

AXCESS

**RFID as Mandatory Protection  
for Laptops, Intellectual  
Property, and.....Executives**

**White  
paper**



## **Table of Contents**

|              |  |          |
|--------------|--|----------|
| <b>1.1</b>   | <b>Introduction</b>  | <b>2</b> |
| <b>1.2</b>   | <b>Concerns Regarding Laptop Theft and Loss</b>                | <b>2</b> |
| <b>1.2.1</b> | <b>The Actual Cost of Laptop Theft and Loss</b>                | <b>2</b> |
| <b>1.2.2</b> | <b>Public Awareness</b>  | <b>2</b> |
| <b>1.3</b>   | <b>Forseeable Threats Regarding Laptop Theft and Loss</b>      | <b>3</b> |
| <b>1.3.1</b> | <b>Mandated Control Over Laptops and Intellectual Property</b> | <b>4</b> |
| <b>1.4</b>   | <b>Profile of Laptop Theft and Loss</b>                        | <b>4</b> |
| <b>1.5</b>   | <b>Ineffective Preventive Methods</b>                          | <b>5</b> |
| <b>1.6</b>   | <b>Automatic Identification and Protection</b>                 | <b>5</b> |
| <b>1.7</b>   | <b>The Active RFID Solution</b>                                | <b>5</b> |
| <b>1.7.1</b> | <b>Active RFID Flexibility</b>                                 | <b>6</b> |
| <b>1.7.2</b> | <b>Highlights of the Active RFID System</b>                    | <b>6</b> |
| <b>1.8</b>   | <b>In Closing</b>  | <b>7</b> |
| <b>1.9</b>   | <b>About the Author</b>  | <b>7</b> |

## **1.1 Introduction**

Laptop thefts and intellectual property losses are rarely made public. We used to watch with great interest the statistics on laptop theft published each year by computer insurer Safeware Inc. Even as the statistic topped a whopping 620,000 laptop thefts in 2002, few people voiced concern. Recent data shows the value of the intellectual property assets lost with those thefts has grown rapidly, threatening to ignite shareholder cries of poor corporate asset management. This is also true for the loss of confidential data, particularly from financial industry firms. Asset mismanagement has far reaching implications these days.

Fortunately, one of the newest technologies for corporate security and supply chain efficiency now offers a solution, and that solution is now becoming mandatory. Radio frequency identification (RFID) technology has now been implemented successfully by enterprise and government IT executives to stem the alarming incidents of laptop thievery.

## **1.2 Concerns Regarding Laptop Theft and Loss**

### **1.2.1 The Actual Cost of Laptop Theft and Loss**

Until recently, a common misconception was that the impact of a stolen laptop was directly related to the replacement price of a laptop, which continues to drop as technology advances. The asset was lost, however another took its place at marginal cost. Then, in 2000 a Rand Corporation study found the average value of the loss at over \$6,000, which included intellectual property loss, software, procurement time, set up time, and any lease payments owed.

The results of the recent 2004 annual study from the Computer Security Institute and the FBI (entitled 2004 CSI/FBI Computer Crime and Security Survey) found the loss is more than \$48,000 on average per incident. Almost 50% of the 269 surveyed reported knowledge of laptops thefts. Laptop loss was the third most prevalent type of cybersecurity attack or misuse, behind viruses and insiders abusing network access.

### **1.2.2 Public Awareness**

Public awareness about these thefts has slowly grown over the years as several high profile occurrences have brought the issue forward. Secretary of State Madeline Albright's laptop was stolen from a State Department conference room and widely publicized years ago. Two DOD laptops were stolen from U.S. Central Command at MacDill Air Force Base in Florida. The Customs Department audit found it was losing 350 laptops per year. The Justice Department lost 400 while the IRS lost over 2,300. Losses reported from government agencies including the FBI itself average around one to four percent

of the total population of laptops per year. However, it was not until 42 laptops came up missing at Los Alamos National Laboratories last year that the executive office became threatened. Los Alamos contended there was no intellectual property on those laptops, however then one has to wonder what was being done with them. Arguably, that report was the trigger for putting the Los Alamos Lab's management contract with the U.C. Berkeley up for competitive bid.

However, now comes the real issue - corporations are unwilling to report cybersecurity incidents. In the CSI/FBI study, 48% of the respondents indicated they did not report such incidents, and virtually all the public reports of theft are by government entities. The two main reasons cited included a fear competitors would use the news to their advantage, and because the negative publicity would hurt their stock price and/or their image. The fact is, despite the lack of reporting the problem is real and potentially catastrophic. Within those companies actually reporting losses in the 2003 study, there was an average of two laptop thefts per company per year.

### **1.3 Foreseeable Threats Regarding Laptop Theft and Loss**

If not addressed, the potential exists for a very, very valuable laptop to be stolen from a corporation, which markedly impacts its future. Certainly, if firewall and virus software is standard issue for defending these attacks and for satisfying the shareholders 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.

"Foreseeability" is the measure of when management should have known enough to act to protect an asset from theft. Laptop theft is now a foreseeable threat. There are two ways the solution can be justified; the ROI makes sense and/or there is a mandate to address it. Both are here. The CSI/FBI study reports that 55% of organizations use some form of ROI to justify cybersecurity expenditures. The ROI here is straight forward. A given laptop has between a 1 and 4% probability of being lost. If we assume only a 1% probability and the average loss is \$48,000, the expected loss per laptop is \$480 (every year). Even if you assume the average capital cost of an RFID solution including tags, readers, and infrastructure is \$50 per laptop (overestimated), the payback period is 38 days. The real ROI is much greater as the laptop is vulnerable to theft every year it is in operation. You get the picture.

#### **1.3.1 Mandated Control Over Laptop and their Intellectual Property**

Now comes the mandate. No doubt spurred on by the recent reports of losses of personal confidential data related to identify theft, the New York Stock Exchange has now instituted a rule that all NYSE-listed company's "employees, officers and directors should maintain the confidentiality of information entrusted to them

by the company or its customers” (reference section 303A, paragraph 10). As reported in the May 23rd issue of the National Law Journal (Confidential Data, Mandatory Protection), the code requires “compliance standards and procedures that will facilitate the effective operation of the code”. Note that the rule goes beyond officers and directors and requires employees to comply. Further to the point of foreseeability, “rather than companies simply reacting to the theft of their confidential information, the NYSE governance rules require listed companies, prior to being victimized by a single theft, to take aggressive and proactive steps to protect their confidential information”.

The trend toward more mandates is clear. Under the Sarbanes-Oxley Act in section 404 and 302, the protection of corporate assets is the responsibility of the executive office where management is to establish and maintain “an adequate internal control structure and procedures for financial reporting”. What is the exposure of not protecting laptops if their loss substantially impacts the value of corporate assets? The courts require that reasonable steps be taken to protect information in order for that information to qualify as confidential information such as a trade secret in the event of a dispute.

#### **1.4 Profiles of Theft & Loss**

The profile of a laptop thief is also very different than the common perception. Most people think the thefts happen by burglars at night or by cleaning personnel. To combat such occurrences, early attempts centered on cabling laptops to the desks. However, the FBI’s statistics show that 75% of the thefts are perpetrated by fellow employees or by the employees themselves, hence the cables offered no protection as they simply get cut by an innocent looking coworker. Additionally, cables impact a laptop’s ability to be mobile as intended.

Major newspapers have been writing about laptop thefts in New York, Atlanta, and San Francisco, Stamford, and Boca Raton and identified a new threat; “Creepers”. Creepers are usually men dressed in business suits who, by virtue of their professional attire, looks, and demeanor are given entry by employees to access-controlled doors without proper credentials. They prey upon the trusting who want to help. Who hasn’t wanted to be let in through a locked door, even though you didn’t have a proper pass (or so the story goes)? Well, instead of stealing purses, Creepers have targeted laptops; more money, guaranteed value. It’s epidemic.

#### **1.5 Ineffective Preventative Methods**

A common misperception is that there is potential to retrieve a stolen laptop – simply embed software into the laptop to recover it when it’s stolen. The idea is that when the stolen computer eventually connects to the Internet, it will report to a secret monitoring web site and the suspect will be traced and caught.

However, this method simply doesn't work, as only 6% of stolen laptops are ever recovered. Even if you implant software to disable the laptop, you are likely to have lost the data forever, whether or not a thief can exploit it. Although, we all back up our laptop data every day, right?

To reduce the loss of laptops, some companies have tried to implement voluntary 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 and traced. Obviously, this is not a great plan unless you expect the thieves to be honest. The solution to the problem then is to make sure the laptop never leaves the building without the proper custodian.

### **1.6 Automatic Identification and Protection**

This financially and competitively costly problem 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 (RFID) systems offer this option, but it's important to realize there are different types of RFID with different levels of solutions. "Passive" RFID systems are suitable to protect CDs, leather jackets and other retail goods. "Hybrid" RFID tags are suitable for toll collection. "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 automatically identified, tracked, and therefore, protected.

### **1.7 The Active RFID Solution**

Battery powered, active RFID tags that are set up to activate at a pre-determined wake-up location such as a hallway or exit doorway provide the highest level of laptop theft protection. Asset passing through these virtual portals can be automatically assessed for their authority to move and with whom they are allowed to move. This is not possible with their passive RFID tag cousins. If a tagged asset passes through the invisible control point without authorization or without the proper custodian, an alert notification to appropriate authorities is immediately created. The alert can constitute an audible alarm or a series of electronic messages to the appropriate responders. This "real-time" alert generates an asset protection intervention opportunity not otherwise possible. RFID tag/asset movement reports can be quickly reviewed. Combining alerts with integrated recorded video clips of the incident helps recover lost assets, and identify physical or personnel security risks. With an active RFID tag, the laptop can be tagged with a tamper-proof feature, which when tripped automatically identifies the asset and location.

Authorized personnel can move an asset and automatically check out the computer without triggering an alarm. The owner or authorized “custodian” has a personnel tag or access card which is “functionally linked™” to the asset, so the system automatically identifies both owner 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.

### **1.7.1 Active RFID Flexibility**

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. (“IT” protects “IT” in this scenario.) The average amortized cost is a paltry \$1.50 each per month. The systems are available from well-known, respected companies like Honeywell, Tyco, Siemens, Johnson Controls, and manufacturers such as AXCESS International.

For convenience and for the perception of increased productivity, have we methodically let employees transfer the intellectual knowledge of the corporation to portable devices we can no longer control? Bingo. The 10th annual “Trends in Proprietary Information Loss Survey” informs us of where this is going. The study estimates proprietary information loss by the type of department in the corporation. Not surprisingly the most vulnerable was Research & Development at \$404,000 lost per incident. Financial data was not far behind.

### **1.7.2 Highlights of the Active RFID System**

RFID tagging using active tags means wherever the asset goes within and around the facility, the system can track it. This is true for laptops, file back-ups, and hard drives. Anything that is portable or that you don’t want to be moved (e.g. desktops and printers) can be tagged and protected. The most simple implementation protects the perimeter entry and exits. A simple electronic radio “wake-up” field is generated at the doorway which puts out a constant signal (132 KHz) with a signature correlating to the door. As the tagged asset approaches the door, the tag is activated as it “enters the field”, as it wakes up it records the activation signal’s ID and transmits it (up to 70 feet) to an unobtrusive receiver. The battery powered “active” tag is key to the reliability of the system as the power provided by the battery ensures the signal can be read. The tags can optionally come equipped with anti-tamper alarms as discussed. And, the system monitors the battery life of each tag, even though the battery usually lasts longer than the asset.

The system uses the standard TCP/IP network, either wired or wireless, to transmit the tag transaction to a database where the system software runs rules on it. Simplistically, if the asset is authorized to leave, the transaction is logged. If not, audio alarms, electronic messages and door locks can be triggered. A particularly useful feature is called “functional linkage” where the asset can be automatically and electronically linked to a person (or “custodian”). Multiple authorized persons can be dynamically authorized via the system, but whenever a person leaves with an asset, the system checks for proper custodianship. Either existing personnel badges or active RFID personnel badges can be used to check out an asset. Additional benefits include an electronic log of where assets are so they can be immediately located and inventoried. The system also includes a floor plan or quick and easy visualization of the location. Full visibility, full protection.

### **1.8 In Closing**

Whether justified by ROI or by mandate, the use of technology such as RFID tags to protect confidential information and intellectual property makes good corporate sense. For everyone involved including the public who is affected by such a loss, it’s a relief to know a solution is here now.

### **1.9 About the Author**

*Allan Griebenow is President and CEO of AXCESS International Inc. AXCESS International Inc. (OTCBB:AXSI), headquartered in greater Dallas, TX, provides Active RFID (radio frequency identification) for physical security and supply chain efficiencies. The battery-powered (active) RFID tags locate, identify, track, monitor, count, and protect people, assets, inventory, and vehicles. AXCESS’ Active RFID solutions are supported by its integrated network-based, streaming digital video (or IPTV) technology. Both patented technologies enable applications including: automatic “hands-free” personnel access control, automatic vehicle access control, automatic electronic asset management, sensor management, and network-based security surveillance. AXCESS is a portfolio company of Amphion Capital Partners LLC. Allan can be reached at 972-407-6080 or at [agriebenow@accessinc.com](mailto:agriebenow@accessinc.com).*

**AXCESS International**  
Corporate Headquarters  
3208 Commander Drive  
Carrollton, Texas 75006  
tel: 972.407.6080  
fax: 972.407.9085

**Internet**  
[www.accessinc.com](http://www.accessinc.com)

**Email**  
[marketing@accessinc.com](mailto:marketing@accessinc.com)

Copyright © 2005 AXCESS International

**Sales**  
800.588.6080  
(toll free in N.A.)  
fax: 972.818.6497

**Service and Support**  
800.577.6080  
(toll free in N.A.)  
fax: 972.818.6497

**Contact**  
Ben Donohue, VP Business Development