THE STATE OF K-12 CYBERSECURITY: 2018 YEAR IN REVIEW

The K-12 Cybersecurity Resource Center

As public schools embrace technology, cybersecurity incidents grow both more common and more significant.

The State of K-12 Cybersecurity: 2018 Year in Review

PART I: INTRODUCTION

There is a particular strand of folklore about public schools that suggests they have changed little over time.[1] While the basic structure of elementary and secondary schools remains recognizable, one of the most significant ways schools have changed from the past has been via the massive infusion of technology. In fact, U.S. K-12 schools are increasingly reliant on technology and sophisticated IT systems for teaching, learning, and school operations.

Consider: The number of U.S. K-12 students with access to the broadband they need for 'digital learning' in schools and classrooms grew from 4 million in 2013 to 44.7 million in 2018.[2] Millions of mobile PCs—notebooks/Macs, netbooks, tablets, and Chromebooks—are being purchased by U.S. K-12 schools every year, with the penetration of mobile PC devices used by U.S. teachers and students now above 50 percent.[3] School telephone systems are migrating to VoIP (voice-over-IP) services; point-of-sale systems are deployed in school cafeterias; HVAC and lighting controls are centrally managed via IP networks; student information systems offer real-time insights to administrators, teachers, and parents; internet-connected surveillance cameras are being deployed in the name of school safety; and school district human resource offices manage hiring, payroll, and benefits via online portals.[4] While uneven, the scope and speed of technology adoption by U.S K-12 schools has been remarkable.

Indeed, the K-12 education technology market has grown to become very big business.[5]

While the benefits of technology in education may be great, its adoption also introduces new risks. As security expert Bruce Schneier writes:

> *"It's no secret that computers are insecure. Stories like the recent Facebook hack, the Equifax hack and the hacking of government agencies are remarkable for how unremarkable they really are. They might make headlines for a few days, but they're just the newsworthy tip of a very large iceberg."*[6]

While reports of data breaches and cybersecurity incidents experienced by businesses and government are shockingly frequent,[7] what do we know of the cybersecurity risks being introduced to schools with this influx of technology? What threats and vulnerabilities might students and teachers be facing, and how well prepared are school leaders to manage these new risks?

What little data we have on the state of cybersecurity risk management in U.S. K-12 public schools does not paint a promising picture. Of the 18 sub-sector peer groups investigated by the Multi-State Information Sharing & Analysis Center (MS-ISAC) in their 2017 review, local K-12 schools were reported to have the least mature cybersecurity risk management practices of any state, local, tribal, or territorial government agency.[8] Likewise, a November 2017 *Education Week* article concludes:

> *The country's K-12 information-technology leaders are likely underestimating the dangers they face. Most don't see cybersecurity threats such as ransomware attacks, phishing schemes, and data breaches as a significant problem….Even more troubling, many school technology leaders are failing to take basic steps to secure their networks and data.*[9]

This report, "The State of K-2 Cybersecurity: 2018 Year in Review," is designed to shed light on the threats and risks facing K-12 schools, students, and educators due to the misuse and abuse of school technology. Based on cyber incident data cataloged on the K-12 Cyber Incident Map, it offers data and insights on the actual threats and risks that were experienced by schools during 2018. Part II provides information on the data sources assembled for this report, 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 this work.

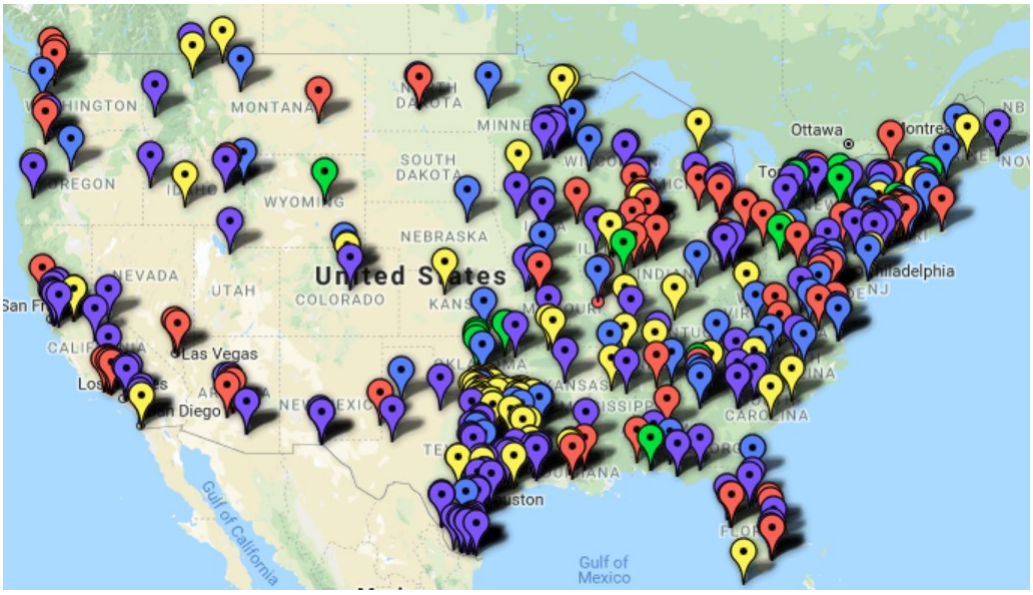
PART II: K-12 CYBER INCIDENT DATA

The K-12 Cyber Incident Map was launched as an effort to build an empirical base of information about the state of cybersecurity in public K-12 schools and districts.[10] While other efforts exist to catalog trends in cybersecurity incidents and data breaches, including in education, none bring a lens that is reliably actionable for U.S. K-12 education policymakers, school leaders, IT practitioners, or privacy advocates.

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 as a singular category of analysis.[11] Other public sources of data breach incidents compiled by experts, such as DataBreaches.net, the Identify Theft Resource Center, and the Privacy Rights Clearinghouse, 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).[12] While there may be lessons to be drawn from each of these valuable efforts, it is time for a K-12 specific lens on the issue.

The K-12 Cyber Incident Map and underlying database captures detailed information about two inter-related issues:

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



The K-12 Cyber incident Map has identified 418 incidents since 2016 involving public schools across the United States (as of January 29, 2019).

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.[13] 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.[14] Similarly, poverty status of school districts is drawn from the U.S. Census Bureau's Small Area Income and Poverty Estimates (SAIPE).[15]

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.[16] 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.

Summary data about K-12 cybersecurity incidents are currently published on an interactive map of the United States via the soon-to-be-deprecated Google Fusion Tables service.[17] Incidents on the map are color-coded by 'primary' incident type:

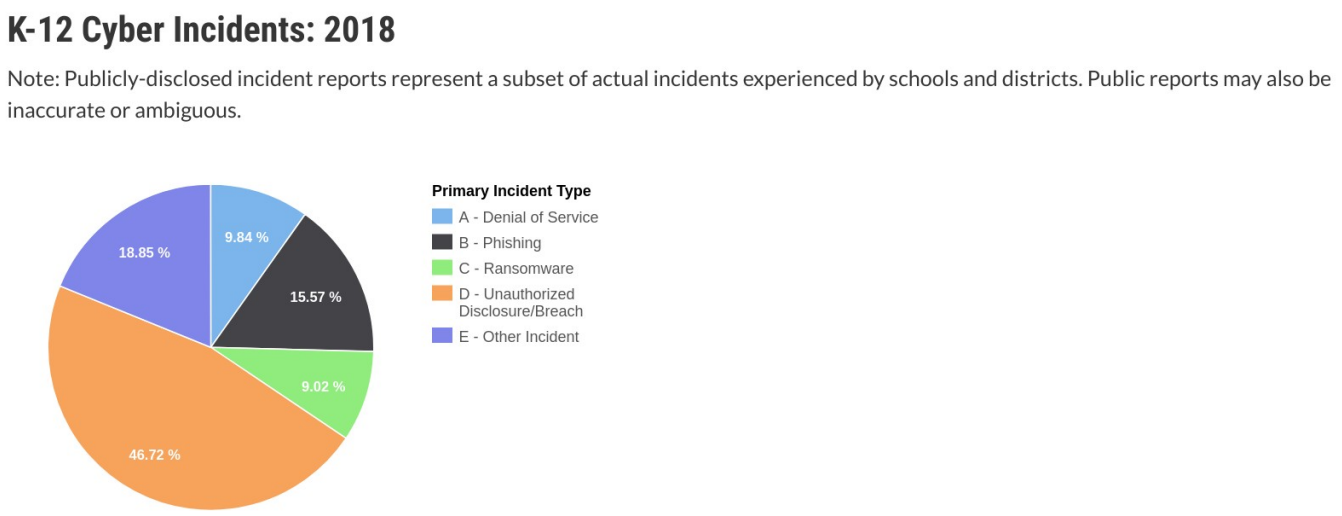
- phishing attacks resulting in the disclosure of personal data (blue pins);
- other unauthorized disclosures, breaches or hacks resulting in the disclosure of personal data (purple pins);
- ransomware attacks (yellow pins);
- denial-of-service attacks (green pins); and
- other cyber incidents resulting 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: 2018

During calendar year 2018, the K-12 Cyber Incident Map cataloged 122 publicly-disclosed cybersecurity incidents affecting 119 public K-12 education agencies across 38 states. (Two school districts were reported to have experienced more than one cybersecurity incident during 2018.) This equates to a rate of about one new publicly-reported incident every three days of the calendar year, a statistic consistent with overall trends observed by the K-12 Cyber Incident Map since 2016.

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.[18]



The most frequently experienced type of K-12 cyber incident reported during 2018 were data breaches, primarily meeting one of the following four profiles:

- Unauthorized disclosures of data by current and former K-12 staff, primarily—but not exclusively—due to human error;
- Unauthorized disclosures of K-12 data held by vendors/partners with a relationship to a school district;
- Unauthorized access to data by K-12 students, often out of curiosity or a desire to modify school records (including grades, attendance records, or financial account balances); or,
- Unauthorized access to data by unknown external actors, often for malicious purposes.

Just over half of all digital data breach incidents experienced by K-12 schools in 2018 were directly carried out or caused by members of the affected school community (i.e., insiders), whether by staff or students. Incidents involving unauthorized student access to school IT systems raise particularly difficult questions about how school districts and law enforcement should respond, as well as about the sufficiency of the cybersecurity practices of districts who find themselves—in some cases—significantly compromised by their own middle and high school students.[19] This issue was highlighted this year by an original report of a student-initiated cybersecurity incident in the Rochester Community School District by the K-12 Cybersecurity Resource Center.

Another 23 percent of data breach incidents reported on the K-12 Cyber Incident Map were the result of a loss of control of K-12 data by school vendors or partners. While such incidents might be addressed through clearer cybersecurity standards for school vendors and better school contracting practices,[20] several incidents in 2018 suggest the issue is more complicated. Partner organizations to school districts—regional service agencies, non-profits, associations, and even state departments of education—with whom student and school staff data are entrusted were among those that experienced data breaches in 2018 (and even then it was sometimes due to the actions of their vendors).[21]

The remaining 23 percent of data breach incidents were carried out by unknown actors, often external to the school community and for malicious purposes (such as identity theft). Especially for school districts without sufficient baseline cybersecurity controls, retrospective attribution of cyber incidents can be difficult.

Student data were included in more than 60 percent of K-12 data breaches in 2018, which should be a cause for concern. First, federal and state student data privacy legislation is intended to reduce the incidence and severity of student data breaches,[22] although data assembled for the K-12 Cyber Incident Map raises questions as to how effective those policy regimes are working in practice. Second, security researchers have documented dark web marketplaces advertising the stolen personal information of children for use by identity thieves.[23] Indeed, student data breaches can have serious and long-lasting consequences.

Data about school district staff have also been regularly implicated in K-12 cyber incidents. During 2018, 46 percent of all K-12 digital data breaches included data about current and former school staff (such as payroll or other personnel records). In some cases, this has led to payroll theft, identity theft, and the filing of false tax returns of educators and other school district staff.

Phishing attacks—the vast majority of which are carried out over email—were also commonly experienced by school districts. In many cases, these attacks were the method of choice that malicious third-parties employed to gain access to sensitive data systems or to deliver and propagate malware on school networks. While some of the phishing attacks experienced by schools were the result of relatively unsophisticated bulk email campaigns,[24] school districts also found themselves specifically targeted by criminal actors.

Perhaps most concerning in 2018 were a number of successful phishing attacks targeted at school district business officials. These scams—designed to redirect large payments from legitimate school contractors/partners to criminal accounts—resulted in the theft of hundreds of thousands or even millions of tax payer dollars. The largest ever such theft recorded on the K-12 Cyber Incident Map occurred in 2018 and totaled approximately $2 million dollars in losses by a Texas district. Other large dollar incidents of K-12 cybercrime in 2018 ranged from $300,000 to a high of $988,000 (affecting school districts in Idaho, Louisiana, New Jersey, and Texas).[25] 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 appear to have diminished in 2018.[26] The K-12 Cyber Incident Map only reported three such incidents during the year (experienced by districts in Alabama, Texas, and Washington).

Responding to ransomware and other malware outbreaks—representing over 15 percent of all K-12 cyber incidents in 2018—was another commonly experienced challenge, as it has been in recent years. The impact of such incidents varied, but frequently involved significant costs and lost time in restoring IT systems, lost data, communications services, and student/teacher devices. In some cases, IT outages caused by malware on school technology systems extended for weeks.[27] In the most extreme cases, school districts were not able to restore their systems from backups and instead made the controversial choice to pay the extortion demands of criminals to regain access to their systems (as districts in Massachusetts and Michigan did in 2018).

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. While only 10 percent of 2018 incidents reported on the K-12 Cyber Incident Map are categorized as denial-of-service (or DDoS) attacks, anecdotal reporting suggests such incidents are much more common. 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.

School-managed social media and website defacement—representing about 5 percent of incidents experienced by school districts in 2018—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.[28] 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.

THE ‘TOP 10’ K-12 CYBER INCIDENTS OF 2018

During calendar year 2018, the K-12 Cyber Incident Map cataloged 122 publicly-disclosed cybersecurity incidents affecting 119 public K-12 education agencies across 38 states. What are the nature of these incidents? What is their real world impact? The 'Top 10' incidents of 2018 offer important insights.[29]

1. **In Pennsylvania, Data Breach Puts Every Teacher in the State at Risk**: As a result of human error, the Pennsylvania Department of Education's Teacher Information Management System (TIMS), which holds the personal information of 330,000 professional school staff across the state, was potentially compromised. Affected individuals were critical of how and when they were notified of the incident.
2. **Targeted Phishing Attack Leads to Identity Theft, Tax Fraud**: Texas district officials said an employee responded to a sophisticated phishing email from a scammer pretending to be the superintendent. The criminal actors requested—and received—copies of W-2 tax forms for all district employees. The IRS has warned K-12 districts nationwide about similar email phishing attacks, resulting in widespread school employee identity theft and tax fraud.
3. **Data Breach at Florida Virtual School Leads to Sale of Student Data on Dark Web**: After a researcher spotted school data up for sale on the dark web, an investigation revealed that Florida Virtual School (FLVS) had unwittingly published unencrypted confidential student and teacher data on the internet for a period of nearly two years. The breach affected at least 368,000 current and former teachers, students, and their families.
4. **School District Pays $10,000 Bitcoin Ransom to Restore Access to Critical Systems**: Affected by ransomware and unable to restore its own technology systems after several weeks had passed, a Massachusetts school district took the advice of local law enforcement and paid extortionists in an effort to regain access to email services, school lunch payment services, and the district's own website.
5. **Police Raid Student's Home in Grade Changing Incident**: A 16 year-old California student phished his teachers to gain access to the grading system at his high school, a hack he described as 'beginner level.' The result: a police raid and potential criminal charges. Incidents of student hacking into school IT systems are not uncommon, although responses by school authorities vary considerably.
6. **The FBI Warns of the Security, Privacy Risks of EdTech Adoption**: In an unprecedented statement, the FBI issued a warning in 2018 to school leaders and parents that the rapid growth in implementation of education technologies in U.S. schools and districts—coupled with the widespread collection of student data—could have privacy and safety implications if it is compromised or exploited.[30]
7. **U.S. Senator Calls for Federal Aid after School Networks Targeted**: Repeated distributed denial-of-service attacks (DDoS) directed at the Central New York Regional

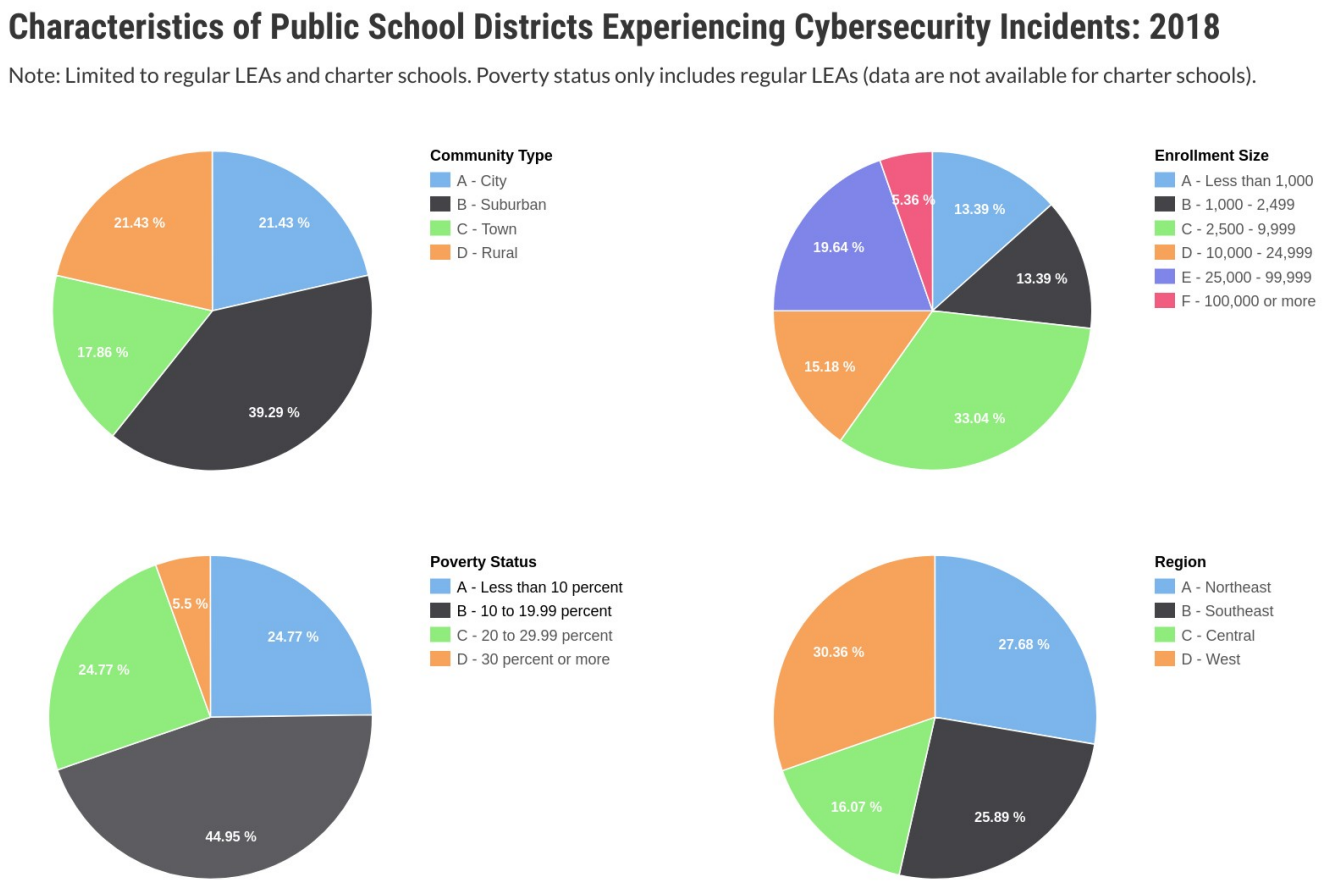
Information Center have disrupted internet connectivity, causing huge problems—and disruptions to teaching and learning—for dozens of school districts across Central New York.

8. **Disgruntled Former Employee Steals Sensitive District Database**: A former Chicago Public Schools (CPS) employee left her job with more than just her final paycheck: she allegedly took the personal information of about 70,000 people contained in a CPS database. This incident was only 1 of 5 publicly-disclosed data breaches experienced by CPS since 2016 (and 1 of 3 in 2018 alone).
9. **Texas District Scammed out of $2 Million School Construction Payment**: Only after the fact did a Texas district learn that payments to a school construction vendor were electronically transferred to a fraudulent account. While exceptional for the magnitude of the theft, other districts in Idaho, Louisiana, New Jersey, and Texas also lost hundreds of thousands of dollars during 2018 in similar scams.
10. **On Cusp of Winter Break, District Discloses Massive Data Breach**: San Diego Unified schools discovered an unauthorized user was gathering log-in information from staff via an email phishing campaign to access sensitive district services. The resulting data breach compromised student and staff data on more than 500,000 individuals (who may have interacted with the district anytime since the 2008-9 school year).

PART IV: SCHOOL DISTRICTS EXPERIENCING CYBERSECURITY INCIDENTS: 2018

During calendar year 2018, the K-12 Cyber Incident Map cataloged 122 publicly-disclosed cybersecurity incidents affecting 119 public K-12 education agencies across 38 states. Of these, all but seven occurred in regular school districts or charter schools. Two incidents were attributed to state education agencies (in North Dakota[31] and Pennsylvania), one involved a state virtual school (Florida), and the remainder involved regional or special LEAs (local education authorities) serving school districts in their respective states. Moreover, two school districts – Chicago Public Schools and Mt. Diablo (CA) Unified School District – were reported to have experienced more than one cybersecurity incident during calendar year 2018.[32]

What do we know about the characteristics of school districts affected by cybersecurity incidents? Are there certain attributes that make some districts more likely to experience an incident than others? Data assembled for the K-12 Cyber Incident Map are instructive.[33]



First, cybersecurity incidents do not seem to discriminate by community type or school district location. While nearly 40 percent of all 2018 incidents affecting school districts were located in

suburban communities, significant numbers of school districts impacted by cybersecurity incidents could be found in cities, towns, and rural communities. Affected school districts and charters can be found from coast-to-coast, from the Florida Keys to Anchorage, Alaska. Slightly fewer incidents were disclosed in the central region of the United States (16 percent), especially as compared to schools in the west (30 percent), although the reasons for this are unclear.

K-12 cybersecurity incidents also did not discriminate by school district size. Over 25 percent of all incidents affected districts and charter schools enrolling fewer than 2,500 students. One third affected districts enrolling between 2,500 and 9,999 students, and the remainder affected districts enrolling larger numbers of students. Of note, not even the largest school districts in the nation were spared from cyber incidents, with greater than 5 percent of incidents affecting districts enrolling 100,000 or more students.

Finally, data about school districts affected by a cybersecurity incident in 2018 suggest a relationship with the poverty of the school community: school districts serving fewer students in poverty were more likely to report a cyber incident in 2018 than districts serving poorer communities. During 2018, nearly 70 percent of incidents affected relatively lower poverty districts (serving less than 20 percent of students in poverty). In contrast, only about 5 percent of incidents affected school districts with a student population of greater than 30 percent in poverty. What might this finding (coupled with a slight proclivity for incidents to occur in suburban communities) suggest about the cybersecurity risks facing K-12 schools during 2018? One plausible hypothesis is that wealthier school communities may be relying on more technology than other district types and hence are exposed to greater risks. The finding may also be an artifact of how cyber incidents are disclosed and identified for publication on the K-12 Cyber Incident Map. Clearly, further research is warranted.

PART V: LESSONS FOR 2019 AND BEYOND

Evidence assembled to maintain the K-12 Cyber Incident Map reveals that school districts have not been immune to the same types of data breaches and cybersecurity incidents routinely plaguing even the most technologically advanced and well-resourced corporations and government agencies. During 2018, the misuse and abuse of school technology and IT systems resulted in 122 publicly-disclosed K-12 cybersecurity incidents. This equates to a rate of about one new publicly-reported incident every three days.

While it may be tempting to dismiss this number as being relatively insignificant given the magnitude of the U.S. K-12 enterprise, keen observers would not draw that lesson. First, one should not mistake publicly-disclosed incidents with the universe of all K-12 cyber incidents that occurred during the calendar year. Many incidents go unreported, and—unless school districts have a strong cybersecurity risk management program in place—there may also be a considerable gap between when school districts experience an incident and when (or if) they become aware of that fact.

Second, cyber incidents do not seem to discriminate by school location, community type, or size. Indeed, if school technology is accessible over the internet, mistakes can and do occur; malicious actors can and are taking note.

Third, the impact of publicly-reported K-12 cyber incidents is significant. During 2018, such incidents resulted in the theft of millions of tax payer dollars, stolen identities, tax fraud, altered school records, website and social media defacement, 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.

As we look to 2019 and beyond, we can expect schools to continue their reliance on technology and in so doing increase their cyber risk profile. To the degree schools broaden their data collection and sharing efforts to include even more sensitive data—such as personal communications,[34] biometric data,[35] and social/emotional and affective data[36]—the impact of any potential cyber incident is magnified. Moreover, given the centralization of data systems and platforms, future cyber incidents have the potential to impact ever larger numbers of students and educators across district and state lines. This is particularly concerning, because issues of K-12 cybersecurity have largely been overlooked by policymakers, regulators, and school leaders, despite greater attention to issues of student data privacy.

Ultimately, the goal of K-12 stakeholders must be to reduce and better manage the cybersecurity risks facing increasingly technologically-dependent schools, but make no mistake: keeping K-12 schools ‘cyber secure’ is a wicked problem—one that is assured to get worse until we take meaningful steps to address it. 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.[37]

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 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. (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/

Cover image credit: CC BY 2.0 AL.Eyad
https://www.flickr.com/photos/linda_lila/23303173449/

The publication of this report was made possible with the generous support of Core BTS, Managed Methods, and PC Matic PRO.

1 See, e.g., https://www.chalkbeat.org/posts/us/2017/09/06/xq-is-taking-over-tv-to-make-the-case-that-high-school-hasnt-changed-in-100-years-but-is-that-true/ ("XQ is taking over TV to make the case that high school hasn't changed in 100 years. But is that true?)" and http://hackeducation.com/2015/04/25/factory-model ("The Invented History of 'The Factory Model of Education'").

2 See https://stateofthestates.educationsuperhighway.org/#national ("2018 State of the States: Expanding digital learning to every classroom, every day"). The 'digital learning' standard for broadband connectivity applied by Education SuperHighway in their analyses became a matter of federal policy in 2014 with the Federal Communication Corporation's adoption of the E-Rate Modernization Order (https://www.fcc.gov/general/summary-e-rate-modernization-order).

3 See https://marketbrief.edweek.org/marketplace-k-12/global-demand-mobile-computing-devices-k-12-grows-powered-u-s-market/ ("Global Demand for Mobile Computing Devices in K-12 Grows, Powered by U.S. Market") and https://www.futuresource-consulting.com/press-release/education-technology-press/the-us-k-12-education-market-beats-forecast-in-q3/ ("The US K-12 Education Market Beats Forecast in Q3, But Stock Issues Spell Uncertainty for Next Year").

4 See, e.g., https://www.educationdive.com/news/software-solutions-can-streamline-school-operations-saving-time-and-money/507751/ ("Software solutions can streamline school operations, saving time and money"), https://webspm.com/articles/2017/09/01/iot.aspx ("The Internet of Things (IoT): The Art of the Possible"), and https://blog.schneider-electric.com/education-research/2017/09/27/k-12-school-districts-drive-innovation-with-new-technologies/ ("K-12 School Districts Drive Innovation with New Technologies").

5 See, e.g., https://youtu.be/KKjEaYM-Ziw ("ISTE 2018 Conference Highlights") and https://www.nytimes.com/2017/11/03/technology/silicon-valley-baltimore-schools.html ("How Silicon Valley Plans to Conquer the Classroom").

6 See https://www.schneier.com/essays/archives/2018/10/internet_hacking_is_.html ("Internet Hacking Is About to Get Much Worse").

7 Publications devoted to reporting on cyber incidents include Dark Reading (https://www.darkreading.com/), Naked Security (https://nakedsecurity.sophos.com/), and ThreatPost (https://threatpost.com/) among many others.

8 See https://www.cisecurity.org/wp-content/uploads/2018/10/NCSR-2017-Final.pdf ("Nationwide Cybersecurity Review: 2017 Summary Report").

9 See https://www.edweek.org/ew/articles/2017/11/29/schools-struggle-to-keep-pace-with-hackings.html ("Schools Struggle to Keep Pace With Hackings, Other Cyber Threats").

10 See https://k12cybersecure.com/blog/introducing-the-k-12-cyber-incident-map/ ("Introducing the K-12 Cyber Incident Map").

11 See https://enterprise.verizon.com/resources/reports/dbir/ ("Verizon Data Breach Investigations Report") and https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/ ("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.

12 The Privacy Rights Clearinghouse maintains a database of public breaches that includes some information about school incidents (https://www.privacyrights.org/data-breaches). Databreaches.net offers a comprehensive history of education-related incidents (https://www.databreaches.net/category/breach-reports/education-sector/. The Identity Theft Resource Center tracks U.S. data breaches, including those affecting schools (https://www.idtheftcenter.org/data-breaches/).

13 See http://veriscommunity.net/index.html ("VERIS, the Vocabulary for Event Recording and Incident Sharing").

14 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 (https://nces.ed.gov/ccd/). 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 (https://nces.ed.gov/surveys/frss/index.asp).

15 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 (https://www.census.gov/programs-surveys/saipe.html). SAIPE also provides estimates of the number of school-age children in poverty for all school districts.

16 Incident reports may be submitted to the K-12 Cybersecurity Resource Center directly via this contact form: https://k12cybersecure.com/contact/. Note: Only publicly-disclosed incidents are eligible for inclusion on the K-12 Cyber Incident Map.

17 See https://support.google.com/fusiontables/answer/9185417 ("Google Fusion Tables Turndown").

18 Interacting with the figure in the online version of this report at https://k12cybersecure.com/year-in-review/2018-incidents/ will reveal greater details about the characteristics of publicly-disclosed K-12 cyber incidents that were reported during calendar year 2018.

19 See, e.g., https://www.edweek.org/ew/articles/2018/06/13/student-hackings-highlight-weak-k-12-cybersecurity.html ("Student Hackings Highlight Weak K-12 Cybersecurity").

20 See, e.g., https://www.eff.org/deeplinks/2018/01/how-assess-vendors-data-security ("How to Assess a Vendor's Data Security").

21 See, e.g., http://www.post-journal.com/news/page-one/2018/05/officials-student-info-breached-in-bemus-point/ ("Officials: Student Info Breached In Bemus Point"), https://www.databreaches.net/san-diego-county-office-of-education-notifies-component-school-districts-of-breach-of-employee-retirement-contribution-data/ ("San Diego County Office of Education notifies component school districts of breach of employee retirement contribution data"), https://www.clarionledger.com/story/news/politics/2018/01/19/mississippi-student-data-accessed-testing-vendor-breach/1050068001/ ("Mississippi student data accessed in testing-vendor breach"), and https://www.news10.com/news/ny-education-department-announces-data-breach-by-outside-assessment-vendor/1081464308 ("NY Education Department announces data breach by outside assessment vendor").

22 For recent reviews of federal and state student data privacy legislation, see the Parent Coalition for Student Privacy/The Network for Publication Education's "The State Student Privacy Report Card" (https://dataqualitycampaign.org/2018-state-legislation-update2/), Data Quality Campaign's "2018 State Legislation Update: New Laws Reflect Value of Data" (https://dataqualitycampaign.org/2018-state-legislation-update2/) and "Education Data Legislation Review: 2017 State Activity" (https://2pido73em67o3eytaq1cp8au-wpengine.netdna-ssl.com/wp-content/uploads/2017/09/DQC-Legislative-summary-0926017.pdf), and the Center for Democracy and Technology's "State Student Privacy Law Compendium (2016)" (https://cdt.org/files/2016/10/CDT-Stu-Priv-Compendium-FNL.pdf). Other student data privacy campaigns are operated by the the Electronic Privacy Information Center (EPIC) (https://epic.org/privacy/student/), Electronic Frontier Foundation (EFF) (https://www.eff.org/issues/student-privacy), and the Future of Privacy Forum (FPF) (https://fpf.org/issues/k-12-education/) among others.

23 See, e.g., https://motherboard.vice.com/en_us/article/zmd78y/childrens-personal-data-social-security-numbers-dark-web ("Children's Personal Data and SSNs Are Being Sold on the Dark Web") and https://icitech.org/wp-content/uploads/2017/04/ICIT-Analysis-Sowing-the-Seeds-of-U.S.-Cyber-Talent.pdf ("Sowing the Seeds of U.S. Cyber Talent: Leveraging K-12 Cyber-Education to Develop the Cyber-Workforce and Improve National Security").

24 See, e.g., https://www.consumeraffairs.com/news/a-new-gift-card-email-scam-just-in-time-for-the-holidays-113018.html ("A new gift card email scam just in time for the holidays"), which did not discriminate in

including school-based emails among its targets ("Check Email Addresses Closely, Police Say:" https://jocoreport.com/check-email-addresses-closely-police-say/).

25 Sample media reports of successful large dollar phishing scams against schools during 2018 include: http://wpgtalkradio.com/reports-galloway-schools-scammed-for-300k-in-cyber-theft/ ("Reports: Galloway Schools Scammed for $300k in Cyber Theft"), https://tylerpaper.com/news/local/henderson-isd-falls-victim-to-fraud-scheme/article_78563c14-ce5f-11e8-a9e4-1b3611a387ce.html ("Henderson ISD falls victim to fraud scheme "), https://www.tetonvalleynews.net/news/school-district-loses-three-quarters-of-a-million-to-fraud/article_95241ec3-66b6-5d44-9ced-7aa0e104b73a.html ("School district loses three quarters of a million to fraud"), https://www.arklatexhomepage.com/news/local-news/caddo-schools-scammed-out-of-nearly-1-million/1692970023 ("Caddo Schools scammed out of nearly $1 million"), and https://www.dallasnews.com/news/crime/2018/12/18/florida-man-bought-bmw-rolexes-after-defrauding-crowley-isd-tarrant-county-school-district-2m-feds-say ("Florida man bought BMW, Rolexes after defrauding Tarrant County school district out of $2M, feds say").

26 See, e.g., https://www.nhregister.com/metro/article/Man-pleads-guilty-to-phishing-scheme-that-13481527.php ("Man pleads guilty to phishing scheme that victimized Connecticut school employees").

27 See. e.g., https://www.leominsterchamp.com/articles/deacon-schools-truly-held-captive-by-ransomware-attack/ ("Deacon: Schools 'truly held captive' by ransomware attack'") and https://www.miamiherald.com/news/local/community/florida-keys/article218340835.html ("Keys public school computers remain down a 5th day after cyberattack").

28 See, e.g., https://foxillinois.com/news/local/hoopeston-school-district-hacked ("Hoopeston Area School District hacked"), https://www.koin.com/news/local/washington-county/lake-oswego-school-district-twitter-hacked/1288191319 ("Lake Oswego School District Twitter hacked"), and https://dfw.cbslocal.com/2018/02/23/school-threats-increasing-shooting/ ("School Threats Increasing In North Texas Since Florida School Shooting").

29 Visit https://k12cybersecure.com/year-in-review/2018-incidents/ to view these incidents on an interactive timeline, including links to local television news reports.

30 See "Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students" (https://www.ic3.gov/media/2018/180913.aspx).

31 See https://www.grandforksherald.com/news/education/4499560-after-one-third-north-dakota-schools-get-hacked-foreign-entities-state ("After one-third of North Dakota schools get hacked by foreign entities, state superintendent addresses attack with cyber security standards"). Given that available public reports did not allow attribution to specific school districts, it was attributed instead to the state education agency.

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

33 Interacting with the pie charts on the online version of this report at https://k12cybersecure.com/year-in-review/2018-districts/ 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 2018.

34 See e.g., https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/ ("Schools are using AI to track what students write on their computers").

35 See, e.g., https://elearningindustry.com/biometrics-in-schools-data-enhance-learning-4-ways ("Biometrics In Schools: 4 Ways Biometric Data Can Be Used To Enhance Learning").

36 See, e.g., https://edtechmagazine.com/k12/article/2016/02/how-affective-data-could-change-learning-outcomes ("How Affective Data Could Change Learning Outcomes").

37 See https://k12cybersecure.com/blog/how-should-we-address-the-cybersecurity-threats-facing-k-12-schools/ (“How Should We Address the Cybersecurity Threats Facing K-12 Schools?”) for further thoughts on the elements of a meaningful framework for address emerging K-12 cybersecurity threats.