



PowerSchool Information Security Report



Contents

Introduction	3
Why Transparency is Critical	4
Background of the Initiative	5
What to Expect in the Future	6
PowerSchool and the Secure by Design Pledge	7
Safe Guarding the Future: Cybersecurity Trends in K-12 Education	9
The Alarming Rise in Cyber Attacks	10
The Cost of Cyber Attacks	11
Preparing for 2024: Insights from Cybersecurity Experts	12
Conclusion: A Call to Action for K-12 Institutions	13



Introduction

In an era defined by digital transformation, PowerSchool recognizes the importance of securing the education technology ecosystem for the over 50 million students it serves across the United States. As the leading provider of cloud-based K-12 software, our commitment to personalized learning and education extends beyond the classroom and into the realm of information security.

The decision to join the [K-12 Education Technology Secure by Design Pledge](#), developed by the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Education, underscores our dedication to ensuring the safety and privacy of student data.

PowerSchool's mission to personalize education for every student begins with the acknowledgment of our responsibility to protect and safeguard the digital infrastructure that supports their learning journey. The landscape of education technology is evolving, and with it, the potential risks and challenges associated with cybersecurity. By voluntarily committing to the Security by Design Pledge, we aim to:

- Fortify our defenses
- Remain vigilant against emerging threats
- Contribute to the overarching goal of creating a secure and resilient environment for K-12 institutions



Why Transparency Is Critical


Transparency is a cornerstone of our approach to information security. We believe that open communication is essential in fostering trust among our stakeholders, including K-12 administrators, teachers, and parents. By being transparent about our cybersecurity initiatives, practices, and challenges, we adhere to the principles of the Secure by Design Pledge and empower the education community with knowledge and insights to collectively navigate the evolving threat landscape.

In an age where digital risks are as prevalent as physical risks, effective risk management requires a collaborative effort. We recognize that our users, including students, teachers, and administrators, rely on our platforms for a seamless education experience. Transparency becomes not just a commitment but a shared responsibility towards building a secure digital future for our education institutions.

In the pursuit of cybersecurity enhancement, under-resourced schools must assess the security practices of technology vendors. Prioritizing vendors with recognized certifications, such as SOC 2 or ISO 27001, becomes paramount. These certifications validate a vendor's commitment to rigorous security standards, ensuring that the integration of technology solutions doesn't compromise data integrity. By proactively selecting vendors such as PowerSchool with established credentials in cybersecurity, schools can bolster their defenses and establish a secure digital infrastructure for sustained educational success.

Background of the Initiative

The K-12 Education Technology Secure by Design Pledge, initiated by CISA, represents a collective commitment by industry leaders to prioritize security in product development.

 **PowerSchool, alongside other prominent providers, has pledged to adopt three key principles:**

- 1** Take ownership of customer security outcomes
- 2** Embrace radical transparency and accountability
- 3** Lead from the top by making secure technology a key priority for company leadership

These principles serve as guiding pillars, outlining specific, publicly measurable outcomes that align with our roadmap towards adhering to Secure by Design principles.



What to Expect in the Future

As part of our ongoing commitment to K-12 cybersecurity, PowerSchool is excited to announce the release of regular information security reports. These reports will provide an overview of current trends in information security, both within PowerSchool and the broader K-12 education sector. Each report will highlight general trends while offering specific insights into notable developments, initiatives, and challenges.

Our dedication goes beyond pledge compliance. We aim to set industry standards and contribute to the continuous improvement of education technology security practices. Security reports will serve as a testament to our ongoing efforts and will provide valuable information for K-12 administrators and teachers to stay informed and proactive in safeguarding their digital environments.

In the upcoming quarters, we will delve into specific areas such as cloud infrastructure security, cyber defense strategies, governance risk and compliance, and other pertinent topics. The aim is not just to share information but to engage in a meaningful dialogue with our stakeholders, understanding their concerns, and collectively working towards a more secure and resilient education technology landscape.

As we embark on this journey, PowerSchool remains committed to upholding the highest standards of security, ensuring the trust and confidence of the education community we serve.





PowerSchool and the Secure by Design Pledge

Since the announcement of the pledge in September, PowerSchool worked hard to fulfill our promise. Here is the status of each of the pledge items:

- **Single Sign-On (SSO) at no extra charge**
PowerSchool already offered standards-based SSO at no extra charge for our products before the pledge. We are working to create clear guidance about the SSO offerings for PowerSchool's products.
- **Security audit logs at no extra charge**
PowerSchool's practices were already ahead of the pledge. Security logs are available upon request to all our customers. Additionally, we will provide product and security subject matter experts to assist with questions our customers may have.
- **Publish a Secure by Design roadmap**
We are finalizing the inaugural roadmap and expect to publish in Q1 of 2024.
- **Publish a vulnerability disclosure policy**
PowerSchool maintains a [Responsible Disclosure Program](#) for customers and researchers to submit bugs to us.
- **Embrace vulnerability transparency**
PowerSchool is creating a standard way to report security fixes in the release notes that accompany all our product releases to make it easy for customers to identify fixes. This is expected in Q1 of 2024. We are also exploring additional transparency around vulnerabilities which are not yet fixed. This requires care to properly balance 1) the need for information to enable protecting against potential vulnerability exploits, and 2) the risk of providing information that would enable an attacker to exploit a vulnerability.

- **Publish security-relevant statistics and trends**

This report is the first step in regular reporting on security by PowerSchool. Look for additional reports to be released throughout the year.

- **Publicly name a top business leader who is responsible for security**

Hardeep Gulati, PowerSchool's CEO, is committed to the safety and security of the data entrusted to PowerSchool by our customers and is directly accountable for our efforts and results. [More details can be found on the PowerSchool website, in this press release](#), and in the Back to School Safely: Cybersecurity for K-12 Schools [White House presentation](#).

In addition to the seven items contained in the pledge, PowerSchool made an additional commitment during the White House announcement. PowerSchool will offer free and subsidized security resources for K-12 organizations. These include on-demand webinars, videos, toolkits, and training, as well as offerings from select best-in-class security providers. [The first of these videos have been released on our website](#). We are working with our partners to create security resources with details available Q1 of 2024.



Safeguarding the Future: Cybersecurity Trends in K-12 Education

In an era where technology is deeply integrated into the education landscape, K-12 institutions find themselves on the frontline of an escalating cyber battle. The trends observed in 2023 underscore the urgent need for schools to fortify their cybersecurity defenses. As we reflect on the challenges faced by schools nationwide, it becomes clear that addressing the cybersecurity deficit is not only a technological imperative but a fundamental commitment to safeguarding the education ecosystem.





The Alarming Rise in Cyber Attacks

The surge in cyberattacks on K-12 schools, exemplified by the ransomware attack on the Los Angeles Unified School District in 2022, is indicative of a broader and concerning trend. Cybercriminals are capitalizing on the vulnerabilities inherent in education institutions, targeting them with a 275% increase in attacks in 2023. The low-hanging fruit analogy holds true as schools, often lacking in-house expertise and robust security budgets, become prime targets.

The [SonicWall 2023 Mid-Year Cyber Threat Report](#) further sheds light on the evolving threat landscape facing K-12 schools. While ransomware attacks witnessed a 19% year-over-year decline, the overall intrusion attempts increased by 21%. Education organizations find themselves the second-most-targeted industry, emphasizing the urgency for schools to enhance their cybersecurity measures.

Malware attacks on K-12 schools saw a staggering 466% increase in the first half of 2023, delivered increasingly through encrypted means. Furthermore, a type of cyber-attack called cryptojacking witnessed an exponential rise, with hackers targeting the education sector more than any other vertical. SonicWall's report underscores the need for schools to stay vigilant, adapt to emerging threats, and adopt robust cybersecurity measures.

The Cost of Cyber Attacks

The hidden costs of such attacks can be substantial. In October 2023, Clark County School District in Nevada experienced a cyber-attack. The incident required them to restrict access to systems and bring in outside cybersecurity experts to assist with the investigation and notify students and parents whose information was disclosed by the attack. The investigation lasted for weeks and was impactful for both students and staff.

With an average of less than 8% of IT budgets allocated to cybersecurity, most schools and districts do not have the resources of a large district like Clark County to combat cyber threats.



Preparing for 2024: Insights from Cybersecurity Experts

For under-resourced schools and districts looking to enhance their cybersecurity in 2024, prioritizing impactful security measures is key. CISA recommends implementing highest-priority security controls and aligning cybersecurity goals with the NIST Cybersecurity Framework. This involves recognizing and actively addressing resource constraints by leveraging state cybersecurity grant programs, utilizing free or low-cost services for near-term improvements, and advocating for technology providers to enable strong security controls without additional charges. Minimizing the burden of security by migrating IT services to more secure cloud versions is also suggested.

Collaboration and information-sharing are emphasized as essential steps. Schools should join relevant collaboration groups such as [MS-ISAC](#) and [K12 SIX](#), and work with other information-sharing organizations, fusion centers, state school safety centers, and regional agencies. Building a strong and enduring relationship with CISA and FBI regional cybersecurity personnel further enhances information-sharing capabilities. Additionally, schools are encouraged to expect and call for technology providers to enable strong security controls by default at no additional cost.

To combat the evolving threat of ransomware, schools should integrate cybersecurity best practices into training and professional development sessions. Awareness and understanding the anatomy of cyberattacks are essential steps in strengthening a security posture. While cybersecurity evolves, preventive measures such as maintaining proper backups through simple and secure storage solutions become crucial. The adoption of a hybrid approach, combining on-premises and cloud storage for data management, ensures security, user-friendliness, and cost-effectiveness in the face of increasing cyber risks.

Conclusion

A Call to Action for K-12 Institutions

As we navigate the intricate web of cybersecurity challenges facing K-12 education, it's evident that schools must act decisively to protect their students, staff, and critical infrastructure. The trends observed in 2023 demand a collective commitment to prioritizing cybersecurity, allocating budgets wisely, and fostering a culture of cyber resilience. By embracing these principles, K-12 institutions can not only mitigate the hidden costs of cyberattacks but also ensure a secure and uninterrupted learning environment for generations to come.

The responsibility to safeguard the future of education rests upon the collective actions of administrators, teachers, and policymakers alike.



K-12 Data Security and Privacy Resource Kit

Access vital resources for guidance, insights, and best practices to improve your school or district's data security and privacy practices.

[LEARN MORE](#)





PowerSchool

Personalized Education for Every Journey

www.PowerSchool.com