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

Absolute® Software

A lost or stolen computer means a student gets left behind

Educators are turning to laptop computers as everyday learning tools – helping students develop valuable computer skills and aiding teachers in delivering more innovative lesson plans. With the enhanced portability of laptops, IT professionals are challenged to effectively audit IT assets, comply with government legislation and control the costs of laptop learning programs by reducing computer theft. A multilayered approach to computer security that includes physical deterrents, encryption, IT asset management, theft recovery and remote data delete capabilities ensures that schools are delivering the highest standard of protection for their computers and the sensitive information stored on them.

Table of Contents

More and more schools are turning to laptops as an everyday learning tool. Laptop learning not only helps students quickly develop their computer skills, it also helps teachers create and deliver more innovative lesson plans. In addition, many schools are promoting distance-learning to accommodate remote students and encouraging mobile computing in order to create stronger teamwork environments.

Key computer security issues for school districts and other educational institutions differ somewhat from the requirements of other industries. For educators, the ability to provide regular audits of computers in use, their location and the hardware and software installed can be critical in terms of regulatory compliance and demonstrating appropriate use of public funding. For most institutions, the loss of state or federally-funded computers through theft, drift or tampering is a major challenge. The option to perform a remote data delete operation or recover lost or stolen computers backed by a $1,000 recovery guarantee provides a strong measure of protection against increased costs and the possible breach of sensitive student records.[2]

Laptop Theft Affects Everyone

A global survey of Higher Education conducted by Gartner/Chronicle found that 63% of U.S. institutions reported stolen laptops or mobile devices, a 29% increase over the previous year.[1]

Single-point security solutions, such as cable locks or encryption, cannot adequately protect an institution's investment in mobile computers. Encryption is a good first step toward data security compliance, but it cannot recover stolen computers and rarely protects sensitive information in cases of internal theft.

Instead, a multifaceted or layered approach to mobile security and data protection is required, comprised of Compliance, Protection and Recovery ("CPR"):

- Compliance – Complying with 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 – Recovering lost or stolen devices returns them to the control of the organization or institution and facilitates prosecution

By adopting the CPR approach to laptop security, school districts and colleges can minimize the impact of computer theft, while protecting student and staff records. Computrace® computer 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.

The Changing IT Landscape

Several factors have dictated the need for a more robust approach to computer security in education in recent years. They include:

- Increased use – and theft – of notebook computers (and fewer desktops)
- Growing volumes of data stored electronically, often in portable formats
- Legislation mandating compliance with data privacy regulations
- Increasing frequency of security audits and evaluations of IT systems

The electronic storage of student and staff records introduces a new dimension to the security of increasingly mobile computers. The Health Insurance Portability and Accountability Act (HIPAA) makes schools responsible for protecting student health records stored on computers. Similarly, failure to protect student education history files stored on computers in accordance with the Family Education Rights and Privacy Act (FERPA) can result in ineligibility for future federal funding.

Another common laptop security challenge is the pilfering or swapping of memory (RAM), hard drives, DVD-writers and other peripherals. Many students today know how to remove components by opening up a computer and swapping components with lower quality, obsolete components. For example, students have been known to swap a gigabyte of RAM for sticks of 256K, gambling that the IT department will never catch up with them.

Without the aid of effective IT asset management tools, it is difficult for IT professionals to detect the theft of computer components such as storage upgrades. In many cases, whole computers can disappear unnoticed until a manual audit determines that the computer has gone missing. With robust IT asset management, every computer with an Internet connection communicates regularly to report system information, software licenses, machine configuration, location and user identity - allowing IT to locate up to 100% of their computers regardless of their location.

The Layered Approach

IT departments getting by with insufficient computer security expose themselves to unnecessary risks and potential liability. Keeping pace with the changing IT landscape requires a layered approach comprised of products, policies and procedures working in concert to provide the broadest security blanket available. They include the following:

Organizational Policy – Guidelines for the use of computers and the information on them publicized across the institution.

Physical Deterrents – Use of visual theft deterrents such as cable locks and locking carts as well as educating computer users on the safe storage of laptop computers.

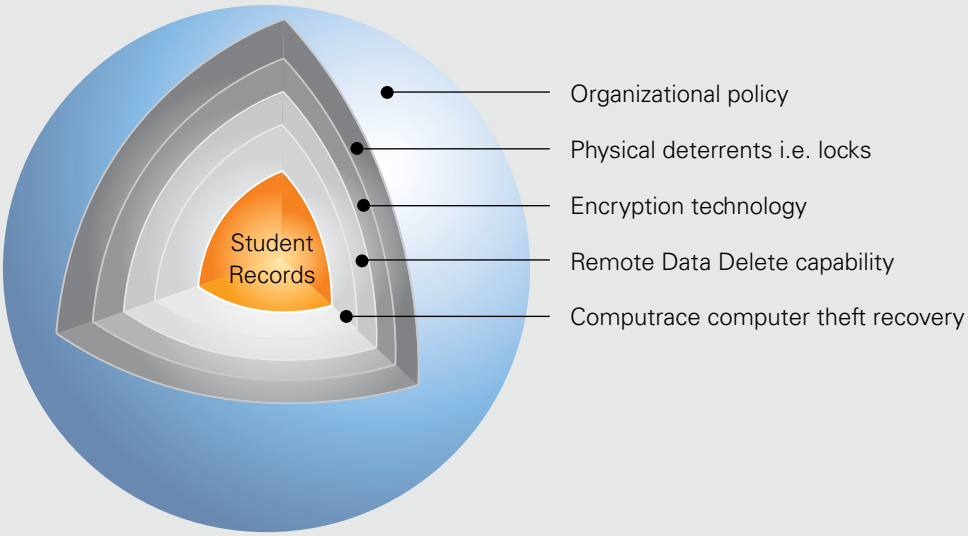
Data Encryption – Protecting information stored on mobile computers with encryption technology.

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

Theft Recovery Software – Technology that assists law enforcement by pinpointing the location of a lost or stolen computer.

To ensure the safety of student and staff information, school districts must provide layers of protection for sensitive information such as student health records – each layer working to bolster protection. The highest level of protection includes: thoughtful organizational policy and education, physical deterrents, secure IT asset tracking, encryption, remote data delete and theft recovery capabilities.

A Layered Approach to Computer Security



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

Encryption tools can lessen the impact of lost or stolen laptops, however, most encryption tools are too expensive or impractical for use in education. Students, teachers and many school board administrators cannot afford the time, implementation costs or maintenance fees to maintain an effective centralized encryption system.

Instead, they often default to a more affordable option, such as the bundled encryption tools offered by Microsoft with their Windows operating systems. Microsoft Vista provides BitLocker Drive Encryption (formerly known as full-volume encryption), while Encrypting File System (EFS) is available with Windows 2000. These encryption solutions can be effective, but most rely on user diligence to achieve acceptable levels of performance. Encryption schemes therefore often fail due to the simple fact that the vast majority of users encrypt their files as often as they back them up – which is almost never.

Data Encryption = A False Sense of Security

Gartner estimates that 70% of security breaches occur as a result of internal sources who have access to encryption keys - suggesting that encryption may only be effective in as little as 30% of all incidents.[3] 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 it will not be compromised.

A dishonest staff member 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 information, even though the company had a policy of conducting extensive background screening of its employees.[4]

Encryption Cannot Track & Recover Assets

Returning a missing computer to the control of school IT professionals is a powerful capability in terms of both data security and public relations. Encryption technology does not assist in tracking or recovering computers. Without the ability to physically recover lost computers, schools may struggle to prove that data on lost computers remains encrypted.

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.

Regulatory Compliance: A New Challenge for IT Professionals

As the managers of information from a wide-variety of sources, school districts must protect student and staff information in order to comply with state and federal regulations. Here are some of the regulations pertaining to K-12 and higher education:

Compliance-Related Statutes

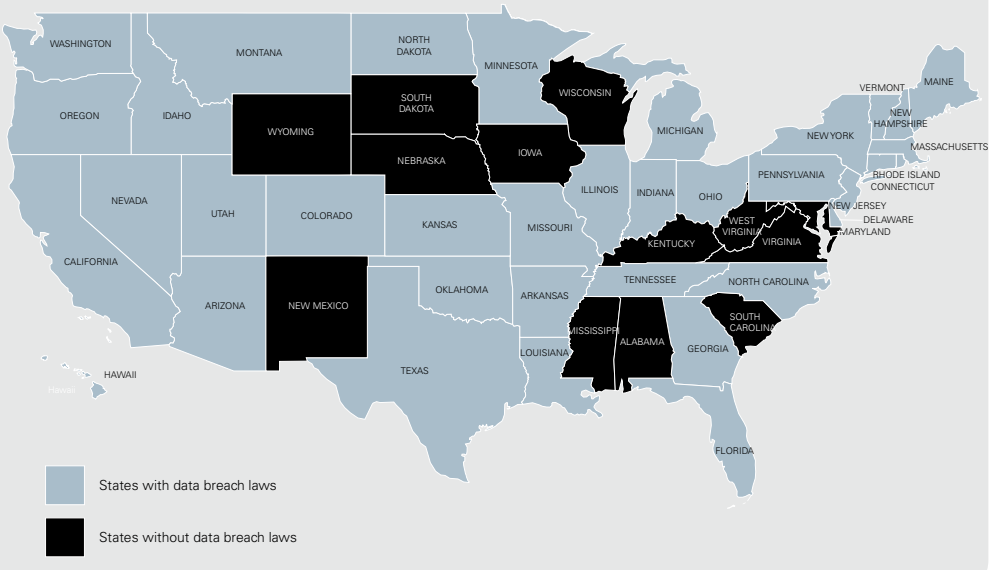
FERPA is a federal law protecting the privacy of student education records, and applies to all schools receiving federal grants under an applicable program of the U.S. Department of Education. Schools can face serious penalties - such as institutional sanctions or loss of federal funding - if records are released for purposes other than those explicitly permitted.

Title 1 Education Funding of the No Child Left Behind Act of 2001 (formerly known as ECIA, ESEA or Chapter 1) is the largest federally funded educational program, and has helped provide network cabling, computers and software. Title 1 provides supplemental funds to school districts educating economically disadvantaged students. Careless treatment of assets purchased through Title 1 can result in suspended funding privileges.

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 applies to organizations - including schools - that process, transmit or store protected health information. Most districts maintain student medical records on at least some of their computers; noncompliance carries significant civil and criminal penalties.

California Senate Bill 1386 requires all organizations in the state of California 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. The bill applies beyond California as it pertains to any business holding data on a California resident. More than 36 additional states have since adopted similar legislation.

Data Breach Legislation has been Enacted in 37 US States



Internal Drift: The Silent Killer of Technology Budgets

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 institution or school district.[5] Assets are taken out of service (broken or obsolete), locked away in the bottom of a filing cabinet and forgotten, or handed down internally to junior employees or the next class of students. Regardless of why devices go missing, some are likely to contain sensitive or confidential data – information for which the school is ultimately responsible and liable. In cases like this, remote data delete capabilities can be efficient and effective; they can also provide proof that the data has been deleted.

Increased portability means increased convenience - and increased risk of loss or theft. Laptops are easy targets: they are expensive, easy to sell and they are highly portable. The problem will likely worsen over time as notebook use increases and thieves become more sophisticated in their methods.

Data Protection with Remote Data Delete Tools

Government legislation such as CA 1386 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 institution can avoid potentially damaging publicity or litigation. Remote data delete tools such as Computrace can remove data at the file, directory and/or operating system (OS) level.

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. Data delete operations can also 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.

Tips for Managing Laptop Computers in Schools

1. **Physical theft protection**. Physical deterrents and common sense can provide a valuable first line of defense in the protection of company laptops. Keep laptops inconspicuous while they are out of the classroom by covering them when in cars, locking them out of sight and avoiding carrying them in tell-tale laptop bags. Take advantage of physical deterrents such as cable locks, which can slow or deter thieves but, like car door locks, shouldn't be relied on to prevent a computer theft.
2. **Accurate asset management.** Knowing where all your computers are, what is installed on them and who is using them is a powerful security measure. Seek asset management systems that can track your laptops regardless of their location.
3. **Post-theft plans**. Consider what would happen if a laptop containing sensitive data was stolen. Imagine a criminal scrolling though the files wondering what value they can derive

Getting to the Source of the Problem

If law enforcement officials are able to locate and recover a stolen computer, they 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. By recovering a device, the IT department contains the problem and minimizes future exposure. 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. Institution-wide policies that include strong disciplinary action for misuse of computer assets, coupled with successful theft recoveries, are an effective combination.

Good Grades from Law Enforcement

"I was very impressed by the Computrace solution. The staff at Absolute Software were very efficient and provided me with a regular flow of information on the stolen computer's location, enabling an easy recovery of an expensive laptop. After personally observing how well Computrace works, I have recommended it to numerous schools and businesses in my jurisdiction."

– Lieutenant Dennis Raucci, River Grove, IL

"Our division has found Computrace to be essential in tracking down stolen computer property. In all cases where Computrace pinpointed the location of a stolen computer, we were able to recover the PC and identify the culprit. When PC theft occurs, the information provided by the Absolute Recovery Team sure makes our jobs a lot easier and a lot more interesting."

– Detective Colin McDonald, Toronto Police Service

Arizona's Fastest-Growing School District Moves to Offer Laptops in the Classroom

Headquartered in the cities of Surprise and El Mirage, Arizona, Dysart Unified School District (DUSD) is Arizona's fastest-growing school district. Despite the district's extremely rapid expansion, it remains focused on its mission of "Increasing in Excellence" – or, preparing students for life in the new century. Recognizing that technology will play a major role in the livelihood of its K-12 students, the district is moving aggressively toward making laptop computers an everyday learning tool for its 23,100 students.

The move toward laptops is evident in the district's work with its computer supplier. In 2006, the school purchased 1,000 desktop and 300 notebook computers. One year later, the emphasis on laptop learning was obvious. In 2007, the district purchased more than 1,700 laptop computers with a goal of putting 5-6 in selected district classrooms.

To keep watch over its new computers, the district's IT Director Evan Allred and his team turned to Absolute Software. "Having made a major investment in new laptops, one of the options we had for keeping track of them was ComputraceComplete from Absolute Software," said Allred. "It uses the Internet to help us track each computer, where it is located, who is logging in and, should one go missing, where it has been taken. We just report the missing computer to Absolute and they work with local law enforcement to find it and recover it for us. We can also inventory our computers at any time – which is an amazing feature for helping us with our budgets and appropriately allocating new computers to schools."

The First Test

"We knew the school construction process would bring countless people onto our campuses and that would create a security vulnerability in the district. It wasn't long before one of our teachers had her laptop stolen."

After a weekend construction project at one of the district's schools, a teacher discovered her laptop missing when she returned to her classroom on Monday. Realizing her computer had been stolen, she reported the theft to the school district. District administrators alerted Absolute's Recovery Team. Within a few days, the computer called into Absolute's Monitoring Center and reported its location. Local law enforcement used that information to secure a search warrant for the home of a contractor who had done some work at the school. When confronted, the contractor said they had purchased the laptop from another contractor affiliated with the school for $300.

Next Steps

Dysart Unified School District plans to continue the expansion of its successful laptop learning initiative and hopes to largely phase out desktop computers for classroom use. "The need for mobile computing is here to stay in today's K-12 classrooms, and the technology for protecting and managing them in the school environment is now readily available," says Allred. "The combination of laptops and ComputraceComplete is proving to be a great package for supporting our laptop learning programs."

Computrace from Absolute Software forms an ideal platform for supporting a multilayered approach to computer security in schools. Perfectly complimenting organizational policy and encryption technologies, Computrace addresses several major security challenges for educational institutions including:

Accurately Inventorying Computers – By logging into the Online Monitoring 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.

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

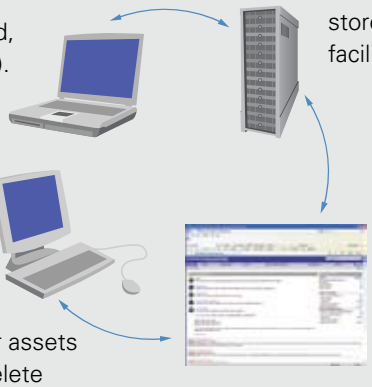
Policy Enforcement – Computrace can detect unauthorized software installations, missing hardware and can report on software installed – allowing IT departments to ensure that key programs such as antivirus are current.

Lifecycle Management – In addition to remotely deleting information in emergency situations, Computrace can be set to automatically delete data from computers at lease end or at a pre-determined retirement date. This helps ensure compliance with HIPAA data delete requirements.

The Computrace agent is built into computers from the world's major computer suppliers during the manufacturing process. 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. 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.

How Computrace Works

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

References

[1] Marti Harris & John Girard, *Stolen Laptops Denote a Growing Data Security Breach for Higher Education*, March 10, 2006, Gartner.

[2] Certain conditions apply. For full details visit: www.absolute.com/pdf/eula.pdf

[3] Gartner, 2002.

[4] 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

[5] Absolute Software Corp., installed base data, 1998-2004.

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

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

Toll-Free: 1 800 220 0733 (US & Canada)
Tel: 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.