Gloria Paproski-GSEC

Fortifying the K-12 Network: A Primer for Principals

Audience: K-12 School Administrators, school principals, School Board members, school network specialists, technical contacts.

Universities have been dealing with the problem of unauthorized access for as long as they have been networked. "For the second time this year, hackers have broken into computers at the Indiana University, this time just two weeks after the school pledged to tighten its computer security policies."(Dello). The intruders were able to download a database containing the names, addresses and social security numbers of 1,700 people who had requested information regarding the school's music program. As school districts upgrade equipment and attach to the Internet, they too will become the playground for the student hackers, the storage facility for unauthorized files, the launching center for other network attacks and other such threats. And as more information that used to be housed in locked cabinets becomes stored on computers, the issue of security becomes critical. With shrinking budgets having to cover more facilities and staffing, districts need to take a good look at how secure their networks really are. This paper will present an overview of ten areas to help school districts begin a project to fortify their networks and assets.

1) Why?
2) Needs Assessment
3) Security Policy
4) Security Management
5) Physical Security
6) Information Security
7) Software Security
8) User Access Security
9) Internet Security
10) Staff Training

1) Why?

We are all conscience of locking the doors to rooms that hold our valuables. But not providing adequate security on computer systems is like leaving the windows open with a sign that says "important stuff inside." How valuable is the data in your system? How easily is it replaced? Are you prepared and protected from natural disasters such as fire, flooding, power outages? Are you protected from physical intrusion (internal as well as external), viruses and related problems? Do you have a security policy that is enforceable? Whose job is security, anyway?

Every district has an asset management department that keeps track of the physical inventory and worth. But what about the data? Much of the data stored on a school district's system is an irreplaceable asset. It is nearly impossible to place a dollar value on decade's worth of student and staff records. Would you be able to calculate cumulative grade point averages for the graduating class if a few weeks before graduation, all grade information was destroyed or stolen? Where are the archived records stored to retrieve the graduation information from someone who graduated in 1968? Schools are very careful to check to whom records are sent to or given to in person. But who can access, modify or change this data via the computer networks. The public puts its' trust in the school system to have those important records anytime they are needed for employment, college or proof of age information is necessary throughout their entire life. Not only does this information need to be available, it needs to be protected from access by those without legal right to the data. The Family Education Rights and Privacy Act of 1974 (FERPA) is a Federal law that protects the privacy of student's education records. Schools are at risk of losing federal funding if this law is compromised.

The goal of security is to protect information and the system without unnecessarily limiting its utility. At the same time, however, unauthorized access, especially to critical systems and sensitive information, must be prevented. (nces.ed.gov) In order for this delicate balance to be achieved, three prerequisites must be in place: 1. Senior management must provide the leadership of placing security in the top priority position, 2. an empowered staff member must be afforded the time and resources necessary to carry out the task, 3. All employees must participate at all times.

The next step is to look at specific areas that need attention.

2) Needs (Risk) Assessment

"It can be a risky world out there-a single mistake can get a principal sued, a school board to forbid the exchange of vital education records, or the local legislature to deny technology funding.")nces
Before you can begin to fortify your information, you must first decide what are the assets you want protected, the threats to those assets, the areas that are vulnerable to the threats, probabilities of the threats happening and a dollar amount placed on the assets if a threat comes to fruition. The risk assessment will tell you what you have, what it's worth, what to worry about, where you are vulnerable and why you should be concerned. There are commercial vendors that conduct risk assessments or the process can be broken down into specific areas, assigned to current employees with a committee coordinating the resultant reports.

The Assets:

The computer equipment itself is the easiest place to begin since its' value is already listed on inventory reports. But the real asset is the data contained on that equipment. What is the value on student academic data, health records, financial information, state and federal reports? What would the process be to reconstruct the data and how long would it take to do so? What is the impact of late reporting or missing records because of data loss? Equipment is replaceable, many times the data is not.

The Handbook of Information Security Management contains formulas for calculating the dollars amounts involved in effectively identifying risks and for planning budgets for security management. (Krause and Tipton).

The Threats:

Threats include natural disasters such as flooding, fire, tornadoes as well as internal phenomena like high temperatures and aging equipment itself. How many times do you reuse those backup tapes?

Other area of threats include unintentional and intentional manmade threats. Unintentional threats include: equipment failures, power fluctuations, magnetic fields, aging facilities and overheated equipment. The unintentional threats that are difficult to plan for include: programming errors, user errors, spilled beverages, viruses, lost encryption keys and lost or non-existent documentation. Assessments also need to include intentional threats such as theft, hacking, viruses, vandalism, sabotage, arson, and unauthorized copying or transfer of data.

Although there is more attention paid to threats from outside one's network, internal threats are more likely to be a problem for a school system. This would involve authorized users who are accident prone, negligent or ignorant. How many times have you walked by someone's computer with student records open or leave the server room door unlocked because they're coming right back?

The steps involved in completing a Risk Assessment

a) Identify the critical systems and sensitive information – information that damaged, compromised or lost would negatively affect the school system (ex. Student or staff records) and the hardware and software that would keep the system from functioning (backbone cabling).
b) Estimate value of your information system – approximate the replacement value for each item identified in Step 1. Include the costs associated with the disruption of service (ex. Overtime for employees, extra days added to the school year). Although extremely difficult, the indirect costs such as loss of federal or state funds and loss of public confidence must also be addressed in the assessment.
c) Identify the threats – include the natural and manmade threats listed above. Which are most likely to occur at what location.
d) Identify your areas of vulnerability – this involves a room-by-room and building-by-building inspection. Pay close attention to the physical (access, construction and climate), equipment and software, media liabilities (printer locations, procedures and location for backing up data), communication flow (email procedures, encryption and locations for accessing data), human factors (personnel and office behaviors). Does equipment have surge protection? Are passwords written on post-it notes? Are backups stored in the same location as the original files? Are doors to equipment locked? Are floppy disks left laying about and shared?
e) Estimate the probability of a threat becoming real – this will take a look at concerns such as the natural threats of floods and fire. If you have no virus protection on the servers and desktops, the likelihood of virus infections will be very high.
f) Identify countermeasures against the identified threats and vulnerabilities – many of these can be thwarted easily without significant cost. Training all personnel to use password protected screen savers or locking their workstation, making sure that doors with locks are kept locked, locating backup media to another location are a few examples of no-cost measures.

g) Determine costs of implementing the countermeasures from step 6 – include both time and money costs. Staff-training, researching, procuring, installing and maintaining the measures all need to be included. Would it be more cost effective to buy anti-virus protection for the servers and have all documents saved to the server than to train employees to use and provide anti-virus software for each workstation on the network?

h) Select those countermeasures for implementation – decide which strategies make the most sense from a cost/benefit perspective. A single countermeasure may be able to cover multiple areas of vulnerability. Institute those no cost or very low cost countermeasures immediately. The use of a properly configured firewall at the point of access to the system's network will do much to eliminate the threat of virus invasion.

The vastness of a school district makes the job of risk assessment extremely difficult. Perhaps a checklist given to each building administrator would be a good place to begin. The more personnel that buy into the necessity, the better the vulnerabilities will be identified and countermeasures enacted.

3) Security Policy

Whose job is information security? The network engineer?, the school principal?, the superintendent?, the school board? The employee's who use the equipment? The answer is all of the above. Therefore, an appropriate and effective security policy needs to be developed, instituted and enforced throughout the school system.

A Security Policy should be developed upon the results of the Risk Assessment. It should identify the sensitive information and systems critical to functioning, incorporate all relevant local, state and federal laws as well as the ethical standards of the school system. The institutional security goals and objectives need to be defined and then a plan developed for accomplishing them. The final portion of a security policy should ensure that all the necessary mechanisms are available to institute and enforce the policy. Use simple, understandable language, define terms and focus on expectations and consequences. Be sure that the consequences are enforceable; if you don't intend to enforce a "no private use of email", then don't include it in the policy. Some mechanism must be in place to ensure that all employees have read and understood both the expectations and consequences of the policy. A reminder via newsletter, posters or email of security practices as well as staff training will enhance the notion that security is the responsibility of everyone.

Trevor Shaw, in his article for eSchool News, states that different security policies need to be developed for administrative accounts and servers from the policy for students and faculty. The second group has less security to make services such as FTP and web publishing available. Shaw feels that schools should align themselves with the educational goals of their institution for maximum efficiency. (Shaw).

4) Security Management

The key to a successful security system is finding the balance between system protection and system usability. A portion of the security manager's job is to make administration and users aware of their role in protecting the entire system. The security manager needs to communicate to all staff, the importance of a secure system, provide the necessary training and monitor user activities.

Another facet of security management is contingency planning. Planning for a security breech or natural disaster is critical to minimize damage and downtime. All staff must know who is responsible for what task, how to implement the task and to whom to report. Establish written procedures and plans, test the plan and analyze the results to develop needed training and clarification. Since a school system has multiple locations, the master plan needs to be in a secure location with specific plans in place for each location. Everyone needs to know what they are responsible for doing when a security disaster happens.

Security management is more than keeping problems out or planning for problems. It involves day-to-day maintenance such as backups, redundancy of critical systems, updating virus protection, installing software fixes and managing user accounts, and monitoring what is taking place on the entire system.

5) Physical Security

Physical security includes the protection of building sites and equipment from theft, vandalism, natural disaster, manmade catastrophes and accidental damage. It also includes the data and software that are housed in the physical components as well as securing the cabling attached to it all. New school construction should include plans for securing the network equipment from as many of the threats as possible however, it usually is last on the list and ends up in one of the electrical closets. Since most school districts include old, retrofitted buildings, it may be difficult to secure all components. Measures such as fire extinguishers, surge protectors, locks on doors, moving equipment high enough to avoid minor flooding should be easy to implement. Just as at your home, windows and doors should be kept locked. Personnel in the area should be apprised of those that should have access and report anyone that they do not recognize to the proper authorities.

Specifics for physical security include:

a) carbon dioxide or halon fire agents should be installed or readily available with all employees trained in how to use them,
b) equipment room temperature should be maintained between 50-80 degrees with 20-80% humidity,
c) as few flammables as possible should be located in equipment rooms which includes curtains, paper storage, cleaning solutions,
d) move all cabling and wiring out of foot traffic
e) maintain an up-to-date record of all equipment and peripherals
f) have plans in place for emergency repairs including vendor names, phone numbers and contact information
g) label all equipment both visibly and inside as evidence of ownership
h) use anti-static mats, sprays, carpeting and train staff the proper way to handle electronic components
i) keep scanners, photocopiers, fax machines in open view to monitor usage
j) don’t print sensitive information to general usage print devices
k) shred all documents to prevent “dumpster diving”

Physical security is in many instances, common sense measures but how often the most overlooked aspect of security. In the aftermath of Topical Storm Allison, Todd Weiss states in a ComputerWorld article, Houston floods teach IT managers readiness lessons, "…that companies with detailed emergency plans fared better than those without. But even those disaster plans were not always enough." Much of the equipment was located in basements and destroyed due to flood waters. A small item like having flashlights available during power outages would have helped many businesses avoid the amount of damage suffered by being able to move critical equipment out of harm's way. Don't overlook the obvious.

6) Information Security

There are local, state and federal laws required that certain information, like student records, be protected from unauthorized release or access. Protecting information is more an issue of training users to follow established procedures and rules. In your school, how many times have you walked by a computer with mainframe screens left up for anyone going by to view, alter or delete? User training and understanding is a must!

"For the hacker looking to get a credit card in another person's name, there is plenty to glean from university student databases." (AP). This would also be true for the personnel databases in the school districts.

The following procedures are countermeasures against information security threats:

a) Do not send sensitive information via email. If it is a necessity, use encryption.
b) Inform staff that everything involving school property is subject to monitoring.
c) Make sure that a dial-up modem is correctly configured—don't use autoanswer features.
d) Dial-in features such as RAS need to be secure to verify only authorized users.
e) Be sure to verify the receiver of information has authority to have the requested information to prevent "social engineering" techniques used by intruders.
f) Have secure procedures for interoffice, receiving and shipping areas.
g) Set up groups and add users to the groups based on "need to know" status.

Procedures for backing up information and programs must be established, users trained and checks to make sure that procedures are being followed. After choosing a backup program that fits the established needs, someone needs to be held accountable for seeing that it is enacted as stated. How often, what information, how many times to reuse tapes, where backups are located, and how often to test backups all need to be established. Tapes need to be labeled and stored in a secured location. Also, a policy of how long information should be kept and how to dispose of it should be clearly established and followed. Computers that are no longer used should have the hard drives removed or the data completely destroyed before they are released from the secure area.

7) Software Security

Software is what makes computers useful to us. It must also be protected from threats. There should be a central repository for software along with required documentation of licensing. Procedures need to be developed that include what programs are added, who can add, delete or modify software programs. It is best that all software be tested before release to be sure that it is compatible with the system, and is free from viruses. Downloads should be monitored and checked carefully before installing into the system. There are many products available for networked inventory logging and management of software. The best policy is to train users to follow the procedures and understand the "whys" of software usage.

Teachers are notorious for wanting to try out "free" software found on the Internet. Downloaded programs are often poorly designed or virus infected. It is best if users cannot load any programs on their own machines. A trained contact for each location would facilitate eliminating this type of problem. Jeff Crume tells us in his book, Inside Internet Security, that installing software using defaults can leave the system vulnerable to attacks. Installing operating systems with the default administrator password allows intruders to enter on their first try. Vendors set up software for easy install, not security. Leave installs up to the experts, however that does put a burden on the technology staff to respond quickly to user requests.

8) User Access Security

User access security limits a user to only what he needs to access to complete a task. There is no need for someone in finance to have access to student records. Users access should be on a "need to know" basis. "Reasonable efforts must be make to inform all users, even uninvited hackers, that the system is being monitored and that unauthorized activity will be punished and/or prosecuted as deemed appropriate. If such an effort is not make, the organization may actually be invading the privacy rights of its intruders" (nces).

Students must also be apprised of the policies and consequences of computer usage. A 16 year old student was charged with six misdemeanor counts of modifying computer data after corrupting school computers with a disk containing 89 viruses that he downloaded from the Internet. Final exams at the school were disrupted although only 350 of the district's 600 computers were affected. Virus protection was in place but one of the viruses was able to infect an older machine running Windows 3.1. It took 45 days and $20,000.00 in payroll expenses to clean and reprogram the infected computers. (eSchool News).

Having user security procedures in place will make employees feel more secure and comfortable about doing their jobs. It will: help them to protect their own files, decrease the likelihood of them improperly releasing confidential information and educate them about appropriate computer behavior.

Policies need to be established to regulate user account systems, authentication procedures, log-in procedures, physical security requirements and remote access policies. The risk analysis will identify those areas of weakness or those in need of change.

The following should be included as a minimum for user security:

a) Each user should have an account. Do not share accounts. Set up generic accounts for temporary employees or for student assistants. Account names such as Temp1, temp2, can be reused as needed.
b) Provide access to only those files and services that are necessary to complete the job assigned.
c) Make sure that the user account list is encrypted and stored as a hidden file.

d) Use auditing to monitor account activities. Monitoring does slow down system processes so be judicial in what is monitored.
e) Disable accounts not in use. Check with the legal advisor before deleting accounts because some of the data in the account may need to be kept under reporting laws.
f) Use an authentication system for user log-in. There are many available from passwords to electronic key cards to biometrics and voice recognition systems that can be used. Establish password policies and enforce them by training users not to write them down or leave the workstation logged on in their absence.
g) Most network operating systems have the capability to set acceptable log-on hours and location, number of log-on attempts, and screen savers with mandatory locking features.
h) Train users why security procedures are necessary.
i) Be judicious when permitting remote access to the system. Train remote users to be cautious when logging on in public places.
j) Require all users to sign an Appropriate Use Agreement before they receive access to the system. The Agreement needs to be written in understandable language with consequences listed and enforceable.
k) Do not permit modems to be installed without being protected by a firewall.

9) Internet Security

As soon as your network is connected to the Internet, it is subject to attacks. If you can get out of the system, hackers can get in. The task is to make penetration as difficult as possible for unauthorized users. One example is that of a 13 year old boy who took down the Gibson Research web site after Mr. Gibson writing an article describing young hackers as "script kiddies." "Young hackers, unlike urban gang members, tend to be suburban kids who try to one up each other's computer skills. These cyber-gangsters aren't necessarily malicious, just bored."(Vamosi). Your school web site might become the playing field for status seeking students.

"When you don't know who is accessing your network, you also don't know their intentions or level of technical expertise—thus, choosing to connect to the Internet has a significant impact on an organization's risk assessment." (nces)

Connecting to the Internet involves two areas—protecting your networks, information and assets from outside users who enter your network from the Internet and safeguarding information transmitted over the Internet.

To protect your network from outsiders involves measures formerly discussed: encryption, virus scanning software, remote access and password policies. The use of a firewall determines what types of messages are allowing into the system. Isolate the network as much as possible by placing the public accessed web server outside the firewall. No confidential information should be on or be able to be accessed by this server.

Information accessed from the outside, such as grade information or registration should use an encryption service like SSL (Secure Sockets Layer) used by the web browser to generate a random encryption key that is matched to the web site hosts' key. There is software available that will authenticate messages using digital signatures, time stamps, sequence numbers, and digital certificates.

"The Internet simply is not secure unless you make it so. Luckily, basic Internet security is not beyond a non-technical person's ability to understand. By collaborating with technical support staff (or outside consultants if necessary), educational administrators can ensure that the near limitless amount of information and resources that exist on the Internet are available to system users without jeopardizing system integrity." (nces)

10) Training

Last on the list, but certainly not the least in importance is the training of your system users. User training is the key to make your security plan successful. E-mail can be of particular concern. "Most people get more e-mail than they can manage. Virus-proliferated e-mail messages feed already overloaded inboxes, and people become careless. As a result, complacency spreads viruses faster than technology can catch them. Organizations should educate continually on how to protect against e-mail viruses—not just during a virus crisis." (Grey & Graft). All the technological and procedural precautions in the world will be ineffective if they are not followed by the users. With a commitment from top administrators, user training becomes a priority. Training will make the users better prepared to avoid problems in the first place such as opening unknown emails. Through proper training, they will be able to minimize the damage from problems that do arise and maximize their assistance in the recovery process when necessary. Since most security problems occur from unintentional human error, training can bring these threats to a rare occasion.

When planning information security training the following goals should be included:

a) raise staff awareness of information technology security issues in general.
b) ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security.
c) explain organizational security policies and procedures.
d) ensure that staff understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.
e) train staff to meet the specific security responsibilities of their positions.
f) inform staff that security activities will be monitored.
g) remind staff that breaches in security carry consequences.
h) assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior.
i) communicate to staff that the goal of creating a "trusted system" is achievable.(nces)

Training needs to be more than "telling" users what they cannot do. Explaining what may happen and why a procedure is necessary is much more effective. Examples of security breaches at other school districts will go a long way to gaining user buy-in of security procedures. It will take away the "they won't allow us to do anything" attitude and change it into one of "they really look out for our well-being."

How often and when training takes place is the next issue to address. Short sessions work better than long, drawn out sessions. A short session presented at each staff/faculty meeting may work best in a school environment. Regularly scheduled, well-presented sessions will not be looked upon as drudgery. While training a staff person for the job tasks, security procedures should be mixed right in. A copy of the security policy should be provided to each new employee at orientation.

Also, a newsletter with hints and tricks along with security procedures and explanations will help with the training issue. In schools with technical contacts, 'train-the-trainer" sessions could be established so the technical contact can provide one-on-one sessions as necessary. As training is set up to teach new personnel how to use email or fill out required paperwork, this time is excellent for security lessons as well. To this day, it is surprising how many teachers don't understand why it is a bad idea to give the "good student" their system password or permit students to use their computer.

Security needs to become important to everyone that uses your networked system. It is sometimes difficult to find the balance between security and users being able to perform their jobs. The job of securing a school district is probably more difficult than securing a network for a corporation. Hopefully, this will give administrators awareness of what is involved and a starting point for fortifying their school network.

Resources-FortifyingK12

Associated Press. (June 1, 2001). University computers a prime targets for hackers. [On-line], June 6, 2001. Available: http://www.cnn.com/2001/TECH/internet/06/01/hacking.colleges.ap/index.html

Dello, M. (June 13, 2001). Hoosier favorite hack victim? [On-line], June 20, 2001. Available: http://www.wired.com/news/culture/0,1284,44501,00.html

ESchool News Staff Reports. (June 1, 1998). Student jailed for unleashing virus on school network. [On-line], (May 26, 2001). Available: http://eschoolnews.com/showstory.cfm?ArticleID=1080

Grey, M. and Graff, J. (June 1, 2001). Commentary: complacency is the worst foe. [On-line], (June 6, 2001). Available: http://news.cnet/news/0-1003-202-6157094-0.html

Krause, M. and Tipton, H.F. Handbook of Information Security Management. [On-line], April 10, 2001. Available: http://secinf.net/info/misc/handbook/ewtoc.html

NCES (1998). Safeguarding your technology. [On-line], May 7, 2001. Available: http://nces.ed.gov/pubs98/safetech

Shaw, T. (August 1, 1999). IT happens: Let's learn to balance security needs with educational goals. [On-line], May 26, 2001. Available: http://www.eschoolnews.com/showstory.cfm?ArticleID=467

Vamosi, R. (June 20, 2001). Know thy enemy—you might be surprised who's hacking you [On-line], June 20, 2001. Available: http://www.zdnet.com/anchordesk/stories/story/0,10738,2777057,00.html

Weiss, T. R. (June 14, 2001). Houston floods teach IT managers readiness lessons [On-line], June 20, 2001. Available: http://www.computerworld.com/storyba/0,4125,NAV47_STO61363,00.html