Gray's Security Plan

by

Gray Pattillo
iMET5
7/25/03

Focus on School Security with Insight from
State Government

Credits to
Glenn Brahman
Willie Pattillo
Ellen Skimmer

INTRODUCTION

As the “Technological Revolution” requires schools to acquire technology to take advantage of opportunities of student-centered, collaborative learning methods, Schools must develop technology plans to ensure all the school needs are met. The plan includes the needs of the administration, teachers, and students. Part of the plan includes developing technology use policy to be followed by all users. An important factor of planning and policy are considerations for the security of the technological system.

Four security activities promote the overall security of the system. first is the policy itself. It delineates the responsibilities of user groups: management, administrative staff, teachers, and students. In addition to delineating responsibilities, it provides the tools or “how to” to enact security. Second is training, at least annually, and it is designed for the user group and the groups are trained to the policy. Next is an “audit” function, to determine the effectiveness of the plan and to recommend corrective action. Last, management enacts corrective actions according to available resources and applied to the priority of risks. that si, management determines the cost to benefit to decide the prioity of risks to address.

Often, the corrective action requires updating the policy experience uncovers risk and a conditions change. For our group’s initial policy, we determined the following top 10 security concerns for a composite of our four work areas. Then we briefly addressed the means and the relative cost to address these issues.

Possible Errors in Security

1-Passwords
2-Network port security
3-Student accounts
4-Virus Protection
5-Backup All important data
6-Monthly In-services on Security Procedure
7-Physical security
8-Climatic Conditions
9-Inventory Control of software and hardware
10-Decommissioning Obsolete Equipment

Errors, Level of Complexity, and Recommendations

1-Passwords

- Change passwords quarterly, and prevent log in if not changed,
- Use at least six charcters, preferably a combination of numbers and letters. Use at least two of one to four of the other. Allow for both upper and lower casreleters as well as special characters.

2-Network port security
-Keep as many ports closed as possible'
- Prevent unauthorized access to unoccupied computers by setting up password protected screen savers to activate after a minute of non-activity, and allow user to key activte the screen saver when tehy must leave their station.
- Log off , shut down computer, and turn it off at the end of a session.

3-Member accounts (Ssudents, teachers, and administation.
Password protect with an administration override.

4-Virus Protection
Install antiviraal software and suscribe to services to automaticaly update.

5-Backup all important data - and have a disaster recovery plan.
Prevent loss of data to equipment failure, or damage, or disaster.
Back up data on alternative media (discs, hard copy, alternate drives)
Back up data on servers daily.
Maintain secure, off site storage of back up data for disaster recovery.

6- Annual In-services on Security Procedures. supplimentary Training as needed.
Articulate mission, goals, policy, and means to enact policy. The starting point of dicipline (and heading off problems) is training.

7- Physical security
- Install locked tie downs on computers and peripherals
- Secure buildings with alarmed windows, and doors with motion sensors in the rooms

8- Climatic Conditions
- Control dust
- Instal reliable cooling so the equipment doesn't over heat
- Keep food, drink, and spillables away from sensitive equipment.

9-Inventory Control of software and hardware
All equipment must be inventoried by identifying number and by age
All software should legal and licenses available for proof of ownership
in the event of any disaster or loss.

10- Decommissioning Obsolete Equipment
- Observe basic security
- Eliminate confidential student or employee information

Cost to avoid the Possible Errors

1-Passwords

Have a file that secretaries pull out and rotate the passwords quarterly

Cost-Initial time to set up quarterly time minimal

2-Network port security

Handled by the network administrator should be their job now!

Cost –little to none

3-Student accounts

some class time by teachers for set up and secretarial time in September

Cost- minimal

4-Virus Protection

This could be installed by computer tech. updated by teacher with once a month reminder emails.

Cost- Cheap- $8 -$10 per machine and initial install by tech

5-Backup All important data

Up to each individual

NO COST if you loose it to bad

6-Monthly In-services on Security Procedures

This could be done on a need basis at monthly staff meetings or during common planning time

Cost-none or a stipend to pay the trainer

7- Physical security

This is a major ticket item if not already in place

Cost- BIG BUCKS site council funds could pay. Place priority on most expensive equipment or most critical data, such as personnel records, accounting records, and student records.

8- Climatic Conditions

Maintaining a dust free and cool environment for computers could also be a big ticket item

If the school has air conditioning maybe filter changes are all that's needed

Cost- BIG BUCKS Float a Bond measure to replace loss.

Again if a district of school site cannot protect all class rooms or devices, prioritize protectins on hte most expensive items and most critical data.

9-Inventory Control of software and hardware

Highest risk area - goal to pevent loss and theft of valuable equipment, and loss or compromise of critical data accounting records, personnel files, andstudent records).

Set up an inventory control management system. Inventory sould be tracked from 'cradle to grave.' That is from purchase, delivery, to user, to disposer.

Once a year check the #s inventory and software license the cost would vary depending

on size of school site . Keep a “Property Book” of all high valued items, (School district sets this level and reconcile the individual items to the property books.
Cost- none a staff members should know what’s in their room and on their equipment. Also, this should be the responsibility of the accounting staff. (Any administrative staff may do this except for purchasers.)

10-Decommissioning Obsolete Equipment (Also part of inventory manage,ent system)
Remove the hard drive and degauss (this ruins the HD) the cost would vary depending on the amount of equipment purchased and rotated through the school.
Cost- this could be done by students who could degauss or reformat with a method to remove and replace all data.
Also set up a protocol to dispose of equipment. A principal or vice principal should be appointed property survey official, and NO propery book item may be removed without their signature. A copy of this survey report shoud also go to the property book custodian, to remove it from site inventory. Last, disposal should be conducted throughauthorized channels. (Prevent loss of newly purchased equipment being’surplused’ to whomever on a regular basis.)