THE STATE OF K-12 CYBERSECURITY: 2020 YEAR IN REVIEW

Douglas A. Levin
K-12 Cybersecurity Resource Center and the K12 Security Information Exchange
March 10, 2021

K12 SIX

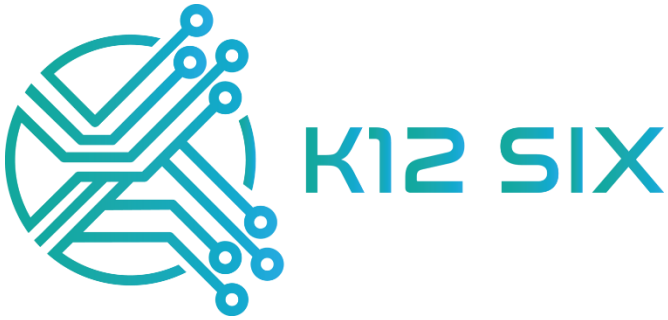
The *State of K-12 Cybersecurity: 2020 Year in Review* report is joint product of the K12 Security Information Exchange and the K-12 Cybersecurity Resource Center based on data from its K-12 Cyber Incident Map, the definitive source of data on publicly-disclosed U.S. public K-12 cyber incidents.

ABOUT THE K-12 CYBERSECURITY RESOURCE CENTER

The K-12 Cybersecurity Resource Center is the home of the K-12 Cyber Incident Map and is devoted solely to reporting news and information related to school cybersecurity and privacy issues. It is maintained as a free, independent resource for the K-12 community by EdTech Strategies, LLC in partnership with the K12 Security Information Exchange (K12 SIX). Learn more at: https://k12cybersecure.com

ABOUT THE K12 SECURITY INFORMATION EXCHANGE

The K12 Security Information Exchange (K12 SIX) is a new national non-profit membership organization dedicated solely to helping to protect K-12 schools—public and private—from 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. For more information, including on how school districts can participate, please visit https://www.k12six.org



Suggested Citation:

> Levin, Douglas A. (2021). "The State of K-12 Cybersecurity: 2020 Year in Review." EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange. Available online at: https://k12cybersecure.com/year-in-review/

Cover photo credit: Brandon Morgan on Unsplash

ACKNOWLEDGEMENTS

Since the K-12 Cyber Incident Map first launched in 2017 it has benefited from many individual and corporate supporters who have contributed financial and intellectual resources to its maintenance and ongoing development. The 2020 report—produced in partnership with the K12 Security Information Exchange (K12 SIX)—was strengthened via collaborations with: Jennifer Gregory, Jacqueline M. Nowicki, Sherri Doughty, and Jessica Mausner of the U.S. Government Accountability Office; Danny Y. Huang of the Tandon School of Engineering, New York University; 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; Tawnell Hobbs, the national K-12 education reporter for The Wall Street Journal; members of the OpsecEdu community; and, Staci Elliott, Jaquar Harris, Eric Lankford, Pat McGlone, and Arshad Somani of K12 SIX.

Nonetheless, K-12 cyber incident data, data analyses, and all other report contents are the sole responsibility of the K-12 Cybersecurity Resource Center (operated by EdTech Strategies, LLC) and do not necessarily represent the views of collaborators, sponsors, or donors. All errors and omissions contained herein are the responsibility of the author.

INTRODUCTION

An unprecedented year offered a profound stress test of the resiliency and security of the K-12 educational technology ecosystem.

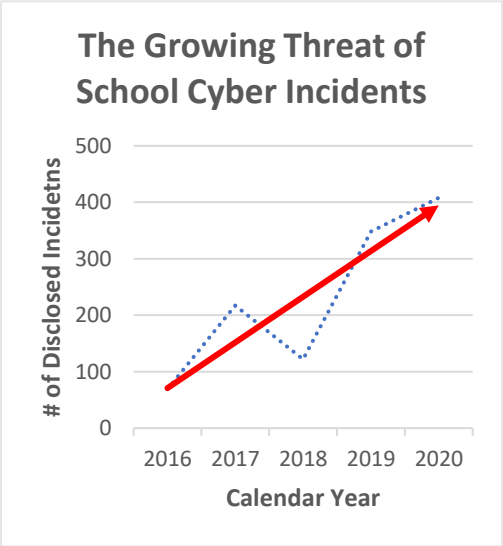
The discipline of cybersecurity concerns itself with ensuring the confidentiality, integrity, and availability of information technology (IT) systems and the data they collect and process. In the public U.S. K-12 context—a $760 billion sector, serving over 50 million students[1]—school IT systems collect and manage sensitive data about students, about their parents, guardians, and families, about educators and other school staff, and about school district operations. In some cases, these IT systems are locally hosted on school district premises or in shared hosting arrangements with other local government entities; increasingly, they are hosted by an ecosystem of vendors 'in the cloud' on systems accessible by any internet-connected device.

While there are myriad benefits to the adoption and use of IT systems by school districts—and to the collection and sharing of education-related data with trusted partners—it is important we acknowledge that any adoption of technology also introduces cybersecurity risk. As one leading cybersecurity expert famously quipped:

> *"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then I have my doubts."*[2]

Indeed, this sentiment illustrates why the goal of leadership is not to guarantee absolute security—a fool's errand and impossible task. Instead, leaders identify potential risks, weigh the likelihood and significance of the real-world impacts of those risks should they come to pass, and—by allocating budgets and directing activities—manage them appropriately in the context of other pressing organizational needs.

Unfortunately, in the context of U.S. K-12 public school districts, cybersecurity risks are now neither hypothetical, nor trivial—as the *State of K-12 Cybersecurity: Year in Review* report series and a growing body of evidence has documented.[3]

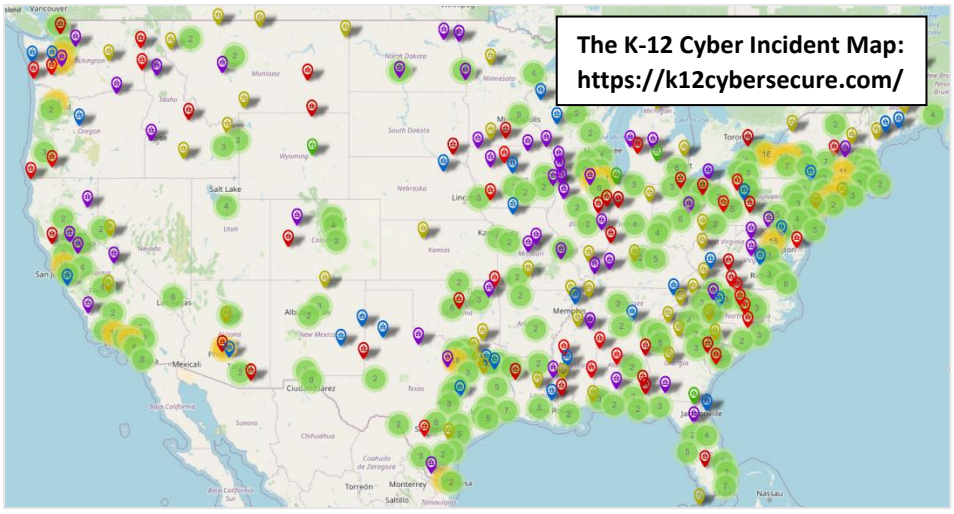


While policymakers and school leaders have historically demonstrated a reasonable duty of care in protecting members of their school communities from physical security risks, natural disasters, and extreme weather events (and—as 2020 has demonstrated—public health risks, too), such a commitment has heretofore largely been absent with respect to school-related cybersecurity risk.

Notwithstanding the heroic education IT-related efforts to ensure remote learning was possible for large numbers of elementary and secondary students and their teachers during 2020, it should hardly be surprising that school district responses to the COVID-19 pandemic also revealed significant gaps and critical failures in the resiliency and security of the K-12 educational technology ecosystem.

Indeed, the 2020 calendar year saw a record-breaking number of publicly-disclosed school cyber incidents. Moreover, many of these incidents were significant: resulting in school closures, millions of dollars of stolen taxpayer dollars, and student data breaches directly linked to identity theft and credit fraud.

This report—the latest in *The State of K-12 Cybersecurity: Year in Review* series—aims to help remedy an information gap on the risks from school cybersecurity incidents. By cataloging and analyzing data from every publicly-disclosed cybersecurity incident affecting public elementary and secondary education agencies across the U.S. in the prior calendar year, the series is intended to spur greater attention to the challenges of securing the K-12 IT ecosystem and suggest ways that policymakers and school district leaders might effectively respond.

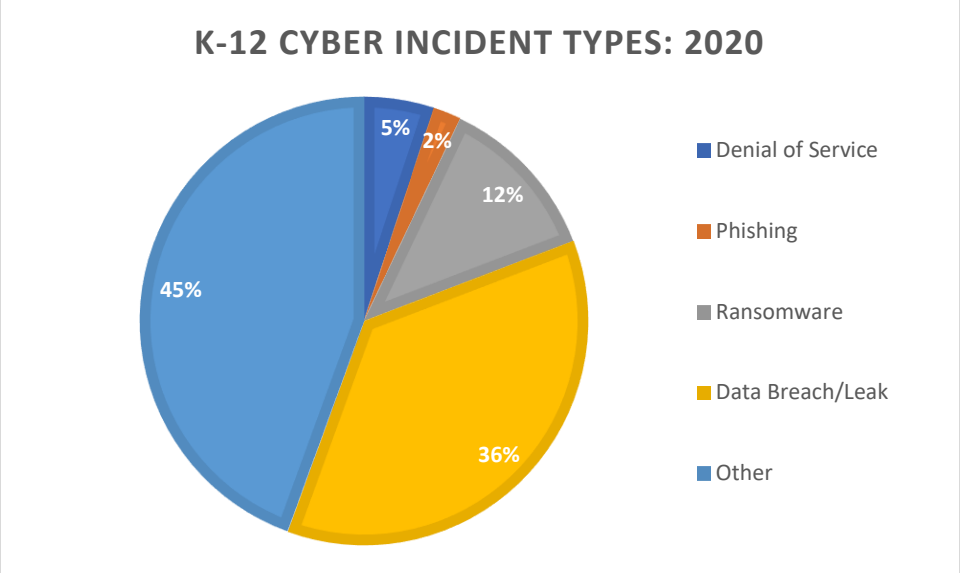


The following chapters of the report present findings from detailed analyses of cyber incidents experienced by school districts during the past year, as well as the characteristics of those districts. It concludes with recommendations to address the growing challenge of cybersecurity risk management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

K-12 CYBER INCIDENTS: ANALYSIS AND TRENDS

During calendar year 2020, the K-12 Cyber Incident Map cataloged 408 publicly-disclosed school incidents, including student and staff data breaches, ransomware and other malware outbreaks, phishing attacks and other social engineering scams, denial-of-service attacks, and a wide variety of other incidents. This is 18 percent more incidents than were publicly-disclosed during the prior calendar year (and—for the second year running—the most since the K-12 Cyber Incident Map first started tracking these incidents in 2016). This equates to a rate of more than two incidents per school day over the course of 2020.

What were the most frequently experienced types of school-related cyber incidents reported during 2020? Data assembled for the K-12 Cyber Incident Map are instructive.



Note: 'Other' incidents include unattributed malware, class and meeting invasions, email invasion, website and social media defacement, and a wide variety of related and/or low-frequency incidents.

The Impact of the COVID-19 Pandemic

Due to the COVID-19 pandemic, the presentation of school cyber incidents over the course of the 2020 calendar year was atypical, testing the nimbleness of school district IT staff and operations.

The first quarter of 2020 largely pre-dated the pandemic. As such—unsurprisingly—the pattern of school cyber incidents disclosed during that period seems a direct extension of trends from the prior year.

However, the second quarter of 2020—coincident with the rise of COVID-19 and the corresponding adoption of remote learning—marked a sharp departure from the prevailing trend line. During this period, many schools ceased in-person operations and adopted video conferencing tools to host

synchronous online classes and school community meetings. This shift also introduced a new class of school cyber threats that plagued districts almost to the complete exclusion of other incident types during that period: class invasion and its two variants.

For the purposes of this report, 'class invasion' is defined as incidents where unauthorized individuals disrupt online classes, often with hate speech; shocking images, sounds, and videos; and/or threats of violence. 'Meeting invasion' represents the same tactic but is aimed instead at public school board and other school community meetings, such as PTA meetings, virtual graduations, and open houses/orientation sessions. And, 'email invasion' involves the compromise of a school district email system for the purpose of bulk sharing of disturbing images, videos, hate speech, and/or threats of violence—or links to the same—to members of the school/district community.

The Impact of COVID-19 on K-12 Cyber Incidents		
2020	**Disclosed K-12 Cyber Incidents**	**Primary Incident Types (sorted by relative frequency)**
Q1	49	• Ransomware and other malware • Student and staff data breaches • Targeted phishing attacks/business email compromise
Q2	67	• Class/meeting invasion • Student data breaches
Q3	160	• Class/meeting invasion • Student data breaches • Ransomware and other malware • Denial-of-service attacks
Q4	132	• Student and staff data breaches • Ransomware and other malware • Class/meeting invasion • Denial-of-service attacks

The start of the 2020-2021 school year in the late summer/fall of 2020 (Q3) brought with it a surge in cyber incidents that lasted through the end of the calendar year. Several factors are likely to have contributed to this marked shift:

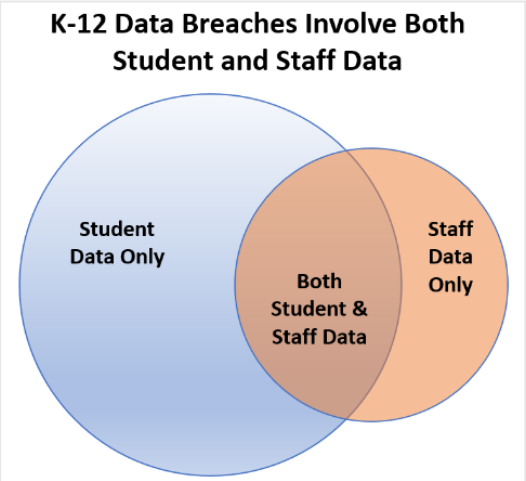
- Schools increased their reliance on technology tools for teaching and learning over the course of late spring and early summer months, including in many cases by (a) deploying thousands of new devices to students and educators under very tight deadlines, (b) adopting new teaching and learning platforms without adequate time to train users and otherwise prepare for their implementation, and (c) by allowing (or encouraging) staff to use free applications and services that had not undergone appropriate vetting.

- School district IT staff—unable to physically service devices due to COVID-19 safety restrictions—may have granted users elevated access to their devices and/or deployed remote access tools to support remote learning.
- Devices used during remote learning—and on untrusted networks in student and educator homes—were re-introduced to school networks in the fall for those districts that returned to in-person learning temporarily or in part. These devices may or may not have been updated and/or scanned for malware before that reintroduction.
- Threat actors may be growing increasingly sophisticated in targeting school districts, focusing their efforts at times during the school year that schools may be most vulnerable, including at the beginning of the school year and over Thanksgiving and winter holidays.

Calendar year 2020 offered a profound stress test of the resiliency and security of the K-12 educational technology ecosystem. The evidence suggests that in rapidly shifting to remote learning school districts not only exposed themselves to greater cybersecurity risks but were also less able to mitigate the impact of the cyber incidents they experienced. This suggests that school districts should revisit their contingency plans for continuity of operations during emergencies, with a focus on IT systems used in teaching and learning and district operations. While no one can predict whether another global pandemic will close schools to in-person learning, important lessons can and should be drawn from this experience to ensure that if such an event (or something like it) occurs again in the future, districts are better prepared.

Data Breaches

Since at least 2016, data breaches have been the most common single type of publicly-disclosed cyber incident experienced by school districts. 2020 was no exception to this long-term trend: The K-12 Cyber Incident Map documented 145 data breach incidents involving public schools (representing 36 percent of all incidents disclosed during the year). These breaches most often involve the unauthorized disclosure of student data but may also include significant amounts of data about school district staff, including educators. In fact, many cases of school data breaches involve sensitive data on both students and staff.



During 2020, the U.S. Government Accountability Office published a study based on the dataset used by this report series exclusively on the topic of student data breaches, *Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm*.[4] The report found:

- Large numbers[5] of K-12 students had their personal information compromised in data breaches between 2016 and 2020
- Compromised data included grades, bullying reports, and Social Security numbers—leaving students vulnerable to emotional, physical, and financial harm
- Breaches were accidental and intentional—with a variety of responsible actors and motives

- Wealthier, larger, and suburban school districts were more likely to have a reported breach

Indeed, there should be little argument that student data breaches can have significant repercussions for current and former students and their families. Take the recent case of Toledo (OH) Public Schools (TPS) as a cautionary tale. In September 2020, security researchers learned that the Maze ransomware cartel had compromised the data systems of TPS.[6] Either because the district did not meet the criminal group's extortion demands or for other reasons of their own, Maze dumped 9GB of compressed TPS data on their site, including sensitive student and employee data. These data did not appear to involve current records, but those held by the district from at least 2008 to 2017.[7] By February of 2021—less than six months from the initial incident—news outlets began reporting that parents were receiving notifications of identity theft and credit fraud involving their TPS students:

> *"[One parent]… learned his son's information is in the hands of people it shouldn't be. Here are some of the messages he's received about his elementary schooler:*
>
> - *The first one was for denial for a credit card.*
> - *Another one happened when the child was denied for a car loan because it said the reason was because of his income ratio.*
> - *One of the last ones was to have fixed electric rates.*
> - *The family got a flier talking about the student's Toledo Edison account and the gift card he could get by switching suppliers.*
>
> *'They've got our children's information and they're trying to use it,' said [the parent]."*[8]

A Growing Threat: Breaches Impacting School Vendors and Other Third Parties

As noted for the first time in last year's *State of K-12 Cybersecurity: Year in Review* report, the K-12 Cyber Incident Map has documented numerous, significant vendor (and partner) related security incidents involving unauthorized access to student and/or educator data.[9] For the second calendar year running, at least 75 percent of all data breach incidents affecting U.S. public K-12 school districts were the result of security incidents involving school district vendors and other partners. Vendors implicated in 2020 incidents include: Active Network (Blue Bear), Aeries, Blackbaud, Interactive Medical Systems, K12 (now, Stride), and Timberline Billing Service.[10] Moreover, security incidents involving school vendors during 2020—such as those experienced by Tyler Technologies and SolarWinds[11]—exposed many school district IT systems and data to significant risks.

Several recent—and alarming—reports of lax vendor security practices in the education sector suggest that at least some school district vendors have not been giving enough priority to architecting and managing their services with security in mind. As one report concluded: "Information security in the education sector has been overlooked, even though it impacts a massive number of people across the country."[12] Another security researcher summed up his investigations into education technology software this way:

> *"When I took a look, there was so much that was vulnerable—just a stupid amount of vulnerability…. I'm not some genius. It's just very obvious that nobody else is looking."*[13]

While many questions remain unanswered regarding the state of K-12 vendor and partner security practices, the GAO concluded that "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."[14] Indeed, 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.[15]

Class Invasions, Denial-of-Service Attacks, and Related Disruptions

As previously noted, the 2020 calendar year gave rise to an entirely new class of school cyber incident: class invasion and its two variants.[16] When combined with denial-of-service attacks launched against school districts and their vendors during periods of remote learning, these incidents represent a significant proportion of all publicly-disclosed incidents experienced by public school districts during 2020.

__'Class invasion'__ is defined as incidents where unauthorized individuals disrupt online classes, often with hate speech; shocking images, sounds, and videos; and/or threats of violence. __'Meeting invasion'__ represents the same tactic but is aimed instead at public school board and other school community meetings, such as PTA meetings, virtual graduations, and open houses/orientation sessions. __'Email invasion'__ involves the compromise of a school district email system for the purpose of bulk sharing of disturbing images, videos, hate speech, and/or threats of violence—or links to the same—to members of the school/district community.

Security failures by school districts and their vendors had several impacts on schools and their communities, including:

- Class disruptions and cancellations, and—in more extreme circumstances—school closures[17]
- School board meeting disruptions and cancellations[18]
- Disruption of email service to and from school community members[19]
- The exposure of young children and youth (as young as kindergarteners) to racist, sexist, and anti-Semitic hate speech; threats of violence; live sex acts; and hard-core pornography[20]

While many of the class and meeting invasion incidents were associated with the Zoom platform, by no means were incidents restricted to that service. Rather, this class of incidents is better thought of as a broader set of security challenges with the rapid adoption of synchronous communications tools to enable remote learning and meetings, especially those involving real-time video sharing. The significance and frequency of these events was so rapid and so alarming that by early April 2020—a few short weeks since schools had begun to shift to remote learning—the U.S. Department of Justice issued a press release (*Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic*) threatening perpetrators of these attacks with state or federal crimes for their actions:

> *"Charges may include—to name just a few—disrupting a public meeting, computer intrusion, using a computer to commit a crime, hate crimes, fraud, or transmitting threatening communications. All of these charges are punishable by fines and imprisonment."*[21]

One month later, the federal Cybersecurity & Infrastructure Security Agency (CISA) issued its own guidance to the nation's schools, recommending over 20 concrete steps that both K-12 organizations and end users could take to minimize the risks associated with the use of video conferencing tools and online platforms for remote learning (*Cybersecurity Recommendations for K-12 Schools using Video Conferencing Tools and Online Platforms*).[22]

Notwithstanding these federal interventions in April and May of 2020—and the widely publicized coverage of these incidents in the media—the K-12 Cyber Incident Map documented four times as many class invasions in the second half of the calendar year as the first half.

Recent research suggests why these attacks may have been so challenging to defend against and offers insights into the types of controls that might effectively mitigate them:

> *"Our findings indicate that the vast majority of calls for [class and meeting invasion] …are not made by attackers stumbling upon meeting invitations or bruteforcing their meeting ID, but rather by* ***insiders who have legitimate access to these meetings, particularly students in high school and college classes****. This has important security implications, because it makes common protections against [class and meeting invasion] …, such as password protection, ineffective. We also find instances of* ***insiders instructing attackers to adopt the names of legitimate participants in the class to avoid detection****, making countermeasures like setting up a waiting room and vetting participants less effective. Based on these observations…****the only effective defense against [class and meeting invasion] … is creating unique join links for each participant*** [emphasis added]."[23]

Ransomware

During 2020, the K-12 Cyber Incident Map documented 50 instances of U.S. public K-12 school districts being impacted by ransomware, a particularly virulent type of malware designed to facilitate the extortion of money from victims. Another 8 districts reported malware outbreaks that resembled ransomware but were not publicly confirmed as such. Incidents were geographically dispersed, with reports of school ransomware emerging from districts across 25 different states.

While the number of incidents alone should be alarming to K-12 leaders and policymakers, what sets 2020 apart from prior years is less the raw number of incidents (after all, there were 24 percent more K-12 ransomware incidents disclosed during 2019) and more the increase in the severity of incidents

experienced. In recognition of the growing threat of ransomware attacks on K-12 schools, in June the FBI issued an alert that:

> *"…cyber actors are likely to increase targeting of K-12 schools during the COVID-19 pandemic [with ransomware] because they represent an opportunistic target as more of these institutions transition to distance learning."*[24]

And, in December of 2020 guidance (*Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*) was jointly released by the FBI, CISA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC), noting:

> *"These issues [cybersecurity incidents, in general, and ransomware incidents, specifically] will be particularly challenging for K-12 schools that face resource limitations; therefore, educational leadership, information technology personnel, and security personnel will need to balance this risk when determining their cybersecurity investments."*[25]

There are at least three ways that the severity of ransomware incidents increased during 2020 as compared to prior years. One—for the first time since the K-12 Cyber Incident has been tracking school cyber incidents, some ransomware actors exfiltrated sensitive data from school districts either before or alongside the activation of their malicious software.[26] Reports suggest that these criminal actors threatened malicious use of the stolen data as an additional lever in extortion negotiations (i.e., if victims did not pay, personal data of students and educators would be openly shared in criminal forums, which would likely result in attempts at identity theft, credit fraud, and account takeover via targeted phishing). Across 7 districts that were victimized by this tactic during 2020, the personal information of at least 560,000 current students and 56,000 current staff were exposed. However, given the fact that districts maintain records of former students and staff as well, the actual number of potentially affected individuals could be 5–10 times higher.

Two—while there are no public reports of school districts having paid extortion fees to ransomware actors during 2020 (unlike prior years), anecdotal reports suggest that extortion demands made to schools may have significantly increased, in some cases far exceeding $1 million per incident.

Three—in an extension of a trend first reported in last year's report and exacerbated by the COVID-19 pandemic, the reports of school closures and class cancellations associated with ransomware incidents (in some cases lasting a week or longer) tripled from the prior year to 15 school districts across 13 states.[27] As Dr. Leslie Torres-Rodriguez, Superintendent of Hartford (CT) Public Schools testified to the U.S. Senate Committee on Homeland Security & Governmental Affairs in December of 2020:

"The cyberattack had extremely disruptive effects on our school system, students, and staff. We were forced to postpone our first day of school on September 8, following months of intense planning for in-person learning amidst the COVID-19 pandemic. While our beautiful and capable students have been attending school either in-person or online for nearly three months now, we are still repairing and recovering from the lingering effects of the attack."[28]

Phishing (Fraud)

Anecdotal reports suggest that school districts are frequently the subject of mass email phishing campaigns targeting individual employees and students, including gift-card scams and account takeover attempts. In one commonly employed tactic targeting teachers, attackers abuse free email services, including Gmail, Outlook, Mail[.]ru, Hotmail, iCloud, and Yahoo to create fake email accounts impersonating K-12 school personnel. According to Microsoft researchers:

"The accounts are created based on publicly available information, which is harvested from various websites or social media platforms. They then use these accounts to send scam emails to their targets…. Typical to BEC [business email compromise] scams and phishing attacks, the threat actors employ various lures and scenarios to fabricate a sense of legitimacy and to suggest urgency."[29]


From:
Sent: Tuesday, January 19, 2021 9:22 AM
To:
Subject: Re: School Counselors

Have you gotten the cards yet ?

On Tue, Jan 19, 2021 at 11:43 AM wrote:

Are you working on the already?

On Tue, Jan 19, 2021 at 11:11 AM wrote:

The amount I want is $100 each in five (5) pieces so that will make it a total of $500 I'll be reimbursing back to you. I need physical cards which you are going to get from the store. When you get them just scratch it take a picture of them and send it to me here individually ok.Let me know if you can help me with that amount right away, plus I will get the cards from you after the meeting but I need the pictures first

On Tue, Jan 19, 2021 at 11:07 AM wrote:

Perfect, how many do you need and in what increments?

From:
Sent: Tuesday, January 19, 2021 8:06 AM
To:
Subject: Re: School Counselors

Yeah, that's fine.

On Tue, Jan 19, 2021 at 11:00 AM wrote:

Yeah sure. I can run to the store right after these MTSS meetings. Will that be ok?

Sent from my iPad

On Jan 19, 2021, at 7:44 AM wrote:

Thanks for the response , it's nothing much Can you help me get an Apple gift cards from the store right now? For some staff for a job well done ,I will surely REIMBURSE you back today once I'm done with the meeting.

On Tue, Jan 19, 2021 at 9:59 AM wrote:

Yeah sure thing. How can I help?

As common as they may be, however, these phishing campaigns are primarily dealt with by district IT staff and rarely rise to the level of public disclosure.

Instead, the types of incidents more likely to be captured on the K-12 Cyber Incident Map are spear-phishing attempts involving the targeting of those with the authority to authorize large financial transactions on behalf of the district. While the absolute numbers of this type of publicly-disclosed phishing attacks against school districts are down from prior years, those that came to light reveal the seriousness with which this type of incident needs to be treated.

Specifically, 4 separate incidents were reported during 2020 that confirmed thefts of school district funds, ranging from a low of $206,000—the result of a school official mistakenly entering school board

banking information into a malicious website—to a high of $9.8 million—involving the compromise of communications of a district's investment advisor and bank.[30]

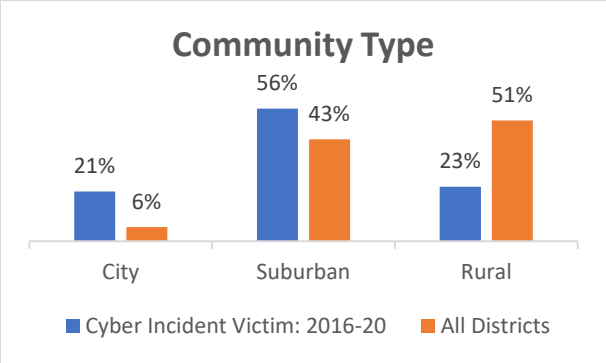
Across the approximately 20 such incidents cataloged by the K-12 Cyber Incident Map since 2016, the median amount of money stolen in spear-phishing attacks against school administrative staff and vendors is $2 million per incident. In many cases, law enforcement is not able to retrieve these funds, and even in the cases where they can it may be weeks or more before funds are restored to the victims.

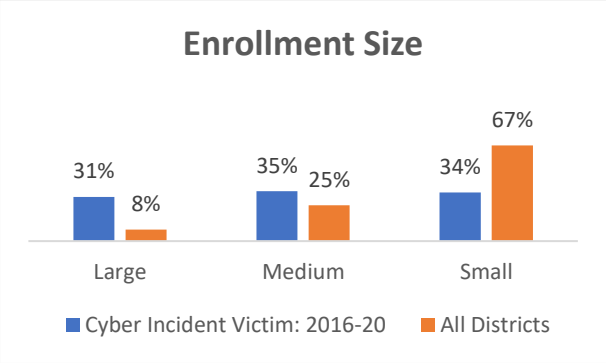
CHARACTERISTICS OF DISTRICTS AT RISK

For the 2020 calendar year, the K-12 Cybersecurity Resource Center catalogued 408 publicly-disclosed incidents involving 377 education organizations across 40 states. Of these, regular public school districts were involved in the majority of cyber incidents. Notably, the number of charter schools that experienced incidents reached an all-time high during 2020 (equating to 11 percent of all incidents experienced during 2020). Other public K-12 educational entities in the 2020 dataset include regional education agencies, state departments of education, state boards of education, and a state charter school board. In line with trends from prior years, 12 percent of all school districts that experienced an incident during 2020 went on to experience at least one other incident during the year.

For the 5-year period from 2016-2020, there were a total of 1,164 publicly-disclosed incidents involving 988 education organizations across all 50 states. Of these, 127 education organizations experienced more than one incident over that time, including one large, urban district that according to public disclosures had experienced 7 different incidents.[31]

Compiling select data on school districts that have experienced a publicly-disclosed cyber incident from 2016-2020 helps to further shed light on the association between district characteristics—like community type, enrollment size, and poverty—and the risk of experiencing a cybersecurity incident.





The enrollment size and community type (or urbanicity) of public school districts is correlated. Cities and suburbs are more likely to play host to school districts with larger student enrollments. By comparing those districts that have experienced one or more publicly-disclosed cyber incidents to all districts nationally, a pattern emerges:

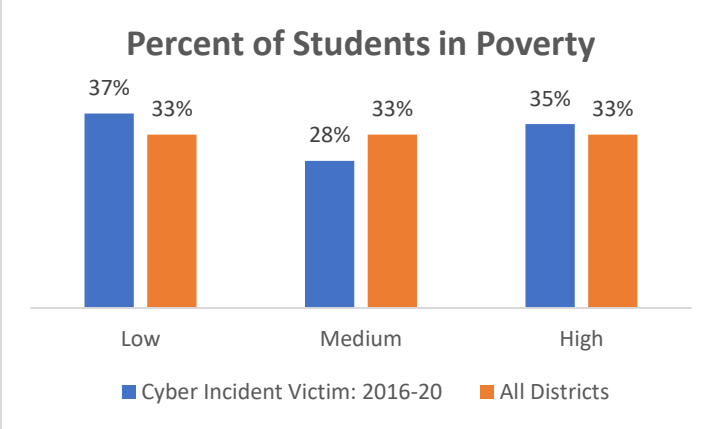
- Larger school districts are at a significantly greater risk for experiencing a cyber incident than other types of school districts, as are school districts located in more densely populated parts of the county.

- Small and rural school districts may be less likely to experience a cybersecurity incident.

There are a few reasons that might explain this pattern. First, larger school districts manage more technology devices and systems than smaller enrollment districts and have more students and employees using that technology. 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, more urban school districts and 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—given that mandatory public disclosures about school cyber incidents are generally not required under federal or state law—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.

Another way to categorize school districts is by the percent of students they serve that are considered by federal measures to be in poverty. By stratifying school districts into three equal categories based on the relative poverty of the students they serve and supplementing that analysis with cyber incident data from 2016-2020, a modest relationship becomes apparent.



School districts in higher income areas are somewhat more likely to experience a cyber incident than those serving greater proportions of low-income students. However, it is middle-income—and not low-income—communities that are least likely to experience an incident. While these are not large differences, they perhaps underscore what may be a more general trend in K-12 Cyber Incident Map data: that a school district's risk of experiencing a cyber incident is directly related to its reliance on technology. That is, wealthier communities may have the resources to acquire technology out of local funds, while lower-income communities are more likely to be specifically targeted by and benefit from federal programs designed to bridge the digital divide.

Nonetheless, it would be a mistake to draw the lesson that there is a certain type of technology-using K-12 organization that does not need to take proactive steps to protect itself from cybersecurity risk. School districts from all 50 states have suffered significant cyber incidents, from small and rural districts to the largest school districts in the nation.

SUMMARY AND RECOMMENDATIONS

This is the third annual 'State of K-12 Cybersecurity: Year in Review' report. It is the first and only vendor-agnostic, independent research effort dedicated to shedding light on the emerging cybersecurity risks facing U.S. public K-12 school districts, 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."[32]

Calendar year 2020 was an unprecedented year that offered a profound stress test of the resiliency and security of the K-12 educational technology ecosystem. Over the course of the year, 377 school districts (and other K-12 education organizations) across 40 states experienced a record-setting 408 publicly-disclosed cybersecurity incidents. Trends in these data reveal:

- Data breaches involving student and staff personal information were the most reported type of incident. In 75 percent of these cases, it was the security practices of school vendors and partners providing administrative services to school districts that were the root cause.

- The impact of COVID-19 on school district operations—forcing a pivot to remote learning—led to the emergence of a new class of cyber threats (class invasion and its variants) and served to magnify the impact of other incidents, including denial-of-service attacks and ransomware. In many cases, this led to the cancellation of classes for up to a week or more in districts that experienced incidents.

- While the absolute number of school districts impacted by ransomware was greater during 2019, the severity of those incidents increased during 2020. Several of the nation's largest school districts were victimized by ransomware actors that—during their attacks—also exfiltrated sensitive data on large numbers of current and past students and employees, leading to credit fraud and identity theft.

- Spear phishing attacks against school business officials and their vendors continue to plague K-12 districts across the country. Since 2016, the median amount of money stolen in such attacks is $2 million per incident. During 2020, a record-setting $9.8 million was stolen from a single school district.

- While every school reliant on technology is at risk of a cybersecurity incident, larger, urban and suburban school districts serving relatively higher-income communities were disproportionately likely to experience at least one cybersecurity incident from 2016-2020 as compared to all districts nationwide. School districts serving larger than average proportions of students in poverty also suffered disproportionately more incidents.

As we look to 2021 and beyond, there are several actions that policymakers, education leaders, and school district vendors can collectively take to better protect students, district employees, and taxpayer funds from the threat of cybersecurity incidents. In last year's report, several actions were

recommended, including: (a) investing in greater IT security capacity dedicated to the unique needs of schools; (b) enacting federal and state school cybersecurity regulations to ensure minimum school district and vendor cybersecurity practices; (c) supporting K-12 specific cybersecurity information sharing and research; and (d) investing in the development of K-12 specific cybersecurity tools. These remain ideas worthy of consideration, and nothing has changed in the broader K-12 context over the course of the last year to suggest that the needs these recommendations would address have been adequately met.

Further, the experience of 2020 suggests several additional lessons:

- School districts should devote resources to better vetting the security policies and practices of all their vendors at the time of procurement and periodically over the life of a contractual relationship. On the flip side, school service providers have an opportunity to differentiate themselves in the education market by focusing on meaningful security features.

- Until school districts have the resources and infrastructure in place to support them in implementing cybersecurity programs, general federal and/or state cybersecurity guidance—in the absence of resources to implement such guidance—is unlikely to be acted upon in a timely manner, if at all.

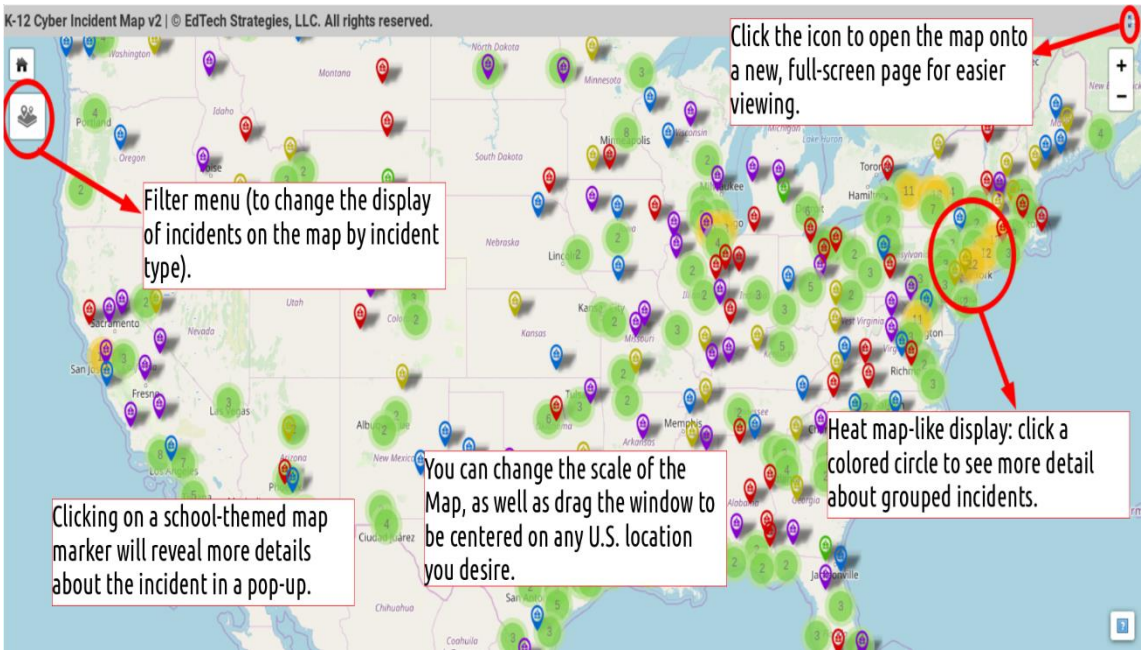
- Awareness and implementation of basic cybersecurity hygiene practices for students, for staff, and for school district vendor staff will be instrumental to making progress in securing the K-12 ecosystem of IT applications and services.

The silver lining in the context of K-12 schools is that awareness of the cybersecurity risks the education sector is facing appears to be growing and there are increasing signs that help may be on the way. For example—at the federal level—late last year U.S. Representatives Matsui and Langevin introduced the *Enhancing K-12 Cybersecurity Act* (HR8612) with the endorsement of several prominent education and technology associations.[33] More recently, a coalition of organizations jointly petitioned the Federal Communications Commission to expand the E-rate program to protect schools "from the rising tide of cyberattacks threatening their networks and confidential data."[34] At the state level, similar proposals have been made in a few states, including several that could include new resources for school districts.[35]

These efforts are laudable and, if thoughtfully-enacted, could make a significant difference in protecting schools from the digital threats they—and by extension, their students, families, and teachers—are facing. There is no time to waste.

APPENDIX: DATA AND METHODS

The K-12 Cyber Incident Map was launched in March 2017 by EdTech Strategies, LLC as an effort to build an empirical base of information about the state of cybersecurity in U.S. public K-12 schools and districts.[36] 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, school leaders, and IT practitioners.



Widely cited research studies, such as Verizon's *Data Breach Investigations Report* series[37] define the education sector overly broadly: 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. 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). 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 entity 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.[38] Similarly, poverty status of school districts is drawn from the U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE).[39]

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 offered to the K-12 Cybersecurity Resource Center. 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.[40] 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] Gene Spafford, "Computer Recreations: Of Worms, Viruses and Core War" by A. K. Dewdney in *Scientific American*, March 1989, p 110.

[3] See, e.g., Levin, Douglas A. (2019). "The State of K-12 Cybersecurity: 2018 Year in Review." Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. https://k12cybersecure.com/wp-content/uploads/2019/02/K12Cybersecurity-2018YIR-1.pdf and 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://k12cybersecure.com/wp-content/uploads/2020/03/K12Cybersecurity2019YearinReview.pdf

[4] 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

[5] Specifically, the GAO found that "thousands of K-12 students had their personal information compromised in data breaches between 2016 and 2020." This finding, however, is based on analyses of a limited dataset of publicly-disclosed incidents and a narrow scope of inquiry. Conservative estimates of student data breach incidents over that same time frame—based on news reports and school vendor incident disclosures—sum to much higher totals. The true figure of U.S. K-12 students who have had personal information exposed by their school districts and/or their vendors over this same time frame is likely to be at least in the tens of millions, i.e., orders of magnitude larger than the GAO estimate. For a discussion of this issue and further context, see, Jill Barshay (November 9, 2020). "PROOF POINTS: What happens when private student information leaks" The Hechinger Report. Available online at: https://hechingerreport.org/proof-points-what-happens-when-private-student-information-leaks/

[6] Dissent Doe (September 14, 2020). "Maze attacking some of the country's largest school districts." Available online at: https://www.databreaches.net/maze-cartel-attacking-some-of-the-countrys-largest-school-districts/

[7] Dissent Doe (October 15, 2020). "Privacy nightmare for Toledo Public Schools: Hackers dumped student and employee data." Available online at: https://www.databreaches.net/privacy-nightmare-for-toledo-public-schools-hackers-dumped-student-and-employee-data/

[8] Shaun Hegarty (February 22, 2021). "Toledo Public School students seeing effects of massive data breach." Toledo, OH: WTVG. Available online at: https://www.13abc.com/2021/02/22/toledo-public-school-students-seeing-effects-of-massive-data-breach/

[9] 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. Available online at: https://k12cybersecure.com/2019-year-in-review/

[10] Active Network (Blue Bear): "School management software provider discloses severe security breach" https://www.zdnet.com/article/school-management-software-provider-discloses-severe-security-breach/; Aeries Notice of Data Breach https://web.archive.org/web/20201210200135/https://www.aeries.com/notice-of-data-breach-4-27-2020/; Blackbaud Data Security Incident: https://www.blackbaud.com/securityincident; Interactive Medical Systems (e.g., "Contractor exposes personal info for 600 Lincoln County Schools employees" https://web.archive.org/web/20200229133510/https://www.lakenormanpublications.com/articles/contractor-exposes-personal-info-for-600-lincoln-county-schools-employees/); K12 (Stride) (e.g., "Online learning company K12 exposes student data in Missouri" https://edscoop.com/online-learning-k12-missouri-data-breach/); and, Timberline Billing Services (e.g., "Data breach impacts Medicaid billing, services company for Iowa students" https://cbs2iowa.com/news/local/data-breach-impacts-medicaid-billing-services-company-for-iowa-students.

[11] See, e.g., "Ransomware attack on Plano tech firm highlights key issue companies need to understand" https://www.bizjournals.com/dallas/news/2020/11/15/ransomware-dfw.html and "The SolarWinds Cyber-Attack: What You Need to Know" https://www.cisecurity.org/solarwinds/

[12] Joseph Cox (August 9, 2019). "Teen Security Researcher Suspended for Exposing Vulnerabilities in His School's Software." Vice. Available online at: https://www.vice.com/en/article/59nzjz/teen-security-researcher-bill-demirkapi-suspended-for-exposing-vulnerabilities

[13] Lily Hay Newman (July 1, 2020). "Schools Already Struggled With Cybersecurity. Then Came Covid-19." Wired. Available online at: https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/

[14] 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/

[15] 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

[16] Note: Class invasion and its variants are classified in the K-12 Cyber Incident Map dataset as 'other incidents.' They make up a large proportion, but not all of the incidents reported in that category.

[17] Two of the most high-profile multi-day school closures due to these types of attacks involved the Miami-Dade County (FL) Public Schools (which serves more than 350,000 students and suffered a multi-day denial-of-service attack) and Fairfax County (VA) Public Schools (which serves over 185,000 students and suffered from widespread class invasions). See, e.g., "2020 Miami-Dade Public Schools cyberattack" https://en.wikipedia.org/wiki/2020_Miami-Dade_Public_Schools_cyberattack and "Tech glitches, harassment mar Fairfax County schools' online learning rollout" https://web.archive.org/web/20200416195916if_/https://www.washingtonpost.com/local/education/fairfax-schools-online-harassment/2020/04/15/841b0406-7f3b-11ea-9040-68981f488eed_story.html

[18] The K-12 Cyber Incident Map documented over 50 meeting invasions during 2020 affecting K-12 schools from coast-to-coast, about half of which involved local school board meetings. *NOTE: Readers may find illustrative examples disturbing*: "Child porn displayed in DC Charter School Board virtual meeting" https://web.archive.org/web/20200428153026if_/https://www.fox5dc.com/news/child-porn-displayed-in-dc-charter-school-board-virtual-meeting, "School Committees reopening meeting interrupted by hackers" https://web.archive.org/web/20200820013749/https://www.thereminder.com/localnews/southamptonwesthampton/school-committees-reopening-meeting-interrupted-by/ , "Hackers interrupt Schenevus meeting with racist obscenities" https://web.archive.org/web/20201011073654/https://www.thedailystar.com/news/local_news/hackers-interrupt-schenevus-meeting-with-racist-obscenities/article_ea7b12f8-c6a8-5f8e-95bd-2de249507671.html, and "USC, school districts getting 'Zoom-bombed' with racist taunts, porn as they transition to online meetings" https://web.archive.org/web/20200407195848/https://www.latimes.com/california/story/2020-03-25/zoombombing-usc-classes-interrupted-racist-remarks

[19] See, e.g., "Chicago suburban school districts experience apparent hacks in which offensive, sexual messages sent" https://abc7chicago.com/school-district-211-hack-207-219-chicago-suburban-districts/7989085/, "Source of Graphic, Racist Email Under Investigation In Enfield" https://patch.com/connecticut/enfield/source-graphic-racist-email-under-investigation-enfield, "Chain of Vulgar Emails Sent out After Niles West Teacher Email is Hacked" https://web.archive.org/web/20201112210828/https://nileswestnews.org/79422/news/breaking-news-chain-of-vulgar-emails-sent-out-after-niles-west-teacher-email-is-hacked/, and "Rome student email accounts temporarily disabled after hacking" https://web.archive.org/web/20200428151904/https://romesentinel.com/stories/rome-student-email-accounts-temporarily-disabled-after-hacking,96920

[20] The K-12 Cyber Incident Map documented over 100 incidents of classroom invasions during 2020. *NOTE: Readers may find illustrative examples disturbing*: "Brookfield Central class Zoom call hacked; masked man flashes gun" https://web.archive.org/web/20200912002952if_/https://www.wisn.com/article/brookfield-central-class-zoom-call-hacked-masked-man-flashes-gun/33993153; "Students believed involved in bestiality video bomb" https://web.archive.org/web/20200922222219/https://www.wcgazette.com/story/2020/09/10/news/students-believed-involved-in-bestiality-video-bomb/33587.html; "Children, parents spammed with porn during kindergarten orientation on Zoom" https://web.archive.org/web/20200828152158/https://www.pahomepage.com/top-stories/children-parents-spammed-with-porn-during-kindergarten-orientation-on-zoom/; "Medford talks security after Zoom bombing incident" https://web.archive.org/web/20201014133131/https://mailtribune.com/news/top-stories/medford-talks-security-after-zoom-bombing; "West Michigan school's Zoom class hacked by person showing gun" https://web.archive.org/web/20200928212713/https://www.mlive.com/news/grand-rapids/2020/09/west-michigan-schools-zoom-class-hacked-by-person-showing-gun.html; "Coronavirus Schools: Naked, Obscenity-Screaming Man Zoombombs Berkeley Virtual Classroom" https://web.archive.org/web/20200409183935/https://www.msn.com/en-us/news/us/coronavirus-schools-naked-obscenity-screaming-man-zoombombs-berkeley-virtual-classroom/ar-BB12nCzQ?ocid=hplocalnews; "People Performing Sex Acts, Saying Racial Slurs Find Way Into Plainfield Middle School Zoom Class" https://chicago.cbslocal.com/2020/11/25/people-performing-sex-acts-saying-racial-slurs-find-way-into-plainfield-middle-school-zoom-class/; "Black teen left in tears after hacker screams racial slurs in Paradise Valley online class" https://web.archive.org/web/20200820010939/https://www.azfamily.com/news/black-teen-left-in-tears-after-hacker-screams-racial-slurs-in-paradise-valley-online-class/article_b4cf2482-e1b6-11ea-a391-2f379a8e9528.html

[21] U.S. Department of Justice (April 3, 2020). "Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic." U.S. Attorney's Office: Eastern District of Michigan. Available online at: https://www.justice.gov/usao-edmi/pr/federal-state-and-local-law-enforcement-warn-against-teleconferencing-hacking-during

[22] Cybersecurity & Infrastructure Security Agency (CISA) (May 13, 2020). "Cybersecurity Recommendations for K-12 Schools using Video Conferencing Tools and Online Platforms." Available online at: https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Recommendations_for_K-12_Schools_Using_Video_Conferencing_S508C_4.pdf

[23] Chen Ling, Utkucan Balcı, Jeremy Blackburn, and Gianluca Stringhini. (September 8, 2020). "A First Look at Zoombombing" arXiv:2009.03822v1. Available online at: https://arxiv.org/pdf/2009.03822.pdf

[24] Catalin Cimpanu (June 25, 2020). "FBI warns K12 schools of ransomware attacks via RDP." ZDNet. Available online at: https://www.zdnet.com/article/fbi-warns-k12-schools-of-ransomware-attacks-via-rdp/

[25] FBI, CISA, and MS-ISAC (December 10, 2020). "Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data." Product ID: AA20-345A. Available online at: https://us-cert.cisa.gov/ncas/alerts/aa20-345a

[26] See, e.g., Tawnell D. Hobbs (September 28.2020). "Hacker Releases Information on Las Vegas-Area Students After Officials Don't Pay Ransom." Wall Street Journal. Available online at: https://www.wsj.com/articles/hacker-releases-information-on-las-vegas-area-students-after-officials-dont-pay-ransom-11601297930; Joe Helm (October 10, 2020). "Hackers post stolen information from Fairfax school district." Washington Post. Available online at: https://www.washingtonpost.com/local/education/hackers-post-stolen-information-from-fairfax-school-district/2020/10/10/edf5f050-0b1a-11eb-859b-f9c27abe638d_story.html; WLOS (September 2, 2020). "Data breach confirmed in ransomware attack on Haywood County Schools." ABC 13 News. Available online at: https://wlos.com/news/local/data-breech-confirmed-in-ransomware-attack-on-haywood-county-schools

[27] See, e.g., Azi Paybarah (November 29, 2020). "Ransomware Attack Closes Baltimore County Public Schools." New York Times. Available online at: https://www.nytimes.com/2020/11/29/us/baltimore-schools-cyberattack.html; Audrey Conklin (September 8. 2020). "Hartford delays first day of school due to ransomware virus" Fox News. Available online at: https://www.foxnews.com/us/hartford-connecticut-public-schools-delays-first-day-ransomware-virus; Bobby Stilwell (November 30, 2020). "Huntsville City Schools cancel classes Tuesday after ransomware threat." News 19. Available online at: https://whnt.com/news/huntsville/huntsville-city-schools-dismissing-early-due-to-potential-cybersecurity-threat/

[28] Testimony of Dr. Leslie Torres-Rodriguez, Superintendent Hartford (CT) Public Schools to U.S. Senate Committee on Homeland Security & Governmental Affairs (December 2, 2020). Available online at: https://www.hsgac.senate.gov/imo/media/doc/Torres-Rodriguez%20Testimony1.pdf

[29] Ionut Arghire (February 3, 2021). "Microsoft Sees Spike in BEC Attacks Targeting Schools." Security Week. Available online at: https://www.securityweek.com/microsoft-sees-spike-bec-attacks-targeting-schools

[30] See Eddie Robertson (October 5, 2020). "FBI investigating after cyberattack targets Wayne County School District." WDAM 7. Available online at: https://www.wdam.com/2020/10/05/cyberattack-targets-wayne-county-school-district/; Luke Smith (October 22, 2020). "Lawsuit: Millions in 16th Section school funds lost to fraudulent transactions." Newscenter ABC 11. Available online at: https://www.wtok.com/2020/10/22/lawsuit-millions-in-16th-section-school-funds-lost-to-fraudulent-transactions/

[31] See https://k12cybersecure.com/map/repeat-incidents/ for an up-to-date list of school districts that have experienced more than one publicly-disclosed cybersecurity incident since 2016.

[32] 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

[33] See "Langevin, Matsui Introduce the Enhancing K-12 Cybersecurity Act" (October 16, 2020). Available online at: https://langevin.house.gov/press-release/langevin-matsui-introduce-enhancing-k-12-cybersecurity-act

[34] Center for Digital Education (February 9, 2021). "Petition Calls for E-Rate Funds for K-12 Cybersecurity Needs." Government Technology. Available online at: https://www.govtech.com/education/k-12/Petition-Calls-for-E-Rate-Funds-for-K12-Cybersecurity-Needs.html

[35] See, e.g., "Press Release Baker-Polito Administration Announces Municipal Cybersecurity Awareness Grant Program Awards" https://www.mass.gov/news/baker-polito-administration-announces-municipal-cybersecurity-awareness-grant-program-awards and Andrew Dunn (March 2, 2021). "New COVID relief bill promises $600 million more for colleges, K-12 schools." Carolina Journal. Available online at: https://www.carolinajournal.com/news-article/new-covid-relief-bill-promises-600-million-more-for-colleges-k-12-schools/

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

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

[38] 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.

[39] 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.

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