



Compliance. Protection. Recovery. A Layered Approach to Laptop Security

EMEA Whitepaper

October 2007

Absolute®Software

Table of Contents

2	Executive Summary
3	The Computer Security & Tracking Challenge
5	Power of Mobility
6	Encryption is Necessary but Insufficient
7	Compliance
8	Protection
10	Recovery
12	Summary
13	Additional Information

Laptop Theft Affects Everyone

Today's computing assets contain more sensitive and valuable information than ever before – making each computer a potential liability without proper protection. Governments, businesses and educational institutions risk costly legal battles and public relations nightmares when even one laptop goes missing.

Laptop theft is staggering. Safeware the Insurance Agency claims that over 600,000 laptops are stolen annually, resulting in an estimated £2.6 billion loss of propriety information.¹

While encrypting data on laptop computers helps promote laptop security, it is important to stress that encrypted data is not necessarily secure data. Corporate computer crime can often be the result of 'inside jobs' and employees committing such crimes usually have access to the necessary passwords and encryption keys, therefore, encryption may not be effective in all incidents.

Single point security solutions cannot adequately protect an organisation from all points of attack. Instead, a multifaceted or layered approach to mobile security and data protection is required, comprising "CPR": Compliance, Protection and Recovery:

- **Compliance** – Complying with all applicable mobile data protection laws and regulations with an easily accessible audit trail
- **Protection** – Protecting data on mobile computers includes encryption, strong authentication and the ability to remotely delete sensitive data on stolen devices
- **Recovery** – Recovering lost or stolen devices returns them to the control of the organisation and facilitates prosecution

By adopting the CPR approach to laptop security, organisations can minimise the impact of computer theft while complying with privacy regulations. Computrace®One™ helps ensure regulatory compliance by protecting data, tracking hardware and users, providing auditing capabilities and acting as an historical record of computer assets and their use. The data delete function can also be used to remotely wipe stolen computers using a NATO approved algorithm.

¹ Ken Bates and Chelle Pell, "Keeping You and Your Property Safe: A Guide to Safety and Security on the Stanford Campus," Stanford University Department of Public Safety, http://ora.stanford.edu/supporting_files/keep_safe.ppt.

Security breaches can be inconvenient and publicly embarrassing for any organisation. A missing computer can result in compliance and data protection issues ranging from the misuse of confidential information to threats of national security.

Laptop usage continues to rise – in some cases, administrators have thousands of remote PCs to manage. Sensitive or even classified information residing on laptops increases with greater mobility among employees. Even those organisations that have been early adopters of technology have been slow to find and implement effective asset tracking methodologies that can help them keep pace with growing security threats while protecting critical operations and PC assets.

IT professionals must be able to accurately track their computers, know who is using them and what is installed on them, and be able to prove that actions taken to secure computers remain deployed and intact until a missing machine can be located. Security audits and evaluations of IT systems are on the rise. Assets that cannot be effectively inventoried and monitored at all times – not just once a year – can undermine even the best security strategies, exposing an entire organisation.

A Changing IT Landscape

Several factors have dictated the need for a more robust approach to computer security policies in recent years, including:

- Increased use and theft of laptop computers
- Intense focus on data privacy and data security concerns
- Regulatory compliance mandated by recent legislation

Keeping pace with the changing IT landscape requires a layered approach comprised of products, policies and procedures working together to provide IT professionals everywhere – in the public sector, private sector or education – with the broadest security blanket available.

Stolen Laptop a Stark Reminder of Identity Theft Threat for 11 Million People

Nationwide Building Society was fined £980,000 in February 2007 by the Financial Services Agency (FSA) following the theft of an employee's laptop. The laptop contained the confidential information of over 11 million customers.

- Feb. 2007 BBC News

In May 2007 26,000 Marks and Spencer staff were at risk of identity theft when an employee's laptop was stolen. Salary details, addresses, dates of birth, national insurance and phone numbers were on the machine which was stolen from a printing firm. Two days after the theft M&S wrote to all the staff, whose names and details were on the laptop, warning them they were at risk and reassuring them that their account and card details had not been compromised. M&S offered free credit checks to the people affected. *May 2007 – BBC News*

The Layered Approach

Single point solutions – such as encryption alone – are no longer enough to adequately protect an enterprise from all points of attack. IT departments getting by with minimal compliance protection expose themselves to unnecessary risks and potential liability. To reduce exposure and ensure full compliance with government regulations, a multifaceted or layered approach to mobile security is recommended, comprising Compliance, Protection and Recovery. Some of the steps involved in CPR include:

Real-Time Asset Tracking – The ability to track in real-time every mobile asset connected to an internal network or the Internet, and provide dynamic reporting which helps with regulatory compliance.

Data Encryption – The ability to protect mobile data from unauthorised parties.

Remote Data Delete – The ability to remotely delete sensitive information from a lost or stolen mobile device through centrally issued commands.

Audit Logs – The ability to produce defensible records that can verify what sensitive information was lost or stolen, its encryption status and the last known location of the mobile asset.

Theft Recovery – The ability to locate and recover a lost or stolen laptop over the Internet to assist law enforcement in retrieving the stolen hardware.

Portability at the Cost of Vulnerability

The power of mobility afforded by laptop computers has meant that tremendous flexibility and productivity has become the standard of business for most information workers. But, for IT executives and managers, mobility brings new challenges in the areas of data security and information privacy. With the proliferation of laptop computers these challenges will only intensify.

- Organisations continue to issue more laptop computers to employees as replacements for their desktop computers. By May 2005, laptops accounted for 53.3% of the total PC retail market.²
- Vast volumes of confidential information are now delivered and stored electronically.
- Hard drive storage capacity continues to grow, increasing the quantity of information stored locally and the amount of data at risk.

For compliance purposes, IT personnel need to know where their assets are, who is using them, and what is on them. The loss of one single laptop poses a serious security risk, as countless organisations can attest.

² Michael Singer, "PC milestone--notebooks outsell desktops," ZDNet News, June 3, 2005, CNET News.com.



While the largest store of sensitive information typically resides in an employee's inbox, other areas include file folders, contact lists and modern unified messaging systems (such as digitalised faxes and voicemails). Beyond the risk of exposed data, the next greatest concern can be the unsecured enterprise access available through a departmental laptop.

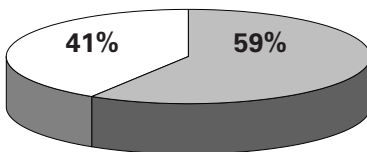
To deliver on the value and promise of mobility, IT departments routinely deploy a range of access points and methodologies, such as remote data connections to VPNs or Web access for enterprise systems. An unscrupulous individual can often access many of these systems simply by accessing an employee's mobile computer.

Laptop Theft Affects Everyone

- Laptop theft was attributed to 59% of computer attacks on government agencies, corporations and universities according to Baseline 2004.³
- Since early 2005, more than 150 million personal records have been exposed.⁴
- 85% of organisations surveyed reported they have had a data breach event.⁵
- 47% of computer security professionals surveyed reported a laptop theft over the past 12 months.⁶
- More than 50% of malicious corporate network penetrations are now conducted through lost or stolen mobile devices.⁷

Computer Attacks

-  % associated with laptop theft
-  % associated with other types of breaches



³ Bates & Pell

⁴ Privacy Rights Clearinghouse, A Chronology of Data Breaches, April 9th 2007

⁵ Scott and Scott LLP and Poneman Institute LLC, May 15th 2007

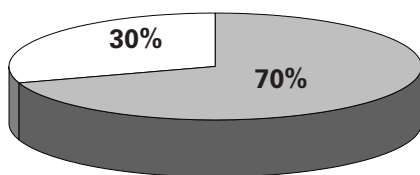
⁶ FBI & CSI's annual Computer Crime and Security Survey, 2006

⁷ Sascha Beyer, Pointsec

Many IT departments implement data encryption solutions trusting that their confidential data will be protected at all times. Encryption is a good first step toward data security compliance, but it cannot recover stolen laptops and it rarely protects sensitive information in cases of internal theft.

Causes of Security Breaches

- Security breaches as a result of internal sources
- Security breaches as a result of external sources



Data Encryption = A False Sense of Security

Data encryption solutions are powerful tools but they are a lot like prison walls: they prevent most common breaches, but are powerless to stop a criminal in possession of keys to the gates. Given that Gartner estimates that 70% of security breaches occur as a result of internal sources, encryption may only be effective in as little as 30% of all incidents. Encrypting data is therefore necessary but insufficient: it is a good first step toward data security but hardly a guarantee that data is secure or that data will not be compromised.

A disgruntled employee with access to passwords can easily obtain and abuse confidential information. Teledata Communications suffered for years at the hands of a rogue employee who was selling confidential credit card information, even though the company had a policy of conducting extensive background screening on its employees.⁸ Organisations that do not have a method for preventing internal theft, or recovering lost or stolen devices, leave themselves vulnerable to having critical information compromised.

Encryption Cannot Track and Recover Assets

Encryption is also powerless to protect hardware from theft and does nothing to help police track down lost or stolen devices. Further, as long as a mobile device continues to exist outside an organisation's control, vulnerability from potentially exposed data continues to exist.

Computer theft represents an enormous loss of assets, as well as an unacceptable risk of compromised data. Since encryption does not help with recovery, an ambitious hacker in possession of a stolen laptop has unlimited time to aggressively attack the code, attempting to circumvent password protected login screens.

Numerous legal challenges have arisen following computer breaches with the burden of proof placed on the organisation to prove that it had in fact encrypted the compromised data. How can an IT department prove that it is protecting its mobile data through encryption and other methods, if it cannot locate the hardware?

User Error: The Enemy of Encryption

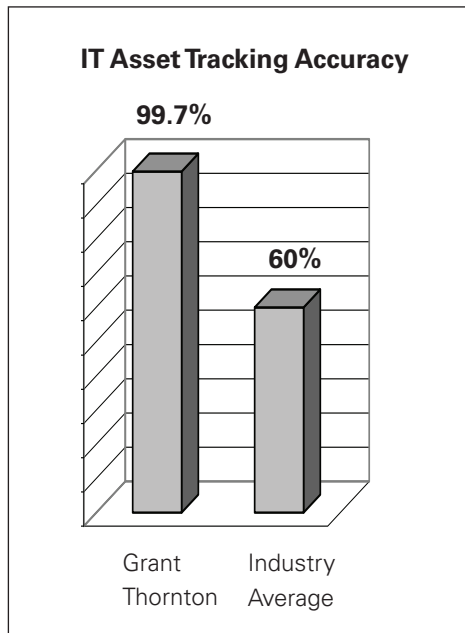
Encryption is often entirely dependent on the daily diligence of users; any mistake in the deployment of encryption tools and data can be left completely unprotected. Because it is impossible to eliminate human error, backup systems such as a remote data delete

⁸ Daniel Roth with Stephanie Mehta, "IDENTITY THEFT: The Great Data Heist," May 16, 2005, Fortune, and Dawn Kawamoto, "Security Strategy: 185,000 people's medical data stolen," April 11, 2005, www.silicon.com

solution must be in place to safeguard data and maintain regulatory compliance.

Compliance-Related Statutes

The Data Protection Act (DPA) places restrictions on organisations which collect or hold data on people, and governs the use and length of time that the data can be kept. For example, schools can only keep data on past students for no more than a decade. Because computers are inherently capable of housing vast amounts of information, IT professionals must remain vigilant in order to comply with DPA regulations.



The Freedom of Information Act 2000 provides the general public with "right to know" information about public bodies, affecting over 100,000 institutions, such as government departments, schools and councils. The Act also mandates regular and proactive publication schemes for the release of information such as annual reports or accounts, Basel II, or The New Accord, represents recommendations by central bankers from 13 nations to revise international standards for measuring a bank's capital. It was designed in part to create consistency in the way banks and regulators approach risk management across international borders. For financial institutions, there is no escaping the fact that a lost or stolen computer represents potentially massive operational risk.

The Turnbull Guidance, published by the Financial Reporting Council (FRC), sets out best practices for internal control for all companies listed on the London Stock Exchange, and mandates that such companies implement pervasive risk management plans for their businesses. The US Securities and Exchange Commission (SEC) has identified the Turnbull guidance as a suitable framework for complying with US requirements to report on internal controls over financial reporting, as set out in Section 404 of the Sarbanes-Oxley Act 2002 and related SEC rules.

Case Study: Grant Thornton LLP Achieves 99.7% Accuracy in IT Asset Tracking

ECompliance is important in every organisation, but especially in a large accounting firm like Grant Thornton LLP. To comply with computer lease requirements and improve lifecycle management, Grant Thornton needed to locate and data cleanse all leased computers at end-of-term.

A layered approach to laptop security was undertaken, with Computrace at its centre. Prior to its implementation, Grant Thornton could account for about 80% of its mobile assets at any one time - considerably better than the organisational average of 60%⁹, but still leaving room for improvement.

With Computrace, the IT department at Grant Thornton is able to quickly determine where a machine is located, who is using it and what software is installed on it – thus achieving IT asset tracking of 99.7%. By tracking its mobile assets, Grant Thornton is able to comply with government legislation.

⁹ Gartner Group, 2002

Laptops Make Easy Targets

Increased portability means increased convenience - and increased risk of loss or theft. Laptops are easy targets: they are designed to be portable, and thus disappear at an alarming rate. This problem will likely worsen over time as laptop use increases and thieves become more sophisticated in their methods.

As organisations open up their networks to mobile workers and contractors, they expose themselves to greater security risks. It is critical to be proactive and identify weaknesses in network security before someone or something external discovers those vulnerabilities. IT professionals must be vigilant in keeping up to date on the tools and techniques used today by cyber criminals.

A stolen laptop can quickly be fenced, or sold, for cash but, often the information contained on a stolen machine is far more valuable than the hardware. Sophisticated criminals today specialise in the sale of confidential information, banking or medical information and trade secrets. The proliferation of portable devices in the last decade has made it far easier for them to acquire sensitive information such as this.

Criminals have been known to destroy a company's or individual's reputation for profit, spite or sport. Countless high profile organisations have faced the humiliation of forming tens of thousands of clients that a device, such as an employee's laptop, has been lost or stolen and that their personal information may have been compromised.

While encryption helps protect data, organisations that do not have a technique for swift recovery can never truly ensure their clients' confidentiality. When a computer has been lost or stolen, there is a very real possibility that the data stored on it will be compromised – whether the data has been encrypted or not. The victim must live with the anxiety of never knowing how or when the data will be exploited – or for what unscrupulous purposes.

Organisational Drift

To ensure regulatory compliance, IT professionals must be able to protect data, track hardware and users, provide auditing capabilities and maintain historical records. Yet mobile assets can be the most difficult to track: a Gartner study suggests that most organisations are only able to locate about 60% of their mobile assets, which raises the following questions: Where are the other 40%? Who is using them? What information resides on them?

Not all missing assets are a result of theft. As much as 10 to 15% of missing computers can be attributed to "drift" within an organisation. Assets are taken out of service (broken or obsolete), or locked away in the bottom of a filing cabinet and forgotten, or are handed down internally to junior employees. Regardless of why devices go missing, most are very likely to contain sensitive or confidential data – information for which the organisation is responsible and liable. In cases like this, a remote data delete software product (see next section) can be efficient and effective; it can also provide proof that the data has been deleted.

¹⁰ Absolute Software Corp., installed base data, 1998-2004

For law enforcement agencies, attempting to locate a lost or stolen laptop computer without tracking software is like looking for a needle in a haystack. ComputraceOne asset tracking solutions report their IP locations to a central administrator every 15 minutes, helping police pinpoint and recover thousands of missing laptops annually.

Data Protection with Remote Data Delete Tools

Government legislation exists in numerous jurisdictions mandating that any security breach that is reasonably believed to have compromised personal information must be publicly reported. By remotely deleting sensitive data on missing computers, an organisation can avoid potentially damaging publicity or litigation. Remote data delete software like ComputraceOne provide this capability, and can remove data at the file, directory and/or operating system (OS) level.

ComputraceOne utilises an algorithm to delete data that exceeds the NATO deletion standard specification for wiping disk storage to guarantee that all data previously contained on that magnetic media is permanently erased.

Lifecycle Management

Even the simple retirement of old hardware (through obsolescence or end-of-lease), requires sensitive data to be removed from a device before it is repurposed internally, sent for recycling or returned to the leasing agency. Numerous examples exist in the media of sensitive information being found on "refurbished" computers. A data delete for lifecycle management can be set to run automatically, serving as a blunt but effective reminder to the user that the computer is overdue to be returned to the IT department.

Minimising Exposure, Facilitating Prosecution

If law enforcement officials are able to locate and recover a stolen laptop, police are in a better position to find and prosecute the perpetrator. Similarly, with the asset recovered and the perpetrator identified, the scope of the information breach can be defined and swift corrective action taken, such as dismissal or prosecution. Well-publicised repercussions send a clear message that an organisation has the ability to strike back.

While a layered approach to data security can reduce theft and loss from an average of 3 - 5% of assets to less than 1%, losses still occur. Therefore, the last line of defense is to minimise the impact of those losses through the timely recovery of stolen hardware.

Prosecution often acts as a powerful deterrent against future theft, especially in cases of internal theft. Human resources policies that include strong disciplinary action for misuse of computer assets, coupled with successful theft recoveries, are a powerful combination.

Getting to the Source of the Problem

For many organisations, the cost to replace lost hardware is enough of a hardship. But this pales in comparison to the battered public image that results from the mandatory announcement to alert clients, patients, students or staff – and of course the media – about the information breach, and the lawsuits that inevitably follow. There are also a host of soft costs associated with the loss of a laptop, including loss of employee productivity, procurement and re-provisioning costs and labor. Aside from the hard and soft costs of replacing the asset, the fact remains that the longer a device floats outside of the organisation's control, the more likely it is for the information inside to be breached. By recovering a device, an organisation contains the problem and minimises future exposure.

Technology to Outsmart Criminals

For law enforcement agencies, attempting to locate a lost or stolen laptop computer without tracking software is like looking for a needle in a haystack. ComputraceOne asset tracking solutions report their IP locations to a central administrator every 15 minutes, helping police pinpoint and recover thousands of missing laptops annually.

Recovery tools such as ComputraceOne are highly effective because thieves know that hardware is more valuable if they can prove that it is in working order. To do so, they inevitably turn the hardware on and – as the vast majority of laptops today are wireless-enabled – it connects to the Internet, at which point the stealthy ComputraceOne agent quietly reports its location information to the Absolute Theft Recovery Team. The central administrator can then provide the necessary information for local law enforcement to recover the device.

Persistence Ensures Effectiveness

Embedded in the BIOS firmware of computers by major computer manufacturers, the ComputraceOne agent can survive operating system re-installations, hard drive reformat and even hard drive replacements. Employing a self-healing technology called “persistence”, the ComputraceOne agent essentially rebuilds the agent software installation even if the agent service is deleted. The software is designed to be removed only by an authorised user with the correct password. This self-healing feature will repair a ComputraceOne installation in newly formatted and installed operating systems as well as freshly imaged systems. The agent is also very difficult to detect, as it runs as a non-descript service, and is not listed as an application. As well, the product does not show up on the programs menu listing or as a system tray icon.

Ten Steps to a Layered Approach to Laptop Security.

Here is a quick checklist of best practices for protecting data on mobile assets:

- 1.** Understand the risks. As organisations open up their networks to their mobile work force, to partners, customers and others, they expose themselves to greater security risks than they encountered when traffic was mostly internal.
- 2.** Be proactive. If you cannot identify the weaknesses in your network's security, someone or something will find those vulnerabilities for you. Educate yourself on the tools and techniques used today by cyber criminals as well as other security risks. Data security is a moving target that requires ongoing attention.
- 3.** Use cable locks on laptops as visual deterrents. Truth be told, most cable locks can be ripped off the plastic exterior of a laptop with a strong tug. Cable locks are therefore akin to ink-filled garment security tags in clothing stores: they leave a mark when removed by force, but are ineffective at preventing many thefts.
- 4.** Avoid leaving unsecured laptops unattended. Lock them in cupboards, carts or other secure facilities when not in use. If they must be left in a vehicle they should be covered up or locked in the boot.
- 5.** Keep laptops inconspicuous. Laptops should be carried in inconspicuous carrying cases, such as rucksacks or tote bags, instead of tell-tale laptop bags.
- 6.** Install anti-virus software and firewalls. Prevent unauthorised access and protect valuable information with data encryption software. Keep all software products updated to the latest versions or patches to help minimise security holes. Ensure web servers, operating systems and line of business applications are fully patched.
- 7.** Back-up valuable data on a scheduled basis. Data back-up needs to happen frequently to minimise the risk to the organisation in the event of loss.
- 8.** Create a contingency plan. Identify possible damage should a breach in security occur; also consider how customers, students or employees would be served in the event of catastrophe. Contingency plans for security should be integrated with the organisation's overall disaster recovery plans.
- 9.** Use asset tracking and recovery software. Install an asset tracking and recovery tool such as ComputraceOne to track and recover computers that are lost or stolen, and monitor any changes or disappearances in computer memory, hard drives or peripherals.
- 10.** Invest in advanced data protection. ComputraceOne allows customers to track fixed, remote and mobile computer assets and remotely wipe sensitive information in the event that a computer is lost, stolen or nearing the end of its lifecycle.

For more information on Compliance, Protection and Recovery, and the software tools used in a layered approach to laptop security, contact Absolute Software today.

Absolute Software EMEA Limited

78 Bartholomew Street,
Newbury, Berkshire,
RG14 7AB
Tel: +44 (0)1635 30424
Fax: +44 (0)1635 30687
www.absolute.com/emea

About Absolute Software

Absolute Software Corporation (TSX: ABT) is the leader in Computer Theft Recovery, Data Protection and Secure Asset Tracking™ solutions. Absolute Software provides organizations and consumers with solutions in the areas of regulatory compliance, data protection and theft recovery. The Company's Computrace® software is embedded in the BIOS of computers by global leaders, including Dell, Fujitsu, Gateway, HP, Lenovo, Motion, Panasonic and Toshiba, and the Company has reselling partnerships with these OEMs and others, including Apple. For more information about Absolute Software and Computrace, visit www.absolute.com.
