# Evaluating your District Cybersecurity Readiness

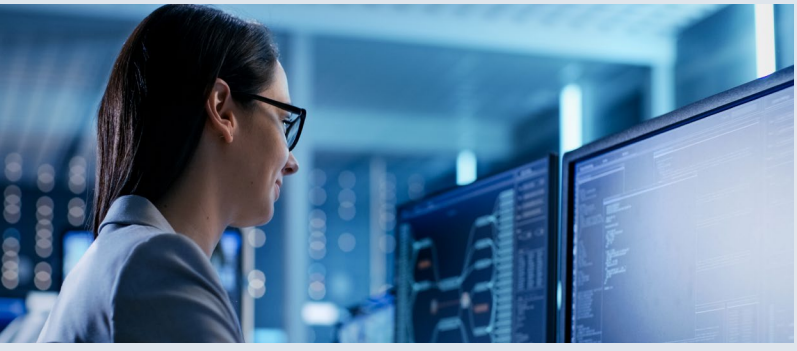
Knowing your enemy is crucial to vanquishing a foe. And, in the case of K-12 school networks, cyberhackers pose one of the greatest threats imaginable. The best defense begins with a deep understanding of the techniques that cyberhackers employ, and how they can exploit your school or district's vulnerabilities.

Cyberattacks are evolving rapidly. And it's not just the cliché of the hacker working out of his or her parents' basement. There are sophisticated "gangs" of hackers developing and distributing malicious code, and various school security assessments show that many schools might not be ready to handle these threats due to outmoded technology and ineffective strategies. For instance, hackers may be able to get access to school data, but the breach itself is only rarely detected.

Some of the most insidious assaults against a school or district's network include:

**Email.** Email is the principal security threat that today's schools face. Schools should implement anti-phishing tools (more than those simply built into email solutions).

**Endpoint Protection.** Ransomware and "cryptomining"—where hackers hijack a computer to harvest bitcoin— can grant hackers full control over a device. The latest endpoint products can examine what processors are doing, what files are being modified, and prevent hostile takeovers.



**Firewalls.** Today's firewalls have the ability to filter on a much deeper level than before, granting IT teams more control over their schools' networks.

**Patching.** An unpatched server can allow "bad actors" (a hacker) who have accessed a point in the network to move laterally, compromising the entire system. Software should be regularly patched, or automatic patching tools should be implemented.

**Spear Phishing.** The practice of spear phishing—an attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity—has also become increasingly complex, allowing hackers the ability to infiltrate a school's entire network through a staff member's email account.

## Common Sense Counter Measures

One relatively simple way to thwart a data breach is for school faculty to choose password phrases rather than replacing letters for symbols or random combinations of numbers and letters. Password phrases are not only harder for hackers to solve, but they are easier for faculty to remember. Schools are also advised to install multifactor authentication software, and to research emerging technology such as AI (artificial intelligence) that can help schools to keep their networks safe.

## Does Your School Make the Grade

Frosty Walker—CISO for the Texas Education Agency—has created a six-level framework for school IT professionals to better assess their school's or district's security measures and readiness.

| | |
|---|---|
| **A+** | Data security is optimized, and the school has refined standards and practices to improve capabilities in ways that are both efficient and cost-effective. Top of the class! |
| **A** | Data security is achieved through an established risk management framework that measures and evaluates risk while integrating improvements: going above and beyond minimal regulatory requirements. Great job! |
| **B** | Security approach is defined, detailed and documented, with the school or district regularly measuring compliance. Good work! |
| **C** | Security strategies are—while repeatable and mostly consistent—still relatively reactive and undocumented. In this scenario, the school or district doesn't routinely measure or enforce compliance with security policies. Acceptable with room for improvement. |
| **D** | The organization's security strategies are ad hoc, inconsistent or reactive. Poor, needs much improvement. |
| **F** | Security measures are basically nonexistent. It's like you didn't even try! |

A baseline assessment makes routine updates easier and more manageable. These regular snapshots help schools and districts to track progress over time. Doing an inventory of data assets can also prove valuable in the event of a data breach, or if an incident requires the rebuilding of a data network.

Lastly, in matters of data security, it is important to go beyond minimal requirements if you want your security to be at the head of the class!