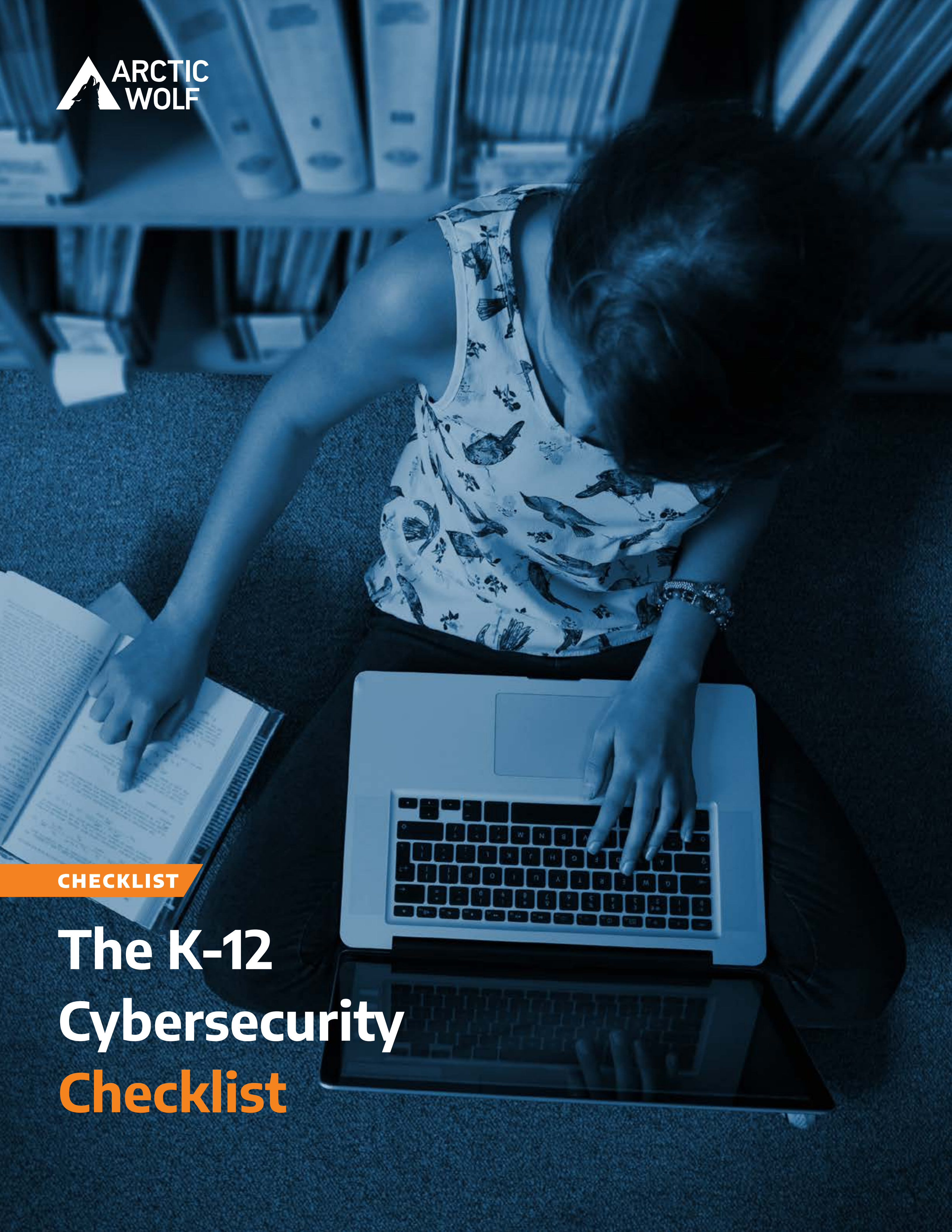


CHECKLIST

The K-12 Cybersecurity Checklist

THERE HAVE BEEN OVER **1,300 BREACHES** ACROSS THE EDUCATION SECTOR SINCE 2005[1]

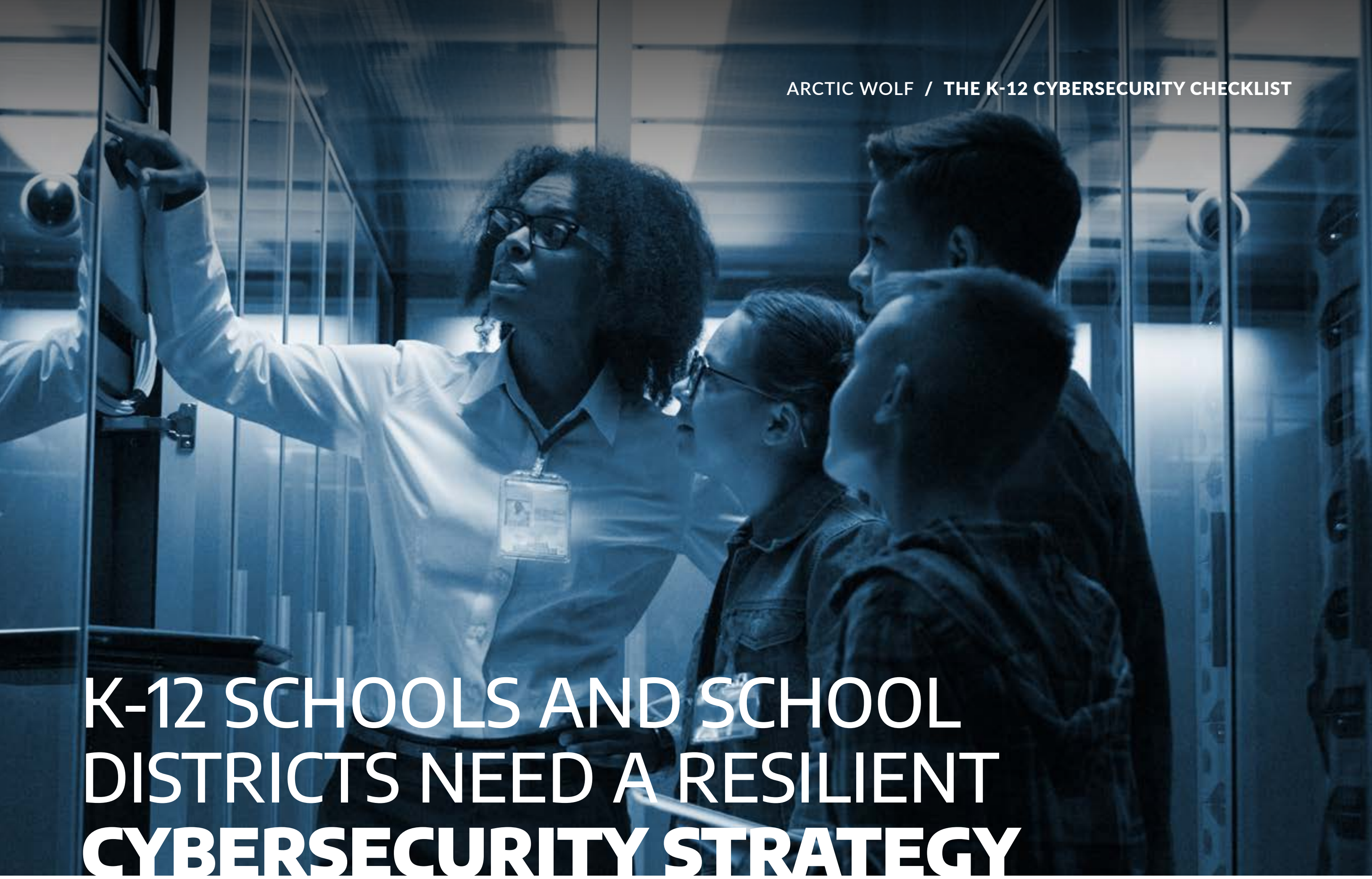
/// Nothing in our connected world is out of bounds for bad actors in cyberspace. As schools increase their use of technology for teaching and learning, cybercriminals prey on under-resourced IT departments that are vulnerable to penetration.

According to a study from Comparitech.com, K–12 school districts, along with colleges and universities across the U.S., have suffered more than 1,300 data breaches since 2005, impacting more than 24.5 million records. Institutions of higher education account for two-thirds of these data breaches, but K-12 school districts are not immune.

In 2019, two breaches linked to aimsweb—the Pearson Education student assessment tool—compromised 673,487 records in school districts in Nevada. And a phishing attack in 2018 on the San Diego Unified School District enabled hackers to access the central student database, affecting approximately 500,000 student records.

$2.3M

The amount a school district in Texas lost due to a single phishing scam.[2]



K-12 SCHOOLS AND SCHOOL DISTRICTS NEED A RESILIENT **CYBERSECURITY STRATEGY**

Schools rely on technology for their day-to-day operations, but few schools can afford to dedicate a full-time IT staff member to cybersecurity. This leaves them vulnerable and often unprepared to prevent or mitigate cyberattacks.

Even a prank distributed-denial-of-service (DDoS) attack can take out a school district's network for days or weeks. More nefarious attacks range from knocking out online testing events to more criminal activities, such as accessing financial information or sensitive personal data.

Whatever the motivation, K-12 schools and school districts need a resilient cybersecurity strategy that meets both existing and future threats, which becomes critically important as schools continue to invest in technology to better educate our young people.

Use this checklist to develop your cybersecurity strategy, step-by-step:

Create a Security-Conscious Workforce

Employees who aren't well trained in IT security take shortcuts to help them work more efficiently. They might share the same password for certain programs or even leave passwords lying around on Post-It notes. The best way to account for human error is to create a culture of security at work, supported by training and resources.

- ✓ **Implement an ongoing schedule of training and education for all workers**. Include updates on known attacks and information about best-in-class security procedures, such as two-factor authentication and password managers.
- ✓ **Monitor IT processes for complexity.** Keep ease-of-use in mind whenever you update or alter processes to avoid users turning to insecure shortcuts.
- ✓ **Implement data usage controls** that can block unsafe actions like uploading data to the web, sending emails to unauthorized addresses, or copying to external drives.
- ✓ **Establish a password policy** that requires using strong passwords as well as regular password changes, and forbids written copies of passwords.

Train Staff on Breach Protocols

It's vitally important to try to protect your networks from data breaches, but it's also critical that your staff know what to do when a breach occurs. Employees should understand the sequence of steps to take following a breach, and IT staff should have the know-how to reinstate security systems as quickly as possible.

- ✓ **Create a response team that's always ready for action.** In addition to IT staff, include legal, operational, HR, risk management, and PR personnel on the response team.
- ✓ **Determine which systems were affected and what data was compromised.** The team's first job is to determine the extent of the breach so a full response can be put in place. As part of your response, make sure to notify relevant authorities and users.
- ✓ **Change user passwords** in terms of systems and software for any accounts possibly impacted.
- ✓ **Fix any vulnerabilities.** Analyze the attack and ensure that the security team addresses any vulnerabilities.

Inventory and Control of Hardware and Software Assets

School staff will often access networks on their own devices, including from personal laptops and smartphones. They may also download tools that they think will prove useful, even if they aren't on your list of approved software. To effectively protect data and devices, you have to know what you have and what you use.

- ✓ **Document and secure all devices that could access the network,** including personal devices.
- ✓ **Use secure configurations** for mobile devices, laptops, wireless access points, workstations, and servers.
- ✓ **Use inventory tools to keep up-to-date records** of existing software and hardware. Block unknown executable files, and automatically install software updates and security patches on all computers.
- ✓ **Quickly disconnect any unauthorized devices** detected on the network, as well as devices that run potentially dangerous software.

Create Privileged Access to Critical Assets

Restrict access to the most sensitive data, providing access to the fewest number of employees as possible. While It's not necessary to expend valuable resources to protect public data, like the school calendar, it is necessary to put the strongest protections on student's personal and financial information. Map and identify the data and systems that need the most protection and then ensure that only a privileged few have access.

- ✓ **Store data securely** to ensure that all the school community's records are kept private and in compliance with the Family Educational Rights and Privacy Act (FERPA).
- ✓ **Restrict access to data and applications** to only those users who need the information to perform their job—and follow the same protocol for physical access.
- ✓ **Oversee all user access to the network,** record authentication errors and unauthorized access, and sweep the network for unusual activity.
- ✓ **Restrict administrative privileges** and carefully manage those employees who can access the most sensitive data.
- ✓ **Regularly audit access lists** to remove former staff members and students who have left the district.

Continuously Analyze, Prioritize, and Manage Vulnerabilities

The only way that K-12 school districts can truly be secure is with 24x7, real-time cybersecurity operations that not only manage vulnerabilities, but also monitor, detect, and respond to threats. For most schools and districts this isn't something that can be managed in-house, but instead it requires an outsourced security team that can help manage operations and respond to malicious and risky activity in real time.

- ✓ **Identify vulnerabilities and prioritize what needs patching.** A risk-based approach to vulnerability management enables schools to eliminate vulnerabilities in a methodical fashion, starting with the most severe risks before addressing less severe ones.
- ✓ **Have a detailed response plan in place,** not only to prevent breaches but also to respond to cyber incidents as they happen.

Make Distance Learning Safe and Secure for Students

Distance-based learning was already a factor for many school districts, but the onset of the COVID-19 crisis has meant huge numbers of students suddenly learning from home. This at-home learning is enabled by collaboration tools and video-conferencing software, but these applications can also provide hackers and cyberattackers with a way into your network.

- ✓ **Only use pre-approved tools.** As interest in videoconferencing has skyrocketed, the number of tools with innovative and powerful features has also grown. It can be tempting to use the newest software, but IT should vet and approve all tools for video calls and collaboration before their use.
- ✓ **Secure access to online meetings.** All video conferences should be secured by passwords with meeting links sent directly to students. Carefully review any meeting invitations sent to the school to ensure that they have come from a known email address.
- ✓ **Educate users on safety.** Both teachers and students should know the basics of protecting themselves in online meetings. They need to be aware of what will be seen on camera when they join an online meeting. They also need to change their default settings on home Wi-Fi networks and use strong passwords.

Maintain, Monitor, and Analyze Audit Logs

Without audit logs, attacks may go unnoticed and uninvestigated. That leaves the door open to additional attacks and untold potential damages. Most IT teams keep audit records for compliance purposes, but attackers know there are many school districts that lack the time or resources to review logs on a regular basis. This results in an ample window of time to access systems and data undetected.

- ✓ **Log, monitor, and analyze security risks.** Record and examine log activity and analyze the resulting log information.
- ✓ **Continuously monitor** to ensure you have an audit trail when an incident occurs.
- ✓ **Perform regular risk assessments to identify weak points in the system.** Schools and school districts can get support from the U.S. Department of Homeland Security or data security firms.
- ✓ **Be ready to report.** Use managed vulnerability assessment services to gain an understanding of your organization's IT security posture and risk profile.

Back up Data Offsite

Data loss is a common consequence of all kinds of attacks. While stolen personal information of students must be handled a certain way, criminals will also steal data or code that is critical to running services. A second cache of this data is essential to ensure continuity of services, and also enables data recovery in the event of a natural disaster or system failure.

- ✓ **Maintain a current, flexible, secure, and speedy process to access data at all times.** Schools need a solution that allows them to recover data and bring applications back online as seamlessly as possible.
- ✓ **Consider cloud and physical backup solutions,** and develop a backup schedule that accounts for the frequency of data changes.

A phishing attack enabled hackers to access

500,000 STUDENT RECORDS

at San Diego Unified School District.[3]

STAY ON TOP OF COMPLIANCE AND **NEW LEGISLATION**

As education technology has evolved, the need for dedicated cybersecurity legislation for school districts has become apparent. Existing legislation enacted at the state level includes:

✓ **Texas Senate Bill 820,** which requires each Texas school district to:

- Adopt a cybersecurity policy.
- Designate a cybersecurity coordinator (appointed by the superintendent).
- Report cybersecurity incidents to the Texas Education Agency (TEA) and district families.

A district is required to have a cybersecurity policy in order to:

- Secure district cyberinfrastructure against cyberattacks and other cybersecurity incidents.
- Determine cybersecurity risk and implement mitigation planning.

✓ **Georgia General Assembly 31** appropriates funds for cybersecurity training and cybersecurity initiatives in schools.

✓ **Keeping Georgia Schools Safe Act** requires public schools to conduct site threat assessments by a certified private individual or company, or by a government agency. Every public school must conduct a site threat assessment before January 1, 2021 and every five years thereafter. Every public school must submit a school safety plan to the Department of Education after the local law enforcement agency has approved the plan. The Department of Education will post a list of which schools have submitted a school safety plan and which schools have yet to meet this requirement. Additionally, the act streamlines communication efforts between schools and state intelligence agencies by designating a single individual at each school as the school safety coordinator. The bill requires schools to use and promote a statewide mobile application ("See Something Send Something") to anonymously report suspicious activity or potential threats.

✓ **ND S 2110** expands the powers and duties of the Information Technology Department in North Dakota to oversee cybersecurity strategy for all executive branch state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, school districts, or other political subdivisions.

TAKE THE NEXT STEP TO BETTER SECURITY

Technology is transforming education today and has been a crucial part of efforts to continue education during the COVID-19 crisis. But without safe and secure services, K-12 schools cannot continue to embrace digitization and get the best experience for students, parents, and staff.

Arctic Wolf can provide the security operations you need to protect your school. A named security team will monitor your network 24x7, both in the cloud and on-premises. We respond to incidents fast, help manage compliance and reporting, and continuously scan for vulnerabilities.

Contact us today to schedule a demo.

ABOUT ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. For more information about Arctic Wolf, visit arcticwolf.com

[1] https://securityboulevard.com/2020/07/us-k-12-and-colleges-suffered-1300-data-breaches-in-15-years/#:~:text=US%20K%2D12%20and%20Colleges%20Suffered%201%2C300%20Data%20Breaches%20in%2015%20Years,-by%20Silviu%20STAHIE&text=More%20than%2024.5%20million%20records,a%20new%20report%20from%20Comparitech.

[2] https://www.scmagazine.com/home/security-news/san-diego-unified-school-district-data-breach-exposed-500000-students-staff-parents/

[3] https://www.cnn.com/2020/01/12/us/texas-school-district-email-scam-trnd/index.html

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com