



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

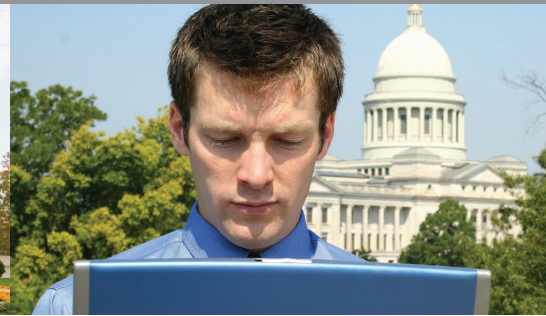
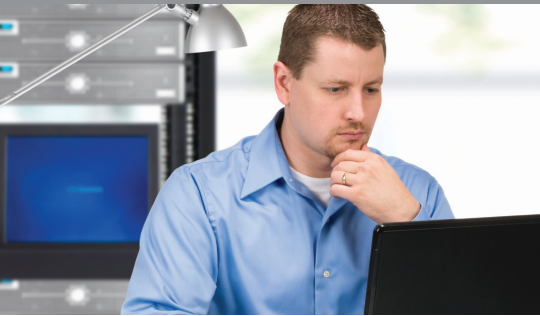


Table of Contents

Executive Summary.....	2
The Challenge	3
The Power of Mobility	4
Laptop Theft is Pervasive	5
Encryption is Necessary, but Insufficient	6
Compliance	7
Protection	8
Recovery	10
Summary	12
About Absolute Software	13

Since 2007, government agencies have compromised approximately 100 million individual records in reported data breaches.¹

With the vast amount of sensitive data now being stored on laptop computers, government agencies risk costly litigation and public relations nightmares when even one notebook goes missing. IT professionals in the public sector must accurately track computers and be able to prove that every action has been taken to secure personal information and sensitive data until a lost or stolen computer can be located.

The U.S. Federal Office of Management & Budget (OMB) will soon require all mobile and remote workers to use encryption to protect data stored on computers², but it is important to stress that encrypted data is not necessarily secure data. 60% of breaches occur due to internal causes.³ Because employees committing such crimes usually have in their possession the necessary passwords and encryption keys, encryption may only be effective in 40% of all incidents.

Single point security solutions cannot adequately protect government agencies 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** – Adherence to all applicable mobile data protection 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** – Recovery of lost or stolen devices returns them to the control of the organization and facilitates prosecution.

By adopting the CPR approach to laptop security, government agencies can minimize the impact of computer theft, while complying with privacy regulations. Computrace® notebook security and tracking software products help ensure regulatory compliance by protecting data, tracking hardware and users, providing auditing capabilities and acting as a historical record of computer assets and their use. An optional Data Delete function can also be used to remotely wipe stolen computers using a Department of Defense-approved algorithm.

The Computer Security and Tracking Challenge for Government

Laptop usage in the public sector continues to rise – in some cases, administrators have thousands of remote computers to manage. Sensitive or even classified information residing on laptops increases with greater mobility among government employees. Even states and agencies 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 computer 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; in fact, for federal agencies, an annual audit is now mandated by Congress.⁴ 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 government department.

It is no coincidence, then, that enhanced computer security for federal agencies and state and local jurisdictions is one of a number of key initiatives recently announced by the O.M.B.

A Changing IT Landscape

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

- Increased use – and theft – of notebook 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 in concert to provide IT professionals everywhere – in the public sector, private sector or education – with the broadest security blanket available.

Security breaches can be inconvenient and publicly embarrassing for any organization, but in the public sector they can be disastrous. A missing computer can result in compliance and data protection issues ranging from the misuse of confidential information to threats to national security.

Stolen Pennsylvania Public Welfare Department computers compromise more than 300,000 personal records

The Pennsylvania Public Welfare Department announced in 2007 that two computers containing the mental health histories of more than 300,000 medical-assistance recipients were stolen from the corporate office. Although the information also was protected by multiple passwords, full names and Social Security numbers of nearly 2,000 people were also on the computers.⁵

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 and data protection is recommended, comprising Compliance, Protection and Recovery. Some of the steps involved in CPR include:

Real-Time Asset Tracking – The ability to track near real-time every mobile asset whether or not connected to the network, and provide dynamic reporting, which helps with regulatory compliance.

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

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

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 notebook over the Internet to assist law enforcement in retrieving 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, telework and mobility brings new challenges in the areas of data security and information privacy. With the proliferation of notebook computers, these challenges will only intensify:

- Organizations continue to issue more laptop computers to employees as replacements for their desktop computers. By the end of 2010, there will be more than 47 million portable computers in the U.S.⁶
- 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, public sector IT personnel need to know where their assets are, who is using them, and what is on them. The loss of a single notebook poses a serious security risk, as the notebook stolen from Pennsylvania Public Welfare Department demonstrated.

While the largest store of sensitive information typically resides in an employee's e-mail inbox, other areas include file folders, contact lists and modern unified messaging systems (such as digitized 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, government 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 and mobile device theft is experienced by 50% of security professionals.⁸
- Every 50 seconds a laptop goes missing - and that's just at U.S. airports.⁹
- 85% of privacy and security professionals had at least one reportable breach in the past 12 months.¹⁰
- The cost of recovering from a single data breach now averages \$6.3 million.¹¹
- 66% of data breaches involved data the victim did not know was on the system.¹²

The majority of reported data breaches in government agencies are due to stolen computers.⁷

Many government 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 notebooks and rarely protects sensitive information in cases of internal theft.

Data Encryption = A False Sense of Security

On June 23, 2006, the OMB, which operates under the White House, issued a “Memorandum for the Heads of Departments and Agencies” outlining new data security standards and practices, including encryption on all laptops and mobile devices unless specifically classified as “nonsensitive.”¹³

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 the keys to the gates. Given that 60% of security breaches occur as a result of internal sources, encryption may only be effective in as little as 40% of all incidents.¹⁴ 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. Organizations 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 & 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 of an organization’s control, vulnerability from potentially exposed data continues to exist.

Every 50 seconds a laptop goes missing - and that’s just at U.S. airports.¹⁵ This represents an enormous loss of assets, as well as an unacceptable risk of compromised data — in the public sector especially. Since encryption does not help with recovery, an ambitious hacker in possession of a stolen notebook 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 organization to prove that it had in fact encrypted the compromised data. 88% of IT administrators, if laid off tomorrow, would take valuable and sensitive company information with them.¹⁶ How can an agency prove that it is protecting its mobile data, through encryption and other methods, if it cannot even 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 solution, must be in place to safeguard data and maintain regulatory compliance.

U.S. Compliance-Related Statutes

While the following examples are U.S. statutes, similar legislation exists or is pending in many other jurisdictions.

Sarbanes-Oxley Act requires accurate reporting of all assets, including computer assets. Non-compliance carries severe penalties (fines of up to \$5 million and imprisonment for up to 20 years) for senior management.

State Data Breach Laws - 44 States have enacted data breach laws, which require organizations that own or license computerized data containing personal information to disclose to residents any breach of security if unencrypted personal information is reasonably thought to have been compromised by an unauthorized person.

Gramm-Leach-Bliley mandates confidentiality of customers' private information. Organizations storing personal customer information must identify and safeguard against the loss of any personal information.

HIPAA (Health Insurance Portability And Accountability Act) establishes rules for handling and securing medical records to ensure the privacy and security of patient information. The act pertains to any department or organization that processes, transmits or stores protected health information. Noncompliance carries significant civil and criminal penalties.

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

Compliance is important at every organization, but especially at 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 ComputraceComplete at its center. Prior to its implementation, Grant Thornton could account for about 80% of its mobile assets at any one time - considerably better than the industry average, but still leaving room for improvement.

With ComputraceComplete, 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 including Sarbanes-Oxley, Gramm-Leach-Bliley, California Senate Bill 1386 and HIPAA.

In response to an ever-increasing volume of sensitive and confidential information stored on remote and mobile computers, and the high profiled breaches of privacy reported in the press, governments have dramatically increased regulatory legislation designed to protect information. Many of these statutes include criminal penalties for those found to be negligent.

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 notebook use increases and thieves become more sophisticated in their methods.

A stolen laptop can quickly be fenced, or sold, for cash but, in the public sector, the information contained on a stolen machine is far more valuable than the hardware. Sophisticated criminals today specialize in the sale of confidential information, Social Security numbers, 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 reputation for profit, spite or sport. Countless high profile organizations have faced the humiliation of informing tens of thousands of clients that a device, such as an employee's notebook, has been lost or stolen and that their personal information may have been compromised.

While encryption helps protect data, organizations 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 become compromised, 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.

Organizational Drift

To ensure regulatory compliance, all levels of government 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 as much as 20% of software licensing and hardware maintenance charges are incurred for assets that are no longer in use.¹⁷

Not all missing assets are a result of theft. 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 organization 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.

As governments 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.

Data Protection with Remote Data Delete Tools

Government legislation mandates 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 organization can avoid potentially damaging publicity or litigation. Remote data delete software such as ComputraceComplete, ComputracePlus and Computrace Data Protection provide this capability, and can remove data at the file, directory and/or operating system (OS) level.

Computrace utilizes an algorithm to delete data that exceeds the United States Department of Defense (DoD) deletion standard DOD5220.22-M and meets the NATO deletion standard. DOD5220.22-M is a DoD 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 previously used in by public sector workers. 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.

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

While a layered approach to data security can reduce theft and loss losses still occur. Therefore, the last line of defense is to minimize the impact of those losses through the timely recovery of stolen hardware.

Minimizing Exposure, Facilitating Prosecution

If law enforcement officials are able to locate and recover a stolen notebook, 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, whether dismissal or prosecution. Well-publicized repercussions send a clear message that an organization has the ability to strike back.

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 organizations, 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 and 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 mobile computer, 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 organization's control, the more likely it is for the information inside to be breached. By recovering a device, an organization contains the problem and minimizes future exposure.

Technology to Outsmart Criminals

Most thieves know that stolen computers are rarely located or recovered. Armed with this fact, they have become bolder in their methods and more active than ever.

Recovery tools such as ComputraceComplete 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 notebooks today are wireless-enabled – it connects to the Internet, at which point the stealthy Computrace agent quietly reports its location information to the AbsoluteTheft 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 firmware of computers by major computer manufacturers, the Computrace agent can survive operating system re-installations, hard drive reformats and even hard drive replacements. Employing a self-healing technology called “persistence”, the Computrace agent essentially rebuilds the agent software installation even if the agent service is deleted. The software is designed to be removed only by an authorized user with the correct password. This self-healing feature will repair a Computrace 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.

Case Study: Computrace Helps GSA Save Money for Spending Elsewhere

As the purchasing arm for the federal government, the General Services Administration (GSA) does its best to spend its money wisely – especially when it comes to computing assets. To ensure they protected their investments in computing assets as well as possible, they installed Computrace on hundreds of mobile computers. Thus far, Computrace has helped track and recover three stolen notebooks.

Shortly after two notebooks were stolen from a GSA office in Atlanta, the Absolute Theft Recovery Team detected one of the machines on the Internet. Federal Protective Service (FPS) agents were notified with location information, and within 48 hours, FPS officers arrested a man in College Park, Ga., with one of the stolen computers. The thief then led authorities to an accomplice who had in his possession eight other stolen computers - including the second stolen GSA laptop. Kingpins in a ring of full-time computer thieves, the two culprits would secure temporary contract work wherever they could, then walk out with expensive laptops.

In an unrelated case, another notebook stolen from a GSA office in South Carolina was also recovered with the help of Computrace.

“I’m pleased with the services offered by Absolute, and it’s important that we raise awareness about Computrace,” said Karen Greenhow, Regional Systems Chief for the GSA. “Laptops can walk away very easily, so we need to make sure our assets are always protected.”

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 organizations 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 notebooks unattended. Lock them in cupboards, notebook 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 trunk.
5. Keep laptops inconspicuous. Laptops should be carried in inconspicuous carrying cases, such as backpacks or tote bags, instead of tell-tale laptop bags.
6. Install anti-virus software and firewalls. Prevent unauthorized access and protect valuable information with data encryption software. Keep all software products updated to the latest versions or patches to help minimize 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 minimize the risk to the organization in the event of loss.
8. Create a contingency plan. Identify possible damage should a breach in security occur; also consider how customers would be served in the event of catastrophe. Contingency plans for security should be integrated with the organization's overall disaster recovery plans.
9. Use asset tracking and recovery software. Install an asset tracking and recovery tool such as ComputraceComplete 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. Computrace Data Protection 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 notebook security, contact Absolute Software today.

Absolute Software

Tel: 1 800 220 0733
or 604 730 9851

Fax: 604 730 2621

www.absolute.com

About Absolute Software

Absolute® Software (TSX: ABT) is the leader in firmware-based, patented 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 firmware of computers by global leaders, including Dell, Lenovo, MPC, HP, Fujitsu, General Dynamics Itronix and Toshiba, and has reselling partnerships with these OEMS and others, including Apple. For more information about Absolute Software and Computrace, visit www.absolute.com

- 1 Attrition.org, 2008
- 2 Office of Management & Budget, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May, 2007
- 3 Ponemon Institute, U.S. Costs of a Data Breach, 2007
- 4 Office of Inspector General Semiannual Report to the Congress, June 12, 2006
- 5 Penn Live.com, Computers stolen from welfare office, September, 2007
- 6 IDC, Quarterly PCTracker, 2008
- 7 Attrition.org
- 8 CSI, The 12th Annual Computer Crime and Security Survey, 2007
- 9 Ponemon Institute, Airport Insecurity: the case of lost laptops, 2008
- 10 Ponemon Institute, Enterprise @ Risk: Privacy & Protection Survey, 2007
- 11 Ponemon Institute, U.S. Costs of a Data Breach, 2007
- 12 Verizon, Data Breach Investigations Report, 2008
- 13 Johnson III.
- 14 Ponemon Institute, U.S. Costs of a Data Breach, 2007
- 15 Ponemon Institute, Airport Insecurity: the Case of Lost Laptops, 2008
- 16 Cyber-Ark, Security Survey Reveals Exiting Employees Have The Power, 2008
- 17 Gartner, Inc., Don't Overlook Opportunities to Save Costs on ITAM by Jack Heine et al, March 27, 2008

©2008 Absolute Software Corporation. All rights reserved. Computrace and Absolute are registered trademarks of Absolute Software Corporation.