Telos®

Xacta for K-12 Education

Do You Have the Resources You Need to Assure Your School System's Cybersecurity and Risk Management Posture?

Schools are under a tremendous amount of pressure to deploy devices and cybersecurity solutions that will operate both on and off campus. The rapid move to remote learning provided an irresistible opportunity for malicious actors, who have been targeting schools with denial-of-service and ransomware attacks that deprive students and teachers of access to remote learning environments, while saboteurs "zoombomb" live classrooms with inappropriate material, verbal harassment, and the doxxing of class participants.

K-12 Saw an 18% Rise in Attacks during 2020

- Ransomware
- Denial-of-service
- Data breaches
- Phishing attacks

K-12 IT leaders are in uncharted territory, and the decisions they make today will lay the groundwork for their schools' safety, both now and in years to come. That doesn't mean imagining every possible scenario – that's impossible. Instead, it means building flexibility into their security postures by choosing technologies that use automation to gather data from across the environment in real-time, use it in workflows to acquire comprehensive visibility, and make the results available to humans in easy-to-understand formats that enable fast and accurate decision-making.

"We could use a cybersecurity framework that meets our needs."

Yet K-12 doesn't have strong guidance to help negotiate the risks of today's expanded attack surface. Every school is an island, struggling to figure out best practices on its own. Many of the cybersecurity frameworks are far more complex than what is feasible to implement in most K-12 environments. There has been little or no guidance provided by the federal or state departments of education.

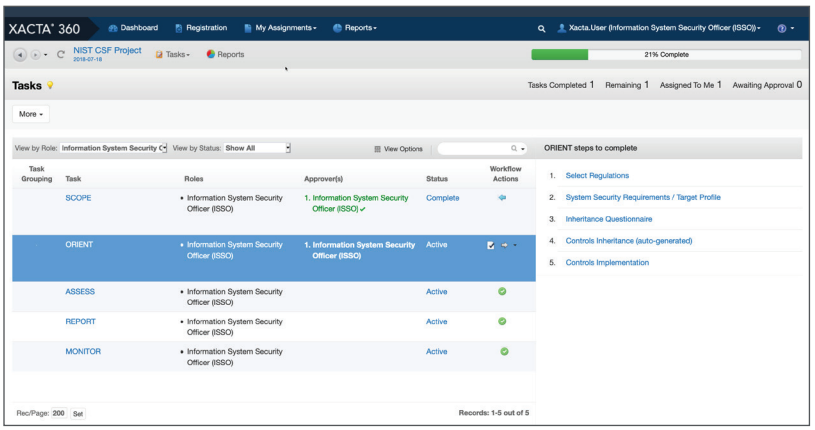
So each school ends up handling their cybersecurity in their own way – or, worse, assuming that their vendors are handling it all for them. A learning management system may include cybersecurity features such as SSL, IP blockers, and password authentication, or they may not... each school leader must decide for themselves how much is enough. But ultimately, the school itself is the primary custodian of its data and the school's decision-makers will be held accountable if a breach is successful.

Only 1 out of 5 school districts in the country have an employee dedicated to cybersecurity

Consortium for School Networking (CoSN) 2020 Member Survey

"We don't know what's on our network."

Ask a superintendent to name the cybersecurity threat they worry about most and they'll say, "Ransomware." Ask a CTO and they'll say, "DDoS attacks." But the real problem starts with a lack of visibility into their risk and security posture.



Xacta automates cybersecurity workflow giving the organization confidence that critical security requirements have been accounted for as part of an enterprise cyber risk management process.

Even before the pandemic, schools had a wide diversity of devices, including instructional technology, IoT devices, classroom iPads and Chromebooks, and BYOD tablets and laptops, as well as the student-owned phones and gaming systems that were brought onto campus each day. Now, networks are connecting with additional devices beyond their control: home computers that may be running outdated operating systems and SaaS services that teachers may be using to store sensitive student data.

Without knowing who or what is accessing the network and where data is moving, there is no way to apply proper policies or decide which assets need which controls. Visibility exposes that information so that resources can be directed where they are needed, whether that means updating a policy, adding a new firewall, or segmenting critical data behind additional defenses.

Limited budget. Limited IT staff. Limitless threats.

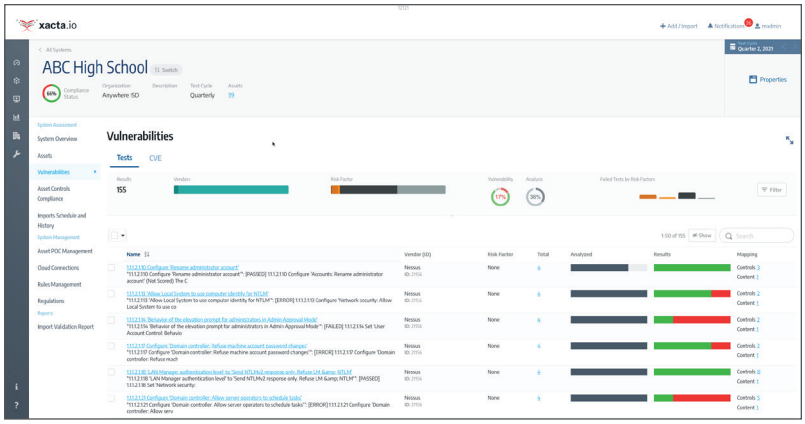
You *Can* Win This!

You don't have the people? You can still have the power — with Xacta.

Get your school district to the next level of cybersecurity maturity with **Xacta from Telos Corporation**, the cyber risk management solution that provides visibility, continuous auditing, and continuous vulnerability reporting.

For school systems implementing a cybersecurity practice, Xacta takes the form of a virtual cybersecurity team – managing the security workload, automating workflows and redundant tasks, and generating reports for action. It helps ensure ongoing cyber hygiene rather than getting by on a once-and-done basis. Xacta frees up limited IT staff to focus on strategic efforts instead of performing repetitive manual tasks that can introduce human error into the process.

Most school districts are operating on a distributed responsibility model: network engineers pull network security data, while endpoint people focus on security



Xacta allows you to drill into an area to pinpoint the vulnerability and allows you to take the appropriate actions before an event takes place.

standards and patching. All that data has to be normalized and shared in order to become actionable. Xacta eliminates those manual steps by using APIs to capture data from across the environment and make it available through a single console. IT staff gains a comprehensive view of the school's security posture, while CTOs get the information they need to make immediate decisions.

You can take remedial action *before* a crisis happens.

Xacta conducts continuous auditing and vulnerability reporting. Is the LMS running on an unpatched server infrastructure? You'll know. Are there repeated attempts to log into the systems happening at night? From China? You'll know, and you can use insights garnered from the Xacta platform to decide if a next step is necessary. Xacta reduces the time needed to analyze and confirm findings from across hundreds of thousands of assets, so you can count on comprehensive visibility at all times.

You can always be ready for an audit (and confident about your documentation).

Sometimes, things can happen no matter how prepared you are for it. As a byproduct of implementing a cybersecurity framework with Xacta, you will create a body of evidence that shows you've taken the right steps to keep students, teachers, and the community safe. But adhering to a framework takes work, and you don't have the staff to build all the processes and workflows from scratch.

Xacta makes this easy and provides process automation and workflows out of the box. Flexible baseline tailoring simplifies and speeds implementation, and a no-code interface makes it easy for IT staff to make changes on the fly in the future.

Contact Telos for More Information

Xacta helps K-12 educational systems protect their students, faculty, and administration by streamlining and automating cyber risk and security automation best practices. To learn more, please contact us for a conversation about the challenges you face and to and arrange a demonstration of Xacta's capabilities. We look forward to assisting you to provide a safe and secure learning environment for your students and staff.

Your investment in Telos offerings for cybersecurity, risk management, and compliance may be eligible for coverage by ESSER or GEER funds through the U.S. Department of Education. Contact the grants and funding office for your district or state or ask your Telos representative for further information.

Telos®

Solutions that **empower** and **protect** the enterprise.™

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | info@telos.com | www.telos.com