

# Hardware Loss Epidemic

## New RFID Technology Provides Proven Solution and Even Automates the Inventory

Daily we watch with great interest the steady drum of news reports on intellectual property and personal privacy loss related to missing IT hardware, particularly laptops. The numbers are epidemic. Ninety three million personal confidential records were compromised last year. In a recently published study, eighty-one percent of respondents report that their organizations have experienced one or more lost or missing laptop computer containing sensitive or confidential business information in the past twelve month period. Laptop thefts in particular are cited in more than 90% of data breaches now reported. Asset mismanagement has far reaching implications these days. Conversely, asset control has become that much more paramount. But since portable assets such as laptops are supposed to leave the facility, how can you protect them?

A type of radio frequency identification (RFID) technology in the form of electronic property tags have been implemented by enterprise decision makers to stem the alarming trend of hardware and laptop “loss”, thievery or not. These tags are not the unreliable circuit-enabled bar codes used to count cartons of consumer packaged goods in the retail supply chain. They are powered tags enabling one to automatically identify, track, and protect laptops and all IT hardware for that matter in and around the enterprise.

Until recently, the perception had been that the impact of a stolen hardware was directly related to the replacement price of it such as with a laptop, which continues to drop. If discovered, corporate security personnel painstakingly took the loss report and filed it away. The asset was gone forever, so was the data. Back in 2000, a Rand Corporation study found the average value of the loss at over \$6,000 including intellectual property, etc. Other costs included the software, re-procurement time, set-up time, and any lease payments owed. Now however, the 2006 annual study from the Computer Security Institute and the FBI has found the average corporate loss is more than \$300,000 per year. And, the situation continues to get worse as all types of

commercial enterprises, educational institutions, and government entities are being affected.

Public awareness about all information security threats has grown rapidly. As most of the early public reports of theft were by government entities, the U.S. General Accounting Office was prompted by Congress to study the matter and found all nineteen domestic agencies were vulnerable. The April 2007 report noted, “Many of the data losses ... were the result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.”

However, only 43% of corporations report such thefts. Perhaps the news of stolen intellectual property would not be well received by shareholders...or customers? Perhaps the losses were not deemed “material” in relation to the total asset base of the corporation, and therefore mandatory for reporting under accounting disclosure rules in the financial statements? While Federal laws, such as Sarbanes Oxley continue to threaten the executive office with sanctions for the inability to control assets, the real pressure now comes from the states. Over thirty states now have what are called “notification” laws. Patterned after the California Security Breach Information Act (SB 1386), corporations are now required to notify EVERY INDIVIDUAL whose personal privacy data may have been compromised by a loss. The notification is required even if no personal loss is proven and even if no real asset “loss” occurred. The extremely costly notification rule applies if the asset is not in control. Now, the economics around preventing an asset loss are overwhelming and so is the need for a solution. Implementing an asset control system which is automated and tracks the assets 24/7 is the only way to address these losses which average up to 4% of the asset inventory per year.

Emphasis on automated asset tracking and control cannot mean discounting other data protection means. The number of virus attacks now roughly equals the number of laptop thefts in an organization. But, if corporate network security provisions such as

Hear  
**Axcess' CEO**

speak at the

**IATAM Conference**November 8th  
1:30 pm – 2:30 pm**BEYOND ASSET DISCOVERY  
to REAL TIME LOCATION****Visit us at  
booths 2 & 3**

## Automated Solutions for a Cognitive Enterprise

firewalls and virus software are deemed to be mandatory to protect the assets of the corporation including its intellectual property, certainly laptop thefts need to be addressed as well as a prospective breach in the corporate firewall.

Data mirroring, encryption, and software recovery tools can all be elements of the protection “cocktail”, but none are sufficient alone and none can prevent the asset from leaving with an unauthorized custodian. The profile of a laptop thief is very different than the common perception. Most people think the thefts happen by burglars at night or by cleaning personnel. So, one attempt has been to cable them to the desk. The FBI’s statistics show that 75% of the thefts are perpetrated by fellow employees or by the employees themselves. Some companies have tried to implement mandatory manual checkout systems whereby a laptop is tagged with a card similar to an access control “proximity” card. The employee is told to hold the laptop 18” proximate to the reader so it can be checked out. This is not a great plan unless you expect the thieves to be honest. The protection system must allow authorized assets to leave with their authorized custodians.

The solution requires what the physical security industry calls “automatic identification and protection”. One needs the flexibility to move about

a facility with your authorized laptop, or even leave the facility with your authorized laptop without security unreasonably impacting you or being “intrusive”. Radio frequency identification systems (or, RFID) offer this option, but it’s important to realize that only the new powered tagging solutions, called “active RFID” have the tag read-rate reliability to automatically ID, count, track, and protect assets.

“Active” RFID tags have embedded batteries to enable the tag to transmit autonomously, either by beaconing or by being automatically activated at a doorway or virtual “control point”. This means that assets can be tracked, automatically identified, and therefore, protected. With an active RFID tag, the laptop is tagged with a tamper proof, self-destructing tag, which is automatically identified as it moves throughout the facility and when it approaches a doorway. If an unauthorized hardware asset leaves, alarms sound. Electronic alert messages are sent making the system truly exception-based. In some companies, the doors lock so the computer can’t be removed. And, the system is very flexible. The owner or authorized “custodian” can have a complementary personnel tag so the system automatically identifies both custodian and computer, linking them to let them pass. Even in high volume entranceways that use turnstiles, the owner and



computer are automatically and “non-invasively” identified and authorized to leave. In the security industry this is called “hands-free” access control and asset protection. It’s the only system that addresses the necessary security, flexibility, and affordability.

The active RFID system can be easily overlaid with an existing door control system. Or, it can be installed as a new system. Ironically, the system uses the corporate network backbone to transmit the tag reads for processing. (“I.T.” protects “I.T.” in this scenario.) The average amortized cost is a paltry \$1.00 each per month (assuming a 36 month asset life).

If not addressed, we now know a very, very valuable laptop will be stolen from the corporation which will markedly impact its future if only economically. Certainly, if firewalls and virus software are standard issue for defending these attacks and for satisfying management that everything “foreseeable” (a security liability catch phrase) is being taken to protect corporate assets, an equal menace such as laptop theft has to be addressed with equal vigor. Hardware loss, particularly in the form of laptops is now a foreseeable threat. So, if the economics of laptop loss haven’t gotten your attention yet, the liability ascribed to it should.

Recognizing that management does not like to commit capital solely to hold off a prospective liability, the bonus in this solution is that it supports

real time automated inventory counts. IT organizations spend money daily finding and counting IT assets only to have the information obsolete the moment it’s completed. Physical inventories along with other snapshot “asset discovery tools” are woefully inadequate in supporting asset reconciliations with IT’s database repository of assets. Since the RFID system keeps a running tally of items and their locations, augmented by precise location updates as assets move, the RFID system offers a real time automated tool for up to date inventory information. That offsets the recurring cost of physical inventories and other snapshot discovery tools giving the RFID system utility to the IT department daily.

In summary, the losses are foreseeable and we know where they come from so we know we have to take action. We know the solution must prevent unauthorized assets from leaving the premises. We know it requires an asset to custodial assignment and detection capability to enable mobility yet accountability. We know the magnitude of the problem requires an around the clock, automated electronic labor-free solution. And, we can solve the asset protection problem while gaining an automated inventory system guaranteed to save money. Fortunately, we know a solution exists in “active” RFID.

*Allan Griebenow  
CEO of Axxess International Inc.*

## **IAITAM would like to thank the following Provider Members for their support of IAITAM and the IT Asset Management Community**

- |   |                                       |                            |
|---|---------------------------------------|----------------------------|
| <b>360 Incorporated</b>                   | <b>Animus Solutions, Inc.</b>         |                            |
| <b>Asset Management International LLC</b> | <b>Avery Island Technologies, LLC</b> |                            |
| <b>AXCESS International Inc.</b>          | <b>BMC</b>                            |                            |
| <b>CA, Inc.</b>                           | <b>Centennial Software Limited</b>    |                            |
| <b>e-Innovative Services Group, LLC</b>   | <b>EPC, Inc.</b>                      |                            |
| <b>Eracent, Inc.</b>                      | <b>Express Metrix</b>                 |                            |
| <b>Hewlett-Packard Company</b>            | <b>IntelliDyne</b>                    | <b>Intechra, LLC</b>       |
| <b>Lifecycle Partners LLC</b>             | <b>ManageSoft Corporation</b>         | <b>Minerva Enterprises</b> |
| <b>Miro Consulting</b>                    | <b>Netaphor Software, Inc.</b>        |                            |
| <b>NetSupport, Inc.</b>                   | <b>Novell, Inc.</b>                   | <b>PlanITROI, Inc.</b>     |
| <b>Regency Technologies</b>               | <b>Redemtech, Inc.</b>                |                            |
| <b>Sassafras Software Inc.</b>            | <b>Scalable Software</b>              |                            |
| <b>Soft-Aid</b>                           | <b>Spectrum Training Brokers</b>      |                            |
| <b>Software Success Partners</b>          | <b>Sunflower Systems</b>              |                            |
| <b>SWident LLC</b>                        | <b>United Recycling</b>               | <b>USU AG</b>              |

