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

The IT environment has changed significantly in a few short years, as several factors have dictated the need for a more robust approach to corporate security policies, including:

1. A trend towards mobility of information,
2. Theft of IT assets arising from a proliferation of mobile devices,
3. Increasing data privacy and data security concerns, and
4. Regulatory compliance mandated by recent legislation.

These factors have made it necessary for network administrators to design and implement comprehensive security policies to keep pace with the changing IT landscape. Effective solutions for these multifaceted problems require a layered approach comprised of products, policies and procedures that can work in concert to provide organizations with the broadest security blanket available.

Table of Contents

Absolute® Software

RECENT HEADLINES

A number of high profile companies have suffered security breaches as a result of computer theft:

- **Oklahoma City, Oklahoma** - Oklahoma Corporation Commission announced that a disposed computer contained more than 5,000 Social Security numbers of Oklahoma residents. The data was found by a resident that bought the computer in a recent auction.[2]

- **Detroit, Michigan** - Blue Cross Blue Shield of Michigan announced that the information of approximately 1,560 members and two staff had been breached. Information contained in a laptop stolen from an employee's home included names and health insurance contract numbers.[3]

- **Northfield, Illinois** - Kraft Foods announced that a notebook computer containing the personal information of 20,000 employees was stolen from an employee traveling on company business.[4]

- **Ontario, Canada** – Ontario Hospital for Sick Children announced that more than 2,900 patients were notified via press release that their health information had been breached when a physician's laptop was stolen from an automobile.[5]

There is a strong relationship between the issues of compliance, data protection and theft recovery. Organizations must take this into account when defining security policies. It is no longer enough to attempt to address compliance issues without addressing data protection. Protection of data on mobile and remote computers requires an understanding of the issues surrounding computer theft. Having a broader understanding of how these areas inter-relate allows organizations to build a more robust security policy that can better address the issues of regulatory compliance, data protection and theft recovery.

Today, accepting the loss or theft of one laptop or tablet computer is simply not an option. A missing computer can result in compliance and data protection issues that may be very costly to an organization's reputation and bottom line. Organizations need to be able to accurately track their computers, know who is using them, what is installed on them, and be able to prove the actions taken to secure computers remain deployed and intact until the computer can be located.

THE POWER OF MOBILITY

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. Mobility means being able to perform professional corporate presentations while visiting clients; update a budget while traveling on business; or even stay connected to the office while on vacation to audit activities, prevent unwanted surprises and minimize an e-mail backlog. But for IT executives and managers, mobility brings new challenges in the areas of corporate security and information privacy.

PORTABILITY AT THE COST OF VULNERABILITY

Sensitive data such as client records, trade secrets and other proprietary information is ever more vulnerable and with the proliferation of laptop computers, this problem is likely to intensify.

- Companies 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.[1]
- Vast volumes of corporate information are now delivered and stored electronically.
- Hard drive storage capacity continues to grow – increasing the quantity of information being stored locally – and increasing the amount of information at risk.

The loss of a single laptop poses a serious risk to a corporation: proprietary information, personal data and trade secrets can fall into the wrong hands. Moreover, for licensing and compliance purposes, IT managers need to know where their assets are, who is using them, and what software and information is residing on them.

While the largest store of sensitive information typically resides in an employee's e-mail inbox, other areas include proprietary information contained in corporate data, contact lists, modern unified messaging systems (such as digitized faxes and voicemails) and unencrypted file folders. Beyond the risk of exposed data, the greatest concern is often the unsecured enterprise access available through a corporate 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 laptop computer.

COMPUTER THEFT STATISTICS

Think a security breach will never happen at your organization? Think again:

- Laptop and mobile device theft is experienced by 50% of security professionals.[6]
- Every 50 seconds a laptop goes missing - and that's just at U.S. airports.[7]
- 85% of privacy and security professionals had at least one reportable breach in the past 12 months.[8]
- The cost of recovering from a single data breach now averages $6.3 million.[9]
- 66% of data breaches involved data the victim did not know was on the system.[10]

ENCRYPTION IS NOT ENOUGH

In response to concerns over mobile data protection, many organizations have turned to deploy solutions that encrypt data on laptop devices. This is a good first step, but unfortunately, encrypted data is not necessarily secure data (a commonly held misconception). Since encryption requires the use of a key, it is an effective tool for slowing the impact of some types of breaches but it is often powerless to curtail internal security violations. Approximately 60% of security breaches occur as a result of internal sources[11]. Employees who have been given access to the keys in the first place. Therefore, encryption may only be effective in as little as 40% of all incidents.

It is important to note that encryption does not provide a means of retrieving stolen hardware and bringing information back under the control of an organization. As long as a mobile device continues to exist outside of an organization's control, the corporate vulnerability resulting from the potentially exposed data continues to exist.

Consider:

- Encrypted information can be breached using a brute-force attack or other more sophisticated tools and approaches, and,
- The perpetrator, who may be an unscrupulous employee or a professional criminal, remains at large.

THE LAYERED APPROACH

Like many security issues, single point solutions are not enough to adequately protect an enterprise from all points of attack. Instead, a multifaceted or layered approach to corporate security needs to be considered. An effective way to think about a layered approach to mobile security and data protection is CPR: Compliance, Protection and Recovery. Protecting data on a lost or stolen computer is a good first step, but recovering the asset, and stopping the internal theft, is equally important in effectively mitigating a company's total exposure.

A layered approach consists of:

1. **Compliance** The ability to comply with applicable mobile data protection regulations and to provide an easily accessible audit trail
2. **Protection** The ability to prevent mobile data losses from occurring
3. **Recovery** The ability to recover lost or stolen mobile data, to retrieve lost or stolen devices and return them to the control of the organization, and to facilitate prosecution

In the next three sections, this paper will discuss these layers in greater detail, and how they can work in concert to create a complete computer security policy for IT management.

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.

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 is a law that mandates that all companies protect the security and confidentiality of their customers' private information. To comply, 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 organizations - including school districts - that process, transmit or store protected health information. Noncompliance carries significant civil and criminal penalties. Since most districts maintain student medical records on at least some of their computers, they must therefore comply with HIPAA.

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

COMPLIANCE AND THE LAW

To ensure regulatory compliance, organizations must be able to protect data, track hardware (and users), provide auditing capabilities and maintain historical records. While many of the statutes apply to an entire enterprise, it is often mobile assets such as laptop computers that are the most difficult to track.

THE ENCRYPTION CONUNDRUM

While statutes like the State Data Breach Laws typically apply to unencrypted data, numerous legal challenges have arisen with the burden of proof being placed on an organization to prove that it had in fact encrypted the compromised data.
How can an organization prove that it is protecting its mobile data (through encryption and other methods) if it can't even locate the hardware containing the data?

ORGANIZATIONAL DRIFT

Not all missing assets are a result of theft. As much as 20% of software licensing and hardware maintenance charges are incurred for assets that are no longer in use.[12] 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 within the organization. Regardless of why devices go missing, the fact remains that despite their age most are likely to contain sensitive personal or corporate information – information for which the organization is responsible and liable.

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 re-purposed internally, sent for recycling, or returned to the leasing agency. Numerous examples exist in the media that highlight incidents in which salvage shops have found sensitive information on "refurbished" corporate computers.

USING DATA PROTECTION TOOLS IN CONJUNCTION WITH ASSET TRACKING CAPABILITIES

To fully comply with government regulations, an organization must have data security, such as encryption or remote data delete capability, coupled with asset tracking capabilities. This combination is necessary to quickly and effectively locate and recover assets containing sensitive information. Asset tracking capabilities help prove that an organization had the device in its possession and was capable of deleting sensitive data.

A BROADER APPROACH

Encryption combined with powerful asset tracking and recovery tools ensure superior protection for sensitive information. The ideal solution for compliance is encryption plus powerful theft recovery software that tracks assets, identifies users and helps law enforcement retrieve stolen hardware.

COMPLIANCE CHECKLIST

- ☐ Knowledge of the relevant statutes for your industry and jurisdiction
- ☐ The ability to track mobile computers, their usage and the types of information on them, including the ability to locate assets on demand
- ☐ Recovery software for retrieving lost or stolen assets

TAKING CONTROL OF THE SITUATION

Some organizations may think they can get by with minimal compliance protection. They are, however, exposing themselves to unnecessary risks and potential liability. Those that wish to truly reduce exposure to compliance issues for themselves and their clients must seek out a more robust solution.

Regardless of the specific solution chosen, a multi-faceted mobile data protection system should consist of the following:

- **REAL-TIME ASSET TRACKING** – The ability to locate all mobile assets whether or not connected to the network. It is imperative that any tracking system make use of near real-time asset tracking and dynamic reporting. Ideally, this system should be able to identify and communicate with remote assets.
- **REMOTE DATA DELETE** – The ability to remotely remove sensitive information from a lost or stolen mobile device through commands issued centrally.
- **DATA ENCRYPTION** – The ability to protect mobile data from unauthorized parties; encryption is the last line of defense against misuse by external parties.
- **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.

GRANT THORNTON LLP ACHIEVES 99.7% ACCURACY IN TRACKING ITS INFORMATION TECHNOLOGY

Corporate compliance is important to every organization, but especially to an accounting firm like Grant Thornton LLP - an organization that requires access to confidential client information and needs to set an impeccable corporate example for the business community.

By delivering full control of its assets and ensuring compliance, Grant Thornton created a layered approach to its security policies. Prior to the exercise, 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.

Central to the layered security approach and improved lifecycle management was the implementation of a sophisticated asset tracking and recovery system. The system deployed by Grant Thornton enables the IT department to quickly determine where a machine is located, who is using it and what software is installed on it. Grant Thornton is now able to track 99.7% of its IT assets.

By tracking its mobile assets, Grant Thornton is able to comply with government legislation including the Sarbanes-Oxley Act, the Gramm-Leach- Bliley Act, California Senate Bill 1386 and HIPAA.

PROTECTION CHECKLIST

- ☐ The ability to locate and recover lost or stolen mobile computing assets
- ☐ The ability to protect sensitive data through strong user authentication and encryption
- ☐ The ability to delete data remotely from mobile computers that have been lost or stolen

OVERWHELMING LOSSES

According to a study by Ponemon Institute, 600,000 laptops are reported missing every year - and that's just at U.S. airports.[13] According to analyst Frederica Troni from Gartner, "owing and supporting a single notebook costs on average more than $7,000 per year. This is what organizations loose when a single laptop goes missing, without even considering the data residing on it". [14] In 2007, theft of proprietary data from mobile devices tallied to $2,345,000, while theft of customer information from mobile devices came to $2,203,000.[15] This represents an enormous loss of assets, as well as an unacceptable risk of compromised data. When devices are not recovered, professional hackers have limitless time to work on cracking encryption codes or circumventing passwordprotected login screens.

Many organizations only use strong authentication or data encryption to safeguard their data, however, neither of these approaches provide help in the area of data recovery. Without tracking software, most victims of theft never see their stolen hardware again.

When a computer has been lost or stolen, there is a very real possibility that the data stored on it will become compromised. The victim must live with the anxiety of never knowing how or when the data will be exploited – and for what unscrupulous purposes.

Portable devices are extremely vulnerable to theft and disappear at an alarming rate. This problem will likely worsen over time as laptop use increases and thieves become more sophisticated in their methods. Organizations that do not have a technique for swift recovery can never truly ensure their clients' confidentiality. Trade secrets and private information are always at risk. Compromised data is most damaging when it falls into the hands of a competitor or is used by individuals wishing to exploit the personal information for financial gain.

INCREASING DANGER

Increased portability means increased convenience - and increased risk of loss or theft. Laptops are easy targets: they are designed to be portable. A stolen laptop can quickly be fenced, or sold, for cash but an even greater danger than loss of valuable hardware is the information inside it.

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.

Criminals have been known to destroy a company's reputation for the significant profits they can realize. Countless high profile companies have faced the humiliation of informing 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.

PROTECT YOUR DATA AND YOUR COMPANY'S EXPOSURE WITH REMOTE DATA DELETE TOOLS

Government legislation mandates that organizations must publicly report any security breach that is reasonably believed to have compromised personal information. By remotely deleting sensitive data on target computers that have fallen outside a company's jurisdiction, an organization can avoid potentially damaging publicity or litigation.

Industry-leading remote data delete tools can remove data at the file, directory and/or operating system (OS) level.

Remote data delete software can also be used for lifecycle management to ensure that computers are left clean and free of sensitive data at their end of life or lease.

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 organization's IT department. This tactic has been particularly successful in one-to-one laptop programs in school districts and colleges across North America.

ENCRYPTED DATA IS NOT NECESSARILY PROTECTED DATA

Encrypting mobile data is a start, but it is not a guarantee that data is entirely safe or that it will not be compromised. Encryption is powerless to protect hardware from theft and does nothing to help police track down lost or stolen hardware. Most significantly, encryption fails to protect sensitive information in cases of internal theft. 60% of breaches occur due to internal causes.[16]

A disgruntled employee with access to passwords can easily obtain and abuse confidential information. Companies that do not have a method for preventing internal theft leave themselves vulnerable to having their private information compromised.

When a mobile asset is lost to external theft, encryption is only effective at delaying thieves and hackers from gaining access to sensitive information. Since encryption does not help with recovery, an ambitious hacker has unlimited time to aggressively attack the code and find ways to circumvent the system.

Given enough time and computing power, brute-force attacks can be used to crack encrypted files. Hacking time can be significantly reduced through more sophisticated attacks, particularly where passwords can be guessed or other vulnerabilities exploited.

Any mistake in the deployment of encryption and data is left completely unprotected. Because it is impossible to eliminate human error completely from any organization, backup systems must be in place to safeguard data.

A LAYERED APPROACH FOR AGGRESSIVE PROTECTION

Hardware and information thieves are aggressive in their methods - protective measures must be equally aggressive. A layered approach is ideal, combining encryption and strong authentication with assettracking and recovery software.

COMPUTER SECURITY CHECKLIST

- ☐ The ability to locate lost or stolen assets for recovery
- ☐ Effective human resources policies that enable strong disciplinary action for misuse of corporate assets
- ☐ The ability to delete data remotely from mobile computers that have been lost or stolen

Thieves know that very few stolen computers are ever located. Armed with this fact, they have become bolder in their methods and more active than ever. Thieves count on the fact that organizations and individuals will not be able to trace and retrieve the stolen hardware. Even when a mobile computer is innocently lost, there are many individuals that would take advantage of the situation.

In 2007, laptop or mobile hardware theft accounted for more than $3.5 million.[17] Recent examples of laptop theft include:

- **Charter Communications:** 12 laptops were stolen from a South Carolina office[18]
- **T. Rowe Price:** theft of several computers compromises personal information of 35,000 individuals[19] - that's an estimated loss of $6.9 million.[20]
- **Gap:** theft of a stolen laptop from a third-party administrator exposes data of 800,000 people.[21]

For law enforcement agencies, attempting to locate a lost or stolen laptop computer is like looking for a needle in a haystack.

THE IMPORTANCE OF RECOVERY

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.

MINIMIZING EXPOSURE, FACILITATING PROSECUTION

Even more important than the hard and soft costs of replacing the asset is the fact that the longer a device floats outside of the organization's control, the more likely it is for the information to be breached. By recovering a device, an organization contains the problem and minimizes future exposure.

If law enforcement officials are able to 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. Prosecution acts as a powerful deterrent against future theft. Thieves seek an easy target. Well-publicized repercussions send a clear message that an organization has the ability to strike back.

ENABLING RECOVERY

Of all the components in a layered approach to security, recovery is one of the most sophisticated and undeniably one of the most significant elements. Sophisticated asset tracking solutions deploy software agents that regularly report their IP locations to a central administrator.

Recovery tools 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 connect to the Internet, at which point the agent - unbeknownst to the thief - reports its location information.

The central administrator can then provide the necessary information for the police to recover the device. But not all software agents are considered equal. IT managers must consider solutions with a client agent that is persistent and able to withstand multiple attacks, up to and including hard-drive reformats and OS re-installs.

GETTING TO THE SOURCE OF THE PROBLEM

To effectively root out a problem such as internal theft, organizations need to get to the heart of the matter. Often, theft is simply a symptom of a larger problem.

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

By recovering the devices, an organization can identify the source of the problem and ensure that the culprit is effectively brought to justice - helping prevent future thefts.

CASE STUDY: POLICE CRIME UNIT BUSTS LARGE THEFT RING WITH THE AID OF ASSET TRACKING AND RECOVERY SOFTWARE

The McKinney, TX, Police Department found that a local crime ring was engaged in counterfeit checks, driver's licenses and various other criminal activities. Using a clever approach to the problem, McKinney PD managed to insert a stolen computer configured with asset tracking and recovery software inside the loop of counterfeiters. Once inserted, the recovery software routinely checked in and reported its location and activities to the McKinney PD.

Utilizing the recovery software, the McKinney PD was able to monitor who was using the stolen computer and where it was calling from as part of the ongoing investigation. "This tracking software will assist in the prosecution of the suspects involved in this illegal activity," commented Detective Jeff Taylor. "[It] greatly assisted the McKinney Police Department in an ongoing investigation of a large crime ring in the Dallas Metroplex area."

BEST PRACTICES: DEPLOYING A LAYERED APPROACH TO DATA SECURITY

With the vast amount of mobile data continually increasing and a greater emphasis being placed on organizations by legislators, activists and now the courts, to protect personal information, data protection has become a top priority for IT departments. Corporations that are not taking measures to protect their data do so at their peril.

It is not just the monetary risk of losing a relatively small asset, but the corporate risk of losing sensitive trade secrets. Even worse is the risk of negative publicity associated with informing customers that the organization has mishandled their personal information.

With thefts and losses happening both internally and externally as a result of events both accidental and intentional, no single IT tool can protect against the full spectrum of potential threats. True corporate security and data protection relies on the implementation of a multi-faceted or layered approach to mobile data protection.

A layered approach to data security should include:

- **REAL-TIME ASSET TRACKING -** the ability to locate all mobile assets whether or not connected to the network; more than the traditional spreadsheet or static database that cross-references a computer to its owner, this system should be able to identify and communicate with remote assets and track changes to computer memory, hard drives and peripherals.

- **REMOTE DATA DELETE -** the ability to remotely remove sensitive information from a lost or stolen mobile computer through commands issued centrally.

- **DATA ENCRYPTION -** the ability to protect mobile data from being read by unauthorized parties. Encryption should be considered the last line of defense against misuse by external parties.

- **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.

Data protection tools need to be properly aligned to achieve the three corporate goals of CPR: Compliance, Protection and Recovery.

COMPLIANCE Compliance with applicable mobile data protection statutes (also the ability to prove that your organization was in compliance with government regulations), as well as easily accessed audit records.

PROTECTION Deterrence and precautionary action to prevent mobile data losses; protection also implies the ability to adequately protect information should a theft or loss occur.

RECOVERY The ability to recover lost mobile data, bring the data back under the control of the organization and facilitate prosecution of the perpetrator.

Starting today, what steps can an organization take to put in place a better, more compliant environment for protecting data, especially in mobile devices? Here are some quick tips on protecting data:

ENCOURAGE BEST PRACTICES

1. Educate employees on the need to avoid leaving laptops unattended. If they must be left in a vehicle, they should be locked in the trunk.
2. Explain the importance of data security for corporate compliance purposes and the benefits of a best practices approach to data protection.

PHYSICAL SECURITY

3. Ensure that all laptop computers are locked in cupboards or other secure facilities at work or at home when not in use.
4. Provide cable locks for laptops that must be left unattended.
5. Implement a sign-in system for visitors and do not let unaccompanied visitors into work areas.

ASSET TRACKING & RECOVERY

6. 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.

DATA ENCRYPTION

7. Deploy a data encryption tool to protect sensitive data.

REMOTE DATA DELETE

8. Use a data delete tool to remove remote sensitive information from a lost, stolen or end-of-life or lease device.

For more information on Compliance, Protection and Recovery, and to learn how your organization can deliver a layered approach to corporate security, please contact:

ABSOLUTE SOFTWARE CORPORATION

Tel 1 800 220 0733
604 730 9851

Fax 604 730 2621

www.absolute.com

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 firmware of computers by global leaders, including Dell, Fujitsu, MPC, HP, Lenovo, Motion, Panasonic, Toshiba and General Dynamics Itronix, 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

1 IDC, Quarterly PC Tracker, 2008
2 KJRH.com, Buyer finds sensitive information on server, May, 2008
3 BCBCM, BCBSM Responds to Protect Members Affected by Security Incidents, July, 2007
4 Quad-City Times, Missing laptop, data could affect Q-C Oscar Mayer employees, March, 2008
5 The Star,Sick Kids' laptop theft angers watchdog, May, 2007
6 CSI, The 12th Annual Computer Crime and Security Survey, 2007
7 Ponemon Institute, Airport Insecurity: the case of lost laptops, 2008
8 Ponemon Institute, Enterprise @ Risk: Privacy & Protection Survey, 2007
9 Ponemon Institute, U.S. Costs of a Data Breach, 2007
10 Verizon, Data Breach Investigations Report, 2008
11 Ponemon Institute, U.S. Costs of a Data Breach, 2007
12 Gartner, Inc., Don't Overlook Opportunities to Save Costs on ITAM by Jack Heine et al, March 27, 2008
13 Ponemon Institute, Airport Insecurity: the case of lost laptops, 2008
14 Gartner, Notebook Total Cost of Ownership by Federica Troni, February 20, 2008
15 CSI, The 12th Annual Computer Crime and Security Survey, 2007
16 Ponemon Institute, U.S. Costs of a Data Breach, 2007
17 CSI, The 12th Annual Computer Crime and Security Survey, 2007
18 CNN Money, Laptops with personal info of thousands stolen, August, 2008
19 Investment News, T. Rowe Price warns of computer thefts, January 2008
20 "A data breach costs an average of $197 per compromised record." Ponemon Institute, U.S. Costs of a Data Breach, 2007
21 CNN Money, Laptop Computer Stolen From Vendor That Manages Job Applicant Data for Gap Inc, September, 2007