



Network Security and Student Safety

As more and more students access the Internet and more school district data is stored on the school network it is imperative that both students and data be safeguarded. Likewise, as the district increases its investment in

technology it seeks to secure it in ways that insure the minimum amount of downtime and highest levels of reliability.

Security

Backups

Is all data backed up and stored off site?

Recovery

If there is a catastrophic event, can the district restore its systems in a reasonable time period?

Prevention

What systems are in place to prevent network and data security incidents?

Student Safety

What systems are in place to protect students from Internet safety threats?

Network Security Description

January 31, 2008

The Real Situation CSD complies with federal E-Rate requirements for content filtering to increase student safety when accessing the Internet. The district contracts with the RIC for a content filter (X-Stop) which blocks students from linking to undesirable sites.

The district employs a firewall to protect it from outside intrusions. The firewall is maintained by Technology Coordinator.

The district uses Symantec AntiVirus to protect its servers and workstations. Updates are done by the Technology Coordinator.

xRIC also supplies a Spam filter for all e-mail.

The Business Office Maintains its own local area network and file server.

Network Security Assessment

January 31, 2008

Perhaps no other area of the this technology assessment needs immediate action than that of security. Here are a few items that need to be addressed:

- The district backs up its data on a daily basis; but the Technology Coordinator reports that these backups are not verified and overwrite the tape. It is assumed that they are not valid backups and that the district's data is at risk.
-

Security Assessment

February, 2008



- On a weekly basis the Technology Coordinator does a backup “by hand”. This backup does not include workstation images, Operating Systems, or applications; and is a “data only” backup. It is assumed that this is a “good” backup. If an incident happened on any day before this backup it would be safe to say that work for that week might be lost.
- There is no “off-site” storage of tapes and data. If there was a catastrophe, all district data including student records, budget information, and payroll records would be lost. This is a huge risk for the district to take.
- There is no formal plan for how the district would restore the data from backups if their file servers were destroyed or if they failed.
- The Technology Coordinator is a 10 month employee. When she is not working, on vacation, or sick; no backups are taking place. This is a huge risk, especially in the summer months prior to the opening of school.
- There are no written security policies or procedures for handling incidents.
- There has been no high-level security audit done.
- The Business office saves spreadsheets and other work products to their hard drives and not the file server. Since hard drives are not backed up, this data is at risk.
- There is a wireless network in the Middle School. This network is not secured.
- Students are allowed to attach Flash drives to the network. The Technology Coordinator periodically checks for .exe files to minimize the chance that the students have installed a program to “hack” the network or one that might generate some other security incident.
- Third parties that manage parts of the network such as the firewall, servers, switches, and business office applications; access the network remotely and have key passwords. There are no formal procedures or processes for this access.



- Physical security of the servers is reported “good” by the Technology Coordinator; however some switches are in public spaces.
- There are older DOS applications on the network that allow students to get to a Command prompt. From this prompt they can navigate many parts of the network that should be off-limits.
- The Technology Coordinator reports that desktop computers are “locked down” and secure from hacking.

- The district does not have any backup support for peak periods, emergencies, or if the Technology Coordinator goes on vacation or becomes ill.
- There is no network documentation. The layout of the network, the profiles and policies, numerous passwords and procedures are not available in case of illness or emergency.
- The district does not subscribe to full servicing of its switches and servers.

Security Assessment

- The workstations do not receive regular service pack updates because the Technology Coordinator has not been trained in the product (X) that would automate this process. Updating the workstations by hand entails going to each computer to apply the patch. This is very time consuming.
- There is no documentation or established procedure for adding, deleting, or administering system rights, profiles, and passwords; as well as rolling over users from year to year. It is not clear what electronic records are archived nor for how long.
- The Technology Coordinator receives no formal training on networking, telecommunications, or security developments. This leaves the Technology Coordinator and the district to a “best effort” rather than “best practice” technical standard.
- The Business Office does not presently subscribe to a 24-48 hour technical support service. In an emergency it may be disruptive to payroll and other core service and take significant time to recover normal operations.





Recommendations

A good security plan focuses on prevention, forensics, and recovery. In addition, staff and students should be trained on basic security processes and best practices.

February, 2008

Improving Network Security and Student Safety

RECOMMENDATIONS:

Backups: Immediately create and implement a backup policy and process.

The backup process that is in place today is significantly flawed. Potentially, only one backup per week includes all the data. This 'clean' weekly backup, however, does not include the OS, the Apps, or the Images.

Backups: Insure there is a backup tape rotation and that some tapes are kept off site.

Without offsite storage, the district could lose all student data, financial data, etc. in a fire or other emergency.

Backups: Train someone to support the Technology Coordinator in the backup process.

There are no backups taking place when the Technology Coordinator, a 10 month employee is not in school. This leaves the district's data at severe risk.

Backups: Insure that the Business Office saves to the server and receives daily backups.

The Business Office server is backed up 'cleanly' only once per week. Staff in the business office do not save their Microsoft Office documents and spreadsheets to the server; but only to their hard drives. None of the hard drives are presently backed up; so the district data is at severe risk.

Backup Option: Subscribe to the RIC remote backup service.

This will insure daily, offsite backups are done, even when the Technology Coordinator is not working.

Recovery: The district needs to create a formal plan to recover if the servers fail.

If there is an emergency or if the servers fail, the district needs to create a formal arrangements to use a 'hot site' to load data tapes and continue core district functions on a temporary basis.

Network Security: The district should drop its firewall since a firewall is maintained at the RIC.

Maintaining a redundant firewall provides little benefit and requires much work for Technology Coordinator. This should free up precious time to focus on technical support requests.

Network Security: The wireless network at the Middle School should be secured.

Presently, the network is open and thus it is a potential risk.

Network Security: Workstations need to be updated with critical patches when needed.

Because there is no automated way to update the workstations today, they do not receive critical updates in a timely fashion.

Policies and Procedures: The district should create and implement a security plan.

This plan should outline key policies and processes for handling different types of security incidents. It should include processes for third parties like BOCES/RIC to notify the district if they are going to access any part of the network, etc.

Policies and Procedures: The district should invest in a high-level audit of security best practices on a regular basis.

This audit would include a scan of switches, servers and workstations, Internet traffic, firewall, as well as several basic security processes. The audit does not have to be an in-depth and expensive project. Having an audit done regularly is a good way for the district to avoid any claims of negligence if there should ever be a security incident.

Policies and Procedures: The district technology committee should review what types of Web 2.0 services are blocked and why.

Presently, the Technology Coordinator has decided to block most Web 2.0 tools. This should be a shared decision with the committee. As much as possible, it is advantageous to open blogging for instructional purposes. The decision to block the ability to create or read blogs should be reviewed.