Is your Inventory Collection automated? If Not, Why Not?

Steve Travis
Software Compliance Officer
Integrity Software Inc.

When was the last time your organization performed a comprehensive inventory of all the software and hardware assets that make up your company network environment? A few weeks ago? A few months ago? Maybe.. *never*?

With the nation in a recession, many industries are looking for ways to increase revenue. One area software manufacturers have found "new" revenue is by locating and fining "pirates". Software manufacturers (and/or organizations they form) are on the hunt for software "pirates" from which they can extract huge fines. They even go so far as to actively solicit current or ex-employees to "Turn In Your Boss"[1] and offer rewards of up to ***one million dollars***[2] for doing so. One organization, the Business Software Alliance or "BSA", has netted some sizable paychecks in the process.

"Criminals" or "Victims"?
In August of 2010, U.S. online car dealer "Autotrader.com" paid out almost a ***half-million dollars*** in fines to the BSA. In their press release[3], Autotrader said:

> "This audit brought to light the importance of having procedures in place to make sure all software purchases and licenses can be accounted for" - *Autotrader.com*

Autotrader.com isn't the only example of a company that has had to dip into the corporate coffers to get themselves off the hook. In October of 2010, Massachusetts-Based Health & Benefits Administrator "Health Plans, Inc." paid over a ***quarter-million dollars*** to settle it's bill for "pirated" software[4]. And they too now claim to have implemented a company-wide Software Asset Management (SAM) process as mentioned in their press release here:

> "The audit performed has permitted our organization to implement processes that will assure that software licensing issues do not resurface," - *Health Plans, Inc.*

These are just two very real example of what happens if you don't pay close attention to your inventory and compliance gets away from you. Paying close attention means knowing ***exactly*** what you've bought ***and*** reconciling that with what is discovered "in the wilds" of your network. Knowing this is paramount to deflecting (and in the worst case defending) your company from the ravages of "piracy" fines. So, if this is so very important, why are large companies (who should know better!) still getting fined[5]?

The "Not So Personal" Personal Computer

Some companies provide transportation to their employees in the form of cars, others provide company credit cards that can be used for business expenses. Most employees given such access understand that it comes with responsibility. Most wouldn't think of taking the company car hundreds of miles across country to visit relatives for the holidays, or using a company credit card to buy a new sofa for the living room of their house.

Yet, when it comes to the computer on their desk at work, many treat it as their ***personal property***. There is usually wide-spread ignorance that an A.U.P, or "Acceptable Use Policy" is in force and/or what it ***means***. Employees rarely give a thought to downloading and installing utilities from web sites, loading software to manage their personal music collections or setting up personal programs. All of these are examples of the prevailing perception that the computer on the desk is to be treated and operated no differently than the computer they have at home. Your best defense against these casual infringement risks is having a comprehensive inventory of "what's out there".

"So, lets get a Hardware/Software Inventory! How hard can it be?"
I have encountered management at companies that believed it would be a "good idea" to send their employees around with a clipboard to collect inventory of company software and hardware assets ***by hand***. They felt this should be a relatively "simple" task. My initial reaction was that this was a ***terrible*** idea!

However, we live in a world of numbers and so I thought it best to explore this concept and to see if my "gut reaction" was correct. So, I "did the math" using average (even conservative) numbers and this is what I found. To perform a manual inventory, you must complete the following steps:

- Spend ~60 seconds to Logon to the workstation
- Spend ~10 seconds to open the Control panel, open ADD-REMOVE programs and let it populate
- Spend ~10 seconds for the manual transcription of each item to clipboard/laptop

Based on inventories I've seen from networks all around the globe, it seems the average computer has about 75 items in the "Add/Remove Programs" list. So the formula for determining how long it takes to manually inventory a single machine is:

`60s+10s+(75x10s)=820s`

"820 seconds" works out to 13.6 minutes ***per machine***. That means a single technician can inventory about 4.4 machines per hour. Let's say that technician is paid US $25.00 per hour (that's a very conservative number here) that comes out to ***$5.68/per machine in labor alone!***

Now, if the data is gathered on a clipboard, then we need to add time (and associated dollar costs) to transcribe and keypunch the data into a spreadsheet or database (opportunities for errors here?). If the data is gathered on a laptop, someone must compile all the various text files and/or spreadsheets into a single report. This time (and again, associated cost) would be in addition to the $5.60/machine labor cost figured above.

Cheops' Law: Nothing ever gets done on schedule or within budget.
Of course, we're also operating under the assumption that all goes as planned (has that *ever* happened?) and there is ***no*** time consumed:

- Locating/identifying the workstation to be inventoried
- Moving from workstation to workstation
- Moving from floor to floor / department to department.
- Driving/walking from building to building / site to site.

It also assumes the machine is powered up and ready for logon ***and*** that the technician performing the inventory has a valid set of credentials that work on every machine. It does ***not*** take into consideration the amount of time the machine's regular user must ***stop work*** so the inventory can take place ("15 minutes down time per employee" = "how many lost dollars in productivity?") Again, add this cost to the base $5.60/machine price calculated above.

"Painting a Battleship"
Performing a ***manual*** inventory on workstations is much like painting a battleship – by the time you're done, its time to begin again. Subsequently, once the manual inventory is complete, the dollars invested have ***no ongoing value*** as the inventory is ***technically inaccurate*** as soon as a single software or hardware change is made to even ***one*** computer! In fact, it may even be obsolete before the manual inventory process is completed (e.g. a hot fix is applied during the time the inventory is being taken). This makes any inventory report more than 72 hours old suspect as to it's accuracy.

The inescapable conclusion we draw from the exercise is that a ***manual*** inventory is a non-starter. So, what about using an automated inventory collection tool? Many companies already have elaborate and/or expensive tools of this nature, yet they are not being used, which begs the question, ***why***?

The "No Win" Situation
Some IT managers are placed in a difficult position by the very tools that were purchased to *keep them* from getting into a difficult position! If the inventory collection tool is found to be "intrusive" or simply drags workstation performance to a crawl, then the users will "push back" against its installation and use. Those employees who ***want*** to work may be prevented from doing so and those employees looking for excuses ***not*** to work, now have a perfect scapegoat.

As a result, the managers of those employees will advocate delaying or even ***omitting*** inventory collection – in many cases taking the complaints "up the chain of command". This may lead to conflicting "mandates from above" i.e. 1) Inventory collection not "interfere" with the day to day operation of departments 2) The IT manager is responsible for making sure the company is in compliance!

Process, not Project!
One major misconception is that an inventory of hardware and software is a ***single event*** *or* "project" when, in actuality, it is an ongoing "process" – your overall SAM process. You need to do more than simply craft a procedure document, purchase a software inventory package and then plop all of it on a shelf and ignore it. You must perform ***regular*** inventories of hardware/software combined with regular reconciliations between **what you own** and **what you find** – then removing any infringing products ***immediately***.

Lastly, find an automated software inventory solution that is low-impact enough that it can be run without interfering with the end users, one that is simple enough to be installed, updated and operated without consuming significant amounts of IT staff time, and one that can act as a repository for all your purchase data. This way, you can reconcile your purchases with what's "in the wild" and become (and continue to be) compliant.

If designed correctly, implemented properly and exercised regularly, a SAM plan can save your company a lot of financial grief. OK, you have your assignment, now get on with it!

References:

1) http://www.itbusinessedge.com/cm/blogs/dunn/turn-in-your-boss-get-paid/?cs=37886
2) http://www.neowin.net/news/bsa-offers-1-million-reward-for-software-piracy-reports
3) http://www.bsa.org/country/News%20and%20Events/News%20Archives/en/2010/en-08242010-autotrader.aspx
4) http://www.tmcnet.com/usubmit/2010/10/17/5071984.htm
5) http://www.bsa.org/country/News%20and%20Events.aspx