THE STATE OF K-12 CYBERSECURITY: 2019 YEAR IN REVIEW

The K-12 Cybersecurity Resource Center

Number of Student Data Breaches, Ransomware Attacks Nearly Triple in Last Year

The State of K-12 Cybersecurity: 2019 Year in Review

PART I: INTRODUCTION

For all the benefits derived from using technology in schools, it also introduces new challenges. Among these challenges are those related to funding, teacher preparation and training, identifying best practices, and student health and well-being. While these concerns are generally well-understood (if often insufficiently addressed), there is an emerging challenge that appears to have caught many school districts off-guard: threats to the confidentiality, availability, and integrity of their data systems and technology from actors both known and unknown to the district. As Michael Melia of the Associated Press reports, “Schools with few or no employees dedicated to information security often are surprised to find themselves as targets.”[1] This challenge is the challenge of K-12 cybersecurity.

During 2019, a nationwide cybersecurity survey of schools was conducted in the United Kingdom. Its findings – while not descriptive of the U.S. school experience – are nonetheless suggestive. Over 80 percent of UK schools reported having experienced at least one cybersecurity incident (with 10 percent of those reporting that their school had been “significantly disrupted” by an incident). At the same time, fewer than half of UK schools (49 percent) felt adequately prepared for a cyber attack or incident.[2]

No such data exists about U.S. schools or districts. This report series – *The State of K-12 Cybersecurity: Year in Review* – aims to help remedy this gap by cataloging and analyzing data from every publicly-disclosed cybersecurity incident affecting public elementary and secondary education agencies across the U.S. It is the only research initiative of its kind and has grown to become the definitive source of statistics on K-12 cybersecurity incidents. The series is intended to spur greater attention to the challenges of securing school- (and school vendor/partner-) IT systems and suggest ways that policymakers and school district leaders might effectively respond.

Why is this report and research needed?

- **Public reporting requirements for school cybersecurity incidents vary by state, but are generally quite weak.** This lack of mandatory disclosure masks the severity and significance of the threats facing schools, leaves policymakers and school leaders without valuable information to guide their decisionmaking, and leaves students, parents, and educators in the dark regarding the threats to which they may be exposed (whether in the past, present, or future). While there is a reasonable debate to be had about how transparent public agencies should be about their response to cybersecurity threats, the current state of information disclosure and sharing is anemic by any measure.[3]

- **Schools are increasing their reliance on technology for teaching, learning, and school operations.** Indeed, the K-12 education technology market has grown to become very big business.[4] This puts districts at greater risk for cybersecurity incidents, with many experts of the mind that it is not a matter of *if* any given school district will experience an incident, but *when*. Moreover, given that school district IT systems are interconnected with other local and state government agency systems (including public safety and election systems), this issue is salient to those whose purview typically excludes education policy.

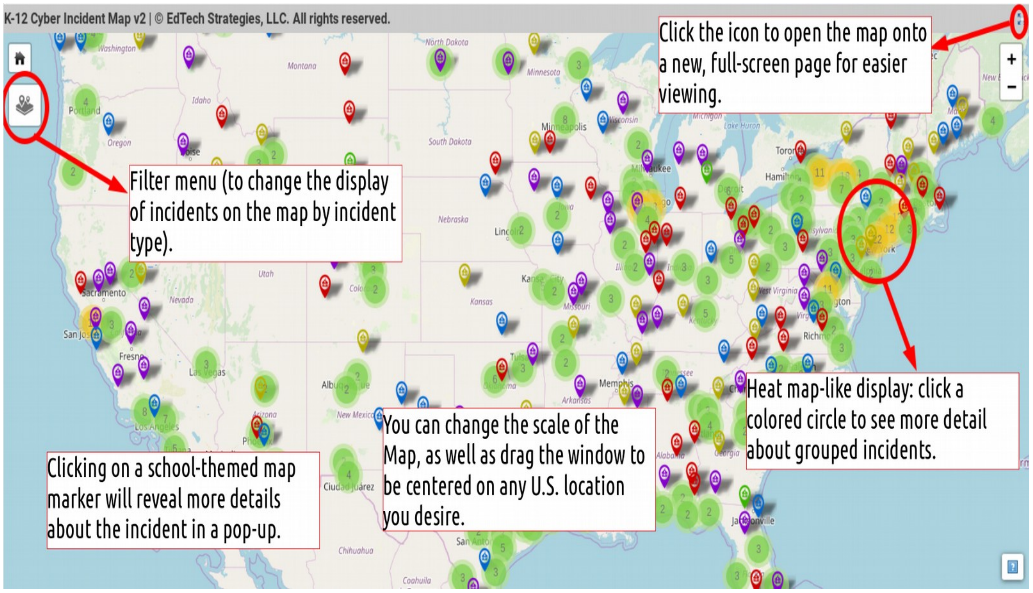
- **As this report series documents, the frequency and severity of school cybersecurity incidents is increasing.** Data held by school districts about students, families, and employees is sensitive, and while school districts don't think of themselves as wealthy targets (given most are cash-strapped in providing services to the students in their care) the fact of the matter is that they manage the expenditure of large amounts of money every year to maintain facilities, provide transportation, food service, public health services, and education to large numbers of students. Without a coordinated, sector-wide response to the issue, it is hard to imagine any situation in which incident frequency and severity declines.

"All I can say is if they had a data breach and are not notifying us, then trust and believe they are about to have much bigger issues on their hands besides a stinking phone system," said one parent.[5]

Taken together with recent warnings from the Federal Bureau of Investigation about growing 'cyber threats' targeting schools,[6] this report serves as a much-needed wake up call for policymakers and school leaders about the heretofore unaccounted for risks of the adoption of technology in the K-12 sector. The following section of the report (Part II) provides background information on the data and analyses that inform this work, while Parts III and IV present findings from analyses of cyber incidents and affected school districts, respectively. It concludes in Part V by suggesting lessons to be drawn from – and possible approaches to responding to – the growing challenge of K-12 cybersecurity risk management.

PART II: K-12 CYBER INCIDENT DATA

The K-12 Cyber Incident Map was launched in 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.[7] 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, IT and cybersecurity practitioners, and civil liberties advocates.


K-12 Cyber Incident Map v2 | © EdTech Strategies, LLC. All rights reserved.

Click the icon to open the map onto a new, full-screen page for easier viewing.

Filter menu (to change the display of incidents on the map by incident type).

Heat map-like display: click a colored circle to see more detail about grouped incidents.

You can change the scale of the Map, as well as drag the window to be centered on any U.S. location you desire.

Clicking on a school-themed map marker will reveal more details about the incident in a pop-up.

The K-12 Cyber incident Map is a visual depiction of every publicly-disclosed cyber incident involving a K-12 public school agency in the United States since 2016.

Widely cited research studies, such as Verizon's annual "Data Breach Investigations Report" and Ponemon Institute's "Cost of a Data Breach Study," 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.[8] Other public sources of data breach incidents compiled by experts define their scope in ways that exclude the reporting of significant cybersecurity incidents (while including incidents that are wholly analog, such as the loss of control of paper-based records).[9] While there may be lessons to be drawn from each of 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, and

- 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, availability, and integrity of a school district's IT system. Whether an incident affects one school 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 due to the fact that school districts are the primary entity charged with responsibility for managing taxpayer dollars, employee confidentiality, and student data privacy. 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 address questions both about the nature and trends of cybersecurity incidents affecting K-12 schools and districts over time, as well as the characteristics of school districts that may be more or less likely to experience an incident. Cyber incident data is categorized in a manner consistent with the Vocabulary for Event Recording and Incident Sharing (VERIS), which is a common language for describing security incidents in a structured and repeatable manner.[10] 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.[11] Similarly, poverty status of school districts is drawn from the U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE).[12]

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, social media and online forums, self-reports, and tips offered to the K-12 Cybersecurity Resource Center.[13] 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 IT management practices. 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 courtesy of an integration with OpenStreetMap.[14] Incidents on the map are color-coded by ‘primary’ incident type:

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

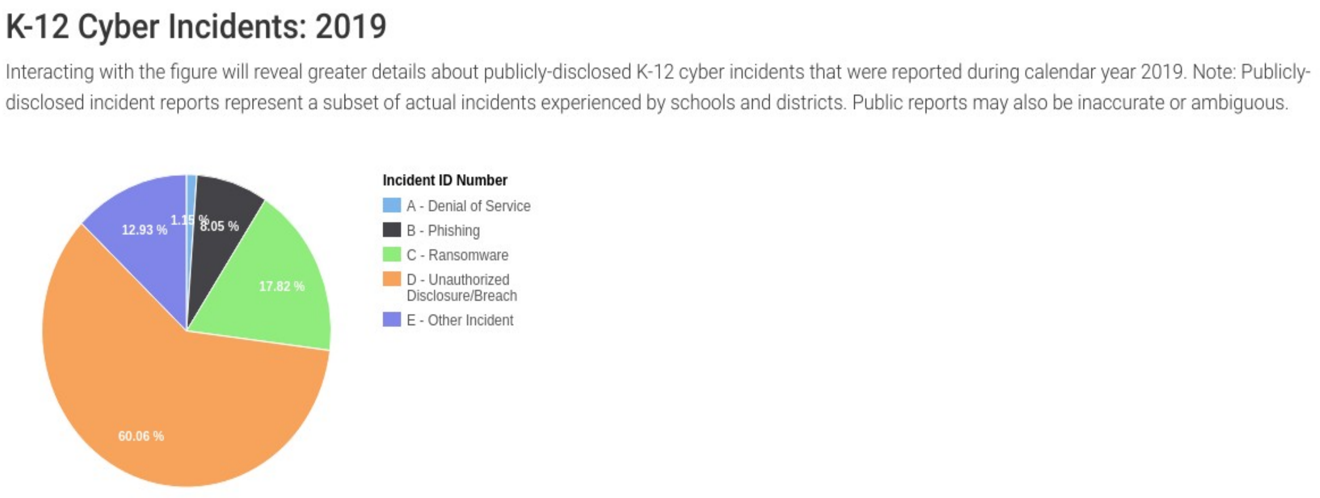
Given that incident types can co-occur (e.g., malware delivery via phishing email, resulting in a data breach), reporting by primary incident type should be interpreted with some caution.

PART III: CYBERSECURITY INCIDENTS: 2019

During calendar year 2019, the K-12 Cyber Incident Map cataloged 348 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 nearly 3 times as many incidents as were publicly-disclosed during 2018** (and the most since the K-12 Cyber Incident Map first started tracking these incidents in 2016). This equates to a rate of nearly two incidents per school day over the course of 2019.

The year-over-year growth in the incident count is likely due to a variety of factors, including a greater reliance on technology by schools, the disproportionate targeting of local government agencies – including school districts – by cyber criminals during 2019, a number of significant school vendor incidents (that involve large numbers of school districts), and a greater public awareness of and reporting about cybersecurity incidents (whether affecting schools or other organizations). The growth in publicly-disclosed incidents notwithstanding, the school data cataloged on the K-12 Cyber Incident Map represents a significant undercount of all such incidents.

Given how different the technological constraints and needs of K-12 schools are as compared to other types of organizations – to say nothing of the uniquely sensitive data they collect and process – what do we know about the actual risks and threats they may be facing? With limited expertise and resources, how should cybersecurity professionals advise schools to respond? Data assembled for the K-12 Cyber Incident Map are instructive.



K-12 Cyber Incidents: 2019

Interacting with the figure will reveal greater details about publicly-disclosed K-12 cyber incidents that were reported during calendar year 2019. Note: Publicly-disclosed incident reports represent a subset of actual incidents experienced by schools and districts. Public reports may also be inaccurate or ambiguous.

Data Breaches and Other Unauthorized Disclosures

The most frequently experienced type of school-related cyber incident reported during 2019 – representing 60 percent of all incidents cataloged on the K-12 Cyber Incident Map – were data breaches, primarily involving the unauthorized disclosure of student data. This mirrors findings from 2018, which also found data breaches to be the most frequently experienced type of school cyber incident. It should be a cause for concern. First, federal and state student data privacy legislation is intended to reduce the frequency and severity of student data breaches,[15] although evidence in this report series suggests those policy regimes may not be working as intended. Second, security researchers have documented dark web marketplaces advertising the stolen personal information of children for use by identity thieves.[16] Indeed, student data breaches can have serious and long-lasting consequences.

Of note, most (though not all) school data breaches during 2019 also included data about school staff, resulting in identity theft and fraud. As such, it should be in administrators' and educators' best interest to embrace common sense steps to protect unauthorized access to school IT systems. While school staff may be obligated to take such steps in order to be compliant with federal and state student data privacy legislation (and out of a moral obligation to protect the students in their care), the implementation of cybersecurity controls in school districts nationwide remains quite varied (at least as evidenced by publicly-available school district IT audit reports).[17]

Just over half (51 percent) of student and educator data breach incidents during 2019 were due to the actions (or inaction) of school vendors or (in some few cases) partners, including regional service agencies, non-profits, associations, and state departments of education. Another 9 percent of incidents were due to the actions of either school staff or middle or high school students themselves.

This means that **most publicly-disclosed data breaches were caused by parties that are known to and already a part of the school community**. While school districts must be on guard against criminal actors preying on school communities from afar, they would do well to focus also on shoring up internal policies and practices involving the collection, storage, and sharing of student and employee data under their direct control.

On July 31, 2019, Parmy Olson of The Wall Street Journal broke the story of a massive data breach involving Pearson and their AimsWeb 1.0 student assessment and progress monitoring platform.[18] According to news reports, it was the Federal Bureau of Investigation that discovered the incident and approached the company to alert them. While Pearson never publicly disclosed the total number of student and educator records compromised in the breach – noting that 13,000 enterprise accounts were involved in the breach – estimates suggest it could represent the single largest data breach affecting the K-12 sector ever and rank among the largest data breaches of the year by any entity (likely involving tens, if not hundreds of millions of individuals).[19] The company is currently facing a class-action lawsuit under Illinois state law for its actions in this data breach.[20]

Since the K-12 Cyber Incident Map launched, it has documented numerous vendor- (and other third-party-) related security incidents involving unauthorized access to student and/or educator data. These include incidents involving: ACT, Blackboard, Chegg, Choicelunch, Edmodo, Elsevier, Follett, GameSalad, Graduation Alliance, K-12.com, Khan Academy, Florida Virtual School, Leadership for Educational Equity, Maia Learning, Naviance, Pearson, Pennsylvania Department of Education, Questar, Schoolzilla, the Texas Association of School Boards, and Total Registration.[21] While the number of public disclosures rose to new highs in 2019, **many questions remain unanswered regarding the state of K-12 vendor- and partner- security practices.**

Ransomware and Malware

The second most frequent type of cyber incident experienced by school districts during 2019 was ransomware and ransomware-like (malware) outbreaks, together accounting for 28 percent of all incidents reported on the K-12 Cyber Incident Map.[22] This represents a dramatic year-over-year growth in the relative frequency of ransomware/malware attacks on school networks versus 2018 (i.e., roughly double the incidence in 2019 vs. 2018) and matches the rise in the reports of significant ransomware/malware outbreaks in other municipal and state agencies.[23]

While the vast majority of school district ransomware victims are quick to claim that student or employee data are not at risk of identity theft (due to the nature of the attack) and hence should not be subject to data breach reporting regulations, that claim should be met with increasing skepticism.[24]

> *“Ransomware attacks are now data breaches,” Abrams said. “During ransomware attacks, some threat actors have told companies that they are familiar with internal company secrets after reading the company’s files. Even though this should be considered a data breach, many ransomware victims simply swept it under the rug in the hopes that nobody would ever find out. Now that ransomware operators are releasing victim’s data, this will need to change and companies will have to treat these attacks like data breaches.”*[25]

Without question, ransomware and malware incidents are among the most expensive and disruptive cyber incidents schools face. **During 2019 – for the first time since the K-12 Cyber Incident Map began tracking school incidents – numerous school districts canceled classes and/or closed schools due to ransomware/malware incidents**, including in Alabama, Arizona, New Jersey, New York, and Ohio.[26] Others reported widespread outages in critical systems, including internet access, curriculum and assessment resources, gradebooks, payroll and HR systems, point-of-sale machines used in school cafeterias, email, phone service, school and district websites, security systems, and other school-related online services and resources.

Toward the end of July 2019 (just two weeks prior to school opening), the Governor of Louisiana declared a state emergency to assist with the recovery of numerous school districts in the state compromised by ransomware.[27] While three districts had initially disclosed serious incidents, the state responded aggressively in reaching out to – and helping to shore up the defenses of – every school district in the state. Two other Louisiana districts were compromised by ransomware during that time frame, while seven other districts – which were found to be compromised – were remediated with help from external IT experts before damage could be caused.[28] Thanks to the aggressive actions of leadership in the state, school districts across Louisiana opened on time this year.

> *“We have all the protections in the world,” [Newport School District Superintendent] Neuhard said.*
>
> *The school has firewalls, anti-virus and anti-malware software to stop known threats, and offsite servers with their own protections for back-up and redundancy. But, even with those defenses, a virus or malware program can still get through if someone clicks on something in an email. While anti-virus software may catch most malicious programs, others could go undetected.*[29]

When a victim of ransomware, school district leaders are faced with juggling multiple competing priorities in ensuring continuity of services and both short- and long-term IT recovery and remediation costs. In an attempt to ensure the short-term continuity of services, during 2019 some school districts publicly disclosed that they made extortion payments to cyber criminals to regain control of their compromised data and IT systems, including in Iowa, Nevada, New York, and Pennsylvania.[30] Anecdotal reports suggest that other school districts also paid ransomware extortion demands, including in some cases in amounts totaling hundreds of thousands of dollars or more.

Other districts refused to make extortion payments and instead chose to rebuild (and in some cases, rearchitect and refresh) their IT systems for the long-term as part of their recovery. Nonetheless, even when school district leaders acquiesce to ransomware demands, they are not spared the time and expense required to decrypt their data, evict the cyber criminals from their IT systems, and harden their systems to limit the impact of any future attacks. Indeed, the cost to mitigate against the threat of ransomware/malware attacks are borne by school districts one way or the other – and those districts that pay a ransom may unfortunately also be serving to encourage cyber criminals to continue to target other school districts across the nation.

Phishing (Fraud)

Many school districts struggle with limiting the impact of email-based phishing attacks, primarily directed to school staff. **During 2019, while only 8 percent of school cyber incidents were primarily classified as phishing, anecdotally such attacks – leveraging previously leaked credentials and contact information published on school district websites – are a frequent vector for data breach incidents, malware outbreaks, and fraud.**

While school district staff are sometimes victimized by low-level mass email phishing campaigns (e.g., gift card scams), more concerning are phishing attacks targeted specifically to school districts (or other regional or state education agencies) by criminals. Such targeted attacks often involve attempts to redirect employee payroll or contractor payments to criminal accounts or to steal employee identity and tax information. During 2019, state agencies in both New Mexico and Ohio issued warnings to school districts in their states about an uptick in such attacks.[31]

Perhaps the most concerning phishing attacks perpetrated against school districts are those targeted at business officials. These scams—sometimes referred to as business email compromise—resulted in the theft of millions of taxpayer dollars. The largest ever such theft recorded on the K-12 Cyber Incident Map occurred in 2019 and totaled approximately $3.7 million dollars in losses by a Kentucky district.[32] Other large dollar incidents of K-12 cybercrime in 2019 ranged from $600,000 to a high of $2.9 million (affecting school districts in North Carolina, Oregon, Texas, and Virginia).[33] Happily, school districts working in partnership with law enforcement, banks, and insurance companies are sometimes able to recover some or all of the stolen funds.

"Teachers are trusting people. They care about kids, they want to do the best for them, and they trust people," Strate said.[34]

On a positive note, likely due to the success of law enforcement in prosecuting individuals who targeted school district business officials in prior years, successful attempts at W-2 tax fraud via phishing attacks against school business officials diminished further in 2019.[35] The K-12 Cyber Incident Map only reported one such incidents during the year (experienced by a district in California).[36]

Other Incidents

Not all cyber incidents perpetrated against K-12 schools are concerned with school-managed personal data or financial accounts. **Two other common cybersecurity-related issues affecting K-12 institutions include denial-of-service attacks and website/social media defacement. However, neither type of incident was frequently publicly-disclosed during 2019.** In the case of denial-of-service attacks, it may be that public reports of education specific denial-of-service attacks are only made when disruptions are atypically significant, for instance, due to their persistence or due to the affected applications/services (such as state testing or school communications services). Short-term disruptions due to DDoS attacks may instead be chalked up by users to insufficient school technology infrastructure and/or networks. Nonetheless, it is important to note that the cost to purchase (illegal) distributed denial-of-service (DDoS)-for-hire services online is well within the reach of students and others who may wish to disrupt school networks.[37]

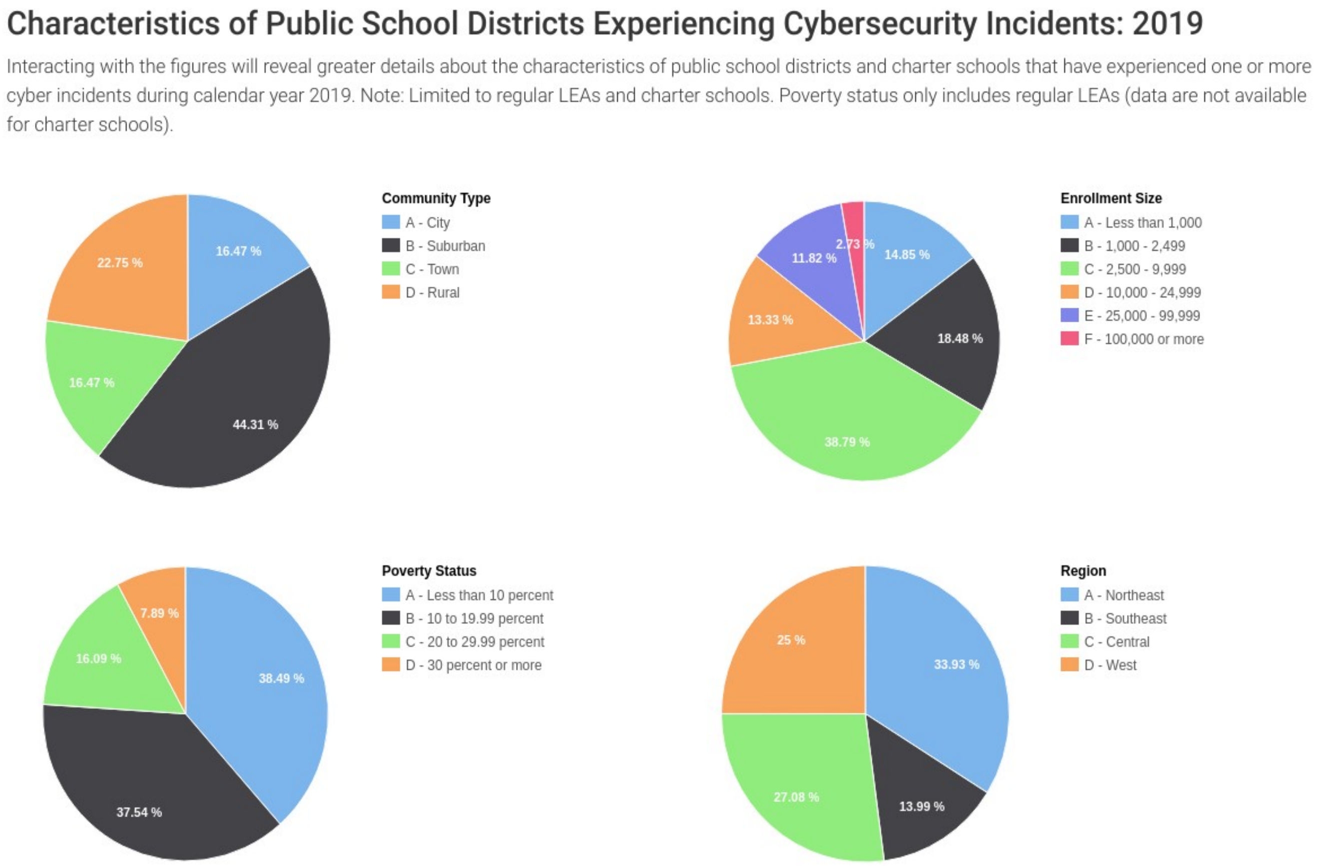
School-managed social media and website defacement is a class of cyber incidents particularly troubling for public institutions charged with serving children. These attacks abuse official communication channels to deliver unauthorized messages or to automatically redirect users from trusted school-managed sites to third-party sites. Most often (but not always) due to a loss of control of passwords of school-managed accounts, individuals internal and external to school communities have compromised the online communication platforms of schools to advance geopolitical propaganda, deliver hateful messages, taunt school leaders and educators, threaten violence, and otherwise disrupt school operations.

PART IV: SCHOOL DISTRICTS EXPERIENCING CYBERSECURITY INCIDENTS: 2019

In 2019, the K-12 Cybersecurity Resource Center cataloged 348 publicly-disclosed incidents involving 336 educational agencies across 44 states. Of these, regular public school districts were involved in the vast majority of cyber incidents (329 of the 348 incidents). However – during 2019 – 14 charter schools, 4 regional/special education agencies (in Illinois, Minnesota, New York, and Pennsylvania), and the New Mexico Public Education Department also experienced publicly-reported incidents.

In a small proportion of cases, school districts have been found to have experienced multiple cybersecurity incidents. For instance, over 11 percent of all school districts that had incidents publicly disclosed in 2019 were found to have experienced at least one other incident since 2016.[38] Of those, twelve school districts experienced two incidents during calendar year 2019 alone. Since 2016, nine school districts have experienced between three and six incidents each. In many cases, school districts that have experienced more than one publicly-disclosed incident seem to have been unlucky (i.e., the incidents seem likely to be unrelated); in a handful of cases, however, multiple incidents occurring in the same school district seem to be indicative of a systemic failure of cybersecurity controls.

Compiling select data of school districts that experienced a publicly-disclosed cyber incident during 2019 helps to shed further light on the association between district characteristics and school cybersecurity threats and vulnerabilities.



Characteristics of Public School Districts Experiencing Cybersecurity Incidents: 2019

Interacting with the figures will reveal greater details about the characteristics of public school districts and charter schools that have experienced one or more cyber incidents during calendar year 2019. Note: Limited to regular LEAs and charter schools. Poverty status only includes regular LEAs (data are not available for charter schools).

Two findings are important to takeaway from this analysis of school district characteristics. First, there are numerous examples of districts of all types, poverty levels, and sizes that have experienced cyber incidents. From Alaska to Florida, Maine to Hawaii and everywhere in between, the K-12 Cybersecurity Resource Center has documented school districts of every size and type that have experienced data breaches, phishing attacks, and ransomware/malware outbreaks. **As such, school district leaders would do well to understand that no school district is safe from a potential incident.**

It's easy to assume that a quiet school in rural Montana won't be the target of a cyber attack. It's also wrong.[39]

Having said that, the odds of experiencing an incident do seem to vary by school district characteristics. Compared to all public school districts nationally, those that experience publicly-disclosed cybersecurity incidents of any type are more likely to be located in more densely populated locales (suburbs and cities) and to have larger student enrollments. School districts located in the suburbs and with enrollments equal to or greater than 2,500 students were more likely to have experienced at least one incident. Those located in cities and with student enrollments of at least 10,000 students were even more likely to have experienced at least one publicly disclosed cyber incident.

In contrast, school districts that are rural, enroll fewer than 2,499 students, and are located in the central region of the United States are significantly less likely to have experienced a publicly-disclosed school cyber incident.[40] School districts enrolling fewer than 1,000 students were among the least likely to have experienced a publicly-disclosed cyber incident.

Of note, the poverty level of the school community does not seem to be associated with the odds that a school district experienced a publicly-disclosed incident.[41]

While some reports have suggested that less wealthy and more rural school districts might be more susceptible to cybersecurity threats, evidence collected by the K-12 Cybersecurity Resource Center does not support that conclusion.[42] In fact, the available evidence suggests the opposite: **larger, more urban school districts are disproportionately likely to have experienced at least one publicly-disclosed cyber incident in recent years than their smaller, more rural peers.**

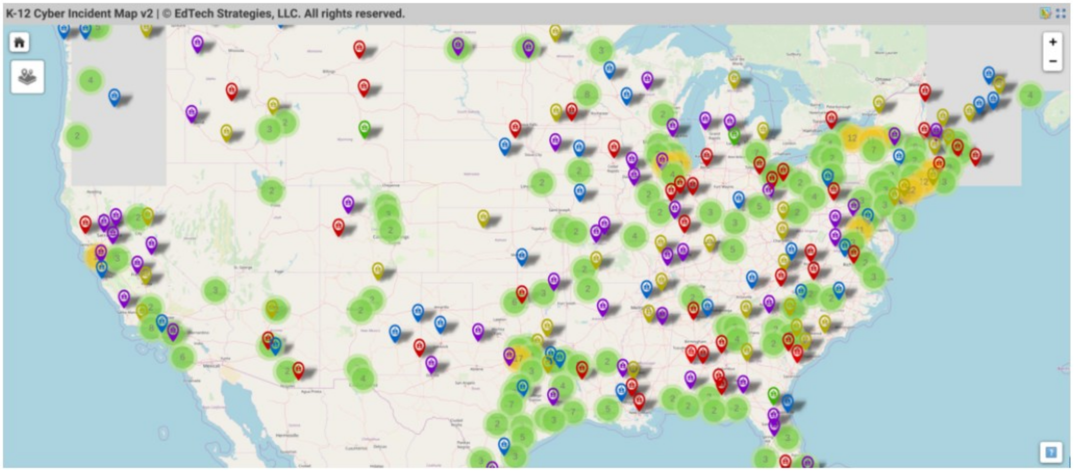
Two hypotheses may explain why larger school districts are more likely to have fallen victim to a publicly-disclosed cyber incident. With more computers and more computer users than other districts, larger school districts may be more susceptible to experiencing a cyber incident due to the simple fact that they have and use more technology than other districts on average. More users increases the odds of a malicious email being received and acted upon – and more computers present a larger attack surface to malicious actors scanning the internet for open ports and unpatched software.

The second hypothesis has to do with the fact that when smaller, more rural school districts do experience a cyber incident it may be less likely that it is publicly-disclosed. Given that mandatory public reporting requirements for school cyber incidents are weak, when a smaller school community experiences an issue it may be less likely to result in the sort of media coverage that more urban districts experience.

PART V: LESSONS FOR 2020 AND BEYOND

Evidence assembled to maintain the K-12 Cyber Incident Map reveals that school districts are not immune to the same types of cybersecurity incidents routinely plaguing even the most technologically advanced and well-resourced corporations and government agencies. During 2019, the misuse and abuse of school technology and IT systems resulted in 348 publicly-disclosed incidents involving 336 educational agencies across 44 states. This is nearly three times more than last calendar year.[43] While no one can predict the future, this does not portend well.

The impact of publicly-reported K-12 cyber incidents is significant. During 2019, such incidents resulted in school closures, the theft of millions of taxpayer dollars, stolen identities, tax fraud, altered school records, and the loss of access to school technology and IT systems for weeks or longer. Due to such incidents, parent, educator, student, taxpayer, and policymaker trust in education technology is being placed increasingly at risk.


K-12 Cyber Incident Map v2 | © EdTech Strategies, LLC. All rights reserved.

The K-12 Cyber Incident Map has cataloged over 775 cyber incidents affecting U.S. public schools since 2016.

While no school is immune from threats to the confidentiality, availability, and integrity of their data and IT systems, districts serving larger numbers of students in suburban and urban settings experienced disproportionately more incidents during 2019 than those serving fewer students in rural communities. Likely this is due to the fact that larger districts have more technology – and more technology users – than smaller districts and hence face greater risks from both internal and external threat actors. Indeed, all it takes is for one person in a school community to click a malicious link in a phishing email to lead to a data breach or ransomware outbreak.

As we look to 2020 and beyond, there are a number of actions that policymakers, school leaders, and technology leaders can collectively take to improve the cyber risk profile of school districts. These include:

- **Investing in greater IT security capacity dedicated to the unique needs of school districts.** As beneficial as it could be, it remains unlikely that most school districts will be able to hire a qualified chief information security officer and sufficient numbers of dedicated digital security staff without significant changes to school district budget priorities – and additional funding – in the near future. Nonetheless, existing school IT staff would benefit from ongoing training and professional development focused on digital security, including by being supported in earning the CISSP (Certified Information Systems Security Professional) and/or related certifications. At the same time, all school districts could benefit from centralized forms of vendor-neutral support and managed tooling provided at the regional, state, or national levels, including by non-profit organizations, government agencies, and managed security service providers. For their part, vendors that provide enterprise technology to large numbers of school districts – especially those providing hardware or connectivity services – could assist by integrating value-added security services into their product lines.

- **Enacting federal and state school cybersecurity regulations to ensure baseline school district and vendor cybersecurity practices.** For all intents and purposes, neither school districts nor their vendors are held accountable under federal or most state laws for implementing even basic cyber hygiene or for the disclosure of cyber incidents. Moreover, there is not a common standard of practice or risk management framework to which most school districts adhere. Most privacy legislation – including recently-enacted student data privacy legislation – is too narrowly written, while cybersecurity-specific legislation generally overlooks the K-12 education sector because it is not considered 'critical infrastructure.' States – such as New York and Texas – have recently moved to enact more stringent school-specific regulations, but they remain the exception to the rule.[44] Given the rise in significant cyber incidents affecting school districts – and due to the fact that district IT systems are interconnected with other state and local IT systems, including public safety and elections systems – it is vital that clear expectations be established for school district and vendor cybersecurity practices, along with the provision of resources to enable school districts to come into compliance.

- **Supporting K-12-specific cybersecurity information sharing and research.** While every school districts has unique needs and constraints, there is more that is similar in their technology implementations and challenges than different. As such, trusted information sharing among school district IT leaders can help schools to prioritize the implementation of cybersecurity controls, respond to emerging threats, and develop and promulgate K-12 specific best practices and model policies. At the same time, more and better research is needed on the cybersecurity challenges facing school districts and cost-effective risk management responses. While this report series is helping to fill a gap in the knowledge base regarding the state of K-12 cybersecurity, it is insufficient to addressing all of the pressing questions facing the sector.

- **Investing in the development of K-12 specific cybersecurity tools.** While there is no shortage of tools to help IT staff to manage enterprise cybersecurity challenges on the market, they are not always a good fit for the K-12 context. School districts may not be able to afford otherwise valuable tools or they may require dedicated staffing to maximize a tool's benefit. Indeed, cybersecurity solutions may be wasted on schools that do not have the trained staff to effectively deploy, monitor, and respond to the information they generate. This represents an opportunity for cybersecurity vendors to develop product lines to meet the growing and unmet needs in the K-12 education market, as well as for IT professionals to customize open source solutions for school district needs.

These ideas notwithstanding, **keeping K-12 schools 'cyber secure' is a wicked problem – one that will surely grow more severe until the practice of ongoing cybersecurity risk management becomes institutionalized in school district culture.** It won't be solved solely by an infusion of money, new technologies, new policies and regulations, or a cybersecurity awareness campaign; all are likely necessary, but how they are implemented and evolve over time to meet the specific and idiosyncratic needs and constraints facing public K-12 schools will matter most of all.

Enhancing the capacity of the K-12 community to share timely information, build a knowledge base, and identify and promulgate promising policies and practices is why the K-12 Cybersecurity Resource Center was launched. This report series is only a small, but necessary step in a much longer journey toward building the will and capacity to act.

ABOUT THE K-12 CYBERSECURITY RESOURCE CENTER

The K-12 Cybersecurity Resource Center was launched in 2018 to build a knowledge base about the emerging cybersecurity risks facing U.S. K-12 public schools and to help identify and implement promising policies and practices to better manage those risks. It is maintained as a free, independent service to the K-12 community by EdTech Strategies, LLC, a boutique consultancy focused on providing strategic research and counsel on issues at the intersection of education, public policy, technology, and innovation. For more information, please visit: https://k12cybersecure.com.

Suggested citation:

> 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/year-in-review/

Cover image credit: Jason Kravitz CC BY 4.0

The publication of this report was made possible with the generous support of Technology Resource Advisors, ManagedMethods, PC Matic PRO, and Gradient Cyber. K-12 cyber incident data, data analyses, and all other report contents are the sole responsibility of EdTech Strategies, LLC and do not necessarily represent the views of sponsors, partners, or donors.

CHAMPION SPONSOR

TECHNOLOGY RESOURCE ADVISORS INC.
CYBERCARE

DEFENDER SPONSORS:

Managed Methods

PC Matic PRO

Gradient.

[1] Melia, Michael. “Cyberattacks inflict deep harm at technology-rich schools.” Associated Press. 16 July 2019. Available online at: https://apnews.com/4db421064ca84bcfad9fa195b7b41384

[2] See National Cyber Security Centre (a part of GCHQ) and London Grid for Learning (LGfL) (2019). “Cyber Security: Schools Audit 2019.” Available for download at: https://www.lgfl.net/cybercloud/securityaudit

[3] Quaintance, Zack. “How Transparent Should Government Be After a Cyberattack?” Government Technology. 6 November 2019. Available online at: https://www.govtech.com/security/How-Transparent-Should-Government-Be-After-a-Cyberattack.html

[4] As discussed in: 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. Available online at: https://k12cybersecure.com/year-in-review/

[5] Riley, Sable. “Chalk Talk: Secrecy giving parents, teachers little confidence in data security.” Dothan Eagle. 2 August 2019. Available online at: https://www.dothaneagle.com/news/education/chalk-talk-secrecy-giving-parents-teachers-little-confidence-in-data/article_5e06add2-b575-11e9-b7ea-8fc4fab5819a.html

[6] Federal Bureau of Investigation (2018). “Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students.” Alert No. I-091318-PSA. Available online at: https://www.ic3.gov/media/2018/180913.aspx

[7] See “Introducing the K-12 Cyber Incident Map.”

[8] See “Verizon Data Breach Investigations Report” and “Ponemon Institute Cost of a Data Breach Study.” Widely-cited figures on the education sector drawn from these reports are unlikely to be representative of the threats and risks facing U.S. K-12 public schools.

[9] The Privacy Rights Clearinghouse maintains a database of public breaches that includes some information about school incidents. Databreaches.net offers a comprehensive history of education-related incidents. The Identity Theft Resource Center tracks U.S. data breaches, including those affecting schools.

[10] See “VERIS, the Vocabulary for Event Recording and Incident Sharing.”

[11] 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.

[12] 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.

[13] Incident reports may be submitted to the K-12 Cybersecurity Resource Center directly via this contact form. Note: Only publicly-disclosed incidents are eligible for inclusion on the K-12 Cyber Incident Map.

[14] 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.”

[15] For recent reviews of federal and state student data privacy legislation, see the the Future of Privacy Forum’s “State Student Data Privacy Laws,” the Parent Coalition for Student Privacy/The Network for Publication Education’s “The State Student Privacy Report Card,” Data Quality Campaign’s “2019 Legislative Update Part I” and “2018 State Legislation Update: New

Laws Reflect Value of Data” and the Center for Democracy and Technology’s “State Student Privacy Law Compendium (2016).” Student data privacy campaigns are operated by the the Electronic Privacy Information Center (EPIC), Electronic Frontier Foundation (EFF), and the Future of Privacy Forum (FPF) among others.

[16] See, e.g., “Children’s Personal Data and SSNs Are Being Sold on the Dark Web” and “The latest dark web cyber-criminal trend: Selling children’s personal data.”

[17] The K-12 Cybersecurity Resource Center complies publicly-available district and state education agency IT audits at: https://k12cybersecure.com/resources/

[18] Olson, Parmy. “Pearson Hack Exposed Details on Thousands of U.S. Students.” The Wall Street Journal. 31 July 2019. Available online at: https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001

[19] To assess the potential magnitude of the Pearson AimsWeb 1.0 data breach, consider the case of Clark County School District (CCSD) in Nevada, only 1 of the 13,000 enterprise customers affected. CCSD disclosed that the Pearson incident impacted “approximately 559,487 students enrolled in the district between 2008 and 2019, and a much smaller number of staff members employed during the same period.” Of note, the K-12 Cyber Incident Map was only able to identify 135 of the 13,000 accounts involved in the breach.

[20] CBS Chicago. “Parent Files Class-Action Suit After Data Breach Exposes Nearly 1 Million Schoolchildren’s Personal Information.” 5 September 2019. Available online at: https://chicago.cbslocal.com/2019/09/05/pearson-school-data-breach-lawsuit/

[21] Hoffman, Matt. “Testing data for more than 8,000 Montana high-schoolers inappropriately released.” Billings Gazette. 15 March 2019. Available online at: https://billingsgazette.com/news/state-and-regional/testing-data-for-more-than-montana-high-schoolers-inappropriately-released/article_06467c9f-e913-5609-8536-658b73931104.html; Greenberg, Andy. “This Teen Hacker Found Bugs in School Software That Exposed Millions of Records.” Wired. 29 August 2019. Available online at: https://www.wired.com/story/teen-hacker-school-software-blackboard-follett/; Whittacker, Zach. “Chegg resets 40 million user passwords after data breach.” TechCrunch. 26 September 2018. Available online at: https://techcrunch.com/2018/09/26/chegg-resets-40-million-user-passwords-after-data-breach/; Castrodale, Jelisa. “School Lunch Baron Allegedly Hacked Students’ Data to Take Down His Competitor.” Vice. 8 May 2019. Available online at: https://www.vice.com/en_us/article/43j3vw/school-lunch-baron-allegedly-hacked-students-data-to-take-down-his-competitor; Cox, Joseph. “Hacker Steals Millions of User Account Details from Education Platform Edmodo.” Motherboard. 11 May 2017. Available online at: https://www.vice.com/en_us/article/ezjbwe/hacker-steals-millions-of-user-account-details-from-education-platform-edmodo; Cox, Joseph. “Education and Science Giant Elsevier Left Users’ Passwords Exposed Online.” Motherboard. 18 March 2019. Available online at: https://www.vice.com/en_us/article/vbw8b9/elsevier-user-passwords-exposed-online; Cimpanu, Catalin. “Round 4: Hacker returns and puts 26Mil user records for sale on the Dark Web.” ZDNet. 17 March 2019. Available online at: https://web.archive.org/web/20200224163456/https://www.zdnet.com/article/round-4-hacker-returns-and-puts-26mil-user-records-for-sale-on-the-dark-web/; Johnston, Ryan. “Student data systems compromised in Hawaii, Tennessee.” EdScoop. 23 July 2019. Available online at: https://edscoop.com/graduation-alliance-data-exposure-hawaii-tennessee/; Bischoff, Paul. “Report: 7 million student records exposed by K12.com.” comparitech. 10 July 2019. Available online at: https://web.archive.org/web/20190728200457/https://www.comparitech.com/blog/vpn-privacy/report-7-million-student-records-exposed-by-k12-com/; O’Donnell, Lindsey. “Critical Flaws in Khan Academy Opened Door to Account Takeovers.” ThreatPost. 22 May 2019.

Available online at: https://threatpost.com/critical-flaws-in-khan-academy-opened-door-to-account-takeovers/144973/; Herold, Benjamin. “Florida Virtual School Reveals Huge Data Breaches.” Education Week. 12 March 2018. Available online at: https://blogs.edweek.org/edweek/DigitalEducation/2018/03/florida_virtual_school_data_breaches.html; Fowler, Jeremiah.”Leadership for Educational Equity Exposes 3.69 Million Members Online.” Security Discovery. 7 August 2019. Available online at: https://securitydiscovery.com/leadership-for-educational-equity/; Patterson, Jordan. “Officials: Student Info Breached In Bemus Point.” The Post-Journal. 26 May 2018. Available online at: https://www.post-journal.com/news/page-one/2018/05/officials-student-info-breached-in-bemus-point/; Schwarz, Joel. “The Cyber-Security Problem Schools and Ed. Tech Need to Face.” Education Week. 30 January 2020. Available online at: https://www.edweek.org/ew/articles/2020/01/30/the-cyber-security-problem-schools-and-ed-tech.html; Olson, Parmy. “Pearson Hack Exposed Details on Thousands of U.S. Students.” The Wall Street Journal. 31 July 2019. Available online at: https://www.wsj.com/articles/pearson-hack-exposed-details-on-thousands-of-u-s-students-11564619001; Murphy, Jan. “Data breach put 360,000 Pa. teachers, education department staffers’ personal information at risk.” 23 March 2018. Penn Live Patriot-News. Available online at: https://www.pennlive.com/politics/2018/03/data_breach_put_360000_pa_teac.html; Harris, Bracey. “Mississippi student data accessed in testing-vendor breach.” Mississippi Clarion Ledger, 19 January 2018. Available online at: https://www.clarionledger.com/story/news/politics/2018/01/19/mississippi-student-data-accessed-testing-vendor-breach/1050068001/; Cameron, Dell. “1.3 million K-12 students exposed by now-secured data breach.” 20 April 2017. The Daily Dot. Available online at: https://www.dailydot.com/layer8/1-3-million-american-students-exposed-data-breach-now-secured/; Levin, Douglas. “Everything’s Bigger in Texas…Including (Maybe) the Data Breaches.” 12 August 2017. The K-12 Cybersecurity Resource Center. Available online at: https://k12cybersecure.com/blog/everythings-bigger-in-texas-including-maybe-the-data-breaches/; Levin, Douglas. “Total Registration, Totally Pwned.” 17 May 2019. The K-12 Cybersecurity Resource Center. Available online at: https://k12cybersecure.com/blog/total-registration-totally-pwned/

[22] This figure includes all incidents coded as ‘ransomware,’ as well as 37 incidents coded as ‘other incidents’ involving unspecified malware. The K-12 Cyber Incident Map is conservative in how it attributes incidents as ‘ransomware,’ but – given the state of public disclosure of school cybersecurity incidents and anecdotal evidence – it is reasonable to assume that many ambiguously-reported malware incidents involve the malicious encryption of IT systems along with extortion demands.

[23] Freed, Benjamin. “Report: Ransomware attacks against state and local government are on the rise.” StateScoop. 13 May 2019. Available online at: https://statescoop.com/report-ransomware-attacks-against-state-and-local-government-are-on-the-rise/

[24] See: Swinhoe, Dan. “How hackers use ransomware to hide data breaches and other attacks.” CSO. 2 April 2019. Available online at: https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html and Tung, Liam. “Ransomware: Cybercriminals are adding a new twist to their demands.” ZDNet. 13 December 2019. Available online at: https://www.zdnet.com/article/ransomware-cybercriminals-are-adding-a-new-twist-to-their-demands/

[25] Krebs, Brian. “Ransomware Gangs Now Outing Victim Businesses That Don’t Pay Up.” Krebs on Security. 16 December 2019. Available online at: https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

26 Gore, Leada. “Alabama school system forced to move start date again due to malware attack.” AL.com. 31 July 2019. Available online at: https://www.al.com/news/2019/07/alabama-school-system-forced-to-move-start-date-again-due-to-malware-attack.html; Irvin, Steve. “Flagstaff schools back open after 2-day ransomware closure.” ABC 15 Arizona. 9 September 2019. Available online at: https://www.abc15.com/news/region-northern-az/flagstaff/flagstaff-schools-back-open-after-2-day-ransomware-closure; “Livingston Public Schools Hacked With Ransomware, Classes Delayed.” 25 November 2019. CBS New York. Available online at: https://newyork.cbslocal.com/2019/11/25/livingston-schools-ransomware/; George, Michael. “NY School Delays Start of Year After Ransomware Attack.” 4 New York. 3 September 2019. Available online at: https://www.nbcnewyork.com/news/local/ny-school-delays-start-of-year-after-ransomware-attack/1990459/; Noll, Scott. “FBI is now working with Coventry Schools to investigate ‘Trickbot’ computer virus.” News 5 Cleveland. 15 May 2019. Available online at: https://www.news5cleveland.com/news/local-news/akron-canton-news/coventry-local-school-district-closed-monday-due-to-trickbot-virus-infecting-school-computers

27 See “Gov. Edwards Activates State Resources to Assist With Ongoing Cybersecurity Incident.” Available online at: https://gov.louisiana.gov/index.cfm/page/76

28 Levin, Douglas. “LA’s Declaration of Emergency: Lessons Learned.” The K-12 Cybersecurity Resource Center. 1 November 2019. Available online at: https://k12cybersecure.com/blog/las-declaration-of-emergency-lessons-learned/

29 Ryan, Jim T. “Cyber attack at Newport schools didn’t expose student data.” Penn Live Patriot-News. 30 March 2019. Available online at: https://www.pennlive.com/perry-county-times/2019/03/cyber-attack-at-newport-schools-didnt-expose-student-data.html

30 6 News. “Glenwood schools recover from cyber-attack for new school year.” 6 News. 21 August 2019. Available online at: https://web.archive.org/web/20200225184642/https://www.wowt.com/content/news/Glenwood-schools-recover-from-cyber-attack-for-new-school-year–557751991.html; Alonzo, Amy. “System hack still locking out school district despite ransom payment.” Reno Gazette Journal. 8 August 2019. Available online at: https://www.rgj.com/story/news/local/mason-valley/2019/08/08/nevada-school-district-recovering-computer-hack-after-paying-ransom-cryptocurrency/1951856001/; Tyrrell, Joie. “Rockville Centre pays almost $100G to hackers after ransomware attack, officials say.” Newsday. 23 August 2019. Available online at: https://web.archive.org/web/20190824142728/https://www.newsday.com/long-island/education/hackers-ramsomware-school-districts-1.35422441; Mulder, James T. “Public officials still mum on cost of Syracuse school ransomware attack.” Syracuse.com. 30 August 2019. Available online at: https://www.syracuse.com/schools/2019/08/public-officials-still-mum-on-cost-of-syracuse-school-ransomware-attack.html; Mehalshick, Andy. “Cybercriminals hold Wyoming Area School District’s data hostage during a ransomware attack.” PA Homepage. 1 October 2019. Available online at: https://web.archive.org/web/20191001215307/https://www.pahomepage.com/top-stories/cybercriminals-hold-wyoming-area-school-districts-data-hostage-during-a-ransomware-attack/

31 See: “Risk Advisory: March 5, 2019 Don’t Get Spoofed Payroll Phishing Fraud Alert.” Available online at: https://www.saonm.org/wp-content/uploads/2019/06/Spoofed_Email_3-4-19.pdf; “Please read: Scam targets school districts’ direct payroll deposits.” Available online at: https://education.ohio.gov/Media/Ed-Connection/March-4-2019/Please-read-Scam-targets-school-districts-direct

[32] WKYT News Staff. “Scott County Schools victim of $3.7 million scam.” WKYT. 24 April 2019. Available online at: https://www.wkyt.com/content/news/Scott-County-Schools-victim-of-37-million-scam-509017341.html

[33] See: “Cabarrus County Government targeted in social engineering scam.” 26 August 2019. Available online at: https://www.cabarruscounty.us/news/cabarrus-county-government-targeted-in-social-engineering-scam; Campuzano, Eder. “Portland Public Schools nearly scammed out of $2.9 million.” The Oregonian/OregonLive. 19 August 2019. Available online at: https://www.oregonlive.com/education/2019/08/portland-public-schools-nearly-scammed-out-of-29-million.html; Barden, Melanie. “FBI investigating after Manor ISD loses $2.3M in phishing email scam.” News 4 San Antonio. 10 January 2020. Available online at: https://web.archive.org/web/20200111153128/https://news4sanantonio.com/news/local/fbi-investigating-after-manor-isd-loses-23m-in-phishing-email-scam; Taylor, Scott. “Email scam costs Spotsylvania schools $600,000.” ABC 7. 6 August 2019. Available online at: https://web.archive.org/web/20200226181438/https://wjla.com/news/local/email-scam-costs-spotsylvania-schools-600000

[34] EdScoop. “Phishing attacks challenging teachers, says Utah ed director.” EdScoop. 22 January 2019. Available online at: https://edscoop.com/video/phishing-attacks-challenging-teachers-says-utah-ed-director/

[35] See: “Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others.” Available online at: https://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others

[36] Doe, Dissent. “Centinela Valley Union High School District notifies employees of W-2 phishing incident.” DataBreaches.net. 20 February 2019. Available online at: https://www.databreaches.net/centinela-valley-union-high-school-district-notifies-employees-of-w-2-phishing-incident/

[37] Lemos, Robert. “More Breaches, Less Certainty Cause Dark Web Prices to Plateau.” Dark Reading. 15 October 2019. Available online at: https://www.darkreading.com/attacks-breaches/more-breaches-less-certainty-cause-dark-web-prices-to-plateau/d/d-id/1336094

[38] School districts that have experienced more than one publicly-disclosed cyber incident since 2016 are reported here: https://k12cybersecure.com/map/repeat-incidents/.

[39] Hoffman, Matt. “Montana schools still vulnerable to cyber attacks, experts warn.” Billings Gazette. 29 August 2019. Available online at: https://billingsgazette.com/news/local/montana-schools-still-vulnerable-to-cyber-attacks-experts-warn/article_4e92a21e-b22c-5969-abd9-94cf5f335455.html

[40] The U.S. Department of Education’s National Center for Statistics classifies districts into one of the four geographic regions used by the Bureau of Economic Analysis of the U.S. Department of Commerce. States included in the central region include: Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin.

[41] The U.S. Census Bureau’s Small Area Income and Poverty Estimates (SAIPE) program provides annual estimates of income and poverty statistics for all school districts.

[42] For example, see: Nicholas Bogel-Burroughs “Hackers’ Latest Target: School Districts” New York Times. 28 July 2019. https://www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html

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

[44] See: New York State Education Department. “Part 121 of the Regulations of the Commissioner of Education.” Available online at: http://www.nysed.gov/data-privacy-security/regulations-strengthen-data-privacy-and-security; Rapaport, Wes. “Texas schools now required to craft cybersecurity plans, staff to undergo training.” KXAN. 30 January 2020. Available online at: https://www.kxan.com/news/education/texas-schools-now-required-to-craft-cybersecurity-plans-staff-to-undergo-training/