Vector

IT STRATEGY WHITE PAPERS

RFID: Building a bridge for Asset Management and Asset Security

Colin Bartram

In today's justifiable climate of concern over asset and data losses, money could be spent reactively on asset and data security solutions. The pressure for action is particularly powerful for bodies that are publicly accountable. But at Vector we believe that diligence in addressing risk can and should be accompanied with effort to achieve broader benefit from the spending of taxpayer's or shareholder's money.

The central proposition of this paper is that RFID and other location technologies can serve multiple purposes. IT innovators can use a Locator technology to form a bridge between the needs and interests of desktop management and those of asset and data security.

Organizations should strive to integrate location information into their IT Asset Management Database (and/or their CMDB) and exploit the data in their Service, Change, Event, Configuration and Asset Management Processes. The physical security aspects of RFID in particular can help create this bridge, if implemented optimally.

By now we have all seen the alarming statistics about theft and loss of mobile IT assets and the even more serious issue of the consequential exposure of sensitive personal and corporate information. To make sure we don't lose sight of the seriousness, we will list some recent examples, but they are kept brief and confined to the end of these notes.

Our main objective is to explore the opportunities organizations have to respond to today's security threats and enhance their IT asset management at the same time.

Bridging Desktop Management and Security

We have visited large and sophisticated network sites where the two departments, security and desktop management, were clearly highly competitive – fighting for money, kudos and anything else they could scrap over. Which came first – security or desktop management? Did security departments evolve because the systems and configurations being deployed by 'IT' were inherently full of holes? When the only way of removing volumes of confidential data was by packing reams of printouts into the briefcase night after night, what was the need for a security department? The problem of data theft has existed since floppy disks were invented, but a USB memory stick fits in the pocket more easily than a floppy disk ever did. Increasing numbers of people working in mobile mode make someone walking out of the office with a laptop a common occurrence.

Today the lid of the Pandora's box of asset and data security is well and truly opened and it's hard to see how it is going to be shut again any time soon. Dealing with the evil spirits flying out of the box is largely a challenge for those charged with security. It is easy to say that the lid should never have been taken off, but could it ever have been kept on?

- How could we prevent data being written to removable – even just 'movable' – media?
  - Unless totally server based, with thin clients, no local data storage on any form of device, any ports blocked, and perimeter and network access management checking any system that connects to the network.
- Uncontrolled movement of media
  - Tracking of every media device, prevention of an 'unauthorized' media device being connected in the first place.
- Data movement without media - emailed to anyone, anywhere
  - Very strict email and content regulation – but how practical is it to distinguish a legitimate spreadsheet from a non-legitimate package of data.

One thing is certain: minimizing the risk to the organization requires the two departments – Security and Desktop Management - to talk. They already do, as necessitated by day-to-day operations, because Security needs desktop management to deploy security products and maintain their configuration, but cooperation could be a lot stronger and a lot more strategic.

The introduction of a locator technology can be the catalyst for more strategic cooperation. Without exception, the situations into which Vector has introduced RFID through one of its industry partnerships have been security driven. Expenditure is justified in part on the basis of the horrendous consequences of confidential data loss, and also on a more straightforward assessment of the reduction in the total costs of replacing lost assets. (Gartner assessed in September 2004 that a single mislaid laptop can cost a company more than $6,000 for hardware, software, user downtime and restoring data – assuming it was backed up in the first place.) However, when the concept of current asset location, and location history, is presented to those responsible for delivering the Change, Service, Incident and Configuration Management processes, the adoption is usually immediate. Let's look next at why that is.

ITIL – the role for Location Information

If for the moment we can presume that the reader is already convinced of the nightmare of physical assets and data on the loose, we can look in parallel at the idea that Location information can have wider application and value in overall management and exploitation of IT assets.

Many organizations handle IT assets separately from the management of 'Fixed Assets'. It's easy to point to the peculiar nature of software as the main reason for this, but many IT assets are so mobile they tend to physically disappear from view within hours of arriving in the organization – which makes inclusion in 'Fixed Assets' just a little ironic. So the term IT Asset Management has evolved for the collection of capabilities and functions needed to properly quantify, regulate and exploit IT hardware and software items in line with the needs of the business.

It is hard today to consider IT Asset Management without thinking about ITIL. As an instance, ITIL stresses the importance of Change Management procedures, and a good ITAM system will support those procedures through automatic change recognition, permitting reconciliation with the change process management systems. Change management is normally associated with changes of configuration, but if we accept that location is an important asset characteristic then current asset location is also required.

As an operational example of the importance of location information, if a Change or Configuration Management report indicates a laptop escaped a recent patch or AV update, but that system is not live on the network, you ideally need to know where it is so the deficiency can be fixed before it causes problems such as introducing a virus to the network.

Until the huge penalties of security breaches arrived on the scene to justify the introduction of location technology, managers had to do without this information.

In this context, the natural repository for the new location information is the ITAM (or the full CMDB) database, from where it can be extracted through the various Change, Service etc process management interfaces. Vector believes it makes sense to adopt the principle that the introduction of an asset location scheme should include the sharing of that data with the database(s) that underpin the organization's Service Management, Change Management, Incident Management, Configuration Management and Asset Management procedures. In short, Location matters in ITIL.

The Value of Location Information in IT Operations

It is a fact of life that in an era of increasing virtualization of resources, someone still has to deal with the lifecycle and maintenance of the real equipment on which those virtual resources are built. And some resources, such as notebooks and PDAs, will continue to exist in parallel to increasing virtualization. If you want to work in an airport lounge and access hosted applications and servers, you still need devices. At an operational level, in what ways can Location Technology contribute to IT management? Some examples –

- Europe at least has strict disposal laws for IT equipment, and it's no longer acceptable simply to write a PC off as fully depreciated and stop worrying about it. (The format for disposal information can be customized within Vector's IT Asset Management solution.) Finding systems that must be disposed of in accordance with regulations has become important.

- Compliance and Audit. The ability to locate highly mobile 'fixed assets' provides verification and support for personal accountability that physical assets are still within the organization. This is important to audit and compliance functions, and technologies such as Dual-Active RFID (see below) can provide data at vastly reduced cost compared with a traditional 'walk-round' refresh of bar-coded information.

- A suitable locator technology can provide information in real-time, contributing value into areas such as Service Management that are inherently real-time driven. Dual-Active RFID is particularly useful in this context.

RFID and the Security Challenge

Immediately we must recognize that locator technology is not a panacea, not a new lock that's going to close the lid on Pandora's box. But it is a significant addition to an arsenal that today includes lockdown technologies, data encryption, port monitoring that detects, validates, and blocks the transfer of data to devices such as USB drives and memory, network perimeter management, content analysis and others. But, frankly, these sophisticated techniques are all fairly useless when someone can walk out with a laptop under their arm.

So, while a determined and savvy internal thief with access to data will be hard to thwart, a key point to take on board is that the current spate of data loss disasters has stemmed not from industrial espionage, but from simple human and organizational errors. This is where a location technology such as RFID can come to something of a rescue by providing information on the location and movement of tagged assets. RFID is probably the most appropriate technology today, as it provides the following unique mix of characteristics:

Intelligence: RFID tags can contain considerable quantities of data and can be re-written.
Real-time: Tag movement past a sensor station is captured in real-time.
Accuracy and Resilience: RFID tags are less susceptible to damage and corruption than most bar code implementations.
Ease of Installation: Sensor stations are simple to install and connect, in particular for systems using powered – 'Active' tag technology.
System Integration: Location data can normally be exported from the RFID system.

In a recent report on RFID use in US Government by GCN Research, in cooperation with the Industry Advisory Council's RFID Committee, it was found that among respondents, 63% percent expected to see increased security, 50% to see increased asset visibility, 39% were looking for increased speed of operation, 37% for increased data integrity, 36% were expecting reduced costs of operations and 35% reduced cost of inventory. Clearly, multiple benefits were targeted.

The technology lends itself to obvious additions to just recording passage of an asset past a sensor. Firstly, directional information. As well as detecting that a 'protected' machine has been detected at an exit from a 'protected' zone, by using two suitably positioned sensor stations it is possible to record the direction of the transition. Second, associations of tagged items. For example, in organizations which have adopted tag-based access control for personnel (a rather particular 'item'), it is not difficult to define associations of assets and either groups or individuals approved to be carrying that asset, so that alerts can be further refined to identify when a machine is being taken out by someone who does not have authority to do so – such as a visitor bearing a visitor status tag. (Examples of theft by phoney visitors are quoted at the end of these notes.)

RFID vendor Web sites provide many examples and case studies of applications, but before leaving this area, we should just clarify the difference between Active and Passive tag technologies.

Passive RFID systems use tags that are not powered, but have induction loops which generate power when passing close enough to a sensor point. That makes them suitable for protecting retail goods. The tags can be very small. Active tags have embedded batteries, and the tags can actively transmit either in a beacon mode or when triggered by passing a sensor point – typically a doorway. This combination enables location to be determined both by reference to the last detected transition from Zone X into Zone Y, but also by regular confirmation of presence in Zone Y.

Asset and Data Security: the Nightmare

Recent examples, and broader survey information, include –

- A comprehensive study by the Computer Security Institute and the FBI estimates the financial impact of the average laptop theft at over $48,000.
- Far too many companies have no record of laptop serial numbers, making recovery near impossible even if police retrieve a haul of stolen machines. (Serial number collection is an absolute must-have for a desktop inventory tool!)
- A laptop containing Gulf War planning information was stolen from the trunk of a car of a UK Ministry of Defence official.
- The Chateau office building in Woodland Hills LA was raided in April 2009 and PCs and laptops taken from over 50 companies. Some of the systems included tax information, credit card information and legal documents.
- Bord Gáis Energy reported that a burglary took place on Friday, June 5th 2009 in one of its Dublin offices. During this incident four laptops were stolen, one of which contained customer information and bank details for 75,000 Bord Gáis Energy electricity customers.

When a laptop is lost or stolen, the value attached to confidential data often far outweighs the value of the lost device. The data may have no inherent value but its confidentiality is paramount. In the last two years, the main concern regarding loss of customer information has moved from the potential for industrial espionage to the potential for identity theft. The cost of informing every individual whose confidentiality has been compromized, and the risk of class action suit from those involved, makes a $1,000 laptop containing identity information for 100,000 individuals simply a nightmare.

In today's climate of personal accountability for the protection of corporate and personal information, can any CIOs ignore the significant operational advantages and preventative benefits that can be achieved from the introduction of RFID location technology and its integration into the rest of infrastructure management?

Author: Colin Bartram is VP Technology with Vector Networks Technology Group. He has been involved in the evolution of IT Asset Management since its inception in the 1980s, holding positions primarily in marketing and product management. Colin is based in the UK and can be reached at cbartram@vector-networks.com.

Information on Vector Networks' IT Asset Management, PC Configuraiton Management, Help Desk and Issue Tracking solutions can be found at www.vector-networks.com.