

2-Reality of Network Security

Cost

- With the adoption of BOYD, 1-to-1 initiatives, and online state testing, the stakes have become increasingly higher for computer performance and network security.
- Furthermore, the need and expansion of wireless networks have increased with the growing popularity of mobile devices in the schools.
- Unfortunately, wireless networks, teamed with an increased number of devices increases the potential weak zones for viruses and hacking to occur.
- Not only does a down network impact time and productivity but it also impacts the financial cost for businesses and schools.
- Much of the cost can be attributed to the cost of hardware, computers, time lost to carry out core daily functions and the cost for experts to rebuild the computer network.
- We cannot always place a value on lost of intangibles items. However, the implications are significantly higher if a network is brought down due to an attack.
- Network security can be pricey. However, network administrators must balance the cost of network security with the cost of potential damages created if a virus or attack were to happen. (Robinson, Brown, & Green, 2010)

Student and sensitive information

- School districts, hospital, and financial institution often have sensitive data housed on servers and computers within their networks.
- Sensitive information attracts potential hackers that look to benefits from accessing this information.
- There could be greater legal, media, and political consequences that these organizations face if sensitive information is accessed via a network breach.
- There is nothing more important than student safety within a school.
- Network Administrators and school officials should know what data is being housed on which servers and make logical efforts to deploy cost-effective solutions that prevent great financial damage and liability from network security breaches.

Teacher Access and Productivity

- Similar to protecting students, administrators must understand that a well-protected system affords teachers the tools they need to be productive. Thus, improving teachers' ability to carry out their core objective of delivering quality instruction on a daily basis.
- With increased access to network resources from remote locations with technologies such as Google Apps, Microsoft 265, and Virtual Private Networks (VPN), networks are becoming more vulnerable and require stronger security (Robinson, Brown, & Green, 2010)

Access and Functionality

- Teachers tend to worry about access to technology to deliver their lessons.
- Part of this worry is also to ensure that devices are in working condition and promote a healthy and safe learning environment for students and teachers.
- Teachers ultimately require efficient access to technology to drive their lessons.

- Both network administrators and teachers care about network security. However, teachers care more about security measures that allow them to carry out their lessons, rather than protecting data or against threats.
- While network administrators are generally more concerned about computer network security measures that to protect against security breaches.
- It is important to take the concerns of network administrators and teachers into consideration when thinking about computer network access versus security to create an efficient and safe educational environment.

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.