What School Districts Need to Know Now About Cybersecurity and Cyber Liability Insurance

December 1, 2021

Cyber Liability, Education, Property & Casualty

Marty Malloy

Senior Account Executive
Director of Education & Government Practice

The cyber liability landscape looks completely different for school districts than it did even a year ago. Policies are increasingly expensive and difficult to come by – and it's easy to see why.

The risk of cyberattacks is growing, with publications like Business Insurance reporting that more than 400 cyber incidents were publicly disclosed by school districts in 2020, and Wisconsin Public Radio stating that, as of August 2021, 830 individual schools nationwide had been affected by ransomware attacks this year. The risk is simply becoming too great for insurance companies to ignore – and many schools are being faced with nonrenewal.

Why are school districts being targeted?

School districts are not viewed as single entities by cybercriminals, but rather a conglomeration of information from individuals across a community. There are several reasons why this fact makes school districts particularly vulnerable to cyber-attack:

Sensitive data: School districts have access to data like personal student and staff information, student IEP/IDEA, and payment information. These files can create damage in the hands of a cyber attacker.

Financially under-resourced: Doug Levin, national director of the school cybersecurity organization K12 Security Information Exchange, said districts are often financially under-resourced, meaning IT teams are often very small and their technology might not have all the latest updates to prevent incidents.

Downtime isn't possible: Doug also offered the idea that cybercriminals know school districts need to be up and running again quickly, so they have a larger incentive to pay ransoms.

Young users: Students (and even staff) who use networks most frequently may be unaware of current methods for data breaches. Even clicking one wrong link can be costly for the district.

Personal devices: When connecting personal devices to the school's network, users are opening up new channels for cybercriminals to enter and wreak havoc.

Lack of cyber loss prevention plans: School districts are less likely than other organizations to have a plan in place in case of a cyber loss, meaning they're less organized and able to adequately respond.

How can school districts better manage their risk?

Underwriters are becoming more scrutinous of school districts' cyber practices when writing policies. They are looking for specific risk management practices to be in place in order to even send a quote for cyber insurance. We've laid out a list of those practices in our recent article on cyber insurance underwriting requirements for schools.

This sudden shift in the cyber market is surely overwhelming for school districts. While cyber insurance used to be low cost and easy to come by, it can feel like you

suddenly have to take on a district-wide project in order to protect students, staff, and community information. And we both know districts don't have time for that.

There is help available:

Your insurance advisor: First and foremost, your M3 insurance advisor is a key resource for not only purchasing the right levels of cyber liability insurance, but also implementing risk management practices to satisfy underwriters. We can conduct risk management reviews and make recommendations for vendors, systems, and processes to protect your district.

Kindergarten Through Twelfth Grade Security Information Exchange (K12 SIX): K12 SIX is a nonprofit threat intelligence sharing community for school districts to prevent and respond to cyber threats, together. Through a secure communications portal, school IT and security teams can share warning about cyber threats and help each other mitigate successful attacks, with support from K12 SIX staff leveraging dozens of data sources and analytic tools.

The National Institute of Standards and Technology (NIST): NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public.

Cyber Security & Infrastructure Security Agency: StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

If your school district does experience an incident…

There is a right way and a wrong way to respond to a cybersecurity incident. While every district should develop their own incident response plan, these are best practices that we recommend:

Follow the district's written incident response protocols

No one should refer to a suspected incident as a "breach" in writing – this could trigger statutes regarding the timing of legally required notifications

The district should avoid emails as much as possible if they suspect an incident.

Report the incident ASAP

- Incident Hotline/Insurance Company
- Insurance Agent
- Law Enforcement

Key Takeaways

Cyber insurance continues to become more expensive and hard to obtain as cyber-attacks continue to increase, particularly within the education sector. School districts must understand their vulnerabilities and work with their insurance advisor to implement risk management strategies that can protect them from cyberattacks.

Reach out to your M3 account executive to discuss your current cybersecurity measures, and what adjustments may need to be made to your risk management strategy in order to obtain cybersecurity insurance in the future.

BACK TO INSIGHT CENTER

Related Content

Risk Insight

January 5, 2022

OSHA Form 300A Summary Posting Requirements Begin February 1st

Read More

Article

January 4, 2022

Benefits Administration Systems Can Reduce Burden at No Cost

Read More

Article

December 28, 2021

OSHA Healthcare Emergency Temporary Standard (ETS) Status Update

Read More

Article

December 22, 2021

What Safeguards Cyber Liability Underwriters Want to See from Tribal Nations

Read More