Collaborating Across Districts for Cyber Resiliency

When schools find ways to pool their problem-solving, they also find innovative ways to strengthen IT operations.

BRANDON SHOPP
Group Vice President for Product Management SolarWinds

U.S. SCHOOL DISTRICTS HAVE publicly disclosed 1,331 cyber incidents since 2016, according to the K12 Security Information Exchange's **2022 annual cybersecurity report**. In 2021, 166 incidents affected schools in 38 states. That seems serious enough, but researchers wrote that "the true picture is surely bleaker; anecdotal evidence suggests perhaps 10 to 20 times more K–12 cyber incidents go undisclosed every year."

When it comes to cybersecurity, many K–12 schools still struggle with the basics. The best advice is to establish a good foundation that includes a strategy and process for deploying software patches as soon as they are issued. In addition, "preparedness activities… include developing and promoting policies on responsible use, storing data securely, and creating firewalls," states the **Cybersecurity for Schools Fact Sheet** published by the U.S. Education Department. "Planning teams should also consider what actions should be taken before, during, and after an incident occurs."

The message is that schools must become more proactive in their security strategies, and they can only do that if they have continuous information about how their systems are performing. A practice known as observability allows IT teams to gain real-time insights into the usage and health of systems and applications – whether they are on-site or off-site – before users encounter a performance issue.

Taking it a step further, when schools share information with one another about the problems they are seeing and the attacks they are facing, they can crowdsource solutions and thereby boost cyber resiliency across districts and across the K–12 sector as a whole. That approach also offers a way for schools to enhance security even when funding for IT systems and staff is less than robust.

Rather than leaving under-resourced districts to tackle cybersecurity in isolation, the K12 Security Information Exchange's report concludes that "school districts should put a premium on sharing threat intelligence, sharing best practices, developing model policies, pursuing mutually beneficial risk mitigation solutions that can be deployed at scale, and educating state and federal policymakers about K–12 cybersecurity challenges and potential solutions."

Pooling resources among districts can have a powerful impact, and schools can also benefit from tapping into federal security standards, many of which offer well defined processes for responding to specific scenarios and situations. K–12 schools are considered critical infrastructure, and, accordingly, the

Cybersecurity and Infrastructure Security Agency offers a wealth of resources to help schools improve both physical security and cybersecurity. The National Institute of Standards and Technology's **Cybersecurity Framework** provides standards, guidelines, and best practices to manage cybersecurity risk. And the recent K–12 Cybersecurity Act acknowledges that schools should not go it alone and seeks to help districts improve security with the support of government and industry.

Sharing insights into cybersecurity is foundational for protecting sensitive data, and it also ensures that students, teachers, and administrators have seamless access to the digital services and resources they need.

Observability Moves IT From Reactive to Proactive

A deeper understanding of their IT networks and the ability to share solutions can save schools time and money while improving security and performance.

THE PANDEMIC SHOWED US technology has a crucial role to play in ensuring K–12 schools can support new learning models while offering a secure, positive experience for users. Instead of reinventing the wheel, districts can learn from one another's experiences by enabling IT administrators from various districts and schools to collaborate with one another and share information on problems and solutions.

Additionally, districts should have well-defined and well-articulated strategies at the superintendent level addressing all aspects of operations, including IT. These strategies should cascade down to individual schools so they can align their strategies accordingly.

Valuable Insights Into the IT Environment

Measuring success against those shared goals hinges on ensuring schools have the tools to identify and address any issues related to connectivity, services, or applications as quickly as possible. Specifically, observability solutions can provide the ability to see and understand what's happening inside hybrid IT environments.

Visibility gives administrators a view into how a specific application or service is performing and whether users are having problems with it. The appropriate level of visibility helps identify bottlenecks, outages, and other issues.

Observability allows for the correlation of information to provide deeper insights into why something is going wrong so administrators can determine how to fix it. Beyond addressing problems as they arise, schools should strive to get in front of them. By adding observability, administrators can begin to see problems as they emerge and address them before they impact service availability, connectivity, or performance.

Ultimately, observability enables IT administrators to become proactive instead of reactive to performance-related issues, including security. And the right visibility and observability tools help schools ensure all students can access the services and applications needed while having a positive, productive experience.

Utilizing Existing Standards

At SolarWinds, our solutions provide visibility across the essential systems involved in the delivery of a service or application. They provide insights not only into the services running in a school district's data center but also into cloud-based services such as Microsoft Office 365 and Google Workspace, as well as the learning apps students use daily.

This comprehensive view is essential for ensuring the security of an IT system. Schools can strengthen their security posture by instituting a process and strategy for deploying software patches as soon as they are issued, but they face other challenges in terms of budgets and staffing. It can be challenging for schools to hire IT security specialists because there's a limited set of people with the relevant skills, and the public sector can't compete with private-sector salaries. This is why many schools are choosing to outsource some of their security needs to managed security service providers.

Schools should also consider tapping into federal standards providing valuable guidance on IT best practices. For example, the Common Criteria offers a framework for validating if a particular product or system satisfies a defined set of security requirements, and the federal government has created many useful product configuration standards.

By adopting the appropriate standards and tools, K–12 schools can benefit from others' expertise and speed their ability to provide IT systems to support their districts' goals for security and performance.

Brandon Shopp *is group vice president for product management at SolarWinds.*