Sign up for the
K-12 Newsletter
GO
Enter
your email address above

BEST PRACTICE

Stop, Thief!

Software helps schools track lost or stolen notebooks.

Karen D. Schwartz

Like corporate America, the K–12 community isn't immune to data leakage from stolen or lost notebooks. And as school districts throughout the country deploy one-to-one computing and the number of notebooks in schools — both inside and outside the building — increases exponentially, IT departments have had to take extra measures to recover lost or stolen units.

Evan Allred of Dysart (Ariz.) Unified School District protects his district's thousands of PCs by using tracking software.

STEVE CRAFT

Last year, Dysart Unified School District in Surprise, Ariz., began outfitting classrooms in its 23 schools with HP 6715b PCs with 80-gigabyte hard drives, 1GB of RAM and AMD dual core processors running Windows XP Professional. The district sought to provide six notebooks for every K–8 classroom and one notebook for every two high school students.

Because of the massive amount of HP notebooks Dysart bought, the potential cost of loss and the desire to remain fully accountable to taxpayers, the district decided to install Absolute Software's ComputraceComplete theft recovery, data protection and secure asset-tracking solution on each of its notebooks. The features, plus the company's guarantee to reimburse customers up to $1,000 for any notebook that couldn't be found, sealed the deal.

Today the program is a work in progress, with most of the 3,300 notebooks distributed either within the classroom or to the 175 administrative staff. The district plans to purchase more over time. Eventually, depending on available funds, each of the nearly 5,500 high school students will be issued his or her own notebook, says Evan Allred, the district's director of information technology.

Keeping track of that many notebooks is complex, and it was quickly becoming clear the job was too big for the IT staff — at least, without some help.

Losses because of U.S. notebook theft totaled more than $6.7 million in 2005, according to the FBI.

"We often had the feeling we were losing assets and didn't even know it," says Michelle Benham, the district's technology services supervisor. "In one case, someone saw someone else using a Dysart-owned notebook and knew they hadn't come by it legally. That laptop was returned to us, but we realized we hadn't even known it was missing."

Data Protection Concerns

Clearly, something needed to be done, not only to keep track of the physical units, but to make sure sensitive information didn't fall into the wrong hands. While justifying the need to track the physical units wasn't difficult — losing just one costs the school district $1,000 — the need to protect data also was an issue.

Two notebooks containing 40,000 names and Social Security numbers of Chicago Public Schools employees were stolen from the school district in 2007 and never recovered, according to district officials.

Students are provided network storage for their needs, so most students today use notebooks more to access information and programs. But administrators and teachers have more leeway. And once

Current Issue
Mar/Apr 2009
In With the Good — Out With the Bad
Uptime Rules of Thumb
A Data Center Turns Inward
TOC

the district meets its goal of furnishing each high school student with his or her own notebook, the pressure will rise, Benham says.

Educators shouldn't give short shrift to data protection, warns Rob Enderle, a principal at Enderle Group, a San Jose, Calif., technology consultancy.

"Laptops can contain critical information about a class or personal information about students; information that uniquely identifies a child or could make them a victim of harassment, and information about parents and siblings that could put other family members at risk," he says.

Take, for example, a school nurse or special-ed administrator who stores files with confidential health information about students. A data breach could fall under the Health Insurance Portability and Accountability Act. A teacher could inadvertently offer someone a stalking blueprint if he enters a student's grade, the time she gets home and her special dietary needs.

Peace of Mind

Here's how ComputraceComplete works: A dormant Computrace software agent is embedded in the BIOS of most leading notebooks. (This feature is added by most manufacturers as a part of the manufacturing process.) The agent hibernates until an organization purchases a license, and then it's activated. Each activated notebook is programmed to call in via the Internet to report its status once each day; if it doesn't call in, the organization knows there may be a problem. To determine exactly where a particular notebook is at a particular moment, a staffer simply consults a dashboard portal, clicks on that machine, and then can identify where the machine is calling from or the history of where it has called from over a specified period of time. If someone suspects a machine has been stolen, the system can be configured to request additional information the next time it calls into the system.

Once every student has a notebook, the pressure is on to secure those assets, says Dysart's Technology Services Supervisor Michelle Benham

STEVE CRAFT

And the system clearly works for Dysart Unified School District. This past year, a teacher at one of Dysart's K–8 schools discovered one Monday morning that her notebook was missing. The theft was reported to the police as well as to Absolute. Because the computer had been reported as stolen, Absolute configured its system so that the next time the computer called into the system, its software would record and report additional information about how and where the notebook was being used. With that system in place, it soon was discovered that the thief had transmitted personal information — information that led the police to recover the notebook and return it to the school district.

When a school district reports a theft, it can decide if it needs to remotely delete files, the entire hard drive, or the entire hard drive and operating system. That process is accomplished with two-factor authentication. When a qualified person initiates the data delete, it triggers the delete process the next time the machine calls in.

That's exactly what happened in the case of one Dysart notebook, which traveled all the way to Guatemala under suspicious circumstances. "The only option for that laptop was the data delete, since it wasn't possible to work with the law enforcement in that country," Allred says.

The system also can be used in the opposite case — to verify that a notebook has not been stolen. In several situations, teachers might report to Benham that a notebook is believed stolen. The first thing Benham does is look up the notebook's ID number in the system to determine when it was last used and if it's still being used.

"There have been several cases where I've been able to tell them that the laptop is still in use at their school and tell them who exactly is logged on at that time," she says.

Although many school districts use Computrace specifically to protect laptops, it also can be used for other tasks, such as tracking inventory. The solution gives organizations the ability to locate computers on and off the local network and inventory their hardware and software, including version information.

That capability is one of the main reasons, along with the ability to recover stolen computers, why Kent School District in Washington state chose to implement Computrace. The K–12 district, with 40 schools and about 27,000 students, implemented the solution in 2006.

By using the system to keep track of the school district's more than 10,000 HP desktop and tablet PCs, the annual inventory process has been reduced from a 10-person, three-month project to a simple five-minute report.

"We used to have 10 people with barcode scanners attempting to find 10,000 computers. At best, we were achieving 70 to 75 percent accuracy in this process, and at great effort," says Thuan Nguyen, Kent School District's director of information technology. “Now we always know where our computers are. That’s accountability.”

Dysart also uses the system’s asset-tracking features, with good results. “When we do our physical inventory once a year, it’s hard to be sure that we have accounted for every laptop at a school. This way, we have another data source that can help triangulate the information so we can be sure we’re tracking everything accurately,” she says. “And on the software side, it will also help us be sure that as we upgrade all computers to Microsoft Office 2007, no laptops are inadvertently missed.”

The system is working smoothly today, which means Dysart is well- prepared for the day three to five years from now when all 5,500 high school students will be issued notebooks for use at school and home.

“We would expect that with more laptops being used by more people off campus, there will be more incidents of [computers] being lost and stolen, and that reinforces the need for the software,” Allred says.

Other Security Solutions

There’s more than one way to protect your school’s notebooks. Here are some other options.

There are low-cost, low-tech solutions that can make a big difference. Installing a notebook security lock, for example, from companies such as Kensington Computer Products Group, Belkin International or Brenthaven, is an easy way to boost security. Notebook security cabinets and carts from Datamation Systems, Plug-In Storage Systems and others are also available.

One step up the ladder are products such as Targus Group International’s DEFCOM 1 Ultra Notebook Computer Security System, which combines a stainless-steel cable, motion-sensor technology and a 95dB alarm to create a combination locking alarm system that attaches to a notebook.

For more comprehensive protection, consider whole-disk encryption — a method of ensuring that data stored on hard drives are not readable or accessible by unauthorized users. Manufacturers with whole-disk encryption products include Absolute, SafeGuard Scientifics, PGP and GuardianEdge Technologies.

GuardianEdge also has other solutions for notebook security, including Device Control, which allows organizations to control access to connections, ports and attached devices; and Device Control Auditor, which provides organizations with facts about the devices and networks to which the notebooks are connected, allowing better identification of threats.

When deciding on what type of notebook protection technology to implement, Rob Enderle, principal of IT consultancy Enderle Group, recommends making sure solutions are automatic and can’t be easily removed. Combining two types of solutions, such as whole-disk encryption and notebook security locks, makes a lot of sense, he says.

Tracing a Stolen Notebook

In December 2007, the ComputraceComplete system generated an alert. The IT staff at the Dysart Unified School District in Surprise, Ariz., picked up the signal that a school-owned notebook’s name had been changed. That immediately raised a red flag, and the IT staff reported it stolen to the Maricopa County Sheriff’s office, as well as to Absolute Software, which began the process of tracking down the unit. In February 2008, the notebook was found in the possession of a construction worker who had been working on a new school in Waddell, Ariz., about 13 miles away from Dysart. The notebook was returned to the Dysart IT department in March by the Sheriff’s office, and once the standard district software image was reinstalled, it was returned to the school’s inventory.