Second, and far more importantly, it reduces the biggest risk. An effective chain-of-custody process deters employee theft, the biggest threat to any ITAD program.
An effective process of establishing chain-of-custody requires a robust reconciliation of inventories – a comprehensive comparison of what was disposed to what a vendor reports receiving. The comparison must be unbiased and independently verified.

When done systematically, the process will produce reliable chain-of-custody evidence for most assets. Conversely, and much more importantly, the process will reveal any asset for which chain-of-custody is lacking. Said differently, an effective process uncovers precisely what is missing!

Deterrence Is Key

When an employee knows something will be missed, they are less likely to steal it. Indemnification sounds significant, but theft deterrence is far more valuable.

To maximize value (i.e. minimize risk of insider computer theft), the process must be promoted. A clear corporate policy must be communicated and understood. The chain-of-custody outcomes must be objectively measured and reviewed. For a policy of deterrence to be effective, employees must be aware of the consequences for non-compliance. Non-compliance cannot be tolerated or excused. Violations must be exposed and punished in order to serve as an example.

Chain-of-custody is necessary regardless of any data destruction policy. Insiders intent on taking retired computers won’t wait until the hard drives are sanitized. Best practice is to secure / destroy data before any move. This is not always practical, so disposal vendors must also perform data destruction.

What’s Missing?

Typically, senior management receives heavily distorted information about ITAD, if any. This is no surprise since organizations often shoot the messenger. Employees tend to report self-serving interpretations, especially when facts could make them look bad.

To know if something slipped through the cracks, you must reconcile your inventory against your ITAD partner's, a tedious and time-consuming task. You need the data from your in house team of what was disposed and the data from your disposal vendor of what they received. Then you need to ensure that all the assets are the same on each list. You may be dealing with a scanned receipt note on one side and an excel spreadsheet on the other. There may have been missing asset labels, complicated serial numbers, hand written (and hence error prone) data, all of which adds time to the reconciliation process. So consider utilizing a vendor to do it for you. Leveraging a third-party to reconcile not only saves time, it ensures that the results are objective.

Tracking chain-of-custody by serial number (i.e. matching) is only about 75% effective. The most rigorous ITAD programs can track 95-98% of assets by matching serial numbers. Organizations that use disposal tags in conjunction with serial numbers can track 99-100% of assets. Disposal tags dramatically improve chain-of-custody evidence. Disposal tags also deter theft and expedite loss detection. When a loss is detected, timing is essential. You want to recover the asset quickly. Regardless, the issue must be resolved, not swept under the rug or hidden from management.

Losses happen. Untracked items are inevitable. Even the airline industry still mishandles 1-out-of-200 bags…despite bar-coded assets moving in a secure, closed-loop environment. The key is to control and reduce the risk. This requires process. The old adage applies; you can't manage what you can't measure.

Some organizations still believe there is no issue with ITAD chain-of-custody. They believe they have an unbroken chain-of-custody for all assets ever retired. Data show this is wishful thinking. If your organization falls into this camp, there are quick tests to verify this.

In Conclusion

Until you prove a disposal vendor has your equipment, you are responsible for it. Unless you prove it, your organization is legally exposed. If something is found in the wrong place, or found with data, your organization, not the disposal vendor, will unfortunately pay the price for the problems. Chain-of-custody, by itself, is about as helpful as a helmet in a motorcycle crash. An effective process that prevents a disaster from happening in the first place is far more effective.

Image Credit