K12 SIX

Cybersecurity Frameworks:

What K-12 Leaders Need to Know

Given that recent K-12 cybersecurity incidents have led to significant disruptions in teaching and learning, the theft and extortion of millions of taxpayer dollars from school districts, and identity theft and fraud stemming from student and teacher data breaches, it should be no surprise that education leaders and policymakers are turning their attention to the question of how to better defend school communities from the myriad cyber threats facing the K-12 education sector. Indeed, recent surveys conducted by the State Educational Technology Directors Association (SETDA) and the Consortium for School Networking (CoSN) both underscore that the imperative to defend school communities from emerging cybersecurity threats has risen to be among the highest priorities of both state and local education leaders.

While there is no shortage of advice and guidance on how organizations of all types (public and private, large and small) can better defend against cyber-attacks, precious little of that advice reflects the context in which schools work or addresses the unique challenges and constraints facing schools. Given that even the most well-resourced organizations remain challenged to protect their IT assets and sensitive data from cyber criminals and nation state actors, state education agencies and school districts working in isolation face a near insurmountable challenge.

Cybersecurity Frameworks: A Tool to Mitigate Cyber Risk

One promising practice being pursued by education leaders and policymakers considering these facts is the adoption of nationally recognized 'cybersecurity frameworks.' Broadly speaking, the aim of a cybersecurity framework is to establish a standard of cybersecurity care by compiling and harmonizing cost-effective best practice advice drawn from the experiences of experts. Since multiple cybersecurity frameworks have arisen over time to meet the specific needs of various stakeholder groups—some sector-specific, some designed to be used across sectors and industries—the choice of framework can be consequential, influencing how organizations prioritize, assess, and manage cyber risk.

To that end, the purpose of this white paper is to help K-12 leaders: (a) to understand the purpose and structure of the three most common cybersecurity frameworks being employed by school systems across the U.S. today, (b) to understand the similarities and differences among these cybersecurity frameworks, and (c) to determine whether the adoption and implementation of a framework might be of benefit to their school community.

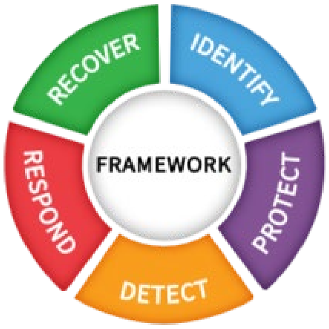
Common Cybersecurity Frameworks Employed by School Systems

To date, three cybersecurity frameworks have gained traction in the U.S. public K-12 sector via regulatory mandate or grassroots adoption:

- The National Institute for Standards and Technology Cybersecurity Framework (NIST CSF)
- The Center for Internet Security Critical Security Controls (CIS Controls)
- K12 SIX Essential Cybersecurity Protections for School Districts (K12 SIX Essential Protections)

A summary of the history and key features of each is offered below.

NIST CSF



The NIST Cybersecurity Framework**,** first published in February 2014, arose from an Executive Order issued by President Obama that called for the development of a voluntary cybersecurity framework that would provide a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” to assist organizations responsible for critical infrastructure services to better manage cybersecurity risk. Its original development was informed by an array of pre-existing standards, guidelines, and best practices, which were further supplemented and synthesized via multi-stakeholder meetings involving representatives from business, civil society, and government from across the U.S. and around the world. The NIST CSF was updated to version 1.1 in April 2018, although a significant 2.0 update was initiated in 2022.

The NIST CSF is complex and broad in scope, designed to be broadly applicable to public and private organizations across widely divergent sectors. Arrayed across five high-level functions—Identify, Protect, Detect, Respond, and Recover—the framework consists of three main components:

- **Core**, which categorizes and documents a total of 108 recommended cybersecurity best practices
- **Implementation Tiers**, which help organizations to convey the rigor of their NIST CSF implementation, including the degree to which cyber risk policies and practices are institutionalized into broader organizational decision making and governance
- **Profiles**, which assist organizations in customizing the Framework to best serve their unique organizational requirements and objectives, risk appetite, and available resources

Notwithstanding the benefits of the adoption of the NIST CSF by school systems, the latest Nationwide Cybersecurity Review (2020) found that K-12 school districts significantly lagged every other category of state, tribal, territorial, and local government agency in implementation of NIST CSF recommended cybersecurity best practices.

CIS Controls

Since 2015, what is now known as the CIS Critical Security Controls have been published by the non-profit Center for Internet Security. Initially developed by the SANS Institute in 2008 in response to significant data breaches experienced by leading companies in the U.S. defense industrial base—and informed by the experiences of U.S. Department of Defense cybersecurity experts—the current CIS Controls focus on recommended best practices that IT professionals across a range of public and private sector organizations should implement to block or mitigate against cyber-attack tactics, techniques, and procedures documented by experts and researchers. Version 8, the most recent edition of the CIS Controls, was released in May 2021.

Today the CIS Controls consist of 153 recommended IT best practices organized into 18 high-level categories. In recognition of significant differences across organizations interested in implementing the CIS Controls, recommended best practices are prioritized and sequenced across three Implementation Groups (IGs):

- **Implementation Group 1 (56 of 153 CIS-recommended best practices)**: IG1 is designed to be suitable for small to medium-sized organizations with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. It is focused on thwarting general, non-targeted cyber-attacks (i.e., essential cyber hygiene). The principal concern of IG1 organizations is continuity of operations; the sensitivity of data they are trying to protect is low and principally surrounds employee and financial information.
- **Implementation Group 2 (130 of 153 CIS-recommended best practices)**: IG2 is designed to be suitable for organizations that employ individuals dedicated to managing and protecting IT assets and systems and which may face federal or state regulatory cybersecurity compliance requirements. IG2 organizations often store and process sensitive information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.
- **Implementation Group 3 (All 153 CIS-recommended best practices)**: IG3 is designed for organizations that employ multiple, specialized cybersecurity experts and are required to adhere to federal and/or state regulatory cybersecurity compliance requirements. IG3 organizations are focused on both maintaining continuity of services and the confidentiality and integrity of sensitive data in their care. IG3 best practices are designed to defend against targeted attacks from a sophisticated adversary and to reduce the impact of potential zero-day attacks.

School systems share features of IG1 and IG2 organizations. Like IG1 organizations, most school systems are small, lack cybersecurity-specific regulatory compliance requirements, and lack dedicated in-house IT security staff. Like IG2 organizations, school systems rely on a disproportionately large number of IT assets and systems, are responsible for managing significant quantities of personally identifiable student and educator data, and face significant risks to public confidence should they experience a cybersecurity incident. They also can find themselves targeted specifically by threat actors willing to do significant research on their operations and personnel.

K12 SIX Essential Protections

The K12 SIX Essential Cybersecurity Protections were first published in October 2021 for the 2021-2022 school year by the non-profit K12 Security Information eXchange (K12 SIX), with updates planned for each successive school year. Developed with the substantial input of K-12 IT practitioners, the K12 SIX Essential Protections recommend a dozen pragmatic, actionable defensive protections which have proven effective in defending against cyber incidents frequently experienced by school systems. Informed by the requirements of insurers offering cyber liability coverage to school districts, current and historical K-12 cyber incident data compiled by K12 SIX, and K-12-specific cybersecurity alerts and guidance issued by the Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA), the K12 SIX Essential Protections are organized into four overarching categories:

- Sanitizing network traffic to/from the internet
- Safeguarding student, teacher, and staff devices
- Protecting the identities of students, teachers, and staff
- Performing regular maintenance

Each of the dozen K12 SIX recommended best practices are arrayed across a four-level rubric—at risk, baseline, good, and better—and offer guidance on the expected impacts of best practice implementation on school system budgets, IT staff workload, and educators' time and effort. Finally, each of the K12 SIX Essential Protections are explicitly aligned to both the CIS Controls and the NIST CSF.

Compared to the CIS Controls and NIST CSF, the K12 SIX Essential Protections are the newest and least comprehensive (12 recommended best practices vs. 100+ for both the CIS Controls and NIST CSF) of the cybersecurity frameworks used in the K-12 sector. This is by design. As school systems embark on their journey to improve their cybersecurity risk practices, it is envisioned that they will graduate from the K12 SIX Essential Protections over time to adopt one of the more robust frameworks available to them. Nonetheless, all school systems can benefit from assessments against the K12 SIX Essential Protections.

Similarities and Differences Among Cybersecurity Frameworks

While there are real differences across cybersecurity frameworks, it is fair to say that they also hold much in common. In general, all cybersecurity frameworks help organizational leaders to prioritize the implementation of technology, operational procedures, and policy development to mitigate and manage the risks introduced by vulnerabilities and cyber-attacks. This prioritization is especially helpful for school system leaders who face many competing demands on their time and resources.

Cybersecurity frameworks also serve an important role in helping to communicate what is important, why, and to benchmark progress over time, including—in some cases—to non-technical stakeholders. Given that the field of cybersecurity can be jargon-laden and intimidating even for tech-savvy individuals, there is a significant benefit to being guided by the consensus opinions of expert practitioners written in plain English.

Another key advantage of adopting any cybersecurity framework is the unlocking of access to a robust ecosystem of third-party resources—including assessments, guidance, specialized software tools, and consulting services—directly aligned to those frameworks. This means that implementation assistance explicitly aligned to existing frameworks is readily available for those seeking extra support.

Finally, since cybersecurity frameworks are derived from a common pool of expert advice and guidance, it is trivial to crosswalk recommendations across frameworks or to adopt different frameworks over time as circumstances change. Each of the popular cybersecurity frameworks used by K-12 leaders is informed by and/or builds off the others, which means that the adoption of a specific framework by a school system need not require protracted analysis and evaluation for fear of lock-in.

Key differences of cybersecurity frameworks are summarized in the table on the following page. Perhaps most pertinent for K-12 leaders are variations in the target audience for each framework, as well as the number—and comprehensiveness—of recommended cybersecurity controls. Frameworks advocating for large numbers of controls run the risk of overwhelming school systems without staff dedicated to their implementation and therefore diminishing their value as a tool for prioritization of resources and actions.

	NIST Cybersecurity Framework	CIS Controls	K12 SIX Essential Protections
Publisher	U.S. Department of Commerce, National Institute of Standards and Technology (NIST)	Center for Internet Security (CIS)	K12 Security Information eXchange (K12 SIX)
Current Version (Date)	Version 1.1 (April 2018) NOTE: Version 2 currently under development	Version 8 (May 2021)	2022-23 School Year (October 2022) NOTE: annual updates planned each school year
Developed by	NIST with the input of industry, academia, and government stakeholders	An international, grass-roots consortium of companies, government agencies, academic institutions, and individual experts across roles and sectors	K-12 IT security practitioners informed by experiences with existing frameworks, K-12 cyber incident trend data, and cyber insurance requirements
Target Audience	Federal agencies, critical infrastructure, and organizations of all types and sizes across public and private sectors in the U.S. and abroad	Public and private companies and organizations of all types and sizes, including state and local government agencies	School districts and other K-12 organizations
Number of Recommended Best Practices	108, sorted into 23 categories across 5 high-level 'functions' (described in a 55-page document)	18—further delineated into 153 'safeguards'—arrayed across 3 implementation groups (described in an 87-page document)	12, arrayed across a 4-level implementation rubric (described in a 17-page document)
Suitability	For school districts with leadership (technical and non-technical) regularly engaged in cybersecurity risk management activities, supported by dedicated, trained cybersecurity staff	For school districts employing dedicated, trained cybersecurity staff	For school districts aspiring to better defend their school communities against cybersecurity threats

Recommendations for K-12 Leaders

The adoption of a cybersecurity framework is an important step in the journey toward more effectively mitigating and managing the cybersecurity risks facing school systems. As such, it is important that state and local education leaders:

- **Commit to improving K-12 cybersecurity defenses by adopting a cybersecurity framework as a management and communication tool**. Since frameworks are closely aligned—and are informed by each other—the choice of specific framework is less important than the overarching commitment to jumpstart the cybersecurity risk management practices of your school system.
- **Consider the cybersecurity capacity of your K-12 organization in choosing to adopt a framework**. It can take years for even the best resourced organizations to build a mature cybersecurity risk management program. Implementing more robust frameworks require more resources and may risk diverting attention from those practices most likely to shore up defenses in the near-term.
- **Understand that cybersecurity framework implementation requires flexibility**. Cybersecurity frameworks evolve over time in response to vulnerabilities and threats, and not every recommended best practice will be suitable for every K-12 organization—especially given differences in technology and IT systems, risk tolerance, cybersecurity capacity, and budget. Avoid checklist-based approaches to framework implementation.

While cybersecurity experts can offer no guarantees, the adoption of a cybersecurity framework can reduce the odds of experiencing a significant cyber incident and allow those that do experience incidents to recover more quickly and gracefully.

Resources for Further Learning

- SETDA 2022 State EdTech Trends Report: https://www.setda.org/priorities/state-trends/
- CoSN 2022 EdTech Trends and Funding Survey Report: https://www.cosn.org/cosn-news/2022-cosn-back-to-school-survey-reveals-increasing-school-district-technology-funding-for-devices-and-cybersecurity/
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- CIS Controls: https://www.cisecurity.org/controls
- K12 SIX Essential Cybersecurity Protections: https://www.k12six.org/essentials-series
- Nationwide Cybersecurity Review: https://www.cisecurity.org/ms-isac/services/ncsr

Commissioned by the State Educational Technology Directors Association (SETDA), the creation of this resource was funded by the Bill & Melinda Gates Foundation. The views expressed are those of the authors and should not be attributed to the foundation.

About the K12 Security Information eXchange

The K12 Security Information eXchange (K12 SIX) operates as an information sharing and analysis center (ISAC) exclusively for the K-12 education sector. Organizations eligible for membership include school districts, charter schools and charter management organizations, private/independent schools, regional education agencies, and state education agencies. To learn more about K12 SIX, including membership benefits and how to join, please visit: https://www.k12six.org/