

A Beginner's Guide to School Security

(Published in TechLearning magazine, 9/15/2003)

By: Wesley A. Fryer

While the creation of a global computer network has brought a wealth of new resources and opportunities to education, it's also opened a Pandora's box of security concerns for district technology staff and other administrators. From students downloading unauthorized software to the threat of viruses destroying sensitive school data, network vulnerabilities are an ever-increasing concern for schools. The good news is that as the diversity and volume of network security dangers increases, the sophistication of tools designed to monitor and protect technology users and resources grows along with it.

The potential for security breaches depends on many factors, including the overall design of the network, the authorized public services running on it, and the behavior of users (both staff and students) within the school or district. Thus, regular security audits, vulnerability assessments, and reviews of established security policies are musts for your technology plan and budget.

Because of the many facets and levels of security, it is a complex topic to tackle comprehensively in one article. This month, we offer a preliminary look at the topic by introducing six major areas you'll want on your security "radar screen" when developing an initial strategy. In succeeding articles on security — watch for our follow-up series this winter and spring — we'll turn our focus to more practical, how-to aspects.

Problem: Ensuring administrators, teachers, and students have access to appropriate network resources.

Solution: Develop a network rights strategy.

When it comes to discussing security, a logical place to start is with how to configure user accounts. Specifically, who should get access to what areas of the network? As a general rule, role-based access works well in a school setting. This means users are granted access rights according their instructional or administrative needs. For example, while teachers might have full rights to a "templates" or "lessons" directory on the network, allowing them to add or edit saved files, students are usually restricted to read-only access in these areas.

Access to areas on the network will vary. For instance, areas containing student assignments can be shared, while other areas remain private and protected. An example is a "home directory." A home directory is a folder to which only the person logging in to the network has access. Home directories (also called home folders in some cases) are usually set up for each user on the network file server. By using a home folder, students and teachers can save their files securely. While in some cases teacher accounts may be given access rights to student home directories, it goes without saying that student users should not have access rights to teacher home directories.

Electronic grade files, like all other computer files, are most secure when saved in a network home directory. Because of their sensitive nature, grade files need to be properly password protected.

To ensure this, teachers should take care not to post user IDs and passwords on computer monitors or in a desk drawer easily accessible to students. Likewise, network administrators need to set up classroom computers to log off automatically or default to a password-protected screen saver after a period of inactivity.

Problem: Balancing instructional needs with desktop security.
Solution: Manage — without completely restricting — desktop computer activity.

Restricting teachers' ability to install programs on their classroom computers may reduce the number of technical support calls to fix software problems, but it can also impede teachers from using their computers flexibly for instruction. One "middle ground" solution is to use desktop security software offered by such companies as Fortres Grand and Faronics that maintains or automatically restores a computer's original software configuration upon reboot (go [here](#) for a list of security products). The upshot is educators and students can use the applications they need but are prevented from permanently changing system settings. Another approach is to re-image classroom computers with software like Symantec's Ghost or Altiris' Carbon Copy on an annual and "as needed" basis. Re-imaging a computer means replacing the contents of the entire hard drive (except for a small, protected partition in some cases) with a clean, uncorrupted "image" of the operating system and standard applications.

Software auditing is also an important issue related to desktop control. Districts have a legal responsibility to ensure all software installed on district computers is licensed. To help meet this formidable demand, asset management software can provide welcome assistance. Asset management tools like Novell's Zenworks and Netopia's netOctopus allow school network administrators to regularly audit applications for unauthorized or unregistered software.

Problem: Lack of accountability for student behavior on the network.

Solution: Monitor user compliance.

Internal security threats can include students hacking into student information databases or other grade files, but more often involve unauthorized use of software—in particular, peer-to-peer programs like Kazaa and Morpheus for swapping music, video, and other files. Intrusion detection software can help network administrators identify misuse of network computers within the district in addition to thwarting external threats. For example, tools like SNORT (www.snort.org), an open source freeware program that runs on Linux, notifies network administrators of suspicious or unauthorized internal activity.

IT specialists can also spot internal security problems using software that monitors and logs all network activity by IP address and user account. Electronic monitoring can take several forms and occur at different levels: at the client computer, at the e-mail server, and on the network as students or staff surf the Net. The decision to electronically monitor users, and at what level, varies widely from district to district. For those choosing to monitor user activity, information about it should be circulated regularly via school publications, Web sites, and classroom teachers.

Problem: Minimizing potential risks from external hackers.

Solution: Block unauthorized access from the outside.

Any district that's connected to the Net—which is just about everyone—should have a firewall to protect the network from unwanted intruders. Otherwise, individuals can gain access to your network and its files.

About five years ago, protection against external security threats largely consisted of locking down or opening up specific ports on the network. In the case of Internet access, for example, port 80 was opened on the

network firewall. One problem with this method is that once a port was open, a malicious user could scan the entire network for vulnerabilities and potentially access and destroy files, install applications, and otherwise wreak havoc.

The advent of "stateful" firewalls, in contrast to older "stateless" firewalls, allow network administrators to exercise much more robust control over the incoming "packets" (data broken into smaller sections) authorized to traverse the network. Essentially, these firewalls track the "state" of TCP/IP packets on the network — whether they are new, related, established, or invalid — and prevent intrusion by authorizing only TCP/IP connections originating within the organization. Proper configuration of a stateful firewall is essential for every school district, regardless of size.

Problem: Keeping public access resources safe.

Solution: Customize the firewall to meet functional requirements.

There are three services that cannot reside wholly within the district's firewall and require extra security measures: mail servers, Web servers, and videoconferencing devices. Each of these present different network security challenges:

Mail Server: District and school e-mail servers should be protected in several ways. If a Microsoft Exchange server is used, the most secure configuration is to use a Linux mail server as a mail relay. This relay connects the Exchange server to the Internet, and allows the Exchange server to physically operate within the firewall. Antivirus and antispam server tools can be installed on this Linux relay server, protecting and insulating the Exchange server in addition to client computers behind the firewall. If Linux isn't used, products like Symantec Mail Security for Microsoft Exchange can be installed. Kerio Mail server provides security not only for Windows-based mail systems, but Linux and Mac OS X systems as well.

Web Server: For Web servers, the risk of external threats depends on the operating systems and types of services being used. As most network administrators are well aware, Microsoft-only server solutions frequently require patch installs and can be susceptible to hacker attacks. Some network administrators consider alternative server operating systems (including Novell, Linux, Sun Solaris, and the UNIX-based Mac OS X server)

to offer more robust security benefits than comparable Microsoft server products. (For a more detailed discussion of servers, see "[Serving Up Success](#).") A Web server running off Windows NT or Windows 2000 is not an inherently insecure product, but if installed in its default configuration it's extremely vulnerable to external security threats. For example, by default Windows 2000 enables remote registry. This means that with the correct administrator password, a hacker can quickly gain unhampered access to the Web server. If your district is using Microsoft Web servers, make sure default features like these are disabled and reconfigured.

Videoconferencing: The H.323 videoconferencing protocol presents significant potential for external security threats. H.320 is the standard ISDN/telephone protocol for videoconferencing, usually involving paid line charges for the number of phone lines used in a connection. H.323, on the other hand, is based on Internet protocols and does not usually incur line charges beyond those already paid for data networking. With the H.323 protocol, it's not possible to check the "reply" state of an incoming packet or data. As a result, if an external user opens a H.323 connection to a resource on the network, he or she can theoretically open up other connections on the network as well.

To address this security concern, configure the firewall to allow incoming H.323 connections from only selected and predefined IP addresses. These IP addresses are essentially "trusted." By coordinating both incoming and outgoing videoconference connections in advance, districts can manage the bandwidth impact of videoconferencing applications while still meeting instructional needs.

Problem: Teachers need to use school servers from home.

Solution: Set up secure remote access.

Schools looking to allow educators and students to connect to internal server resources from home will often create a virtual private network, or VPN. A VPN is a private "tunnel" through the public network that allows authenticated users to securely access network resources from afar.

Once logged in to the VPN, a user enjoys the same access rights to network folders and other shared resources as at the school location. This can be a great benefit if teachers save their files in their private home directory or another location on the file server, and want to access them from home.

VPN solutions, like firewalls, can be hardware- or software-based, and are offered by a range of companies such as Cisco, Microsoft, and Novell. There are also "VPN alternatives" available, such as Neoteris's Instant Virtual Extranet technology. While VPN for most school districts is a nice luxury, a secure firewall is an absolute necessity.

A Final Word

Through thoughtful planning, budgeting, and staff implementation, security risks can be managed and averted. For districts, it's an area where several bytes of prevention are clearly worth many gigabytes of cure.

Wesley A. Fryer (www.wtvi.com/teks) is director of distance learning for the College of Education at Texas Tech University in Lubbock.

This article is available on:

<http://www.techlearning.com/news/0049/a-beginners-guide-to-school-security/45153>

--

This content is licensed by Wesley Fryer under a Creative Commons Attribution 4.0 International license.

http://creativecommons.org/licenses/by/4.0/deed.en_US

<http://www.wesfryer.com>

Republished in January 2014 on <http://publications.wesfryer.com>