

**Computrace<sup>®</sup> Plus**  
**Computer Tracking and Loss**  
**Control Solution**

**White Paper**



Absolute® Software helps organizations overcome security risks and asset management challenges associated with remote, mobile and desktop computers. Over 2000 customers, including Fortune 1000 companies, small and medium size businesses, education and government organizations rely on these solutions to secure and manage their computer population. Founded in 1993 - with international partners in South Africa, Australia and the United Kingdom - Absolute employs over 80 people in its headquarters in Vancouver, BC, and sales offices throughout the U.S.

The Computrace® Technology Platform is the client/server architecture that delivers Absolute's computer security and asset management products as software services or as enterprise software. Thanks to the hands-free communication between the secure, patented Computrace Agent client and Monitoring Center server, Absolute's products are exceptionally easy to manage on all computers across the enterprise.

Absolute Software Corporation  
Suite 800  
111 Dunsmuir Street  
Vancouver, BC V6B 6A3

tel: 604.730.9851  
fax: 604.730.2621

1-800-220-0733  
[www.absolute.com](http://www.absolute.com)

© 2004 Absolute Software Corp. All rights reserved.

Absolute Software and Computrace are trademarks or registered trademarks of Absolute Software Corporation. Other product or company names are trademarks or registered trademarks of their respective owners.

<b>Problem Description .....</b>	<b>4</b>
<b>Computer Loss Rates in Corporations.....</b>	<b>4</b>
<b>Causes of Loss: Internal Loss, Internal Theft and External Theft.....</b>	<b>5</b>
1. Internal Loss.....	5
2. Internal Theft .....	5
3. External theft .....	6
<b>The ComputracePlus Computer Tracking and Loss Control Solution.....</b>	<b>6</b>
Track Computers in Real Time .....	6
Proactively Manage Leases.....	7
Identify Internal Theft Sources.....	7
Reduce Theft through Deterrence.....	7
Recovers Lost and Stolen computers .....	7
<b>Protect Corporate Data .....</b>	<b>8</b>
<b>Other Measures.....</b>	<b>8</b>
<b>Conclusion .....</b>	<b>8</b>

## Problem Description

*"The mobile PC is rapidly moving up the must-have list of organisations across the US, according to the latest study from Gartner. The firm pumped out its latest assessment of the PC marketplace and discovered that mobile PCs experienced comparatively exceptional growth."*

-The Register, "Notebooks jump, desktops slump", August 5, 2002.

While this trend is good news for manufactures of notebook computers, the mobilization of the workforce makes the task of asset tracking and management a much more complex task for IT administrators and physical security officers.

In this white paper we will first examine the major causes of computer loss and then explore how different strategies can be deployed to effectively deal with the issues at hand.

## Computer Loss Rates in Corporations

Determining the loss rates of computers in a typical organization is in itself a challenge. In the enterprise market, many organizations are unable to accurately track of their computers, let alone know why many are being lost. However, one objective source of information is computer leasing companies, who track with great accuracy the number of machines shipped at the start of a lease versus how many are returned at the end. When missing computing assets are tallied at the end of a two-year lease cycle, up to 20% (10% annualized loss) of the total population is not returned<sup>1</sup>. While this relates to computers in general, given the inherent mobility of laptops, the rate of loss with laptops is certain to be as large, and very likely greater.

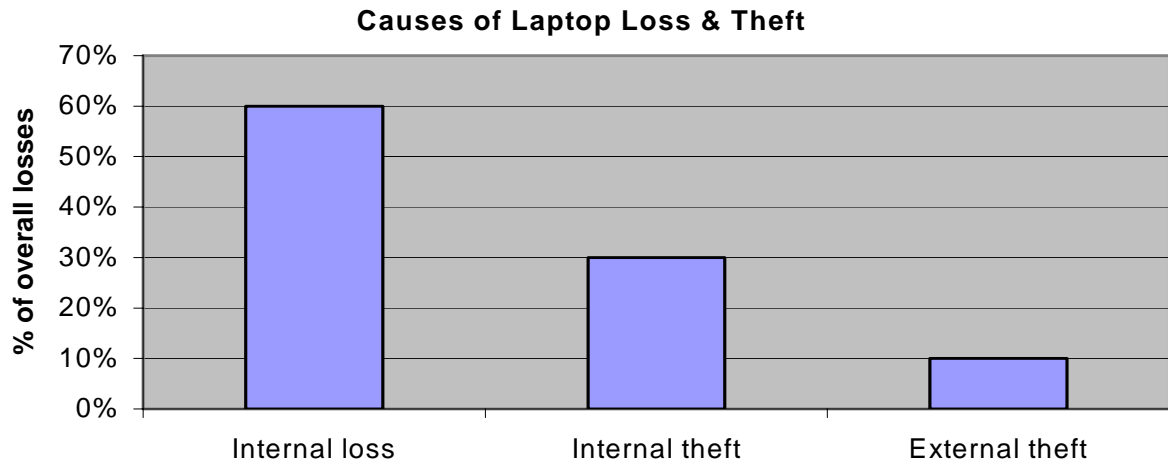
What then are the causes of loss? No single piece of data or research is available to answer this, however, the Internet provides a wealth of sources<sup>2</sup> that allow some general conclusions to be drawn. First, the loss of laptops due to theft is stated to be in the range of 3% to 5% per annum, with 4% being a representative consensus. When compared with the results on overall loss above, this means that loss from causes other than theft (i.e. internal loss) is greater than all sources of theft. Second, the same sources consistently state that internal theft is the leading source of theft. Some sources place this as high as 95%, however most place it at around 75%. Applying this to the previous data, the major causes of laptop loss are:

- Internal loss - approximately 60%
- Internal theft - approximately 30%
- External theft - approximately 10%

---

<sup>1</sup> Source for this information was data provided to Absolute by a major US computer leasing organization, based on over one hundred leases representing a total of 650,000 desktop and laptop systems.

<sup>2</sup> Sources include: *Business 2.0*, "Where the Hell Is My Laptop?", October 2, 2002 ([www.business2.com](http://www.business2.com)); *Computing SA*, "Increase in laptop theft cause for concern", 21 May 2001 ([www.computingsa.co.za](http://www.computingsa.co.za)); Kensington Europe Research, June 2001 ([www.microssaver.com](http://www.microssaver.com)); *Tech Republic*, "Survey responses show laptop theft is a serious problem", November 8, 2000 ([www.techrepublic.com](http://www.techrepublic.com)); *SC Magazine*, "Playing Hard to Get", October 1999 ([www.scmagazine.com](http://www.scmagazine.com)); FBI statistics 1997 & Safehouse Insurance, as quoted by Georgia Technology Authority ([www.gagat.com](http://www.gagat.com)).



While this information was not collected in a single independent market study specifically related to laptop security, its validity is strongly corroborated from feedback Absolute has received from numerous prospective and existing customers.

## Causes of Loss: Internal Loss, Internal Theft and External Theft

### 1. Internal Loss

Absolute's experience and discussions with customers and within the industry indicate that the largest cause of corporate computer loss is the routine drift of systems outside the central control processes of the organization. Computer drift includes all unreported loss and unreported theft. It also includes computers moving from employee to employee without record and systems that disappear when the processes that track them fail. The basic root cause of these losses is the fact that ownership and usage of machines are not tracked over their lifecycle.

### 2. Internal Theft

From coverage in the media, the general public might expect that smash and grab situations or thefts of opportunity to be the leading cause of laptop theft. As has been noted above, the boring truth is much less dramatic, but nevertheless potentially more damaging to the enterprise. Based on Absolute's extensive experience in the field, we are able to identify and rank the leading causes of internal loss, which in decreasing order of overall organizational impact are:

- The internal theft ring: This is an organized group of individuals operating within an organization who are coordinating the theft of corporate assets for criminal profit. This is very high impact, because computers, while of high-value, are typically only some of the assets being stolen.
- The downsized employee: The scenario here involves the person who refuses to return their assigned computer back to the corporation after being terminated or misinforms the corporation regarding the whereabouts of the machine. Absolute rates this as a high impact case as the stolen machine typically moves out of the organization with valuable proprietary or confidential information.

- The bad apple: This is similar to the theft ring, but involves a single individual stealing computers and possibly other assets. Again, the overall impact in stopping this individual is typically high.
- The disenfranchised employee: This person for self-appointed reasons decides he/she is somehow entitled to help themselves to company assets including computers.

### 3. External theft

External theft, the smallest category for loss, can also be broken down into several sub-classes, which are again ranked based on our experience across hundreds of case studies. These include:

#### a) Opportunistic theft

- Carelessness: In spite of the value of the device itself and the information stored on it, carelessness or inattention is the leading root cause of loss for external theft. One need go no further than daily newspapers to read stories of notebook computers stolen from airports (specifically at airport x-ray scanners), or machines left unattended for “just a moment” at conferences or in other public forums.
- Smash and grab: In the typical smash and grab the hapless owner has their notebook computer stolen from their vehicle or home.
- Facility theft by non-employees: This type of theft can range from thieves driving through a front window and stealing as many desktops or notebooks as they can carry in a two minute period, to thieves dressed as executives casually gathering up notebooks and leaving the premises virtually unnoticed.

#### b) Theft for Corporate Espionage

This is a somewhat rare but growing phenomenon whereby a specific user likely to have sensitive information on their computer is targeted for theft. This does not account for much theft but when it does occur the impact on the organization is potentially devastating. Executives with confidential financial information, internal strategy documents, source code, customer lists, scientific formulas, trade secrets, and other proprietary and conditional information are all potential victims.

## The ComputracePlus Computer Tracking and Loss Control Solution

### Track Computers in Real Time

Tackling internal loss, or machine drift, requires a proactive approach along with an effective and efficient tool that minimizes effort for the system administrator. In order to reduce loss, it is essential to record and monitor machine location and usage information on an ongoing basis. Obvious signs of machine drift include use by individuals other than the normal user or failure of the machine to be used in a reasonable duration.

Absolute's core competency is tracking computers in real time and providing this data to our customers in an easy-to-use web service format. With ComputracePlus the customers' database of computer assets is updated daily when users connect to the corporate LAN or Internet. The data is reported in numerous report formats for periodic review, but more valuable, critical data-points can be automatically monitored to generate email or pager alerts on out-of-bounds conditions. For example, an alert can be generated identifying assets that have not contacted the monitoring center in more than a set number of days. The reports and alerts also include information such as login name and email address to assist the administrator in contacting the last reported user.

## **Proactively Manage Leases**

With any leased computer, the IT administrator can normally state with confidence the name of the original user of the computer. The trick in managing the lease is knowing the name of the most recent or current user.

ComputracePlus is well suited to this task. Purpose-specific fields stored in Absolute's monitoring center track information such as lease-start and lease-end date. When used in conjunction with the monitoring center's alert mechanism, administrators can then be alerted at a user-defined interval before end of lease that a machine's lease is about to expire. Again, information captured throughout the lease and provided in the alert allows the administrator to determine who is the current or last user of the machine.

## **Identify Internal Theft Sources**

With every computer recovery comes investigative data that may provide clues as to who the perpetrator is. With the assistance of this data many customers have recognized Absolute for solving spectacular incidents of crime. For example, one recovery led to closing 42 documented computer theft cases. Another recovery led to the break-up of a multi-million dollar theft-ring that operated without check for over three years. Another recovery involved identifying a recently downsized employee who had stolen data worth, according to the customer, over \$2.5 million dollars. Identifying a theft ring or individual theft source often has a tremendous impact on *preventing future internal theft*.

## **Reduce Theft through Deterrence**

We all know that prevention is better than a cure! With successes and testimonials such as those just described, it's hardly surprising that Absolute's ComputracePlus customers experience a theft rate well below the industry forecast. Absolute's customers on average experience a computer loss rate of approximately 0.5 %, versus the industry forecast of 3% to 5%<sup>3</sup>. The difference is attributed to the "Computrace Deterrence Effect", which has proven extremely effective in minimizing internal theft, the largest contributor to corporate computer theft.

## **Recovers Lost and Stolen computers**

ComputracePlus has the added value of being able to track and, if reported missing, recover computers in North America and elsewhere. Using a combination of Internet and telephony call tracing, ComputracePlus reliably identifies the whereabouts of the missing systems. Then using this information, Absolute works with law enforcement to recover stolen computers. Absolute's five-year track record in this area is second to none. The computer theft recovery process reinforces the deterrence effect and *helps recover assets due to theft or accidental loss*.

---

<sup>3</sup> Ibid

## Protect Corporate Data

ComputracePlus provides peace-of-mind in one other respect. In the event that a machine is stolen, or because its profile of usage falls outside corporate security policies, ComputracePlus has the ability to delete all data on a specific machine. To take advantage of this capability, an authorized customer representative contacts Absolute Software and follows a protocol to determine the authenticity of their request. Once this has been established, Absolute sets a flag that will activate systematic deletion of data the next time the targeted machine contacts the monitoring center. The request for data deletion can either be for user files only, or a more exhaustive process that will eventually render the system unusable.

## Other Measures

In addition to using ComputracePlus to prevent loss and deter theft, a number of other measures should be adopted to achieve a holistic approach to machine and data loss. These include:

- **User training:** Simple user awareness training is an essential part of any security program. This should include precautionary measures to apply both inside the office as well as while on the road.
- **Physical constraints:** Again, simplicity is the key to success. While not foolproof, use of security cables are an obvious and easy way to reduce unnecessary loss.
- **File encryption:** In cases where the value of the data is of concern, file encryption is highly recommended. Many products exist in this space, though changes in user work habits have often prevented their effective implementation.

## Conclusion

The critical success factors to reduce computer loss include:

- 1. Track computers in Real Time** – Computer tracking must be a proactive process used to automatically and continuously monitor the status of computer assets. It must automatically alert administrators to systems that begin to drift.
- 2. Proactively Manage Leases** – Data identifying the current user of the computer must be available on a continuous basis to ensure that leased computers can be located and returned in a timely manner.
- 3. Identify the Source of Internal Theft** – Data must be on hand to identify sources of internal theft, thereby enabling corrective and preventive actions to be taken. Internal successes then readily lead to building a significant theft deterrent.
- 4. Recover Lost and Stolen computers** – First, information on the physical location of the device is required. Then, processes and relationships must exist to locate and recover lost and stolen computers with the collaboration of law enforcement authorities.

ComputracePlus is an effective tool that addresses these factors, thereby enabling organizations to efficiently and systematically deal with internal loss, internal theft and external theft. These strategies are rapidly becoming more relevant in an environment that is becoming increasingly mobile and therefore increasingly susceptible to uncontrolled loss.