HOW **CYBER ATTACKS** IMPACT YOUR SCHOOL DISTRICT

K-12 schools are a goldmine of sensitive information. Unfortunately, hackers are well aware. They're targeting districts left and right, harvesting personal data, and selling it to the highest bidder. Why? Because most of the time, it's an easy score.

The truth is that cyber attacks are a consequence of living in the digital age — but that doesn't mean they should be taken lightly. **Security breaches have real-world, long-term, and devastating costs, both for your district and its students.**
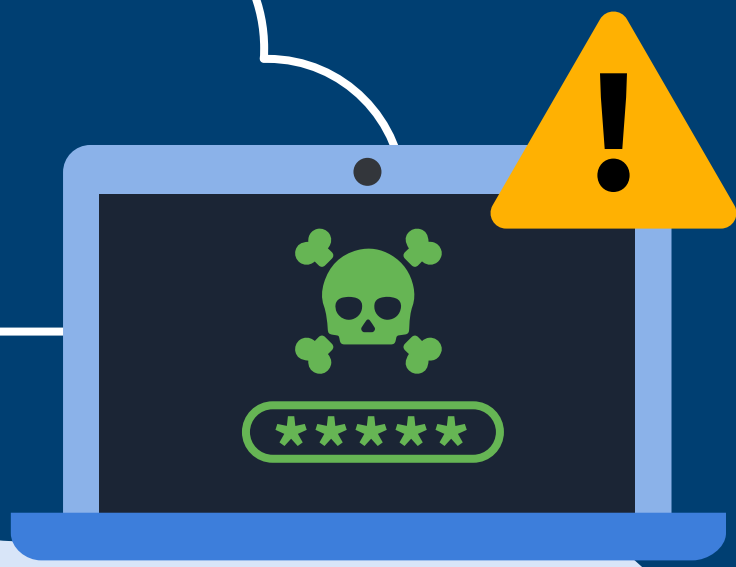
1 PERSONAL IMPACT

K-12 schools have leaked over **5.3 million records since 2005**, including names, addresses, and Social Security numbers.[1]

These incidents often happen when files are improperly shared outside the district, exposing students and staff to identity theft, fraud, and other schemes that could tarnish their credit.

2 FINANCIAL IMPACT

8 in 10 K-12 schools were impacted by ransomware in 2022, with an average recovery cost of **$1.59 million**.[2] Schools paid, on average, **$1.2 million** in ransom.

Other attacks led to monetary losses ranging from **$50,000 to over $1 million**.[3] These can come in the form of insurance deductibles, overtime costs, and replacing affected systems.

3 SAFETY IMPACT

In some cases, **hackers directly threaten to harm students and their families** if districts don't pay ransom, forcing school closures. **Attacks may also disrupt security systems**, such as cameras or locks, putting those in the building at risk.

The stakes couldn't be higher for K-12 school districts. When it comes to student safety and personal well-being, data privacy and security are paramount.

That's where ManagedMethods comes into play. With a portfolio of cybersecurity, cloud monitoring, and content filtering tools made specifically for K-12, you can rest assured your school is well-prepared and protected for what lies ahead.

Ready to see it for yourself? **Request a demo today** and discover the power of ManagedMethods.

Managed Methods