4-Preventative Methods II

Disabling Drives

- Although many threats may come from the outside and can be protected against, other threats come from inside a school.
- Inside threat can be the hardest to fight against because doing so many prevent access and thus lower productivity within a classroom.
- For example, the misuse of a personal thumb drive that carries viruses can easily bring a virus into a school's network, knowing or unknowing, by a user.
- A common method to protect internal users is to block USB drives, the ability to install applications and download files from the Internet. (Robinson, Brown, & Green 2010)

Policies and Procedures

- Computer network policies and procedures are generally considered critical to planning for network security.
- Teachers, students, and/or staff need to be made aware of the policies and possible consequences.
- Sharing policies and procedures may prevent individuals from attempting to attack a network because of the fear of possible consequences.

Restrict Permissions

- Restricting both end-users' and technical staff's permission can improve internal control and protect a network.
- A sound restriction permission policy allows only those that need to have access to specific features and limits access to those that could knowingly or unknowingly cause internal damage.

Reference

Robinson, L., Brown, A., & Green, T. (2010). Network Security Versus Access. In Security vs. access balancing safety and productivity in the digital school. Eugene, Or.: International Society for Technology in Education.