Endpoint Security: Data Protection for IT, Freedom for Laptop Users

A worldwide shift towards the use of mobile devices coupled with recently-enacted data breach legislation has created a new challenge for IT organizations: balancing the enhanced productivity of mobile computing with the requirement to protect sensitive information from data breach. Many organizations have tackled mobile computer security with corporate policy, others with encryption technology. Both strategies are heavily reliant on end-user diligence to remain effective. Only the introduction of end-point security – the ability to force mobile computers to secure themselves – offers end-users the freedom to embrace mobility and IT departments robust protection for sensitive information.

Table of Contents

Suite 1600, Four Bentall Centre, 1055 Dunsmuir St, Vancouver, BC V7X 1K8
1 800 220 0733 | www.absolute.com | http://blog.absolute.com

Absolute® Software

Endpoint Security Defined

Endpoint security is a security strategy that emphasizes distributing security software onto end-user devices such as mobile devices or laptop computers while retaining central management over the security software.[1] Traditionally, organizations used corporate firewalls and other intrusion detection systems to protect corporate networks from potentially compromised endpoints. In today's laptop-dominated environment, endpoint security strategies place the responsibility for security on the device itself. This next generation of security strategy is already common in the form of anti-spam filters, desktop level firewalls and anti-virus software programs. Recognizing that organizations cannot rely on end-users to consistently follow IT policy or diligently apply security software, endpoint security seeks to eliminate the requirement for end-user involvement to be effective.

In 2008, one in every two computers in the world will be a laptop.[2]

The worldwide shift from stationary desktop computers to highly-portable laptop and tablet PC computers offers organizations increased productivity, flexible work schedules and greater work/life balance. Driven by the need for increased productivity and the ability to present up-to-date information at a moment's notice, secure mobile computing can be an organization's greatest strength. However, research indicates that lost or stolen laptop computers cause nearly 50% of public data breaches.[3] With recently-expanded state data breach legislation, even a single lost or stolen computer can expose organizations to the negative publicity and increased costs associated with public data breaches.

To protect themselves, many organizations have developed sophisticated IT asset use policies while others have combined policy with encryption technology in hopes of better securing computers and the sensitive information they contain. While these are necessary steps, organizations still struggle to compensate for the "human factor." According to a recent survey of 1,400 enterprises, more than 60% of data breaches are the work of those operating within the firewall – insiders such as employees, contractors and others with ready access to sensitive information.[4] Accidently or by design, employees will always be the weakest link in computer security strategies that rely on their diligence to provide consistent protection.

Rather than imposing strangling IT asset policies aimed at forcing end users to comply, endpoint security strategies use centrally-managed technology to ensure that mobile devices such as laptops secure themselves. Using readily-available computer theft recovery, remote data delete and Internet-based IT asset management, organizations can free end-users from computer security responsibilities while ensuring maximum protection for computers and the information stored on them.

Survey Sheds Light on Holes in Data Breach Protection

In September 2007, Research Concepts LLC asked 185 members of NetworkWorld's Technology Opinion Panel about the state of computer and data security in their organizations. The results revealed that, although computer and data security are high priorities for corporations, they are nevertheless unprepared to prevent data breaches and computer theft. Common approaches to computer security aimed at minimizing the possibility of data breach were consistently undermined by employees. Indeed, those surveyed reported that only one in 100 employees consistently follows corporate data and security policies.[7]

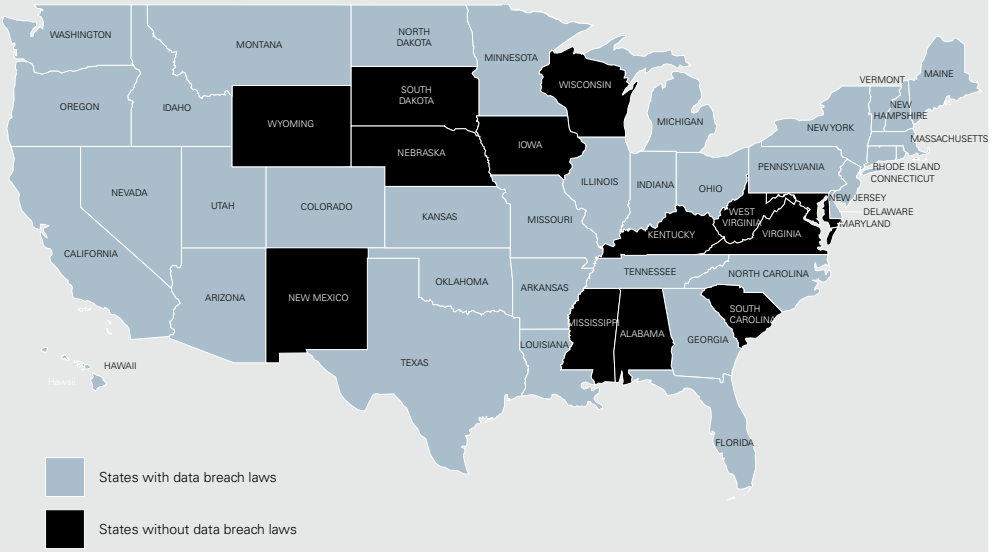
Physical Security and Authentication

The simplest form of laptop computer security involves protecting the computer and its physical environment. According to Research Concepts, more than 31% of organizations surveyed provide laptop users with cable locks to secure their computers when out of the office. Nearly 94% reported the use of password-based authentication on laptop computers. Interestingly, this same survey group indicated that they believed employees were responsible for most incidents of data breach within their organizations. Clearly, many organizations believe that despite basic precautions such as providing laptop locks and password-protecting computers, employees remain the weakest link in security plans.

Data Breach Regulation Across 37 States

The 2002, California Senate Bill 1386 added a new, public dimension to regulatory compliance. In the event of a data breach such as a lost laptop computer containing sensitive information, the bill requires organizations to notify all parties whose personal information has been exposed.[5] Following California's lead, 36 additional states have enacted similar data breach laws. The Ponemon Institute estimates that it costs a company $197 per missing record when a breach occurs.[6]

Data Breach Legislation has been Enacted in 37 US States



Organizational Policy

Research Concepts found that 58% of organizations currently promote polices for the safe use of mobile computing devices and for accessing sensitive files. The University of Miami Office of HIPAA Privacy and Security for example, details the circumstances under which students and medical staff may download electronic protected health information to a laptop computer. The fact remains however, that despite these organizational policies, busy salespeople, unknowing marketers and harried administrative staff will contravene policy and load sensitive information onto portable computers. With more than 600,000 laptops stolen each year in the United States, companies relying on organizational policy to protect sensitive data will continue to fuel data breach media headlines.[8]

Stolen Laptop Leads to Dismissal

"Just last month, security company VeriSign(VRSN) announced that a contract worker reported that her laptop, which held employee information, was stolen from her car. The employee no longer works at the company. A company spokeswoman told InformationWeek at the time that the woman, who worked in VeriSign's human resources department, failed to comply with company policies that mandate that data be encrypted and that employee information not be downloaded on laptop computers."[10]

High Tech Protection: Encryption and IT Asset Management

More than 50% of organizations surveyed by Research Concepts indicated that they protected sensitive information with encryption software. A further 43% reported the use of asset tracking software. Simply knowing where all mobile computers are located is a powerful security measure, however, traditional IT asset management solutions are designed to track only those laptops that connect to a local area network (LAN) or virtual private network (VPN) connection. For a large proportion of laptop users, returning to head office is an intermittent event – allowing many laptop computers to remain below the radar of IT.

Encryption software is commonly referred to as the computer security "fall back". In the event that a computer protected by organizational policy and physical deterrents is stolen, sensitive information on the laptop is made unreadable by encryption. For encryption software to be effective however, laptop users must consistently and accurately follow company encryption policy. Even more worrisome is the fact that more than 30% of companies believe employees are actively involved in the theft of company computers.[9] Armed with the necessary passwords and encryption keys to access data, disgruntled or dishonest employees represent a threat that cannot be addressed by encryption alone.

The common failing of these laptop security measures is the fact that they are heavily reliant on the diligent action of laptop-using employees to remain effective. If a cable lock is not used, an authentication password is taped to the keyboard for convenience or a regular encryption process not completed, organizations remain unnecessarily vulnerable to public data breach. By the same token, complex, expensive and ultimately productivity-dampening security measures may be effective but greatly reduce the benefits of laptop computers. Endpoint security solutions complement other security measures by providing a final, user-independent layer of protection.

Hospital Employee Tapes Encryption Key to Stolen Laptop

IT and security staff at a 2,400-physician Michigan-based hospital were justifiably concerned when they learned that a nurse's laptop computer had been stolen. Of greater concern was the fact that the nurse had contravened the hospital's data security policy and affixed the laptop's encryption key to the front of the computer. Fortunately, the hospital had protected the laptop with the Computrace endpoint security solution from Absolute Software.

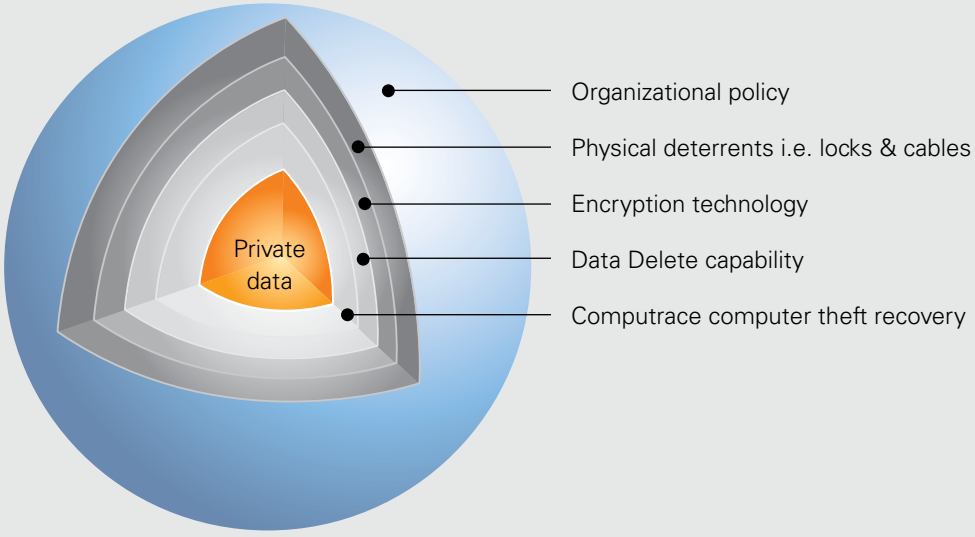
After alerting police, the hospital contacted the Absolute Recovery Team and let the team know that they were very concerned over the health information contained in the laptop. Rather than attempting to physically recover the computer, the Absolute Recovery Team recommended an immediate Data Delete operation to remove the sensitive information from the laptop.

Having promptly deleted all sensitive information from the computer, hospital officials maintained the computer's security. Hospital officials estimate that the quick action resulted in cost savings of between $80 and $100 per health record in data breach-related costs.

Endpoint Security Remains Effective When Other Security Layers Fail

Organizations that deal with sensitive information need to provide layers of protection for the data they hold – each layer working to bolster protection. With endpoint security at the core of security strategies, organizations are able to remotely delete data and physically recover stolen computers in the event that other security strategies are compromised.

A Layered Approach to Computer Security



Boston, Massachusetts - Forrester Research announced that a laptop stolen from one of the research firm's employees had potentially exposed the names, addresses and social security numbers of an undisclosed number of employees and directors. In a letter mailed to those affected, Forrester's Chief People Officer Elizabeth Lemons indicated that the laptop was password protected but made no mention of encryption. The incident proved especially embarrassing for the research firm that often consults on data security strategies for mid-market and Fortune 500 companies.[11]

Data breaches that went unnoticed historically are now highly-publicized affairs as a result of recent state data breach legislation.

Aspen Hill, Maryland – U.S. Department of Veterans Affairs announced that a notebook computer containing the names, birthdates, Social Security numbers and limited health information of 26.5 million veterans and active-duty military personnel had been stolen. It took Veteran's Affairs officials more than two weeks to publicly disclose the breach. The laptop, stolen from the data analyst working for VA, became part of the largest data breach in U.S. history. The theft prompted a series of hearings in the U.S. Congress that criticized the VA's data security processes and resulted in legislation that compels the VA to immediately notify congress in the event of a data breach.[12]

Detroit, Michigan – Blue Cross Blue Shield of Michigan announced in a Website statement and via personalized letters to members that the information of approximately 1,560 members and two staff had been breached. Information contained on a laptop stolen from an employee's home included names and health insurance contract numbers. Approximately 120 records also included Social Security numbers. Despite BCBSM internal policy that requires the encryption of health information and closely-monitored circumstances that allow downloading health information onto portable devices, the employee's laptop was unprotected. Disciplinary actions are pending completion of investigations into the incident.[13]

Computrace from Absolute Software is an on-demand endpoint security solution designed to provide robust data breach protection regardless of end user action. Centrally managed via an Online Customer Center, Computrace operates without end user knowledge or assistance – tracking computers regardless of location, remotely deleting sensitive information and assisting police in recovering those computers that go missing.

Perfectly complementing organizational policy and encryption technologies, Computrace addresses data breach protection challenges including:

Emergency Data Delete – Computrace allows IT professionals to remotely delete sensitive information from missing laptops. Organizations can then assess whether they are required to publicly announce a data breach.

Accurately Inventorying Computers – By logging into the Online Customer Center, IT personnel can create near real time reports on the computers in their inventory, their configuration, current user and location – whether they are connected to the local area network or in the field.

Recovery – Using Computrace, the Absolute Recovery Team can track missing computers and work with local law enforcement to recover the computer backed by a $1,000 Recovery Guarantee.[14]

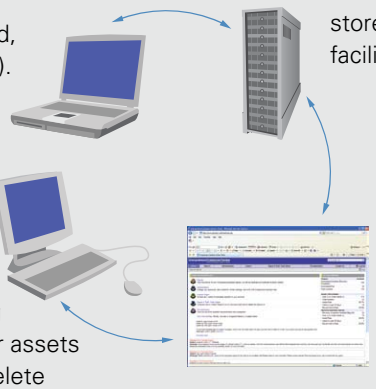
Policy Enforcement – Computrace can detect unauthorized software installations, missing hardware and can report on software installed – allowing IT departments to ensure that key programs such as anti-virus are current.

Lifecycle Management – In addition to remotely deleting confidential information in emergency situations, Computrace can be used to automatically delete data from computers at lease end or at retirement date.

How Computrace Works

The Computrace Software Agent is built into computers from the world's leading computer manufacturers during the manufacturing process. Customers activate Computrace when they purchase a subscription to Absolute's endpoint security solutions. When a computer protected by Computrace is reported stolen, the embedded Computrace agent sends a silent signal to Absolute's Monitoring Center providing critical location information. Absolute then works with local law enforcement to recover the computer. If the missing computer cannot be recovered within 60 days, the Computrace customer may be eligible for a Recovery Guarantee of up to $1,000. The stealthy Computrace Software Agent can survive accidental or deliberate attempts at removal or disablement. With embedded support in the BIOS of a computer, the Computrace agent is capable of surviving operating system re-installations, as well as hard-drive reformats, replacements and re-imaging.[15]

Remote Computer
Location, user, hardware and software data is transmitted daily without user input or knowledge. (client-initiated, TCP-based and encrypted).



Absolute Monitoring Center
Information is confidentially stored in our secure offsite facility.

Online Customer Center
Absolute Website: Log onto Customer Center to track and manage your PC assets.

IT Administrator
Responsible for managing remote / mobile computer assets and for setting up Data Delete

For more information on data breach protection and Absolute's complete range of endpoint security solutions , contact Absolute Software today.

Absolute Software
Suite 1600, Four Bentall Centre
Vancouver, BC, Canada
V7X 1K8

Tel: 1-800-220-0733 or 604-730-9851
Fax: 604-730-2621

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 or http://blog.absolute.com.

References

[1] "SearchSecurity.com Definitions," December 17, 2007, SearchSecurity.com

[2] "Are Fortified Notebooks the Answer?," May 19, 2006, Processor.com.

[3] "2007 Annual Study: US Average Cost of a Data Breach," November, 2007, Ponemon Institute, LLC

[4] "The Inside Job," August 13, 2007, Information Age

[5] "Bill 1386 Chaptered " February 12, 2002, California State Senate

[6] "2007 Annual Study: US Average Cost of a Data Breach," November, 2007, Ponemon Institute, LLC

[7] "Research Concepts Computer Security Survey Commissioned by Absolute Software," September, 2007.

[8] 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.

[9] "Survey of 400 Absolute Software Corporate Customers " June, 2007, Absolute Software

[10] "Seagate Targets Data Theft with Encrypted Hard Drive " September, 2007, Dark Reading

[11] "Forrester Loses Laptop Containing Personnel Data" December 2007, eWeek

[12] "Two Charged in VA Laptop Theft" August 2006, CSO

[13] "BCBSM Responds to Protect Members Affected by Security Incidents" July 2007, BCBCM Corporate Website

[14] Please visit http://www.absolute.com/PDF/EULA.pdf for full terms and conditions.

[15] For a complete list of BIOS-supported computers visit www.absolute.com/BIOS