SETDA Cybersecurity & Privacy Collaborative

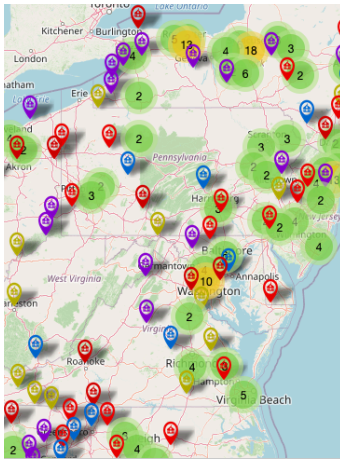
MARCH, 2022

K-12 CYBERSECURITY LANDSCAPE SCAN

Contents

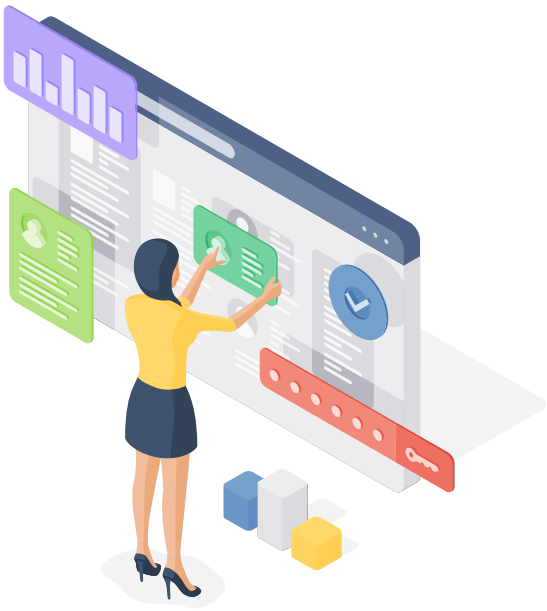
In 2020, one of the largest school districts in the country received a report from an outside consultant warning them that their network showed a "severe inability to identify, defend, contain and remove a real-world threat." In 2021, that assessment proved correct, as district systems were breached by hackers who accessed decades worth of personal information from 800,000 individuals. In 2022, we learned what the district had been reluctant to share about this event – the two perpetrators of this crime were students.

This is a familiar story. Many districts, much smaller than the one in this example, struggle to access the cybersecurity expertise or other resources needed to secure their networks and data appropriately. This isn't because mitigation strategies don't exist. Often, the barrage of suggestions and warnings directed at school IT leaders are too overwhelming to navigate, are not properly scoped for educational situations and infrastructure, or the financial and human resources to implement them are inadequate. Proper cybersecurity practices and routines, much like the networks and other infrastructure they are meant to protect, are new, continually developing, and changing at the pace of technological innovation.



Learning from the experiences of others would sometimes point the way, but this is hampered by the fact that districts are reluctant to discuss those moments that might not play well in the news. Even with this tendency to under-report, the number of incidents we know about is still staggering. The K12 Security Information Exchange (K12 SIX) hosts the K12 Cyber Incident Map, tracking incidents since 2016. No state has remained unaffected with more than 1,300 hacks, attacks, and other incidents.

To better share information and create awareness to help states address these growing concerns, SETDA, with the support of the Bill & Melinda Gates Foundation and in partnership with K12 SIX and CoSN, has created a Cybersecurity and Privacy Collaborative. This unique group brings together the expertise of technology leaders from some twenty state departments of education and a dozen trusted edtech partners from the private sector. As the group begins its work together, this report represents their shared perspective on the K-12 cybersecurity landscape for 2022.



CRITICAL VULNERABILITIES AND DIFFICULTIES FOR K-12

As more school data moves online and more daily instruction occurs in digital environments, schools and their instructional and informational infrastructures are common targets for malicious actors. Some act for financial gain, others for intellectual curiosity. Still, others are vandals, unintentionally or otherwise. Districts are aware of these actors and have been working for some time to mitigate the threats they pose. Many confounding factors make this an uphill battle for schools. Members of the collaborative shared their most pressing concerns for states and local education agencies (LEAs):

- **Human factors** - Although districts have implemented hardware and software to strengthen the security of their networks and data, they also contain thousands of humans (adults and students) who act for various reasons or motivations, sometimes in ways that compromise or circumvent that security. Attackers can easily launch millions of phishing attacks; meanwhile, defenders can be compromised by one person clicking the wrong link. Social pressures and circumventions are significant risks that require attention, training, and continual revision and reminder.

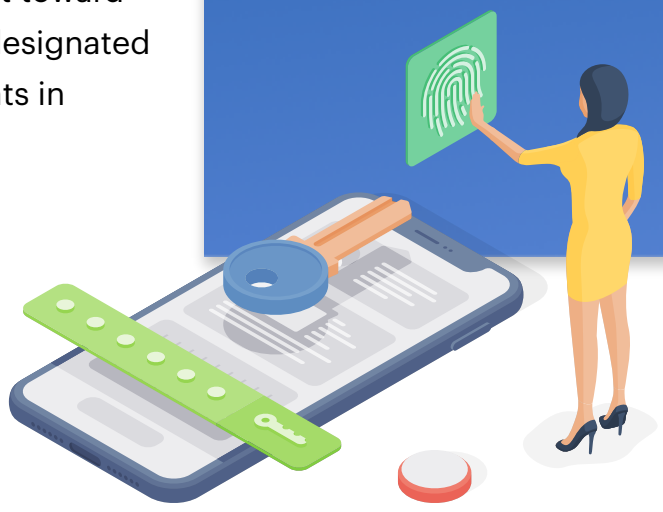
- **Third-party connections** - As networks increase in complexity and scope, when light switches, security cameras, and thermostats are all potential targets for intruders, the growing patchwork of connected devices present in schools and offices creates more complexity and risk. Hundreds of edtech applications also demand access to school networks and data, and these external relationships must be meticulously managed to eliminate opportunities for data or hardware to become compromised.

- **Leadership awareness** - Not raised with technology themselves, many superintendents are not fully aware of the importance of cybersecurity until they face a crisis. It is also easy for cybersecurity to get lost amid other priorities to which school leaders must devote attention and professional development. These concerns can be somewhat offset if the superintendent has a strong IT/edtech voice at the cabinet level, but many districts have yet to elevate this critical role.

- **The complexity of funding** - A fundamental misunderstanding of what it takes to "buy" vs. "own/manage/support" school technology has been exacerbated by pandemic relief to schools, creating additional vulnerabilities amidst a swarm of new devices and equipment. While legislation shows some movement toward investing in cybersecurity, more designated funding is necessary. If investments in security measures are seen in competition with classroom instruction or student productivity, security posture is likely to be compromised.

Michigan Educational Technology Leaders

Michigan has established a group of regional & intermediate unit technology experts. Their cybersecurity task force has developed a website to share resources such as cybersecurity essentials, the quick audit tool, and professional learning for staff.



- **Access to security expertise** - Information is easily distributed, and people with that necessary information and knowledge are not. While some districts are large enough to support an entire cybersecurity division, smaller districts aren't likely to afford even one position with security expertise or have access to that expertise from a distance. Lack of access to security expertise poses a threat to staff and students alike.

- **Proof of proper controls** - Rapidly increasing demands from cybersecurity insurance companies has districts scrambling to avoid being left with a diminished capacity to recover from an incident. Districts must now show proof of proper controls, including evidence of planning, procedures, risk assessments, and awareness training just to cross the threshold of insurability. While this has the effect of pushing schools toward a stronger security posture, it will also provide a greater hardship to those unable to keep pace with these demands.

LEGISLATIVE IMPACT AND NEEDS

The increase of legislative attention to cybersecurity shows that states and the federal government are aware of immediate needs. According to CoSN's 2021 State and Federal Cybersecurity Policy Trends, 2021 saw the introduction of 170 new cybersecurity bills which focused on the education sector. This number nearly doubles the 87 bills introduced in 2020. Many of the 51 bills that became law in 2021 were focused on incident reporting and information sharing and the dedication of funding for state agencies. Members of the collaborative shared that these were the things they most wanted policymakers to know:

- **Incidents remain underreported** - Despite the number of incidents already being documented, state leaders believe the actual number is much higher due to districts' tendency to under-report their incidents. Efforts to encourage secure, no-fault reporting and information sharing would greatly help districts identify and address threats.

- **Training is critical** - Many school data breaches result from human error, not failures in software/hardware. It is vital that user training be required and resourced.

- **Collaboration lessens the burden** - While there are considerations around digital security unique to schools, educational entities shouldn't be alone in this work. In-state collaborations, inter-agency coordination, and state-wide solutions are necessary and, where implemented, beginning to provide effective and affordable solutions in several states.

- **Investments must be sustained** - While less expensive than incident management, mitigation strategies involve ongoing maintenance costs rather than one-time fees. Districts who cannot afford or locate security professionals, or keep staff who gain this expertise, will need to contract with managed service providers. Time, professional learning, and attention of leadership to these issues also add to costs.

- **Dependable access requires network security** - The federal E-Rate program provides funding for Internet connections to 95 percent of K-12 students, limiting cybersecurity readiness expenditures. Expanding the E-Rate program to include necessary and essential cybersecurity equipment and services ensures equitable and dependable access for schools and districts, allowing them better tools for protecting students and their data.

Massachusetts Municipal Grant Program

The Massachusetts Executive Office of Technology Services and Security has offered and managed a Municipal Cybersecurity Awareness Grant, which provides comprehensive online end-user training, evaluation, and threat simulation to awarded municipalities and public school districts. Also, the Cybersecurity Health Check is an opportunity for any city, town, or school district to access basic cyber security services at no cost.

STRENGTHENING STATE RESPONSE

State-level education agencies are uniquely positioned to strengthen the K-12 response. Members of the collaborative are primarily focused on the following activities to help LEAs manage the burden of cybersecurity:

- **Sharing learning and resources** - States explore their ability to share more than just guidelines and documentation. They are partnering with cybersecurity experts to create a common roadmap for LEAs.
- **Educating district and school leaders** - States can help put cybersecurity on the radar for local leaders. State leaders who prioritize communicating threats and opportunities help make cybersecurity a priority for local leaders.
- **Promoting response and recovery strategies** - Knowing that cyberattacks are a matter of "when" rather than "if," states must insist that LEAs discuss and plan for how they will react when the inevitable happens and provide the resources to support recovery strategies
- **Sharing incident data** - States would significantly increase their insight into threats and patterns if they could lessen the stigma of reporting details of a cybersecurity breach. Creative solutions are needed to allow this data to get to state leaders without greatly increasing the sphere of people who need to know about a particular system's breach.
- **Developing mitigation strategies** - States are working to identify a tiered list of mitigation strategies that might support districts entering the conversation at differing stages of implementation.

Minnesota Partnerships

A Minnesota cooperative has a network/security administrator who works with schools to provide risk assessments, policies, and procedures to help mitigate risk and security awareness training for staff. They have also formed a partnership with two private companies that share the mission of bringing quality, affordable cybersecurity services to K-12 schools.

- **Building collaboratives** - States are making progress by sharing resources and best practices. Districts are banding together through service centers or cooperatives to supplement LEA cybersecurity expertise and help train their staff.
- **Engaging expert partners** - States have increased K-12 expertise by partnering with state police and other public entities and organizations and companies who can provide their schools with affordable cybersecurity services.

- **Group purchasing** - There are vast economies of scale in state-wide purchasing or LEAs collaborating on cybersecurity-related services such as risk assessments, vulnerability scanning, penetration testing, and security awareness training.

KEY RESOURCES

There is no shortage of information and guidance for strengthening your cybersecurity posture. One trick for K-12 is that much of the information is not appropriately scoped for educational infrastructure. One example of an excellent resource that might not be in the best form to be taken up by school leadership is NIST's 55-page Framework for Improving Critical Infrastructure Cybersecurity. Often, these resources are designed to be considered within local contexts and needs. However, states and districts often crave a more accessible starting point. Collaborative state leaders have generated the following list of resources they lean on for support and direction:

- **Cybersecurity & Infrastructure Security Agency** (CISA) - The Operational Lead for Federal Cybersecurity, known for resources like their free cybersecurity services and tools.
- **Center for Internet Security** (CIS) - Community driven nonprofit, recognized for best practices for securing IT systems and data. Also manages the Multi-State Information Sharing and Analysis Center (MS-ISAC), trusted for cyber threat prevention, protection, response, and recovery.

- **K12 Security Information Exchange** (K12 SIX) - Cyber threat information sharing community dedicated solely to the needs of U.S. primary and secondary education organizations, known for their K12 Cyber Incident Map and Essential Cybersecurity Protections for School Districts.

- **CoSN Cybersecurity** - CoSN is a membership organization supporting K-12 education technology leaders with resources for cybersecurity and other priority topics.

Further work in the SETDA Collaborative will be to curate resources that scope best for SEAs and LEAs to use with access to varying levels of expertise.

NEED FOR STATE ADVOCACY

By identifying these trends and opportunities, SETDA is working with states to further their thinking about the role of cybersecurity in the K-12 sector. While schools have made strides in adding curriculum to teach cybersecurity, this does not address the current security of school networks and data. States have a responsibility to establish cybersecurity as a priority, and ensure that schools and districts are good stewards of the student data entrusted to them. Communication is the greatest opportunity, as we educate leaders and advocate for support. Concise information sharing is needed to raise public awareness and help legislators increase the priority for cybersecurity funding.

The best path forward is collective action, attacking the problem together rather than in isolation. Many government entities are facing similar threats, and are critical partners in sharing best practices. Keeping pace with rapidly evolving threats requires bringing multiple angles and perspectives to bear on the problem. Successful states are already building coalitions within their borders, and SETDA has brought the best of these together in a collaborative that will allow those ideas to be spread more broadly.

This report was funded by the Bill & Melinda Gates Foundation. The views expressed are those of the author(s) and should not be attributed to the foundation.