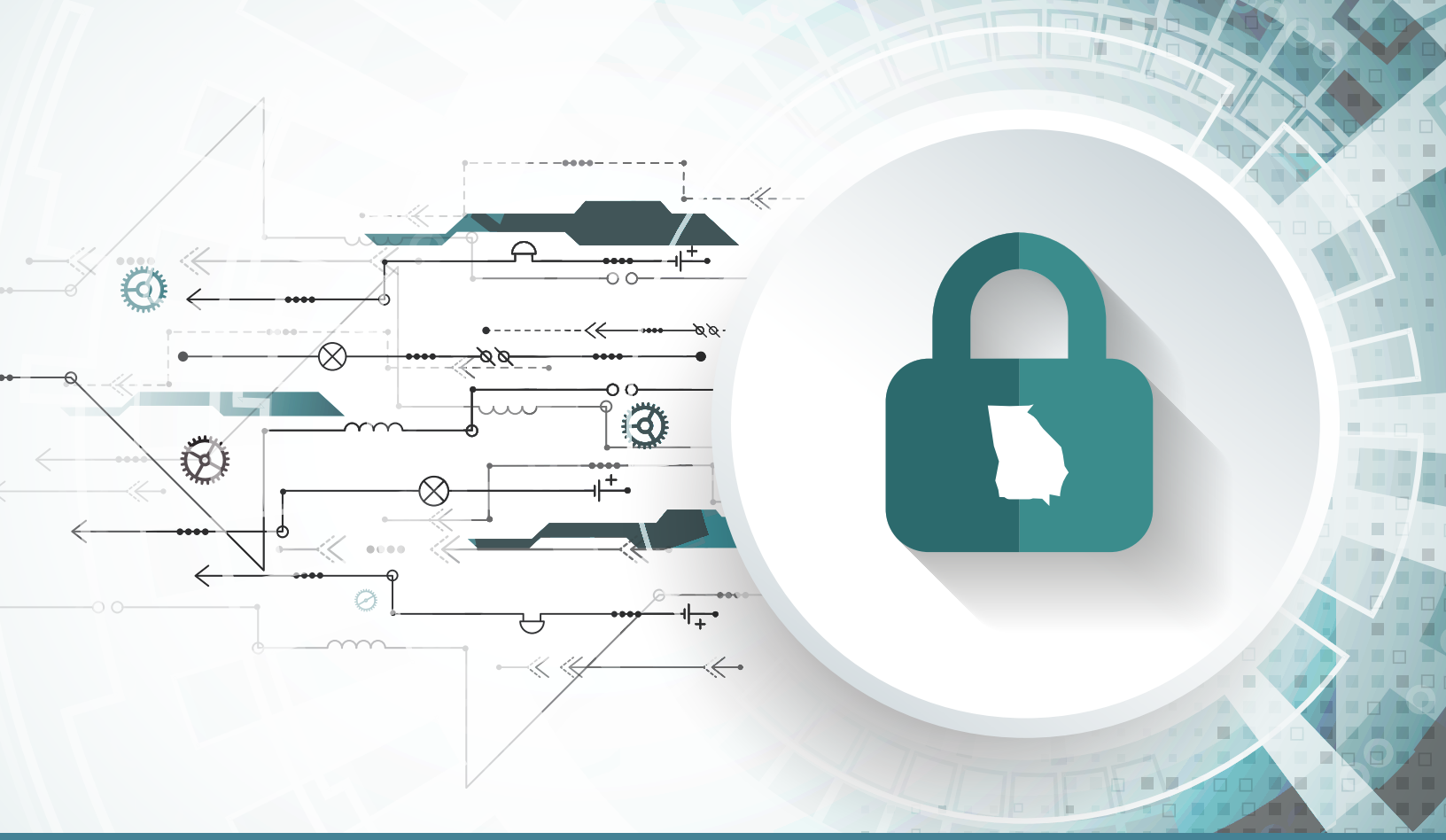


AHOY, CYBER DEFENDERS: GEORGIA SAFEGUARDS ITS SCHOOL DISTRICTS

NASCIO 2023 State IT Recognition Awards

STATE: Georgia

AGENCY: Georgia Department of Education
Georgia Technology Authority

CATEGORY: Cross-Boundary Collaboration and Partnerships

PROJECT INITIATION DATE: January 2022

PROJECT COMPLETION DATE: December 2022

CONTACT: Shawnzia Thomas
CIO for the state of Georgia and Executive Director of Georgia Technology Authority
Shawnzia.thomas@gta.ga.gov | (404) 463-2300

EXECUTIVE SUMMARY

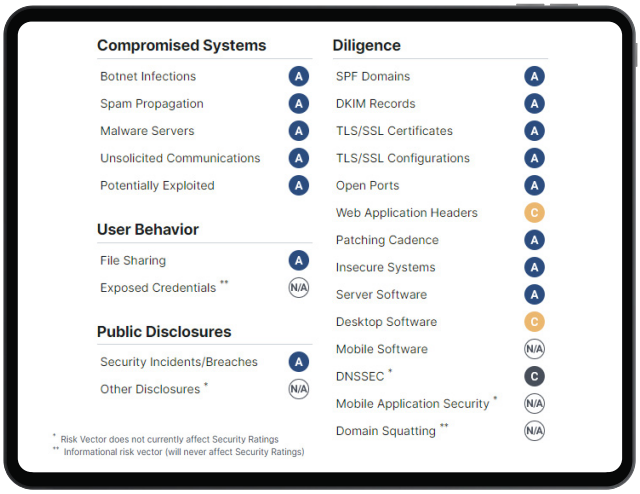
Open ports may be a welcome sight for sailors, but they can be real trouble in cybersecurity. Those unsecured ports on a network are like open doors on a house and provide an easy way in for intruders. Locking them down has to be a high priority for cyber defenders. K-12 school systems, like so many other organizations, know firsthand just how treacherous the sailing can get if defenses slip.

The Georgia Department of Education (GaDOE) works to ensure the state's 181 local school districts have the cybersecurity capabilities needed to avoid rough seas. Through a partnership with the state's central IT agency (the Georgia Technology Authority), GaDOE secured a cyber risk management solution it now makes available to the districts.

The Bitsight security monitoring technology allows school districts to proactively identify, quantify, and mitigate the risk of vulnerabilities ranging from unintended open ports to vendor partner security practices, to unsecured wi-fi networks.

Already, 70 percent of Georgia's school districts are using Bitsight's 24/7 network monitoring and notification. With it, they can better track potential malicious activity and respond sooner.

GaDOE leveraged its buying power to purchase a license for the service for all school districts in the state. Today, each district has access to its own unique Bitsight tenant (or operating space) where it sees information on only its cybersecurity landscape. It has been well received by participating districts, and GaDOE anticipates renewing the licensing. Broadly, this initiative is bolstering security, aligning with best practices, reducing overall costs, maximizing efficiencies, increasing knowledge transfer, reducing duplication of work, and streamlining processes and services. The centralized approach costs only a fraction of what all districts acting individually would have cost.



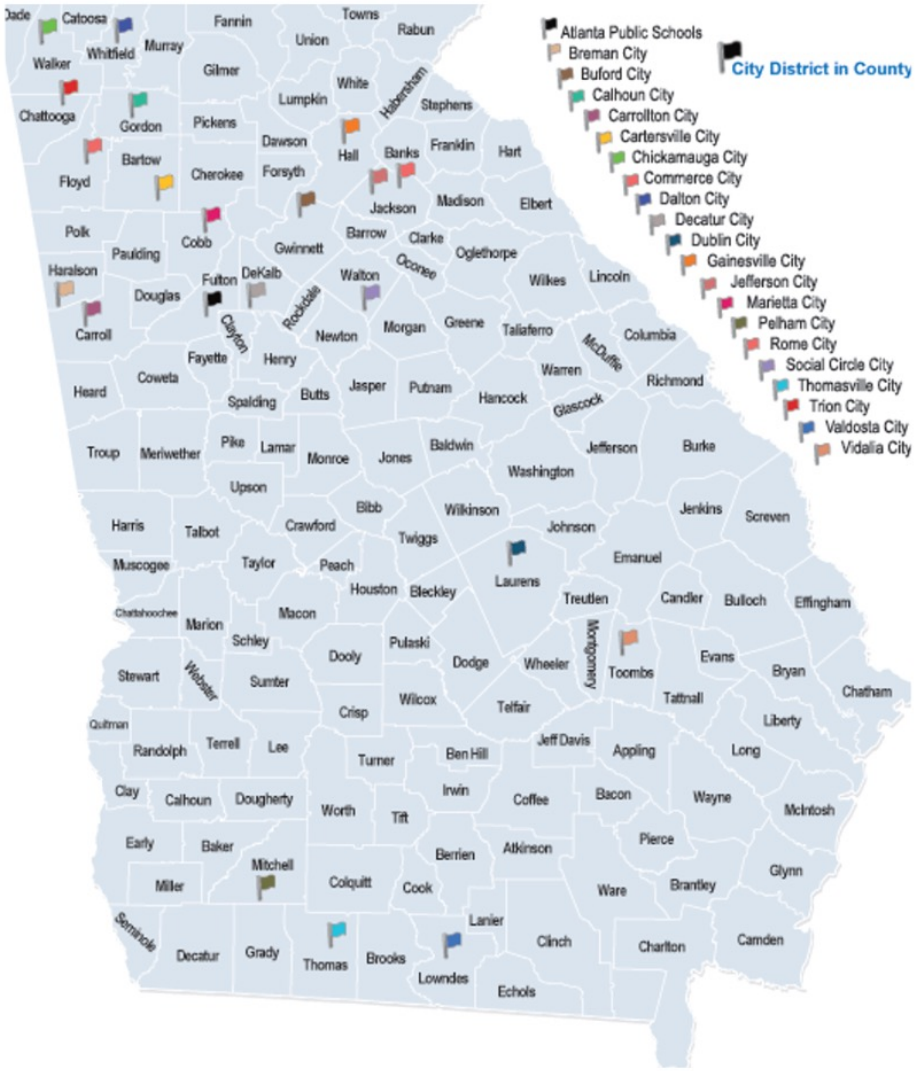
This view from the Bitsight dashboard shows at a glance what's been compromised, what's vulnerable, what breaches have happened, and what user behaviors could create risk. Letter grades, A-F, are assigned based on findings from security monitoring. As grades descend from A toward F, likelihood of a security incident rises.

The added security earned by Georgia school districts is paralleled at other state agencies (e.g., the Technical College System of Georgia and its 22 colleges) that have adopted Bitsight through GTA. With that track record of success, GTA's Office of Information Security has good reason to continue extending Bitsight to still more state agencies. Georgia's experience with Bitsight deployment leaves it convinced that building relationships and earning trust across state entities is a repeatable approach that could be successfully applied by other states and areas of government to enhance cybersecurity and benefit citizens.

70 percent of Georgia's school districts are using Bitsight's **24/7** network monitoring and notification

IDEA

As with many states, schools in Georgia operate in districts governed by locally elected school boards and superintendents. While they enjoy considerable autonomy in operations, there is an interconnectedness among districts and state entities like the Georgia Department of Education. Information is routinely exchanged between local and state IT systems. So even when cybersecurity risk originates locally, it has potential to quickly spread across districts and the state.



Resources (e.g., financial, human, and more) vary widely across Georgia's 181 school districts and their 2,200 schools. Not surprisingly, there is great disparity in cybersecurity capabilities. Some districts, especially smaller ones, may even contract out the whole of their IT operations. The Georgia Department of Education understands that spectrum. GaDOE sought a practical means of helping them all – from districts with mature cybersecurity programs to those just getting started.

The Georgia Technology Authority shares an interest in promoting cyber defenses across state government. The prospect of gaining visibility into cybersecurity posture across a range of component entities (whether state agencies or school districts) brought GTA and GaDOE together. Bitsight's security monitoring platform presented a means of opening up that consolidated view. It could provide consistent, real-time risk monitoring data on a continual basis, and that could be used to inform cybersecurity decisions.

Early monitoring by Bitsight confirmed that school districts had plenty of opportunities for shoring up defenses. As mentioned already, those often took the form of:

- **Unintended open ports**
- **Security practices of a district's vendor partners**
- **Unsecured wi-fi networks**

The case was made – additional attention to security was needed. And the Bitsight monitoring could help identify in real time where it was needed most.

IMPLEMENTATION

In 2022, GTA partnered with GaDOE on cybersecurity. The Georgia State Board of Education approved the state school superintendent's recommendation to provide licensing for a nationally recognized cybersecurity platform to each school district through a contract with GTA.

GaDOE dedicated $970,000 in federal funds to the licenses. (School districts would not be responsible for the cost.)

Several prospective beneficial outcomes were imagined:

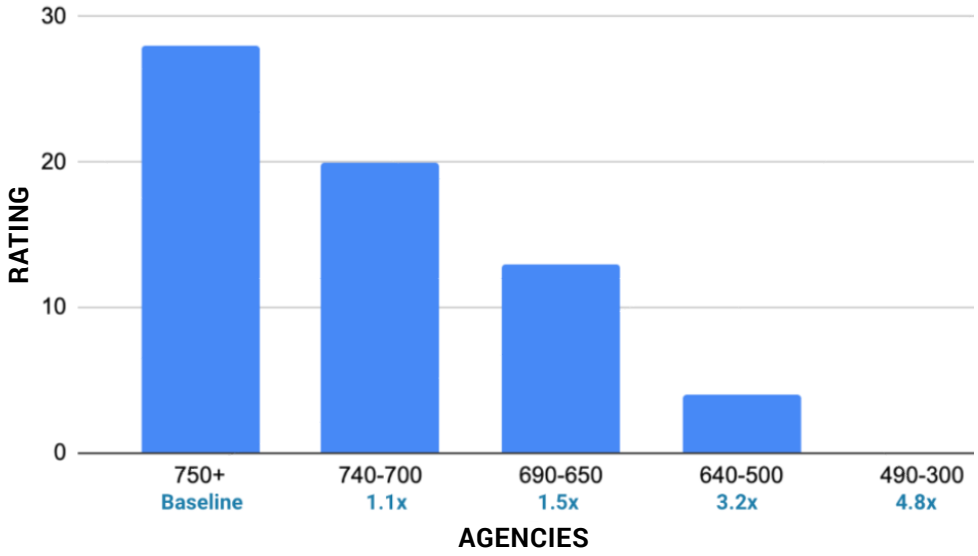
WHAT IF **School districts could see their cybersecurity vulnerabilities the same way potential attackers would, and then address weak spots sooner?**

WHAT IF **A tool already in use by GTA could be leveraged and made available to school districts so they could build security capabilities previously out of reach due to cost, limited resources, or other factors?**

WHAT IF **Overall cost could be reduced, efficiencies maximized, knowledge transfer improved, duplication of work reduced, and the gulf separating the haves and have-nots among districts trimmed or made less consequential?**

Since 2022, GaDOE has worked with local school districts to onboard their information security team members onto the Bitsight platform. Those district technology directors then complete an initial one-hour training session organized by GaDOE and delivered by the Bitsight training team. It explains the workings of the Bitsight dashboard, where security vulnerabilities are summarized. The Bitsight training team then conducts subsequent monthly training sessions where the technology directors, or information security officer if a district has one, can develop aptitude interacting with the dashboard, checking the risk categories, and understanding the security ratings.

Bitsight distills its findings into understandable risk categories like compromised systems and user behavior. It also calculates an overall security rating, something like a credit score. The security ratings can range from 250 to 900, with higher ratings associated with better cybersecurity posture. Bitsight has determined organizations rated at the lowest end of the scale are nearly five times as likely to experience a cybersecurity incident as organizations with ratings of 750 or higher. The chart to the right shows a distribution of point-in-time security ratings for Georgia agencies that use Bitsight monitoring. The numbers in blue indicate the cyber incident risk multiplier as security ratings decrease.



IMPLEMENTATION *(continued)*

GaDOE also uses its *GaDOE Community* online platform for information exchange on topics such as Bitsight with the school district community. This is complemented by monthly calls between GaDOE and district CIOs to cover not just Bitsight but the fuller range of technology considerations. This active conversation among the community is what keeps the school districts alert to trending vulnerabilities they should check on their own dashboard.

Each participating district now has its own tenant (or operating space) in Bitsight. That ensures a district's security posture evaluation is accessible only to that district and not to the others. Each district preserves the autonomy to manage how it addresses security vulnerabilities identified.

Because every school district's network connects at some level with GaDOE, a vulnerability at any school district is, in fact, a vulnerability for all districts, and the state's network. Couple that with an absence of any unified or standard network architecture across the 181 districts, and GaDOE's decision to prioritize detection and response capabilities for the whole community seems well chosen.

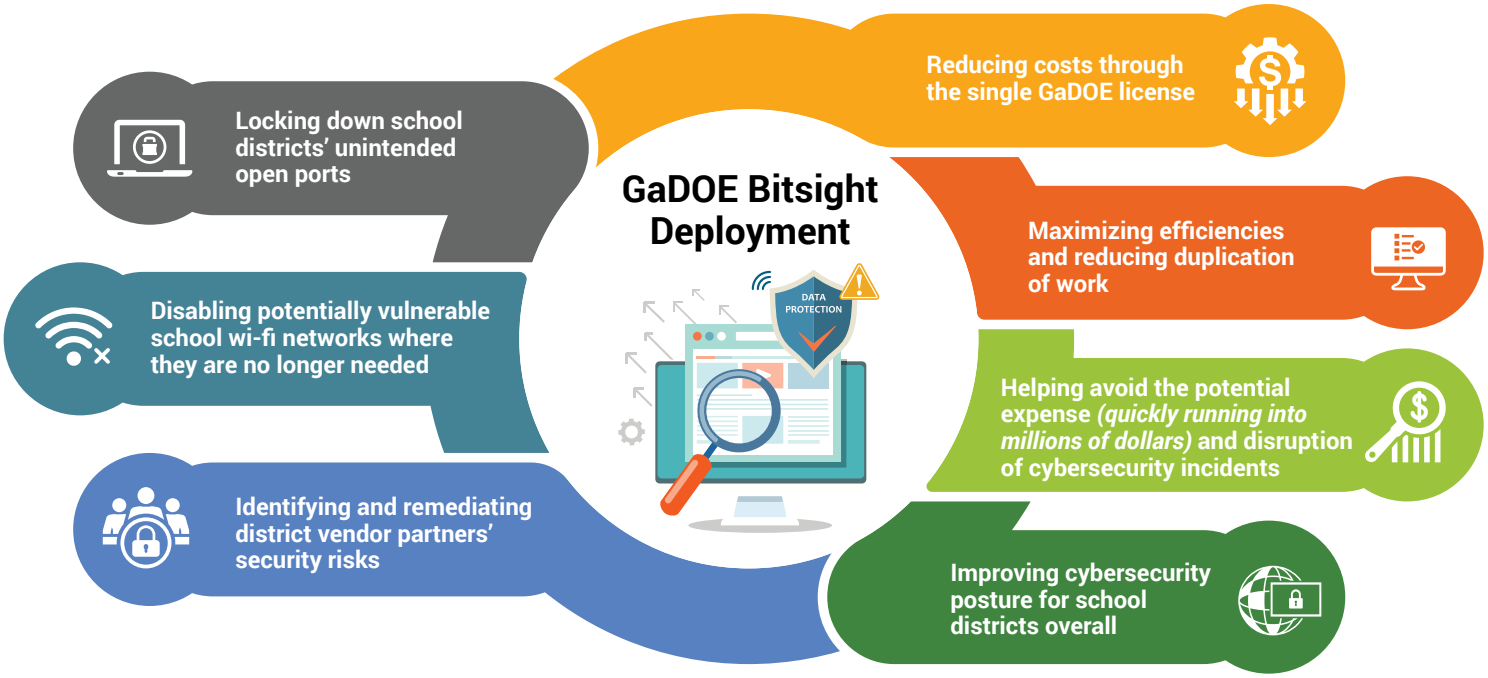
After GTA coordinated onboarding GaDOE to Bitsight, the Department of Education then helps onboard local school districts. Some 70 percent of districts are onboarded and now benefit from Bitsight's 24/7 network monitoring and alerts of any potential vulnerabilities. The school districts gain enhanced detection and awareness of any potential malicious activity or attacks against their networks and can respond more rapidly. GaDOE gains insights across the extended school district network perimeter.

GTA, GaDOE, and the school districts have reported favorably on rewards of the Bitsight monitoring, and GaDOE anticipates renewing the license in the future.

IMPACT

As of 2023, GTA's Office of Information Security has helped put Bitsight monitoring in place for 60 state agencies, Georgia's Department of Education being one. And GaDOE's implementation has Bitsight deployed for 70 percent of the state's K-12 school districts.

Positive outcomes of the GaDOE Bitsight deployment specifically include:



GaDOE hopes to build on the strength of its BitSight implementation with several related efforts. First, it plans to organize training for school districts on how to effectively secure their cloud environments. Second, it envisions a CISO-as-a-service offering through the Georgia Cyber Center allowing school districts to purchase services such as creating security plans, business continuity plans, and more. And third, GaDOE is considering enhancing dashboards to highlight high-performing school districts in a given security category. The thinking is this might promote informal collaboration among districts toward adopting successful security practices.

The broader rollout of Bitsight by GTA to other state entities has also paid dividends wherever the tool has been adopted. Importantly, it has cultivated new partnerships and collaboration across Georgia government – an essential element of effective cybersecurity, where the task is simply too big for any organization to manage on its own. It has broadened GTA's insight into security practices of Georgia government entities. And of course, it has bolstered the state's overall cybersecurity posture.

Georgia's approach to deploying this monitoring and notification platform offers one model other states might replicate for introducing security services to a broad range of government entities.

And for cultivating security partnerships across those entities. When industry watchers (e.g., the Ponemon Institute and IBM Security) estimate recovery costs running into the millions of dollars for a single data breach or ransomware attack, understanding where your vulnerabilities are becomes a survival tactic. Ignore that security capability, and something as tame-sounding as an open port could just swallow you whole. The Bitsight implementation is helping Georgia government and the states' school districts stay top-side.