K-12 Cyber Threats:

5 Hidden Risks You May Not See

Malware, ransomware, phishing scams — you're probably familiar with all three. K-12 school districts like yours are constantly under attack. That much is clear as day, which begs the question: What risk factors aren't you seeing?

To help you prepare for the school year, let's uncover five hidden threats you may not be aware of:

1 THIRD-PARTY VENDORS:

55%

of K-12 breaches between 2016 and 2021 happened because of third-party vendors.[1] They may provide essential services, but weak security can compromise your own defenses.

2 MISCONFIGURED CLOUD STORAGE:

43%

of breaches are due to misconfigurations,[2] such as incorrect permissions and share settings. This can leave sensitive information systems accessible to unauthorized users.

3 UNPATCHED SYSTEMS:

By one estimate, unpatched systems are involved in **60%** of cyber incidents.[3] Delaying updates leaves vulnerabilities open to exploitation, giving hackers a way to bypass your security.

4 ACCOUNT TAKEOVERS:

As seen in multiple recent school district attacks, compromised accounts can lead to widespread system access. For one district, a single breach led to over 200,000 student files leaking online.[4]
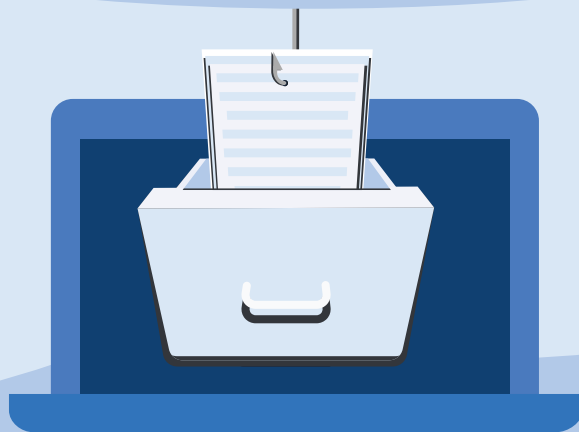
5 MALICIOUS WEBSITES:

Hackers often distribute trojans through malicious sites, hijacked domains, and fake advertising — all made to trick users into downloading a virus.[5]

Without support, spotting these hidden threats can be challenging, if not impossible. Your district needs a solution that can uncover potential risks as early as possible, allowing your team to investigate, mitigate, and recover.

At ManagedMethods, we offer Cloud Monitor and Content Filter. They provide easy solutions to protect Google Workspace and Microsoft 365 and block malicious websites at scale. In turn, you can protect student data and eliminate threats before they impact your district.

Want to learn more? Schedule a free demo today.

Managed Methods