



SECURITY

Keeping Students and Systems Safer

Anytime anywhere learning provides opportunities to create digital learning environments for new teaching styles and personalized learning. As part of making sure the program is effective, the safety and security of students and assets are essential—and mandated by law.

The Children's Internet Protection Act (CIPA) addresses Internet content and requires that schools that receive funds from the federal E-rate program must install protection. The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records.

All things are stored digitally today—from a district's records to students' work, and it all lives on the network. Access to information is fast, accurate and useful as a result, but districts must guarantee that everything is protected. Security measures include the provisions made in the district's network infrastructure and policies adopted by the network administrator to protect the network and network-accessible resources from unauthorized access.

Network Security

There are multiple standards-based approaches to ensure network access security can be applied and co-exist. A recent safety index report states that monitoring access to district records and email helps prevent data breaches and deters unauthorized access to the network. 66% of districts are protecting their networks from unauthorized software and viruses by preventing outside devices from accessing the network. In addition, security software can be embedded in the BIOS or firmware of notebook PCs and desktops for hardware security and asset tracking.

Wireless Security

The freedom and mobility of wireless networking is what gives students the opportunity to expand their learning. When districts launch a one-to-one program, they must address new security needs, including the physical security of notebook PCs and tablets being transported from school to home and to other locations. Security needs also include protection against viruses, spyware, and unfiltered Internet access. Student notebook PCs should have updated protection software and prevention against using unsecured networks.

Sponsored by:



AbsoluteSoftware

About the Fundamentals of K-12 Technology Programs

Brought to you by *Tech & Learning* and sponsored by HP, this new series will cover the educational technology topics that matter most to the profession's leaders, practitioners, and innovators. Look for the other issues, where we address key subjects such as Anytime, Anywhere Learning, Infrastructure and Networking, Educational Technology Leadership, 21st Century Learning and Assessment and others.

For more information, go to

<http://www.techlearning.com/K12/Fundamentals>

Ten Tips for Internet Safety

It isn't always easy to find the balance between protecting students from Internet dangers and distractions and reaping its benefits—but it's certainly on every district's tech priority list. Here are suggestions for keeping students safe online.

1. Get technological safeguards such as filters—both hardware and software—in place.
2. Put together a cyberspace safety curriculum for parents.
3. Take advantage of already available Internet-safety education programs.
4. Write an acceptable-use policy for staff and students and adopt discipline strategies for violations.
5. Put an "early-warning system" into effect.
6. Encourage teachers to become part of the virtual world.
7. Use the Internet inside a "walled garden."
8. Install an image library with appropriate materials.
9. Create a repository for information about what works.
10. Encourage parental involvement as a critical element, especially for use of social-networking sites like MySpace.

Tips for Managing School Notebooks

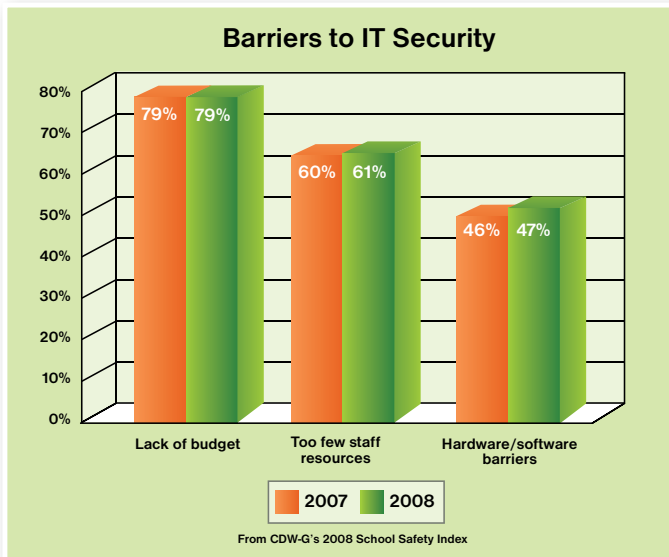
1. **PHYSICAL THEFT PROTECTION.** Physical deterrents and common sense can provide a valuable first line of defense in protecting notebook PCs. Keep notebook PCs inconspicuous while they are out of the classroom and take advantage of physical deterrents such as cable locks.
2. **ACCURATE ASSET MANAGEMENT.** Know where all your computers are, what is installed on them and who is using them. Seek asset management systems that can track your notebook PCs regardless of their location.
3. **POST-THEFT PLANS.** Consider what would happen if a notebook PC containing sensitive data was stolen. Put measures in place to recover lost notebooks and, failing that, delete the information on them.

Case Study: Dysart Unified School District

Dysart Unified School District (DUSD) is Arizona's fastest-growing school district and it is moving aggressively toward making notebook PC computers an everyday learning tool for its 23,100 students. To manage the growing number of notebook PCs, the district implemented Absolute's IT asset management and notebook PC recovery software. The software was installed to deter theft and help recover notebook PCs should they go missing. This turned out to be money well spent when the school district experienced its first notebook PC theft since implementing the program and the computer was recovered within two weeks.

School Safety Index

A recent report shows that school districts improved their physical safety score by 39% over 2007 while their cyber safety score declined by 25% in the same time period. More than half of districts are using network access control to protect data and ensure that only authorized users and approved applications access their networks. However, budget constraints, lack of staff resources and the need for more IT tools cancelled out districts' efforts to improve cyber safety.



KEY FINDINGS INCLUDE:

• New Tools Lock Down the Network

Districts are actively using new tools and techniques to improve cyber safety, including network access control (NAC), to ensure only authorized users and applications can access the network.

• Barriers Still Loom Large

Despite the availability of tools to improve cyber safety, IT security breaches are up, and one-third of districts reported that their networks are vulnerable to attack. Budget constraints and limited staff resources are also barriers to improving cyber security.

Security Technologies

There are a number of security technologies that encrypt transmitting signals such as WPA (WiFi Protected Access). In addition, you can encrypt the data itself with SSL (Secured Sockets Layer). There are multiple standards-based approaches to network access security that can be applied and co-exist, including 802.1X, web-based authentication and wireless data privacy with virtual private networks (VPNs). And enterprise-class network switches can recognize who a user is and the types of services and access they are authorized to have. This means that any unauthorized traffic is stopped before it can cause harm.

The most secure methodology is to limit access to just those who require it and lock out all others. The Wireless Access Points (WAP) should be outside the firewall and require VPN to get in. If that's outside the capabilities of your school, at least implement the WPA encryption and watch for "rogue" WAP's being attached to your wired network.

CLIENT MANAGEMENT SOFTWARE

Client Management software enables the IT department to more effectively manage the influx of new devices and is an important part of reducing the labor costs of supporting a one-to-one initiative. Select a comprehensive client management tool that automates the five key functions for desktop management support: software distribution, IT asset management, remote control, PC backup, and settings and configuration management.

ANTI-VIRUS SOFTWARE

It is important to protect the district from outside viruses, worms and Trojan horses when students take notebook PCs home. Establish an anti-virus package standard and be sure to include updates for the life of your one-to-one program. The virus definitions and updates should be able to be pushed to the notebook PC without student intervention and if possible, without intervention from the school technology staff. Don't depend on students to update their virus definitions.

FIREWALLS

In addition to district servers, individual notebook PCs should have a personal firewall, whether it is the one that is included in the operating system or a standalone product. These applications are intended to protect the notebook PCs from Internet hackers and shield student identity and privacy.

ANTI-SPYWARE

Anti-spyware protects you from external threats. Spyware can secretly capture and transmit personal information, make unwanted changes to system settings, and be the source of unwelcome pop-up ads. Anti-spyware has the ability to block, and to reverse the effects of these types of intrusions.

FILTERING SOFTWARE

Many districts install Web-filtering software that limits the sites that a student can visit. These applications must keep a district in compliance with Children's Internet Protection Act (CIPA) requirements. There are several products, and they each approach the issue differently. Almost all have provoked controversy, basically pitting those who want to protect students from harm on the Web to those who stress personal responsibility and teaching appropriate use.

PROTECTING COMPUTERS

Districts need an affordable and effective computer security and tracking solution that provides reliable visibility into every computer in the district – leading to enhanced security, control and regulatory compliance. Computrace® from Absolute Software is a guaranteed computer theft recovery, data protection and secure IT asset

management service that enables IT professionals to centrally track and manage up to 100% of their district's computers – even while they are off the network in the homes of students and staff.¹

Computrace helps schools and districts demonstrate accountability by:

- * Monitoring notebook use and productivity regardless of physical location.
- * Working with local law enforcement to track and recover stolen or missing computers.
- * Generating asset reports for upgrades, roll-outs and computer retirement.
- * Generating daily reports on unauthorized software use.
- * Remotely deleting data to protect student privacy and files.
- * Includes a Service Guarantee of up to \$1000 if a computer isn't recovered.²

Being able to quickly and accurately inventory laptops as well as recover those that go missing lowers the district's total cost of ownership (TCO) and keeps schools compliant with privacy regulations.

OTHER STRATEGIES

Firewalls and filters will provide security only up to a point. Some of the threats require different strategies such as educating students about ethical behavior online, requiring them to sign an Acceptable Use Policy, and enforcing the rules consistently. Schools also need to get parents and staff involved and informed to prevent such behaviors as cyberbullying. A number of Web sites provide information that help schools to address the social, legal and ethical issues associated with technology use, teach ground rules for online behaviors that are acceptable, appropriate and effective, and involve families.

An Ounce of Prevention

Here's a list of practices that can help prevent security disasters and control the damage in the event that an attack happens.

BACKUP DATA

Your IT department should have a backup policy that is coordinated with a disaster recovery plan.

KEEP SENSITIVE DATA BEHIND FIREWALLS

Sometimes information that doesn't need to be accessible from the outside world sometimes is, and this can make the damage from a break-in worse.

USE REDUNDANCY

Redundancy can help you protect your district from having a minor security breach become a catastrophe.

KEEP PATCHING

Watch the vendors' security advisories and install patches. Exploiting old bugs is a common means of breaking into systems.

WATCH FOR SECURITY ADVISORIES

In addition to watching what the vendors are saying, keep a close watch on groups like Carnegie Mellon University's Computer Emergency Response Team. Make sure that at least one person is subscribed to these mailing lists.

HAVE SECURITY ADVISORS

Task someone with keeping up with security developments. This need not be a technical wizard, but could be someone who is simply able to read advisories from various incident response teams, and advise what to do.

“With increased portability, comes increased opportunities for theft, and keeping track of computers that are no longer bolted to a school desk becomes challenging. We wanted to use technology to help us deter theft, track our notebook PCs and recover those that went missing... It wasn't long before one of our teachers had her notebook PC stolen.”

– Evan Allred, Director of Information Technology,
Dysart Unified School District

Network Threats

UNAUTHORIZED ACCESS

The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, student records should be off limits unless an IT administrator is sure that the person making a request is someone who should get it.

Attackers can gain access to your equipment through any connection that you have to the outside world like Internet connections. A system cracker might look for passwords, data, phone numbers, vulnerabilities and anything else that can allow access to sensitive data.

CONFIDENTIALITY BREACHES

Student records, staff data, and financial information are all items that districts need to protect against unauthorized access. It's possible that compromise of a normal user's account on the machine can be enough to cause damage. For example, student hackers who change their grades have compromised the system, and it won't be clear what other data might have been falsified.

DESTRUCTIVE BEHAVIOR

Among the destructive sorts of break-ins and attacks, there are two major types. In one case, the break-in isn't obvious and the attacker can have long-term access to data such as Social Security numbers, student data, and other information and might compromise a good portion of the system. The other type is discernable because there's destruction. As long as data is backed up, there's no long-term damage.

DATA DESTRUCTION

Perpetrators can destroy or delete data. In these cases, the impact on your computing capability – and consequently your effectiveness – compares to the results of a fire or other disaster causing your computing equipment to be completely destroyed.

ANONYMOUS PROXIES

Students, staff and spammers are becoming increasingly sophisticated at breaching security measures. A new threat is when students use anonymous proxies—Web sites or applications that allow users to access other sites through them—to tunnel through districts' filtering systems to avoid blocked sites. Acceptable use policies, better filtering and security tools can help fight this battle.

Security Planning Step by Step

When you are planning for technology, what you need is security architecture and an approach that will evolve continually as the threat environment changes over time. Here's a look at methods and tools to help you minimize the risks to your network.

STEP 1: DOCUMENT

To measure the strength of your security solutions, document what you are doing now and test how well your current setup works. The two types of security are preventative and detective controls. Strong and effective preventative controls are superior to detective controls.

STEP 2: TEST CONTROLS

Once you have documented how you are controlling your environment, you should test the controls in order to verify that both the design and execution are effective.

STEP 3: IDENTIFY MISSING OR INEFFECTIVE CONTROLS

After you document how you control the environment, you will see gaps that should be fixed. Create a list and find solutions to remedy them.

STEP 4: CONSIDER COST

Include hardware, software, implementation, and ongoing maintenance costs in your estimates and seek ways to revamp your security infrastructure at the lowest cost. Tools to prevent unwanted access to your network are critical.

STEP 5: ENSURE OPERATING SYSTEM SECURITY

The first line of defense is the operating system and the policies you have implemented that are built into it. Leverage the security built into the OS.

STEP 6: STRENGTHEN THE PERIMETER

A strong perimeter and a modern, up-to-date, well-configured firewall are critical pieces of your security framework. Keep in mind content filtering and egress filtering for preventing the initiation of connections from the inside of your network to undesirable locations on the Internet.

STEP 7: PROTECT WEB APPLICATIONS

Employ firewalls that prevent exploitation of weaknesses in Web-based applications by learning what is normal behavior and preventing abnormal behavior.

STEP 8: SECURE REMOTE ACCESS

If you allow staff and students to have remote access into the school or district network, either for e-mail or in order to access school applications or files, make sure that all remote connections into the school or district network are made through a secure connection and authenticate users.

STEP 9: IMPLEMENT DETECTIVE TOOLS

Employ tools such as anti-virus software that narrows the window of vulnerability and monitors threats. Consider using different products for server, e-mail, and desktop anti-virus. In addition, multiple layers of anti-virus defense should exist: at e-mail gateways and servers, on other servers, desktops, and possibly at the Internet gateway.

STEP 10: LOOK AT ANTI-SPAM SOLUTIONS

Stop the spam at the edge of your network in order to minimize the use of services to handle it. If you stop the spam even before it hits the mail server, the mail server can deliver and route appropriate e-mail more easily.

STEP 11: CONSIDER ANTI-MALWARE

Employ spyware, adware, and trackware solutions to protect against infections.

STEP 12: REVIEW INTRUSION DETECTION/PREVENTION (IDS/IPS)

Intrusion detection solutions monitor your network and systems for anomalous behavior and then alert you that the behavior has occurred. Intrusion prevention goes one step further and attempts to prevent the unwanted behavior. An IDS/IPS solution can help you detect and solve problems quickly.

STEP 13: CHECK OUT NETWORK/SERVER LOGGING & ALERTING

A network/server logging and alerting tool can help you see what's happening and take action if someone is attempting a brute force attack on an administrative password or if someone is using a large amount of bandwidth over a long period of time.

STEP 14: ENSURE WIRELESS SECURITY

Employ wireless security solutions, such as VPN or WPA for users connecting to your wireless network, and use wireless network monitoring tools to monitor rogue access points and rogue users.

STEP 15: PROTECT PHYSICAL IT ASSETS

In addition to digital asset management, districts must do physical asset management to protect the financial, contractual and inventory functions that support life cycle management and strategic decision making for the IT environment.

¹ The CompuTrace agent is shipped turned off, and must be activated by customers when they purchase a subscription. Subscriptions can be purchased for terms ranging from one to four years. Service is limited, check with Absolute for availability outside the U.S.

² The Absolute Recovery Guarantee is a limited warranty. Certain conditions apply. For full details visit: www.absolute.com/pdf/eula.pdf. Data Delete is an optional service provided

by Absolute Software. If utilized, the Recovery Guarantee is null and void. In order to use the Data Delete service, customers must first sign a Pre-Authorization agreement and then purchase one or more RSA SecurID tokens from Absolute Software.

Note: Some of the lists included in this report were compiled and adapted from Tech&Learning resources.

