THE STATE OF K-12 CYBERSECURITY: YEAR IN REVIEW

2022 Annual Report

K12 Security Information Exchange

K12 SIX

The *State of K-12 Cybersecurity: Year in Review* report is a product of the K12 Security Information Exchange (K12 SIX) based on data from the K-12 Cyber Incident Map, the definitive source of information about publicly disclosed cyber incidents affecting U.S. public schools and education agencies.

ABOUT THE K12 SECURITY INFORMATION EXCHANGE

The K12 Security Information Exchange (K12 SIX) is a national non-profit membership organization dedicated solely to helping protect K-12 schools—public and private—from emerging cybersecurity threats, such as ransomware and phishing attacks. It was launched in late 2020 as an affiliate of the Global Resilience Federation in response to the growing cybersecurity challenges facing schools nationwide, and in recognition of the unique challenges and context of K-12 operations.

Benefits of K12 SIX membership include:

- Engagement in a private, nationwide community of K-12 information security professionals via a secure communications platform
- Access to a cyberthreat information sharing portal and mobile app with actionable alerts, reports, and best practices
- Enrollment in the K12 SIX emergency notification system (via phone, email, and SMS) for issues that require immediate action
- Weekly virtual CISO open office hours and access to dedicated K12 SIX security analysts
- Weekly newsletters providing situational awareness tailored specifically to the K-12 community
- Semi-monthly and ad hoc member meetings to share information about—and coordinate joint actions in response to—incidents of significant impact, scale, and sensitivity
- Leadership, staff development and training opportunities, through participation in K12 SIX events, committees, and advisory groups

K12 SIX also works in partnership with other information sharing communities (ISACs and ISAOs), federal agencies, national and state education associations, and serves the broader K-12 sector through professional development, awareness-building, and advocacy. For more information, including on how school districts can participate, please visit https://www.k12six.org

---

TLP WHITE

Suggested Citation:

> Levin, Douglas A. (2022). "The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report." K12 Security Information Exchange (K12 SIX). Available online at: https://www.k12six.org/the-report

ACKNOWLEDGEMENTS

Since the K-12 Cyber Incident Map first launched it has benefited from many individual and corporate supporters who have contributed financial and intellectual resources to its maintenance and ongoing development. This year's report was strengthened via collaborations with: Dissent Doe, the pseudonym of a privacy advocate and activist who blogs about privacy issues and data security breaches on PogoWasRight.org and DataBreaches.net; investigative reporters, including Kevin Collier (NBC News), Tanya Eiserer (WFAA Dallas), Grace Ferguson (Daily Dot), Dana Kozlov (CBS 2 Chicago), Brian New (CBS 11 Dallas Fort-Worth), Scott Travis (Sun Sentinel), and Julie Watts (CBS 13 Sacramento); and, Staci Elliott, Eric Lankford, Patrick McGlone, Cassandra Orsi, and Arshad Somani of K12 SIX.

2022 ANNUAL REPORT SPONSORS

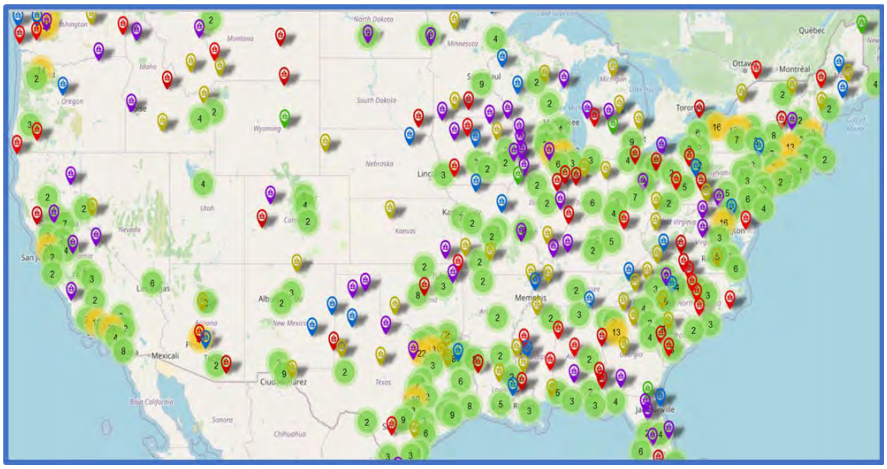
INTRODUCTION

School districts and their vendors regularly fall victim to cybersecurity threats, placing millions of students and teachers directly in harm's way.

If the response to the COVID pandemic has underscored anything, it is that the resiliency of the U.S. public education system is integral to the national economy and the well-being of communities—whether rural, suburban, or urban—across the nation. Serving over 50 million students in over 100,000 schools nationwide, the U.S. public education sector is an enormous—albeit highly decentralized—enterprise.[1]

While many outside the public education sector have been slow to recognize it, school districts (like other local government agencies) are amid a digital transformation of their operations—digitizing paper-based processes and adopting 'smart' technologies for core services including facilities management, transportation, HR/staffing, business services, and teaching and learning. While the adoption of technology provides benefits, it also introduces new risks—both to the resilience of school district operations as well as to the safety of school community members, including students and teachers.

This report is the fourth in an annual series[2] designed to shed light on cybersecurity incident trends in the U.S. K-12 public education sector, based on a data source that the U.S. Government Accountability Office (GAO) found to be the "most complete resource that tracks K-12 cybersecurity incidents, including student data breaches."[3] Published by the non-profit K12 Security Information Exchange (K12 SIX), it remains the first and only vendor-agnostic, independent research effort dedicated solely to cataloging and analyzing cybersecurity incidents affecting U.S. public K-12 school districts.



The K-12 Cyber Incident Map, a visualization of publicly disclosed school cyber incidents from 2016 to present. Available online at https://k12six.org/map

By focusing on publicly-disclosed incidents experienced by school districts and other public education agencies, this report provides unique insights into how K-12 cyber risk management practices are exploited and suggests how they may best be remedied. Nonetheless, an exclusive focus on publicly-

disclosed incidents also dramatically understates the scope of the issues facing K-12 schools, especially when disclosure requirements are weak and routinely circumvented. The true picture is surely bleaker; anecdotal evidence suggests perhaps 10 to 20 times more K-12 cyber incidents go undisclosed every year.

In the following sections, this report presents findings from detailed analyses of cyber incidents experienced by school districts, as well as the characteristics of those districts. It concludes with recommendations to address the growing challenge of cybersecurity risk management in the K-12 sector writ large. An appendix offers information on the data and methods relied on for this report.

> "IT'S JUST THAT FEELING OF HELPLESSNESS, OF CONFUSION AS TO WHY SOMEBODY WOULD DO SOMETHING LIKE THIS BECAUSE AT THE END OF THE DAY, IT'S TAKING AWAY FROM OUR KIDS. AND TO ME THAT'S JUST A DISGUSTING WAY TO TRY TO, TO GET MONEY," SUPERINTENDENT CHANNELL SEGURA [TRUTH OR CONSEQUENCES MUNICIPAL SCHOOL DISTRICT] SAID.

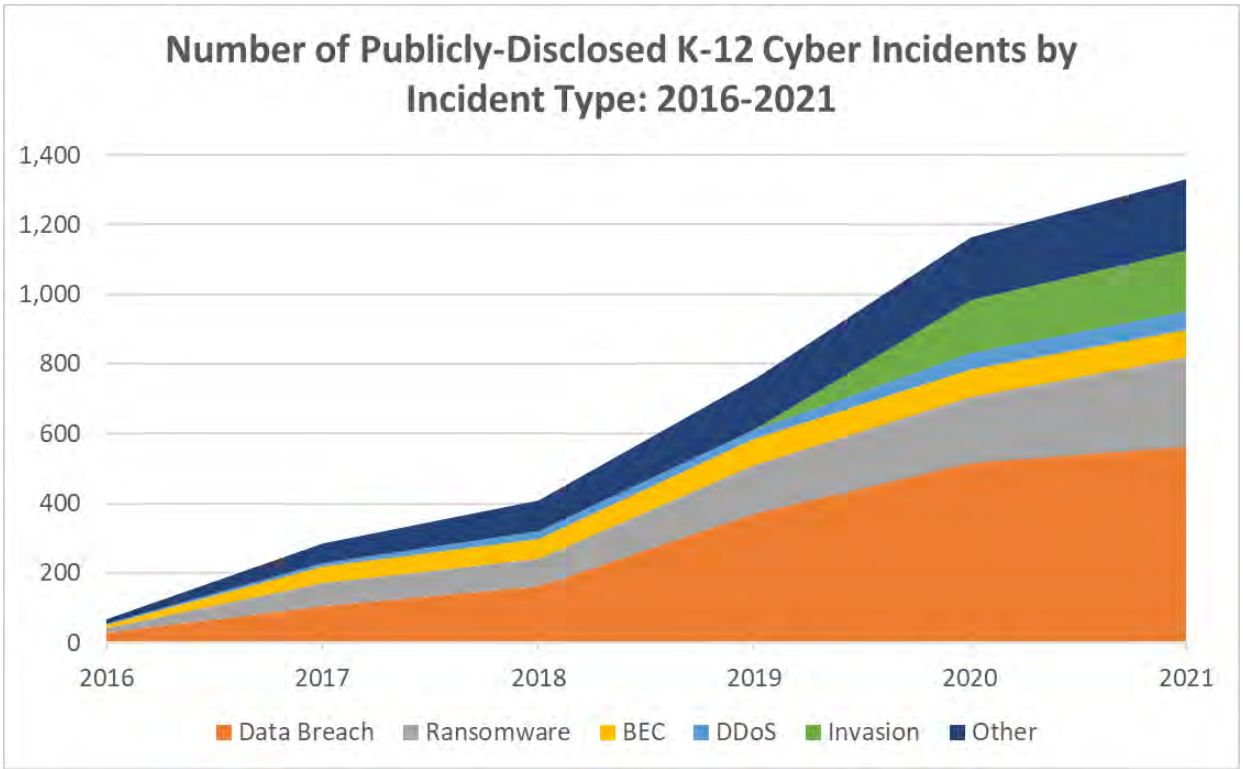
Source: Cedar Attanasio, Cedar (February 1, 2022). "Hackers prey on public schools, adding stress amid pandemic" Associated Press. Available online at: https://apnews.com/article/coronavirus-pandemic-technology-health-business-hacking-aecb37a35f3677e4f2cc62362a23defa

K-12 CYBER INCIDENTS: ANALYSIS AND TRENDS

Since 2016, the K-12 Cyber Incident Map has cataloged a total of 1,331 publicly disclosed school cyber incidents affecting U.S. school districts (and other public educational organizations) across a wide array of incident types, including:

- Student data breaches
- Data breaches involving teachers and school community members
- Ransomware attacks
- Business email compromise (BEC) scams
- Denial of service (DoS) attacks
- Website and social media defacement
- Online class and school meeting invasions
- Other incidents

Averaged over the last six years, this equates to a rate of more than one K-12 cyber incident per school day being experienced by the nation's public schools.



Who is responsible for these incidents and why do they keep occurring? Actors both internal and external to school communities share responsibility:

- School community members—including teachers, administrators, and school board members—who may lack the training and guidance necessary to avoid the errant sharing of personal data and credentials
- Tech-savvy students, who—in the absence of mentoring and adult guidance—may attempt to circumvent existing cybersecurity controls and/or be lured into parlaying their legitimate access to school IT systems to disrupt, cheat, or even cause harm to others
- School suppliers and vendors, whose security practices are not adequately considered during school district procurement decisions and product/service implementation
- Online criminals—some based in the U.S., but many based overseas—who seek to profit from weak school district cybersecurity controls by stealing or extorting money from school districts, their employees, and vendors or via credit and tax fraud enabled by stealing personally identifiable information from school districts. Two types of criminal hackers prey on schools:
    - Those pursuing 'soft targets'—though not specifically schools or school personnel—via mass phishing campaigns and broad-based internet scans for unpatched and unsecured servers
    - Those who specifically target school districts for attack, as evidenced by their sophisticated use of information about school district personnel, communications, vendors, and other operational details to carry out their schemes

While risk management—including digital risk—is a core task of local school system governance, the absence of meaningful cybersecurity risk management standards for schools at either the state or federal levels—coupled with a lack of resources dedicated to meeting any such standards—all but guarantees that many districts will continue to place the safety and security of students, teachers, and community members at avoidable risk.

The 2021 Calendar Year in Focus

During calendar year 2021, the K-12 Cyber Incident Map cataloged a total of 166 school incidents affecting schools in 162 school districts across 38 states. Compared to the prior two years, this represents a decrease in publicly-disclosed incidents—a finding that will be counter-intuitive to many.[4] Three factors may help explain this year-over-year decline.

First, the response to the COVID pandemic—including the unanticipated need to shift to remote learning—may have temporarily inflated the number of cyber incidents experienced by school districts. Indeed, it did give rise to a whole new class of incidents: online class and meeting invasions (known colloquially—though not accurately—as 'Zoombombing').[5] Returning to normal district operations may have helped districts to better protect their communities.

Second, in seeking to shift cybersecurity risk to private insurers, school districts are being forced not only to pay dramatically higher premiums but also to implement commonsense cybersecurity controls—such as multifactor authentication for employees—for the first time. Thanks to this market dynamic and heightened awareness of the cybersecurity challenges facing the K-12 sector in general, school districts

may have done a modestly better job of defending their communities from cybersecurity threats during 2021.[6]

Third, by and large, public-disclosure requirements for school districts and their vendors are quite weak. If it were not for the public interest reporting of security researchers and investigative reporters during 2021—employing, e.g., freedom of information requests to compel districts to share incident details they sought to keep from the public eye—the number of publicly-disclosed incidents cataloged by the K-12 Cyber Incident Map during the past year would have been even smaller. The lack of more robust K-12 cyber incident public disclosure requirements only serves to obscure the realities of school district and vendor operations from those charged with oversight, and to place school community members at unnecessary risk. As such, the smaller number of incidents reported during 2021 may instead reflect a concerning shift away from public disclosure, undermining the ability of independent researchers—and the policymakers and school system leaders who rely on their work—to accurately assess trends and issues.

District Takes "Extraordinary Steps" to Avoid Public Disclosure

As reported by Scott Travis of the *South Florida Sun Sentinel*, the Broward County School District "took extraordinary steps" to keep the public, including 50,000 potential data breach victims, from learning about a March 2021 ransomware attack perpetrated by the Conti ransomware gang, including:

- Waiting 5 months to report key information to affected individuals as well as to the U.S. Department of Health and Human Services, 3 months longer than a federal rule allows. The department is investigating the district's response.
- Communicating to the public that it had conducted its own investigation into the cyber incident but later claiming the findings of the investigation were never put in writing.
- Employing a public relations firm to help dodge questions from the news media and persuade the public that personal data wasn't at risk.
- Rejecting a public records request for emails related to the ransomware incident, with a district lawyer saying "it is not worth any of our time" to review the emails to see if they were exempt under state law.
- Lobbying the Florida state legislature for a law that would keep school district cybersecurity investigations hidden from the public.

Source: Scott Travis (February 17, 2022). "Investigation: Broward schools took extraordinary steps to hide key details of massive data breach." South Florida Sun Sentinel. Available online at: https://www.sun-sentinel.com/news/education/fl-ne-broward-schools-hacker-investigation-report-20220217-6jy2t5rzrzbjxn63oyq5wwuyb4-story.html

Shedding Light on K-12 Cyber Incidents

During 2021, public interest reporting was instrumental to revealing details about K-12 cyber incidents that would have otherwise avoided public disclosure. The work of several researchers and investigative reporters is worthy of special attention:

- Kevin Collier and colleagues at NBC News, who collected and analyzed school files posted on the dark web and found it littered with the personal information of students ("Hackers are leaking children's data — and there's little parents can do." Available online at: https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926).

- Dissent Doe, the pseudonym of a privacy advocate and activist who regularly blogs about privacy and cybersecurity incidents—including those affecting U.S. K-12 schools—at https://www.databreaches.net.

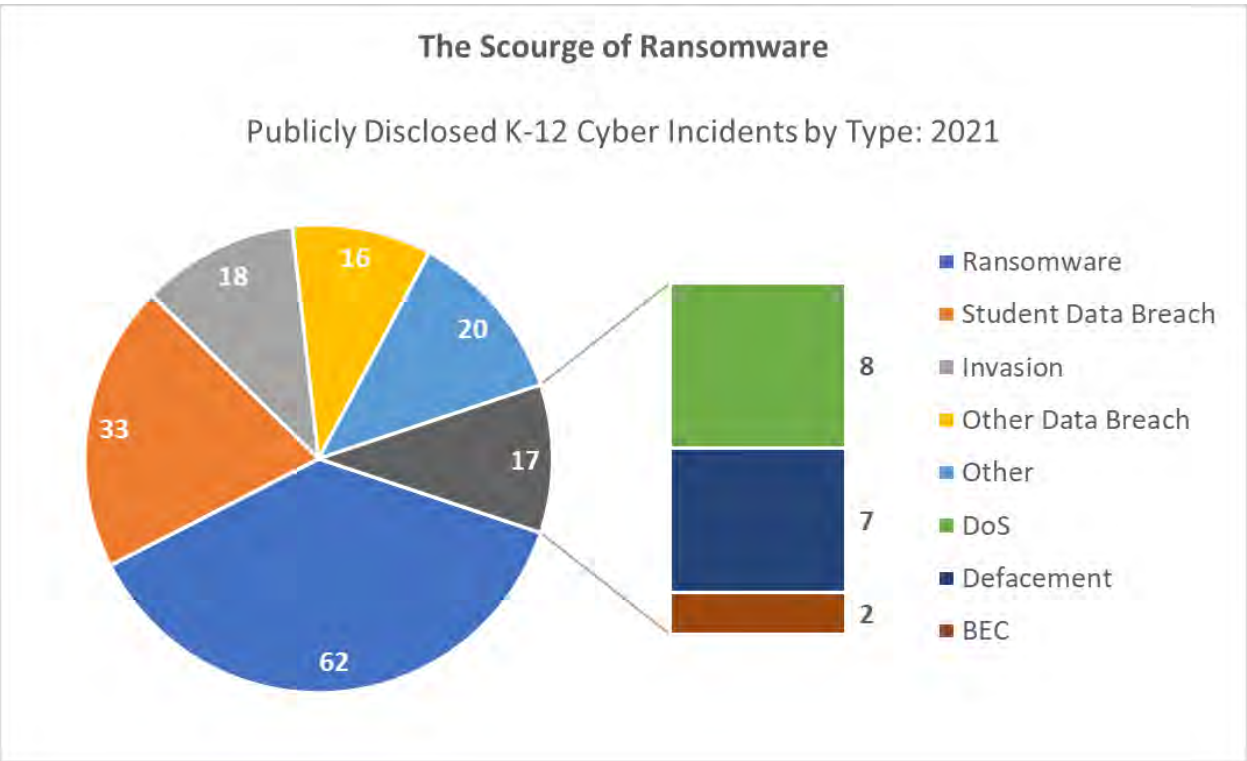
- Grace Ferguson of the *Daily Dot*, who submitted public records requests to 15 school districts across the country to learn more about the impact of K-12 ransomware incidents ("Schools across the nation are getting hit with ransomware attacks—but they won't admit how much it's costing them." Available online at: https://www.dailydot.com/debug/ransomware-public-schools-foia/).

- Dana Kozlov and CBS 2 Chicago colleagues, who submitted public records requests to 60 Illinois school districts asking for correspondence about cyber incidents ("Student And Staff Data From Area School District Were Dumped On The Dark Web, And Parents And Staffers Had No Clue." Available online at: https://chicago.cbslocal.com/2021/09/21/student-staff-data-palos-school-district-dumped-dark-web-caught-off-guard/).

- Brian New and CBS 21 Dallas Fort-Worth colleagues, whose investigative work identified 67 school districts across Texas that had have suffered at least one cybersecurity incident—many of which had previously been undisclosed ("Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation." Available online at: https://dfw.cbslocal.com/2021/08/16/dozens-texas-school-districts-hammered-cyberatacks-ransomware/).

- Julie Watts and CBS 13 Sacramento colleagues, who uncovered "alarming school cyber-attack statistics and a lack of school policies for tracking and reporting these attacks" among California school districts ("Schools Aren't Required to Report Increasing Cyber Attacks: Kids at Risk, Parents in The Dark." Available online at: https://sacramento.cbslocal.com/2021/09/29/school-report-increasing-cyber-attacks-kids-risk-parents/).

What were the most frequently experienced types of school-related cyber incidents reported during 2021? As in prior years, during 2021 school districts experienced a wide array of incident types, including ransomware, data breaches (primarily involving student data), and class and meeting invasions. However, for the first time ever, ransomware incidents were the most frequently disclosed incident type.



The Scourge of Ransomware

During 2021, the K-12 Cyber Incident Map documented 62 instances of U.S. public K-12 school districts being victimized by ransomware, a highly disruptive cyber-attack tactic employed by online criminals to extort money from victims. Incidents were geographically dispersed, with reports of school ransomware emerging from districts of varying sizes across 24 different states.

This is the third straight year that there have been more than 50 publicly disclosed K-12 ransomware attacks and the first year it was the most frequently experienced type of cyber incident cataloged by the K-12 Cyber Incident Map. While the increasing frequency of ransomware attacks should be alarming to K-12 leaders and policymakers, the evolving—and increasingly damaging—tactics of ransomware gangs are primarily what sets 2021 apart from prior years.

While many public reports are ambiguous, the names of ransomware gangs most associated with attacks against U.S. public schools during 2021 included 'PYSA,' 'DoppelPaymer/Grief,' and 'Vice Society.' For their part, the U.S. Federal Bureau of Investigation (FBI) issued an alert specifically warning of the gang behind PYSA ransomware[7] targeting U.S. K-12 educational institutions in March 2021, writing:

> *FBI reporting has indicated a recent increase in PYSA ransomware targeting education institutions in 12 US states and the United Kingdom. PYSA, also known as Mespinoza, is a malware capable of exfiltrating data and encrypting users' critical files and data stored on their systems. The unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors use PYSA to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments.*[8]

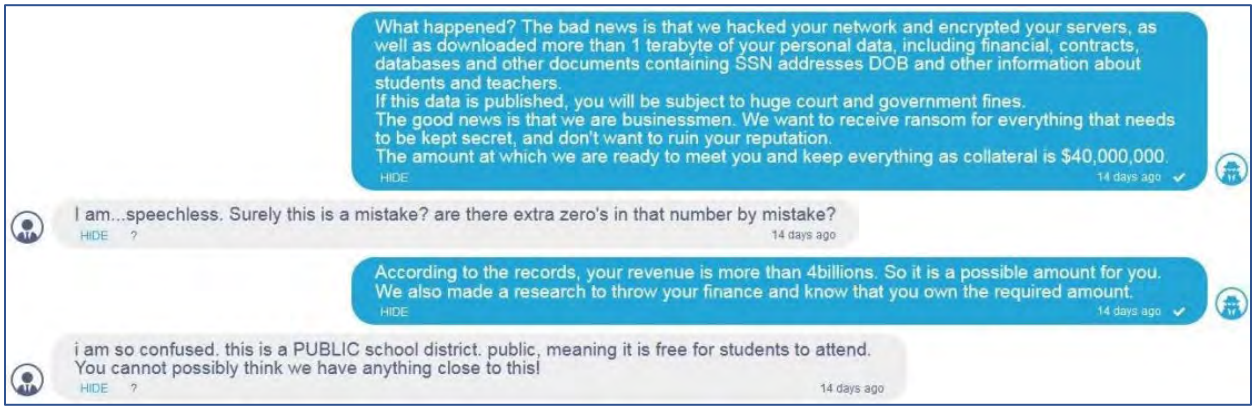
Continuing a trend first observed in 2019, ransomware attacks against school districts commonly resulted in class cancellations and districtwide closures. For instance, during 2021 a Missouri school district was forced to cancel classes for two days as part of their ransomware recovery process which "close[d] down the internet altogether, including the district's phones, paging systems, and security cameras."[9] Further highlighting the challenge of school district resiliency to these attacks, an Oregon school district was forced to distribute printed 'activity packets' to students in an effort to supplement learning while it attempted to recover from its incident:

> *Now with teacher, administrator and student logins all dependent on district domains and portals, the [ransomware attack]… has ground instruction and internal operations to a halt at the district of more than 6,000 students.*[10]

While school districts are often reluctant to disclose whether they (or an insurance company on their behalf) may have been successfully extorted by ransomware gangs, such public disclosures are not unheard of. For instance, in responding to a June 2021 ransomware attack a Texas school district paid $547,045.61 to "protect sensitive, identifiable information from being published." It went on to say:

> *While these are funds that we would have rather spent on the needs of our employees, students and their families, there was no other choice for the district to ensure your safety – our number one priority.*[11]

Even in cases where school districts don't pay a ransom, short- and medium-term unbudgeted remediation costs can be staggering. According to Baltimore County (MD) Public Schools officials, the cost of ongoing recovery from a Ryuk ransomware attack late in 2020 grew to nearly $9.7 million dollars



Excerpts of a conversation between a Broward County Public Schools official and a member of a criminal ransomware gang posted to the gang's blog

Source: Collier, Kevin (April 12, 2021). "Parents were at the end of their chain — then ransomware hit their kids' schools." NBC News. Available online at: https://www.nbcnews.com/tech/security/parents-end-chain-ransomware-hit-rcna646

one year later.[12] In New York, the Buffalo School Board approved spending nearly $9.4 million on external IT consultants to respond to the ransomware attack it suffered in March 2021.[13]

Ransomware gangs continue to evolve their tactics to put pressure on victims to meet their extortion demands. For instance, first documented in last year's 'State of K-12 Cybersecurity' report, ransomware gangs are now routinely employing so-called 'double extortion' tactics against school districts:

> *With this tactic, ransomware actors steal a victim's data before their malware strain activates its encryption routine. They then have the option of demanding two ransoms. The first one is the provision of a decryption utility. The second one guarantees verbal confirmation of having deleted the victim's data from their servers. They can also leverage that data theft to pressure victims — even those that have a robust data backup strategy.*[14]

The experience of Weslaco Independent School District (TX), a late 2020 victim of a ransomware attack, is typical of this double extortion tactic:

> *…the hackers, spurned by Weslaco's decision to not pay, dumped the files they pilfered on their website. One of those, still posted online, is an Excel spreadsheet titled "Basic student information" that has a list of approximately 16,000 students, roughly the combined student population of Weslaco's 20 schools last year. It lists students by name and includes entries for their date of birth, race, Social Security number and gender, as well as whether they're an immigrant, homeless, marked as economically disadvantaged and if they've been flagged as potentially dyslexic.*[15]

Not satisfied with double extortion tactics, ransomware gangs have even resorted to triple extortion of school districts: reaching out to parents directly to encourage them to drive their school districts back to a negotiating table from which they had reportedly walked away:

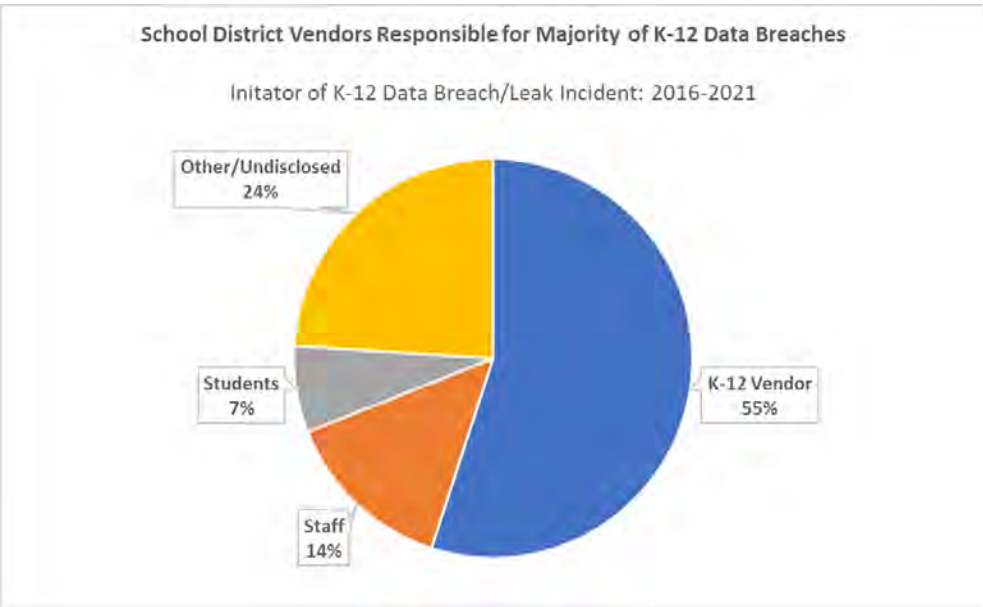
> *Allen ISD was first hacked in September when their phones, WiFi, and printer systems all went down, but say no sensitive information was stolen. However, now parents are coming forward saying they're being threatened by those same hackers.*
>
> *Phil Carpenter, is one of many parents who received an email stating sensitive information has been collected from the district. "[the hackers] claim to have a log of sensitive data from Allen ISD," Carpenter said. "That they have hacked into a lot of the IT resources. It does seem to be some sort of phishing attempt." The email claimed to have control of Allen ISD's network.*
>
> *Another version of the email his wife received, tells parents their school district has five days to send them their demanded payment, or their demand will go up to $10 million. If the money isn't received, the hackers say parents risk having sensitive student information published.*
>
> *For parents it's worrisome.*[16]

Breaches and Leaks of Confidential Student and Teacher Information

School districts and their vendors are routinely the subject of data breaches and leaks involving the confidential information of current and former students and staff. As in previous years, most publicly disclosed K-12 data breach incidents involve student data, but a significant number include teacher and other school data in addition or instead.

The most significant vector for student and teacher data breaches—in terms of numbers of individuals affected—remain school district vendors and other trusted non-profit and government partners. During 2021, school districts reported significant breaches of personal information by: ACT,[17] PCS Revenue,[18] Student Transportation of America,[19] Independent Health,[20] and the Public School and Education Employee Retirement Systems of Missouri.[21]

It is important to note that reports of vendor security issues and vulnerabilities affecting school district IT systems cannot always be directly attributed to K-12 cyber incidents. During 2021 for instance, significant vulnerabilities were disclosed in Netop Vision Pro Education[22] software and Verkada surveillance cameras,[23] as well as in several popular proprietary and open-source software applications commonly used by schools.[24]



While students and school staff generally have little recourse under the law for a data breach incident (no matter the root cause), stockholders and other investors in education companies are granted greater protections in cases where those companies are negligent or materially misstate the potential impact of cyber incidents on their current or future operations. The cease-and-desist order—and accompanying $1 million penalty—issued by the U.S. Securities and Exchange Commission to the education company Pearson in August 2021 is illustrative:

> *Pearson, a multinational educational publishing and services company, made material misstatements and omissions regarding a 2018 cyber intrusion that affected several million rows of student data across 13,000 school, district, and university AIMSweb 1.0*

> *customer accounts in the United States. In its July 26, 2019 report furnished to the Commission, Pearson's risk factor disclosure implied that Pearson faced the hypothetical risk that a "data privacy incident" "could result in a major data privacy or confidentiality breach" but did not disclose that Pearson had in fact already experienced such a data breach. On July 31, 2019, approximately two weeks after Pearson sent a breach notification to affected customers, in response to an inquiry by a national media outlet[25], Pearson issued a previously-prepared media statement that also made misstatements about the nature of the breach and the number of rows and type of data involved.[26]*

The fact that data breaches and other security incidents continue to plague school district vendors and their partners should raise significant questions about the sufficiency and effectiveness of both industry self-regulatory efforts and existing data privacy and security regulations.[27] Indeed, the U.S. Government Accountability Office has recognized "cyberattacks carried out directly against ed-tech vendors…tend to have an especially severe impact on K-12 because they affect a large swath of students across multiple school districts at the same time."[28]

Another significant source of K-12 data breaches are school district staff and school board members, who—whether due to a lack of training or lax cybersecurity controls—inadvertently share personal information of students and/or staff in the course of their duties. This may be in preparation for a school board meeting,[29] in responding to a freedom of information request,[30] or in regular communications with parents and other members of the school community.[31] In perhaps the most politicized data breach incident of 2021, the Governor of Missouri accused a journalist of hacking the Missouri Department of Elementary and Secondary Education website and improperly accessing social security numbers of teachers across the state.[32] Further investigation revealed that:

> *The site, which has both a public side and a secure side available only to certain school-district employees, featured a search tool to look up educators' qualifications and backgrounds. Officials interviewed during the course of the investigation said that as a member of the media, [the journalist] would've only had access to the public-facing portal. But the HTML code for the search tool revealed that Social Security numbers were not encrypted. With records dating back to 2005, an estimated 576,000 teachers' information may have been exposed…. An ITSD application developer and client manager later told state police investigators that data on the teacher lookup website should've been encrypted and that the site is now being redesigned to shield individuals' private information. But the officials also said that in the 10 years since the site was launched, no one in the state's IT division had noticed.[33]*

The final group of individuals commonly responsible for school data breaches—for which information is publicly available—are students themselves. In stories reminiscent of famous movie scenes, every year reports emerge of students who compromise school IT systems, often facilitated by weak school district password policies and a lack of multifactor authentication.

Take the case of Dallas Independent School District (DISD), which announced it was a victim of a massive data breach in September 2021 affecting 800,000 current and former students, staff, and parents:[34]

> *"The confidentiality, privacy, and security of information in our care is one our highest priorities," the district said in the news release. "We take this matter very seriously and have invested significant resources to protect sensitive data. Despite our efforts, the district is now one of a growing number of public and private organizations experiencing cyberattacks."*[35]

What the district did not disclose at the time—and later only emerged through the investigative reporting of Tanya Eiserer and WFAA Dallas colleagues—was that the source of the breach was not a cyber criminal operating overseas, but two DISD students.

> *…the incident was concerning enough to [the district's]…chief information security officer that he quit, and blasted the district's handling of the breach in his resignation email.*
>
> *"I am afraid the details of the breach will become public at some point, and Dallas ISD will lose credibility," [he] wrote… on Oct. 28. "I am now convinced that Dallas ISD IT cannot keep our data safe...."*[36]

While the DISD superintendent resigned following this incident, he did recently accept a national award for "championing the use of technology to enhance teaching and learning" during his tenure.[37]

Other K-12 Cyber Incident Types Disclosed During 2021

While ransomware and data breach incidents are more frequently experienced by school districts, they routinely fall victim to a wide array of other types of incidents. The most common of these include:

- **Business email compromise (BEC) scams**: Involving the use of email to scam school business officials and staff members out of sensitive information and/or millions of dollars of money, including by issuing fake invoices to districts,[38] by redirecting authorized electronic payments to bank accounts controlled by criminals,[39] and by stealing W-2 tax information of district employees.[40]

- **Online meeting and class invasions**: Involving unauthorized access to online classes and K-12 meetings for the purpose of disruption—often by hate speech; via the sharing of shocking images, sounds, and videos; and/or, threats of violence. Despite the attention drawn to these incidents—and availability of advice on how to defend against them—school districts continued to fall prey to these incidents during 2021.[41]

- **Email invasion**: Involving the compromise of a school district's email systems by unauthorized individuals for the purpose of bulk sharing of or links to disturbing images, videos, hate speech, and/or threats of violence to members of the school community.[42]

> *"My heart breaks for anyone who was hurt reading this email this morning and for anyone falsely implicated," [the Superintendent of Bay District Schools]…said. "We know the sentiments expressed in the email do not reflect the values of our school system or our community and I sincerely hope the actual sender is identified quickly."*
>
> Source: The News Herald Staff (July 20, 2021). "Some Bay County students and teachers received the same racist email today. How and why?" The News Herald. Available online at: https://www.newsherald.com/story/news/crime/2021/07/20/bay-county-schools-investigating-racist-email-sent-staff-students/8025767002/

- **Website and social media defacement**: Involving unauthorized changes—such as posting inappropriate language and images—to a school website or official social media account.[43]

- **Denial of service (DOS) attacks**: Intended to make school IT resources unavailable to students and staff by temporarily disrupting their normal functioning.[44]

"Tirthankar Ghosh, the associate director of the University of West Florida Center for Cybersecurity, said distributed denial of services attacks like the one on the [Pinellas County] school system are common and generally of low sophistication.

"The scale of this attack, it really stood out," Ghosh said. "A denial of service attack is pretty common but the fact that 145 schools, their networks came down, that says something."

Source: Ellenbogen, Romy and Fiallo, Josh (May 28, 2021). "St. Petersburg High student's hack crashed internet for all 145 Pinellas schools." Tampa Bay Times. Available online at: https://www.tampabay.com/news/crime/2021/05/28/st-petersburg-high-school-student-crashed-pinellas-schools-systems-internet-with-hack/

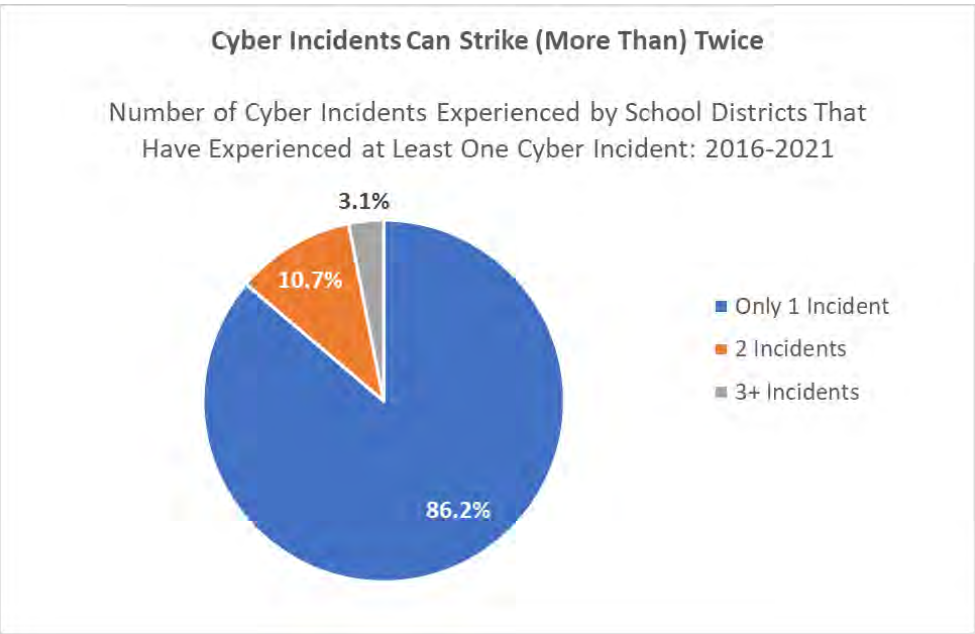
"TECHNOLOGY IS JUST AS IMPORTANT TO THE LEARNING EXPERIENCE IN 2022 AS HEAT IN THE DEPTHS OF WINTER. SO, THE PUBLIC ALSO NEEDS TO KNOW HOW THE SCHOOL SYSTEM WILL PREVENT A SIMILAR CYBERATTACK INCIDENT FROM OCCURRING AGAIN. THE SCHOOL BOARD SHOULD KNOW, TOO, WHETHER IT CAN TAKE STEPS TO PREVENT DIFFERENT AND MORE SEVERE ATTACKS FROM HAPPENING."

Source: Salisbury Post Editorial Board (February 13, 2022). "Editorial: RSS' cyberattack still plaguing systems." Available online at: https://www.salisburypost.com/2022/02/13/editorial-rss-cyberattack-still-plaguing-systems/

CHARACTERISTICS OF DISTRICTS AT RISK

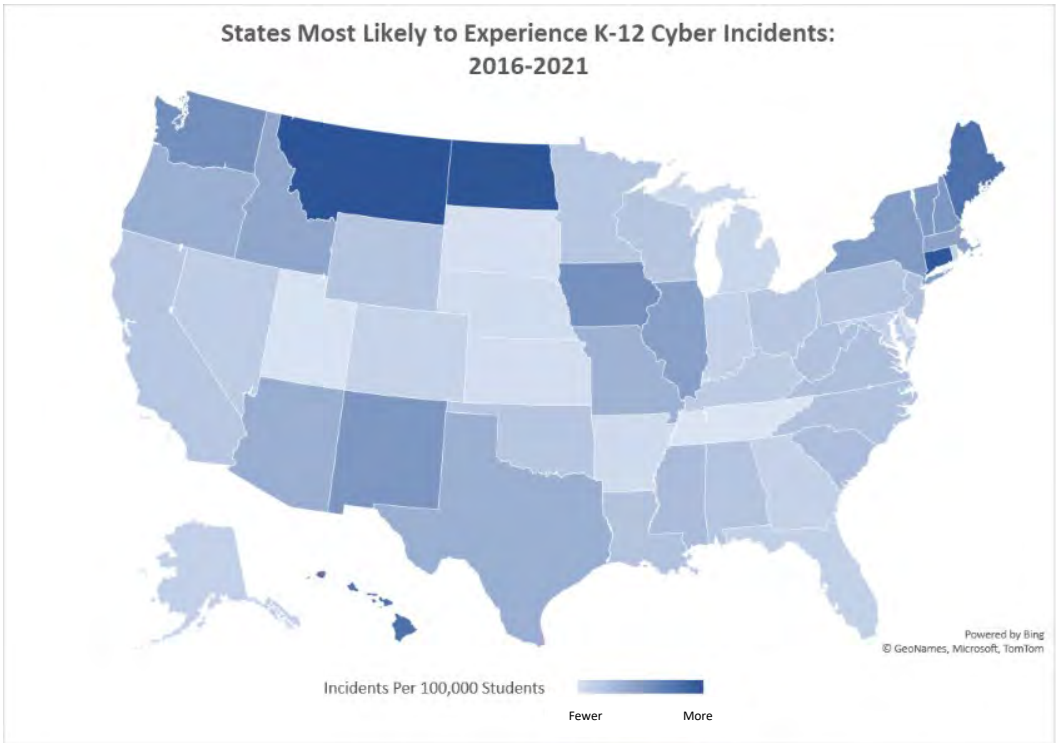
For the 6-year period from 2016-2021, there were a total of 1,331 publicly disclosed K-12 cyber incidents involving 1,123 school districts and other public education agencies.

Of these, 155 school districts—representing nearly 14 percent of school districts and other public education agencies cataloged by the K-12 Cyber Incident Map—have experienced more than one incident. Whether experiencing multiple incidents is a sign of poor cybersecurity risk management practices or just bad luck (or some combination of the two) is beyond the scope of what can be addressed by this dataset, although in cases where districts have experienced five, six, or even more incidents over this period it is suggestive of a story to be told.

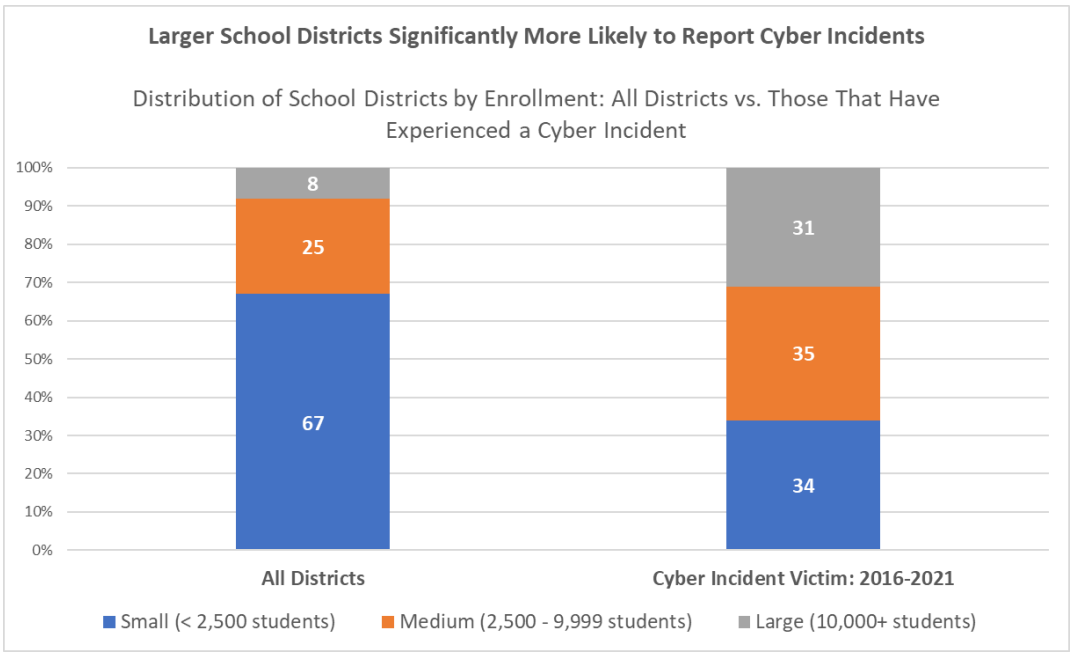


School districts in all 50 states and the District of Columbia (DC) have been cataloged on the K-12 Cyber Incident Map. Not surprisingly, school districts in states with larger student enrollments—including Texas, California, New York, Illinois, and Washington, respectively—are more likely to have experienced K-12 cyber incidents than smaller states over the past six years.

A different picture emerges, however, when controlling for student enrollment. By assessing the rate of K-12 cyber incidents per 100,000 students, what becomes evident is that states such as Montana, North Dakota, Connecticut, Maine, and Hawaii may be experiencing more than their expected share of K-12 cyber incidents.



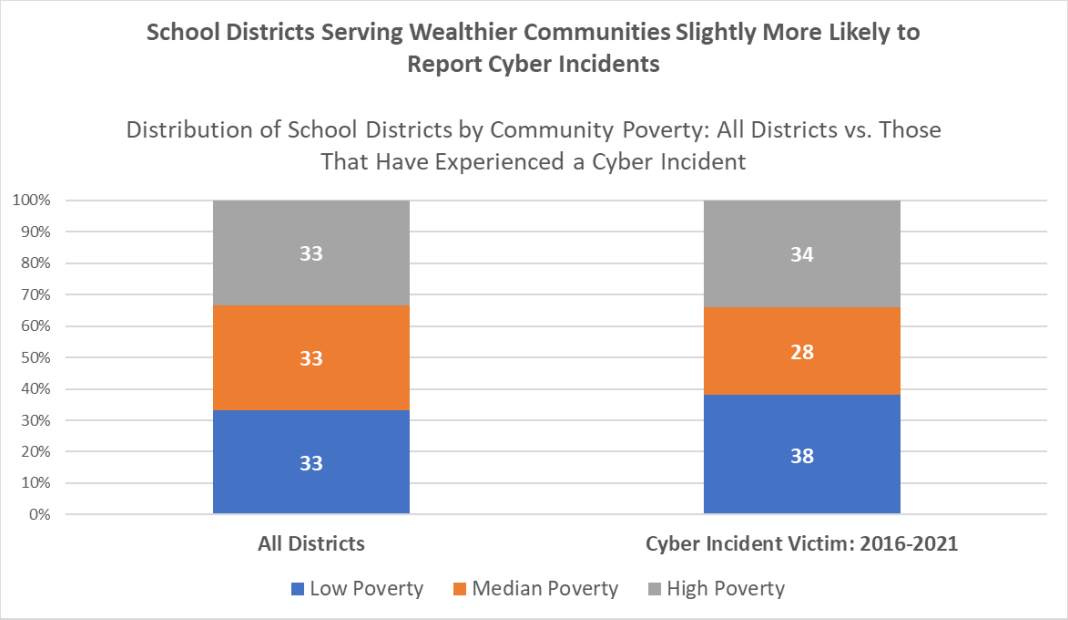
By comparing those districts that have experienced one or more publicly disclosed cyber incidents to all districts nationally, two other themes emerge about the types of school districts at risk of cybersecurity incidents. First, larger school districts (as defined by student enrollment) appear to be at a significantly greater risk for experiencing a cyber incident than small school districts.



There are a few reasons that might explain this pattern in K-12 Cyber Incident Map data. First, larger school districts manage more technology devices and more complex systems than smaller enrollment districts and have more students and employees using that technology. They may also be subject to more directed attacks because they have larger budgets. Smaller enrollment translates to offering a smaller threat profile to malicious actors and a lower chance of a being affected by user actions (whether intentional or by mistake).

Second, incidents that occur in smaller school districts may be less likely to become publicly disclosed than in larger school districts. Hence the fact that they appear to be experiencing fewer incidents may be an artifact of the data collection method used by the K-12 Cyber Incident Map. This may be due to greater media coverage being provided about larger school districts or to the fact that smaller districts may be more limited in terms of their capacity to identify incidents (like data breaches) in a timely manner or at all. Further research would be needed to answer these and related questions.

The second theme that emerges by comparing those districts that have experienced one or more publicly disclosed cyber incidents to all districts nationally is that school districts serving relatively wealthier communities are slightly more likely to have experienced an incident than those serving poorer communities.



Whether this is a function of more frequent public disclosure of K-12 cyber incidents in wealthier communities or that school districts serving relatively wealthier communities may employ more technology for teaching, learning, and school operations than other districts remains unclear.

Nonetheless, it would be a mistake to draw the lesson that school districts in certain states or of certain types or profiles are not at risk from a cyber incident. School districts from all 50 states have suffered significant cyber incidents, from very small, rural districts to the largest urban school districts in the nation. The more important question is what steps can be taken to reduce both the frequency and severity of future K-12 cyber incidents.

SUMMARY AND RECOMMENDATIONS

Since 2016, the K-12 Cyber Incident Map has cataloged a total of 1,331 publicly disclosed school cyber incidents affecting millions of current and former students and teachers in 1,123 U.S. school districts and other public education agencies across all 50 states. Of this total, 166 new incidents were identified over the course of 2021 alone. Averaged over the last six years, this equates to a rate of more than one K-12 cyber incident being disclosed per school day by the nation's public schools.

Given increasing reliance on technology for school district operations, there is every reason to expect that absent significant intervention cyber incidents will continue to plague school districts, placing members of the public at significant—and avoidable—risk.

Existing at the intersection of the K-12 education and cybersecurity sectors, the K12 Security Information Exchange (K12 SIX) is uniquely positioned to both diagnose and point the way toward collective actions that would help stem the rising tide of school cybersecurity risks. Several needs are clear:

- **The need for more and better information sharing about K-12 cyber incidents**. Absent mandated incident disclosure, many school district leaders have demonstrated a lack of willingness to be forthright about cyber incidents with community members and other stakeholders. Yet, when thoughtfully navigated, there are myriad benefits to disclosure: (1) it can assist law enforcement in identifying and prosecuting criminals; (2) it facilitates research to inform policy decision making and the development of K-12 specific cybersecurity guidance and tools; (3) it allows other school districts to take proactive measures to defend themselves from copycat incidents; and, (4) it allows school community members to take steps to protect themselves in a timely manner when they may be at heightened risk personally due to an incident.

- **The need for school districts and other K-12 education agencies to implement commonsense, baseline cybersecurity controls**. Based on the evidence assembled by the K-12 Cyber Incident Map—in conjunction with K-12 specific alerts issued by the FBI and the Cybersecurity and Infrastructure Security Agency (CISA)—it is possible to delineate a small set of cost-effective essential protections that if implemented could dramatically improve the cybersecurity posture of all school districts from the most common threats they are facing. K12 SIX identified this very need and published national cybersecurity standards for school districts—including a free and private school district self-assessment—in the fall of 2021, arguing for a small number of specific controls across four broad categories.[45] Indeed, if the K12 SIX 'Essential Protections' were widely adopted, school districts would fall victim to far fewer cyber incidents and—even in the cases where incidents occurred—school districts would be able to respond and recover more quickly.

- **The need for vendors and suppliers serving the K-12 market to improve their cybersecurity practices**. As the 'State of K-12 Cybersecurity' report series has repeatedly documented, school vendors are responsible for a significant number of the largest K-12 cyber incidents, including

but not limited to student data breaches. Given that school operations are increasingly reliant on outsourced software applications—often hosted off-premises, 'in the cloud'—it is vital that a holistic effort focused not only school district cybersecurity risk management practices and policies, but those of K-12 vendors and suppliers as well, is what will be required to significantly reduce the frequency and severity of cyber incidents experienced by the K-12 sector.

The K12 SIX Essential Cybersecurity Protections[46]

Recommended Protective Measure	Description
1.0 Sanitize Network Traffic to/from the Internet	
1.1 Filter out malware	Block access to known malicious websites
1.2 Campaign against email scams	Reduce the odds that email-based social engineering attacks succeed
1.3 Block malicious documents	Block access to malicious office suite documents, commonly responsible for ransomware
1.4 Limit exposed services	Limit internet exposure of services like remote desktop protocol (RDP)
2.0 Safeguard Student, Teacher, and Staff Devices	
2.1 Restrict administrative access	Keep devices protected and in compliance with security policies
2.2 Apply endpoint protection	Ensure devices used for school remain safe whether used on or off premises
3.0 Protect the Identities of Students, Teachers, and Staff	
3.1 Protect user logins	Implement multi-factor authentication (MFA) to safeguard against compromised passwords
3.2 Improve password management	Prevent password compromise, sharing, and re-use—commonly responsible for data breaches
3.3 Stop online class invasions	Ensure online classes can only be attended by authorized teachers and students
4.0 Perform Regular Maintenance	
4.1 Install security updates	Protect against known vulnerabilities through timely patching of IT systems, computers, and equipment
4.2 Backup critical systems	Build resilience against destructive attacks like ransomware through offline, immutable backups
4.3 Manage sensitive data	Ensure sensitive data is protected, archived, and deleted when no longer needed

See https://www.k12six.org/protective-measures-series for more information about the K12 SIX Essential Protections series of products.

- **The need for cybersecurity threat intelligence, guidance, and best practices *to be tailored specifically for the K-12 sector***, including ensuring it is timely, actionable, and cost-effective. This is especially important given that most school districts do not employ cybersecurity professionals or currently have the capacity to implement with fidelity the dozens of controls

recommended in popular risk management frameworks, such as the National Institute for Standards and Technology (NIST) Cyber Security Framework or the Center for Internet Security (CIS) Controls. In this way, school districts should be thought of as being akin to small- and medium-sized businesses, while being responsible for operating large, complex enterprise IT environments. Moreover, operating as local government agencies, school districts also are subject to sector-specific regulations at both the state and federal levels. Finally, to ensure that threat intelligence and guidance is more likely to be acted on, it is vital that it be communicated to school district leaders via information sources and organizations that are a part of the K-12 sector—such as K12 SIX—and upon which school leaders already rely and trust.

- **The need for school districts and other K-12 organizations to work collectively to address the growing cybersecurity challenge**. If nothing else, the dataset underlying the K-12 Cyber Incident Map demonstrates that U.S. school districts share more in common with each other than not, with respect to the cybersecurity threat landscape. Given limited resources and capacity, it is in the best interests of school district leaders—not just those working in IT positions—to collaborate with each other to increase their schools' resilience to cybersecurity threats. School districts should put a premium on sharing threat intelligence, sharing best practices, developing model policies, pursuing mutually beneficial risk mitigation solutions that can be deployed at scale, and to educating state and federal policymakers about K-12 cybersecurity challenges and potential solutions. While there are many zero- and low-cost steps that individual school districts can and must take now, significant progress won't be made if the burden remains on under-resourced districts working in isolation.

Challenges and Opportunities Ahead

Two sets of actors have the potential to dramatically reshape the K-12 cybersecurity landscape in the near term: cyber risk insurance providers, who have a direct financial incentive to reduce the cybersecurity risks that school districts are facing as a condition of coverage, and policymakers at the state and federal levels, who have an array of proverbial carrots and sticks at their disposal to uplift the cybersecurity risk management practices of the K-12 sector.

Until recently, cyber risk insurance was perceived as a near foolproof safety valve in case of a school cyber incident, such that school district leaders would sometimes purchase insurance in lieu of enacting commonly recommended preventive measures. Take the experience of one Pennsylvania district (as reported in late 2020):

> *The district had two cyberattacks in two years, but avoided paying ransom in both cases.*
>
> *School board members voted Wednesday night to purchase a new cyber liability insurance policy with $2 million worth of coverage, twice what they had last year. The cost of the insurance is $19,000 per year.*
>
> *"It's going to be a policy everyone's going to be looking to get from now on. It's something that 5-10 years ago we wouldn't have even thought about, but now it's a necessity," said [the school district]…business manager.*[47]

From a strictly economic perspective, such a decision could even have been viewed as rational. What school district leaders are beginning to find, however, is that relatively inexpensive school cyber risk insurance is quickly going the way of the dodo. Indeed, those providers still willing to insure school district cyber risks in 2022 are both significantly raising costs and requiring increasingly stringent cybersecurity risk management practices as a precondition for coverage.[48] To the extent that these preconditions are aligned to existing cybersecurity risk management frameworks already employed by forward-leaning school districts, like the K12 SIX Essential Cybersecurity Protections, the more economies of scale could be realized in assisting other school districts to uplift their cybersecurity risk management practices.

While the impact of changes to the K-12 cyber risk insurance market shouldn't be understated, ultimately policymakers will be required to act to accelerate change. After all, as local government agencies, school districts are neither motivated by strictly economic factors nor are they subject to the same type of existential risks as private organizations in the case of catastrophic cyber incidents.

According to the Consortium for School Networking (CoSN), many state and federal policymakers have been actively engaged with issues of cybersecurity with at least indirect relevance to the K-12 sector over the last year.[49] At the federal level, school district leaders would do well to pay particular attention to the enactment of two federal laws passed in 2021:

- *The K-12 Cybersecurity Act*—the first ever federal K-12 specific cybersecurity law—which requires CISA to issue a study of the cybersecurity risks facing the K-12 sector in spring 2022, including recommendations for further actions that could be taken to help schools to better defend themselves[50]

- *The State and Local Cybersecurity Improvement Act*, which authorized the appropriation of $1 billion for grants to state, local and tribal governments—including school districts—to address cybersecurity threats and risks to their IT systems[51]

Coupled with increasing engagement from the U.S. Department of Education—spurred in part by lawmaker requests[52]—there are signs that momentum is building for meaningful federal regulations and resources in support of improved K-12 cybersecurity practices. Nonetheless, careful attention will have to be paid to ensuring that any new regulations and resources lead to meaningful improvements in K-12 cybersecurity risk management practices. Too many students', teachers', and community members' livelihoods are at stake—even if some have been slow to recognize it.

APPENDIX: DATA AND METHODS

The K-12 Cyber Incident Map (https://www.k12six.org/map) and underlying database—currently maintained as a public service by the K12 Security Information Exchange (K12 SIX)—was originally launched in March 2017 as an effort to build an empirical base of information about the state of cybersecurity in U.S. public K-12 schools and districts.[53] While other efforts exist to catalog trends in cybersecurity incidents and data breaches, including in education, none bring a lens that is both vendor-neutral and reliably actionable for U.S. policymakers, K-12 school leaders, and school district IT practitioners.

Widely cited research studies such as Verizon's *Data Breach Investigations Report* series[54] define the education sector overly broadly for purposes useful to targeted domestic action: combining K-12 and postsecondary institutions, public and private institutions, U.S. and global institutions all in a singular category of analysis. Other public sources of data breach incidents compiled by experts exclude the reporting of other significant types of cybersecurity incidents, such as business email compromise and ransomware. While there may be lessons to be drawn from these valuable efforts for education stakeholders, the unique focus of the K-12 Cyber Incident Map has allowed it to become the definitive source of information about the state of K-12 cybersecurity.

The K-12 Cyber Incident Map and underlying database captures detailed information about:

- Publicly-disclosed cybersecurity incidents affecting public K-12 schools, districts, charter schools, and other public education agencies (such as regional and state education agencies) in the 50 states and the District of Columbia, especially those that occur on K-12 managed networks and devices and/or under the direction of school districts
- The characteristics of public school districts (including charter schools) that have experienced one or more publicly-disclosed cybersecurity incidents.

Cyber incidents are defined as those that impact the confidentiality, integrity, and availability of a school district's IT and data systems (whether on-premises or hosted by a vendor working for the district). Whether an incident affects one school or classroom within a district or many—or is due to the actions (or inaction) of a school vendor or partner, including a regional or state education agency—incidents are generally assigned to school districts. This is because school districts (or local education agencies as they are also known) are the primary government entities charged with responsibility for managing taxpayer dollars, employee confidentiality, and student data privacy under state and federal law. As such, when a school vendor or regional/state agency experiences an incident, it is possible that it affects more than one school district and may therefore get reported as more than one incident on the Map. Related incidents are coded as such in the database underlying the K-12 Cyber Incident Map.

By associating incidents with school districts, the K-12 Cyber Incident Map can identify patterns in school district characteristics that may be associated with the odds of experiencing an incident, such as district size and student poverty. School district data are supplemented with select information drawn from the U.S. Department of Education's Common Core of Data, categorized in a manner consistent with that employed by the National Center for Education Statistic's Fast Response Survey System.[55] Similarly,

poverty status of school districts is drawn from the U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE).[56]

Data about K-12 cyber incidents are sourced from a large variety of outlets, including state and local governments, law enforcement, press reports, other data breach reporting services and information sharing communities, social media and online forums, self-reports, and tips. While some reports may be ambiguous (and are often incomplete), all are screened for authenticity and relevance before being recorded.

Nonetheless, the database of K-12 cybersecurity incidents is incomplete and only captures a small fraction of incidents experienced by schools, districts, their partners, and vendors. To the degree that there are mandatory cybersecurity incident reporting requirements for K-12 school districts, they vary across states. Required disclosures are often not publicly accessible and/or are limited to narrow categories of cyber incidents (such as data breaches over a certain magnitude). School districts may resist self-reporting if they believe an incident may reflect poorly on their administration. Finally, given a deficit of attention paid to cybersecurity risk management in many school districts, there may also be a considerable gap between when school districts experience an incident and when (or if) they become aware of that fact.

As of December 2019, summary data about K-12 cybersecurity incidents are published on an enhanced, interactive map of the United States via an integration with OpenStreetMap.[57] Incidents on the map are color-coded by 'primary' incident type:

- phishing attacks resulting in the disclosure of personal data (blue icons)
- other unauthorized disclosures, breaches or hacks resulting in the disclosure of personal data (purple icons)
- ransomware attacks (yellow icons)
- denial-of-service attacks (green icons)
- other cyber incidents resulting in school disruptions and unauthorized disclosures (red pins)

Given that incident types can co-occur (e.g., malware delivery via phishing email, resulting in a data breach), reporting by primary incident type should be interpreted with some caution.

NOTES

[1] Institute of Education Sciences, National Center for Education Statistics. "Digest of Education Statistics: Most Current Digest Tables." Washington, DC: U.S. Department of Education. Available online at: https://nces.ed.gov/programs/digest/current_tables.asp

[2] Levin, Douglas A. (2019). "The State of K-12 Cybersecurity: 2018 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Available online at: https://www.k12six.org/s/K12Cybersecurity-2018YIR.pdf; Levin, Douglas A. (2020). "The State of K-12 Cybersecurity: 2019 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Available online at: https://www.k12six.org/s/K12Cybersecurity2019YearinReview.pdf; Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. Available online at: https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf

[3] U.S. Government Accountability Office (GAO) (September 2020). Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm. GAO-20-644. Washington, DC: GAO. Available online at: https://www.gao.gov/products/GAO-20-644

[4] See, Levin, Douglas A. (2020). "The State of K-12 Cybersecurity: 2019 Year in Review." Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. https://www.k12six.org/s/K12Cybersecurity2019YearinReview.pdf; Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf

[5] As discussed at length in Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf; see also https://en.wikipedia.org/wiki/Zoombombing

[6] See, e.g., Consortium for School Networking (2021). "EdTech Leadership Survey Report." Available online at: https://emma-assets.s3.amazonaws.com/paqab/2ad6dcd4fb0d923337a5a6d6a5344ee0/Survey_Report_2021_Final.pdf; Project Tomorrow (2021). "Creating a Common Culture of Action Around Cybersecurity." Available online at: https://tomorrow.org/speakup/pdfs/Creating-a-Common-Culture-of-Action-Around-Cybersecurity.pdf;

[7] Gatlan, Sergiu (June 23, 2021). "PYSA ransomware backdoors education orgs using ChaChi malware" Bleeping Computer. Available online at: https://www.bleepingcomputer.com/news/security/pysa-ransomware-backdoors-education-orgs-using-chachi-malware/

[8] U.S. Federal Bureau of Investigation (FBI) (March 16, 2021). "Increase in PYSA Ransomware Targeting Education Institutions." Alert Number CP-000142-MW. Available online at: https://www.ic3.gov/Media/News/2021/210316.pdf

[9] Wehmhoener, Karl (December 7, 2021). "Eldon School District canceled classes Tuesday due to ransomware attack." ABC 17. Available online at: https://abc17news.com/news/2021/12/07/eldon-school-district-cancels-classes-due-to-ransomware/

[10] Manning, Rob (April 27, 2021). "Instruction halted as east Multnomah Co. school district suffers apparent cyberattack." OPB. Available online at: https://www.opb.org/article/2021/04/27/instruction-halted-as-east-multnomah-co-school-district-suffers-apparent-cyberattack/

[11] KENS 5 Staff (August 4, 2021). "'There was no other choice' | Judson ISD pays more than $547,000 following ransomware attack." KENS 5. Available online at: https://www.kens5.com/article/news/local/judson-isd-pays-more-than-547000-following-ransomware-attack/273-4e3d2c4c-657e-47c2-a217-4e8be2079855

[12] Corfield, Gareth (June 16, 2021). "Ryuk ransomware recovery cost us $8.1m and counting, says Baltimore school authority." The Register. Available online at: https://www.theregister.com/2021/06/16/baltimore_ryuk_ransomware_dollars_8_1m_recovery_cost/?&web_view=true; Simpson, Amy (November 24, 2021). "A year later, Baltimore County Schools ransomware recovery costs nearly $9.7 million." WBFF Baltimore. Available online at: https://www.msn.com/en-us/news/us/a-year-later-baltimore-county-schools-ransomware-recovery-costs-nearly-9-7-million/ar-AAR6f3l

[13] Watson, Stephen T (October 18, 2021). "Buffalo School District to Spend $10M on Ransomware Response." Government Technology. Available online at: https://www.govtech.com/education/k-12/buffalo-school-district-to-spend-10m-on-ransomware-response
[14] Bisson, David (December 23, 2021). "Ransomware Attackers' New Tactic: Double Extortion." Security Intelligence. Available online at: https://securityintelligence.com/articles/ransomware-double-extortion/
[15] Collier, Kevin (September 10, 2021). "Hackers are leaking children's data — and there's little parents can do." NBC News. Available online at: https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926
[16] Nielsen, Nicole (October 6, 2021). "Allen ISD Parents Concerned About Receiving Cybersecurity Breach Emails." CBS DFW. Available online at: https://dfw.cbslocal.com/2021/10/06/allen-isd-parents-receive-cybersecurity-breach-emails/
[17] New, Brian (August 16, 2021). "Has Your Kid's Texas School District Been Hammered By Cyberattacks? I-Team Investigation." CBS DFW. Available online at: https://dfw.cbslocal.com/2021/08/16/dozens-texas-school-districts-hammered-cyberatacks-ransomware/
[18] Freedman, Linn Foster (April 22, 2021). "School Nutrition Vendor Sued for Compromise of 867,209 K-12 Student Records." Robinson + Cole. Available online at: https://www.dataprivacyandsecurityinsider.com/2021/04/school-nutrition-vendor-sued-for-compromise-of-867209-k-12-student-records/
[19] Cooper, Kenny (September 7, 2021). "Parents outraged after bus company email reveals students' information." WHYY. Available online at: https://whyy.org/articles/springfield-delco-parents-outraged-after-bus-company-email-reveals-students-information/
[20] WGRZ Staff (October 8, 2021). "Williamsville School employees' private health data inadvertently leaked by Independent Health." WGRZ. Available online at: https://www.wgrz.com/article/news/local/private-health-data-of-williamsville-school-employees-inadvertently-leaked-by-independent-health/71-2d476804-2d70-4689-b7c9-d4fb224b54c6
[21] Erickson, Kurt (October 19, 2021). "Missouri teacher pension system probing possible cyber attack." St. Louis Post-Dispatch. Available online at: https://www.stltoday.com/news/local/govt-and-politics/missouri-teacher-pension-system-probing-possible-cyber-attack/article_49c5817e-ac8d-5c88-a581-dc5b5c34d8f0.html
[22] Keierleber, Mark (October 18, 2021). "Popular student monitoring software could have exposed thousands to hacks." Fast Company. Available online at: https://www.fastcompany.com/90686770/netop-student-monitoring-software-hack
[23] Turton, William (March 9, 2021). "Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals." Bloomberg. Available online at: https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
[24] E.g., PrintNightmare https://en.wikipedia.org/wiki/PrintNightmare; Log4j https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance and https://www.k12six.org/news/k12-six-releases-k12-specific-log4j-collaboration-resource; Fung, Brian (August 24, 2021). "Data leak exposes tens of millions of private records from corporations and government agencies." CNN Business. Available online at: https://www.cnn.com/2021/08/24/tech/data-leak-microsoft-upguard/index.html
[25] Olson, Parmy (July 31, 2019). "Pearson Hack Exposed Details on Thousands of U.S. Students." Wall Street Journal. Available online at: https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001
[26] U.S. Securities and Exchange Commission (August 16, 2021). "SEC Charges Pearson plc for Misleading Investors About Cyber Breach." Available online at: https://www.sec.gov/news/press-release/2021-154; SEC Order: https://www.sec.gov/litigation/admin/2021/33-10963.pdf
[27] There is a growing body of best practices and guidance for the management of vendor and supply-chain risk that could be adapted for use in the K-12 education sector. See, e.g., National Institute of Standards and Technology (NIST). "Best Practices in Cyber Supply Chain Risk Management – Conference Materials: Cyber Supply Chain Best Practices." Available online at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf; NIST. "Best Practices in Cyber Supply Chain Risk Management – Conference Materials: Organizational Strategies for Cyber Supply Chain Risk Management." Available online at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Organizational-Strategy.pdf; NIST. "Notional Supply Chain Risk Management Practices for Federal Information Systems." NISTIR 7622. Available

online at: https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf; NIST. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." NIST Special Publication800-161. Available online at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf; NIST. "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry." NISTIR 8276. Available online at: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

[28] David Saleh Rauf (November 16, 2020). "Cyberattacks on Ed-Tech Companies Rare, But Hugely Disruptive, Report Finds." EdWeek Market Brief. Available online at: https://marketbrief.edweek.org/marketplace-k-12/cyberattacks-ed-tech-companies-rare-hugely-disruptive-report-finds/

[29] See, e.g., Attrino, Anthony G. (June 9, 2021). "N.J. school worker accidentally leaked Social Security numbers of staff to public." NJ Advance Media for NJ.com. Available online at: https://www.nj.com/bergen/2021/06/nj-school-worker-accidentally-leaked-social-security-numbers-of-staff-to-public.html; Gallion, Bailey (May 7, 2021). "Cybercriminals potentially accessed data of 10,000 people in Brevard School Board breach." Florida Today. Available online at: https://www.floridatoday.com/story/news/education/2021/05/07/brevard-county-school-district-warns-10-000-people-data-breach-email-addresses/4995507001/

[30] See, e.g., Horner, Rick (July 23, 2021). "Student private information breached in Fairfax County Public Schools." Fairfax County Times. Available online at: https://www.fairfaxtimes.com/articles/student-private-information-breached-in-fairfax-county-public-schools/article_d8f36b5a-eb17-11eb-b460-bb82b3b50727.html; McConnell, Jim. (April 19, 2021). "School system mistakenly releases names of students, staff with COVID." Chesterfield Observer. Available online at: https://www.chesterfieldobserver.com/articles/school-system-mistakenly-releases-names-of-students-staff-with-covid/; Johnson, Alec (February 4, 2021)."The Shorewood School District is apologizing for accidentally releasing student data." Milwaukee Journal Sentinel. Available online at: https://www.jsonline.com/story/communities/northshore/news/shorewood/2021/02/04/shorewood-school-district-apologizes-releasing-student-data/4355690001/

[31] See, e.g., Salhotra, Pooja (August 12, 2021). "Brooklyn Tech students uncovered a NYC schools data breach. Here's how they took action." Chalkbeat New York. Available online at: https://ny.chalkbeat.org/2021/8/12/22622143/brooklyn-tech-nyc-schools-data-breach; Tooten, Tim (April 13, 2021). "BCPS takes responsibility for data breach that affected teachers." WBAL TV 11. Available online at: https://www.wbaltv.com/article/baltimore-county-public-schools-accept-responsibility-for-data-breach/36109608; KTRK Staff (February 1, 2021). "Friendswood ISD students' Social Security numbers mistakenly sent to school photographer." ABC 13. Available online at: https://abc13.com/friendswood-isd-school-student-social-security-numbers-leak-sent-to-photographer/10221735/; Cross, Ian (November 29, 2021). "Bay Village school district accidentally releases seniors' personal info, including grades, to all families." ABC News 5 Cleveland. Available online at: https://www.news5cleveland.com/news/local-news/oh-cuyahoga/bay-village-school-district-accidentally-releases-seniors-personal-info-including-grades-to-all-families

[32] See, e.g., Treisman, Rachel. (October 14, 2021). "A Missouri newspaper told the state about a security risk. Now it faces prosecution." NPR. Available online at: https://www.npr.org/2021/10/14/1046124278/missouri-newspaper-security-flaws-hacking-investigation-gov-mike-parson

[33] Freed, Benjamin (February 22, 2022). "Missouri website vulnerability was present since 2011, investigation finds." StateScoop. Available online at: https://statescoop.com/missouri-website-vulnerability-was-present-since-2011/

[34] Barber, Katy (February 9, 2022). "Turns out a couple kids were behind a massive Texas school system hack." KTSA. Available online at: https://www.ktsa.com/turns-out-a-couple-kids-were-behind-a-massive-texas-school-system-hack/

[35] Osborne, Ryan (September 3, 2021). "Cyberattack hits Dallas ISD data; current and former students' records could be impacted." WFAA. Available online at: https://www.wfaa.com/article/news/education/cyberattack-dallas-isd-data-breach-hack-current-former-students-records-impact/287-bc42c3ec-1092-4b51-ade0-cbf0d9fdcbb7

[36] Eiserer, Tanya, and Trahan, Jason (February 7, 2022). "'They pretty much had access to everything': WFAA reveals the masterminds behind last year's Dallas ISD cyber breach. And it's not who you think." WFAA. Available online at: https://www.wfaa.com/article/news/local/investigates/wfaa-reveals-masterminds-behind-dallas-isd-cyber-breach/287-15b22b82-b226-424d-9b27-a7d5b5120ac3

[37] AASA (February 18, 2022). "Texas, Utah School District Leaders Recognized for EmpowerED Digital Superintendent Award at AASA's National Conference on Education." Available online at: https://www.aasa.org/content.aspx?id=47626

[38] Meadows, Jonah (November 29, 2021). "ETHS Defrauded Of $48,570 In Hack That Exposed 1,139 Identities." Patch. Available online at: https://patch.com/illinois/evanston/eths-defrauded-48-570-hack-exposed-1-139-identities

[39] Hanna, Maddie and Vella, Vinny (March 4, 2021). "Chester Upland School District says millions of dollars are missing. The DA has launched a probe." The Philadelphia Inquirer. Available online at: https://www.inquirer.com/news/chester-upland-school-district-investigation-delaware-county-20210304.html

[40] Colburn, David (February 17, 2021). "ISD 2142 hit with phishing scheme." The Timberjay. Available online at: http://www.timberjay.com/stories/isd-2142-hit-with-phishing-scheme,17343

[41] See, e.g., Associated Press (February 12, 2021). "School meeting hacked with racial epithet, obscene video." The Washington Times. Available online at: https://www.washingtontimes.com/news/2021/feb/12/school-meeting-hacked-with-racial-epithet-obscene-/; DeNardo, Mike (February 22, 2021). "Police investigate racist hack that disrupted Ben Franklin High students' virtual field trip." KYW Newsradio. Available online at: https://www.audacy.com/kywnewsradio/news/local/police-investigate-hack-that-disrupted-virtual-field-trip; Purvis, Leon (March 4, 2021). "Internet hack, threat disrupt learning in South Hadley." Western Mass News. Available online at: https://web.archive.org/web/20210317210021/https://www.westernmassnews.com/news/internet-hack-threat-disrupt-learning-in-south-hadley/article_750b2bb8-7d31-11eb-9822-0379f7330fa0.html; Maldonado, Zinnia (March 17, 2021). "Waterbury middle school hacked, students exposed to inappropriate content." FOX 61. Available online at: https://www.fox61.com/article/news/crime/waterbury-middle-school-hacked-students-exposed-to-inappropriate-content/520-706d99a2-5a3e-43ea-99d0-456ca7abe5b7; Wagner, Jacob (November 24, 2021). "School board Zoom meeting hacked." The Star. Available online at: https://www.grandcoulee.com/story/2021/11/24/news/school-board-zoom-meeting-hacked/14776.html

[42] See, e.g., Arevalo, Greena (January 8, 2021). "Disturbing email sent to Virginia high school students, parents upset at delayed notification." CBS 17. Available online at: https://www.cbs17.com/news/south/disturbing-email-sent-to-virginia-high-school-students-parents-upset-at-delayed-notification/; Blanchard, Peter (January 25, 2021). "Council Rock Apologizes For 'Inappropriate' Emails." Patch. Available online at: https://patch.com/pennsylvania/newtown-pa/council-rock-apologizes-inappropriate-emails; Eliopoulos, Peter (January 24, 2021). "Thousands in Massachusetts school district receive violent, racist emails from student account." WCVB. Available online at: https://www.wcvb.com/article/thousands-in-gardner-massachusetts-school-district-receive-violent-racist-emails-from-student-account/35301402; Cote, Jackson (March 1, 2021). "Shelter in place ordered at Chicopee Comprehensive High School after public school email system hacked and 'questionable' message received, police say." Mass Live. Available online at: https://www.masslive.com/police-fire/2021/03/shelter-in-place-ordered-at-chicopee-comprehensive-high-school-after-public-school-email-system-hacked-and-questionable-message-received-police-say.html

[43] See, e.g., Wisely, John (March 15, 2021). "Hackers post racist slurs on Troy schools website." Detroit Free Press. Available online at: https://www.freep.com/story/news/education/2021/03/15/hackers-slurs-troy-schools/4706894001/; Scripps staff (March 16, 2021). "Leon County Schools website hacked." WTXL Tallahassee. Available online at: https://www.wtxl.com/news/local-news/leon-county-schools-website-social-media-accounts-hacked; Tarrazi, Alexis (June 24, 2021). "Vulgar Messages Appear As Bridgewater Schools' Websites Hacked." Patch. Available online at: https://patch.com/new-jersey/bridgewater/vulgar-messages-appear-bridgewater-schools-websites-hacked

[44] See, e.g., February 5, 2021. "Winthrop Officials Investigating Cyber Attack on Town, School Servers." Available online at: https://www.town.winthrop.ma.us/home/news/winthrop-officials-investigating-cyber-attack-town-school-servers; Bray, Hiawatha (February 10, 2021). "Hacking attacks plague Massachusetts schools." Boston Globe. Available online at: https://www.bostonglobe.com/2021/02/10/business/hacking-attacks-plague-massachusetts-schools/; Mooney, John (January 21, 2021). "Cyber Attack Causes Disruption of Scotch Plains-Fanwood Schools." Tapinto. Available online at: https://www.tapinto.net/towns/scotch-plains-slash-fanwood/sections/education/articles/cyber-attack-causes-disruption-of-scotch-plains-fanwood-schools

[45] To learn more and access products in this series, visit: https://www.k12six.org/protective-measures-series

[46] Developed by K-12 IT practitioners, for K-12 IT practitioners—and aligned to cybersecurity risk management best practices—the K12 SIX 'Essential Protections' series establishes baseline cybersecurity standards for U.S. school districts and provides guidance on their implementation. K12 SIX-recommended practices are designed to defend against the most common cyber threats facing school districts, including those recently identified by the Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA). To learn more and access products in this series, visit: https://www.k12six.org/protective-measures-series

[47] Reber, Chris (November 12, 2020). "Thorpe raises cyber insurance." Times News Online. Available online at: https://www.tnonline.com/20201112/thorpe-raises-cyber-insurance/

[48] See, e.g., Blosfield, Elizabeth (March 2, 2022). "Education Providers Face Challenges With Growth in Cyber Threats, Insurance Costs." Insurance Journal. Available online at: https://www.insurancejournal.com/news/2022/03/02/656160.htm; Childers, Angela (July 12, 2021). "Schools hit with cyber price hikes." Business Insurance. Available online at: https://www.businessinsurance.com/article/20210712/NEWS06/912342944/Schools-hit-with-cyber-price-hikes; Toulas, Bill (January 22, 2022). "School District reports a 334% hike in cybersecurity insurance costs." Bleeping Computer. Available online at: https://www.bleepingcomputer.com/news/security/school-district-reports-a-334-percent-hike-in-cybersecurity-insurance-costs/; Schaffhauser, Dian (October 12, 2021). "The Changing Face of Cyber Insurance in K–12." THE Journal. Available online at: https://thejournal.com/articles/2021/10/12/the-changing-face-of-cyber-insurance-in-k12.aspx

[49] Consortium for School Networking (December 2021). "2021 State and Federal Cybersecurity Policy Trends: Insights for Education Technology Leaders & Policymakers." Available online at: https://emma-assets.s3.amazonaws.com/paqab/20bc4de8816d684fc9af37751b204c19/CoSN_2021_Cybersecurity_Legislation_Report_11_30_21__2_.pdf

[50] See, e.g., Sabin, Sam (October 12, 2021). "New K-12 cybersecurity law is just the first step." Politico. Available online at: https://www.politico.com/newsletters/weekly-cybersecurity/2021/10/12/new-k-12-cybersecurity-law-is-just-the-first-step-798142

[51] See, e.g., Lohrmann, Dan (November 14, 2021). "Dedicated State and Local Cyber Grants Are Finally Arriving." Government Technology. Available online at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/dedicated-state-and-local-cyber-grants-are-finally-arriving

[52] See, e.g., GAO (October 2021). "CRITICAL INFRASTRUCTURE PROTECTION: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats (GAO-22-105024). Available online at: https://www.gao.gov/products/gao-22-105024

[53] "Introducing the K-12 Cyber Incident Map" (March 30, 2017) available online at: https://k12cybersecure.com/blog/introducing-the-k-12-cyber-incident-map/

[54] Information about the Verizon Data Breach Incident Report (DBIR) series can be found online at: https://enterprise.verizon.com/resources/reports/dbir/

[55] The Common Core of Data (CCD) is the U.S. Department of Education's primary database on public elementary and secondary education in the United States. The U.S. Department of Education's Fast Response Survey System (FRSS) was established to collect issue-oriented data—representative at the national level—quickly and with minimum response burden.

[56] The U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE) program provides estimates of income and poverty for every state and county. SAIPE also provides estimates of the number of school-age children in poverty for all school districts.

[57] For more information on the K-12 Cyber Incident Map, the technology used to build it, and functionality, see "Introducing the K-12 Cyber Incident Map, Version 2." https://k12cybersecure.com/blog/introducing-the-k-12-cyber-incident-map-version-2/