United States Government Accountability Office

Report to the Republican Leader, Committee on Education and Labor, House of Representatives

September 2020

DATA SECURITY

Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm

Accessible Version

GAO-20-644

GAO Highlights

Highlights of GAO-20-644, a report to the Republican Leader, Committee on Education and Labor, House of Representatives

September 2020

DATA SECURITY

Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm

Why GAO Did This Study

When a student's personal information is disclosed, it can lead to physical, emotional, and financial harm. Organizations are vulnerable to data security risks, including over 17,000 public school districts and approximately 98,000 public schools. As schools and districts increasingly rely on complex information technology systems for teaching, learning, and operating, they are collecting more student data electronically that can put a student's information, including PII, at risk of disclosure. The closure of schools and the sudden transition to distance learning across the country due to the Coronavirus Disease 2019 (COVID-19) pandemic also heightened attention on K-12 cybersecurity.

GAO was asked to review the security of K-12 students' data. This report examines (1) what is known about recently reported K-12 cybersecurity incidents that compromised student data, and (2) the characteristics of school districts that experienced these incidents.

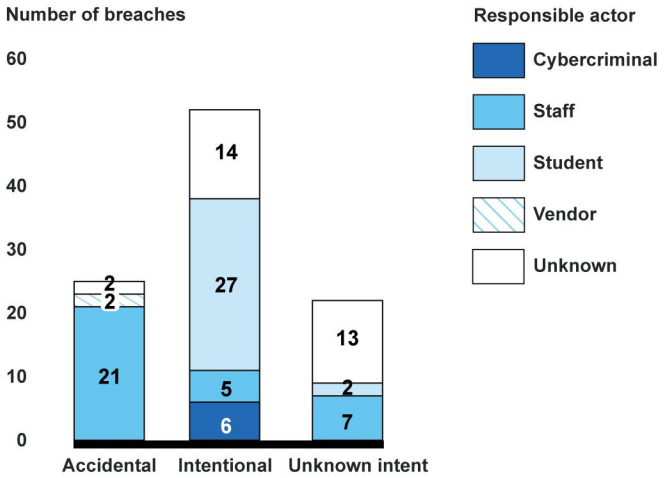
GAO analyzed data from July 1, 2016 to May 5, 2020 from CRC (the most complete source of information on K-12 data breaches). CRC is a non-federal resource sponsored by an educational technology organization that has tracked reported K-12 cybersecurity incidents since 2016. GAO also analyzed 2016-2019 Department of Education data on school district characteristics (the most recent available), and interviewed experts knowledgeable about cybersecurity. We incorporated technical comments from the agencies as appropriate.

View GAO-20-644. For more information, contact Jacqueline M. Nowicki at (617) 788-0580 or nowickij@gao.gov

What GAO Found

A cybersecurity incident is an event that actually or potentially jeopardizes a system or the information it holds. According to GAO's analysis of K-12 Cybersecurity Resource Center (CRC) data from July 2016 to May 2020, thousands of K-12 students were affected by 99 reported data breaches, one type of cybersecurity incident in which data are compromised. Students' academic records, including assessment scores and special education records, were the most commonly compromised type of information (58 breaches). Records containing students' personally identifiable information (PII), such as Social Security numbers, were the second most commonly compromised type of information (36 breaches). Financial and cybersecurity experts say some PII can be sold on the black market and can cause students significant financial harm. Breaches were either accidental or intentional, although sometimes the intent was unknown, with school staff, students, and cybercriminals among those responsible (see figure). Staff were responsible for most of the accidental breaches (21 of 25), and students were responsible for most of the intentional breaches (27 of 52), most frequently to change grades. Reports of breaches by cybercriminals were rare but included attempts to steal PII. Although the number of students affected by a breach was not always available, examples show that thousands of students have had their data compromised in a single breach.

Responsible Actor and Intent of Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Notes: The actor or the intent may not be discernible in public reports.

For this analysis, a cybercriminal is defined as an actor external to the school district who breaches a data system for malicious reasons.

Of the 287 school districts affected by reported student data breaches, larger, wealthier, and suburban school districts were disproportionately represented, according to GAO's analysis. Cybersecurity experts GAO spoke with said one explanation for this is that some of these districts may use more technology in schools, which could create more opportunities for breaches to occur.

Contents

Letter 1

Background 4
Known K-12 Student Data Breaches Compromised a Range of Information and Exposed Students to Harm 9
Certain School Districts Disproportionately Experienced Reported Student Data Breaches 17
Agency Comments 21

Appendix I: GAO Contact and Staff Acknowledgments 23

Appendix II: Accessible Data 24

Data Tables 24

Table

Table 1: Types of Student Data Compromised in Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020 12

Figures

Figure 1: Characteristics of K-12 Student Data Breaches 5
Figure 2: Examples of Federal Resources That May Help Education Stakeholders Address Vulnerabilities and Ensure Data Security 8
Figure 3: Reported K-12 Student Data Breaches and the Number of School Districts Affected, July 1, 2016-May 5, 2020 10
Figure 4: Reported Number of K-12 Cybersecurity Student Data Breaches by Actor and Intent, July 1, 2016-May 5, 2020 14
Figure 5: Data System Involved in Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020 16
Figure 6: Student Enrollment in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020 18
Figure 7: Poverty Status in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020 19

Figure 8: Locale of K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020 20
Accessible Data for Responsible Actor and Intent of Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020 24
Accessible Data for Figure 1: Characteristics of K-12 Student Data Breaches 25
Accessible Data for Figure 2: Examples of Federal Resources That May Help Education Stakeholders Address Vulnerabilities and Ensure Data Security 26
Accessible Data for Figure 3: Reported K-12 Student Data Breaches and the Number of School Districts Affected, July 1, 2016-May 5, 2020 27
Accessible Data for Figure 4: Reported Number of K-12 Cybersecurity Student Data Breaches by Actor and Intent, July 1, 2016-May 5, 2020 28
Accessible Data for Figure 5: Data System Involved in Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020 29
Accessible Data for Figure 6: Student Enrollment in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020 30
Accessible Data for Figure 7: Poverty Status in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020 31
Accessible Data for Figure 8: Locale of K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020 32

Abbreviations

CCD	Common Core of Data
CISA	Cybersecurity and Infrastructure Security Agency
COPPA	Children's Online Privacy Protection Act
COVID-19	Coronavirus Disease 2019
CRC	K-12 Cybersecurity Resource Center
DHS	Department of Homeland Security
Education	Department of Education
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
FERPA	Family Educational Rights and Privacy Act
FRPL	free or reduced-price lunch

PII	personally identifiable information

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 15, 2020

The Honorable Virginia Foxx
Republican Leader
Committee on Education and Labor
House of Representatives

Dear Dr. Foxx:

Disclosing a student's personal information can potentially lead to physical, emotional, and financial harm. As schools and districts increasingly rely on technology and complex information technology systems for teaching, learning, and operating, they are collecting more student data electronically, including students' personally identifiable information (PII).[1] The 2017 Equifax breach, which compromised a significant portion of Americans' PII, highlighted organizations' vulnerability to data security risks.[2] The over 17,000 public school districts and approximately 98,000 public schools in the country are not immune to these risks. A cybersecurity incident is an event that actually or potentially jeopardizes a system or the information it holds, or that constitutes a threat to or violation of security policies, security procedures, or acceptable use policies. A student data breach is one type of cybersecurity incident in which K-12 student data are compromised. However, the extent of cybersecurity incidents is difficult to fully know or track because organizations may not be aware an incident has occurred, or may not report it if they are aware. When the Coronavirus Disease 2019 (COVID-19) pandemic forced the closures of schools across the nation and the sudden transition to distance learning, attention to

[1]PII includes any data that could potentially be used to identify a particular person, such as a Social Security number, full name, and birthdate.

[2]GAO has previously reported on the 2017 Equifax breach. For example, see GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach,* GAO-18-559 (Washington, D.C.: Aug. 30, 2018).

cybersecurity heightened, as notable incidents such as Zoom Bombing were widely reported.[3]

You asked us to review the security of K-12 students' data. This report examines (1) what is known about recently reported K-12 cybersecurity incidents that compromised student data, and (2) the characteristics of school districts that experienced these incidents.

To determine what is known about recent reported K-12 cybersecurity incidents that compromised student data, we analyzed data from July 2016 through early May 2020 from the K-12 Cybersecurity Resource Center (CRC).[4] CRC has tracked incidents in K-12 public schools reported in open sources that go back to reports from 2016. Experts and federal agency officials agree that CRC is the most complete resource that tracks K-12 cybersecurity incidents, including student data breaches. Further, while others' resources track incidents that occur in both elementary and secondary settings, as well as in higher education, CRC focuses specifically on K-12 schools.

We limited our analysis to incidents that are known to have compromised student data. For the purposes of this report, we refer to this type of incident as a student data breach. To analyze both the number of breaches that occurred and the number of school districts affected by them, as discerned from public reports, we treated student data breaches that occurred simultaneously or close together and involved the same actors as one breach.[5]

We determined the CRC data were sufficiently reliable for our purposes by checking individual data elements against public reports of incidents

[3]Zoom Bombing refers to disruptions of teleconferences and online classrooms, often with pornographic or hate images and threatening language. The term is derived from the Zoom videoconference platform, but is used to describe disruptions to videoconferences more generally.

[4]EdTech Strategies, the consultancy behind CRC, focuses on strategic research and counsel on issues at the intersection of education, public policy, technology, and innovation. EdTech Strategies' clients include non-profit organizations, associations, education and technology companies, school districts, and philanthropic and government leaders.

[5]In contrast, CRC generally assigns incidents to individual school districts regardless of whether an incident affects one school district or many. For example, in the case where the breach of a large vendor's data system affected at least 135 school districts, CRC counted this breach as 135 separate incidents, while we considered the incident to be one breach. For these reasons, our incident counts are lower than CRC's public counts.

and testing the data to identify outliers and obvious errors. We analyzed the CRC data to determine the types of student data compromised, the actor associated with the breach, the degree to which the breach was accidental or intentional, and the data system compromised for every reported breach. In some cases, these characteristics were unknown and we treated them as such in our analysis. In addition, we reviewed CRC documentation and interviewed CRC staff, including to resolve any errors or inconsistencies found from our testing. CRC data are non-generalizable to all schools and school districts as it is likely that there have been other student data breaches in addition to the ones identified by CRC. For example, some breaches go undetected, while others are not reported by media outlets and other open sources.

To analyze the characteristics of school districts that experienced student data breaches, we matched CRC's data to the Department of Education's (Education) Common Core of Data (CCD), which is the agency's primary database on public elementary and secondary education in the United States. Using the date the breach was recorded in the CRC data,[6] we matched the breach to the appropriate school year.[7] We examined the extent to which certain school district characteristics—locale, size, and poverty status—were over- or under-represented in CRC data compared to all K-12 school districts in the country. For locale, we classified districts as urban (city in CCD), suburban (suburban or town in CCD), or rural. We used student enrollment to measure the size of a school district. To measure poverty status, we used the percent of students in the district eligible for free or reduced-price lunch as a proxy.[8] We grouped school districts into quartiles based on the percent of students eligible. We determined the CCD data were sufficiently reliable for the purposes of this report by reviewing documentation and conducting electronic testing.

[6]Dating data breaches can be challenging because while the exact time a breach occurred can be identified for some breaches through monitoring and surveillance, others may have gone undetected for an undetermined period of time.

[7]Breaches recorded in school year 2019-2020 are matched to school year 2018-2019 data in the CCD, as these CCD data are the most recent available.

[8]The National School Lunch Program, administered at the federal level by the U.S. Department of Agriculture, provides reduced-cost or free lunches to eligible children in schools. Students are eligible for free lunches if their household income is at or below 130 percent of the federal poverty guidelines or if they meet certain other eligibility criteria, such as eligibility for the Supplemental Nutrition Assistance Program. Students are eligible for reduced-price lunch if their household income is between 130 percent and 185 percent of the federal poverty guidelines.

To answer both objectives, we spoke with K-12 privacy and cybersecurity experts about student data security. We interviewed officials from Education, the Federal Trade Commission (FTC), the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) to identify the role of federal agencies in securing K-12 students' data. We also reviewed (1) data security resources provided by federal agencies, (2) relevant federal laws and regulations, and (3) studies and reports published by researchers and student privacy stakeholder groups.

We conducted this performance audit from September 2019 to September 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

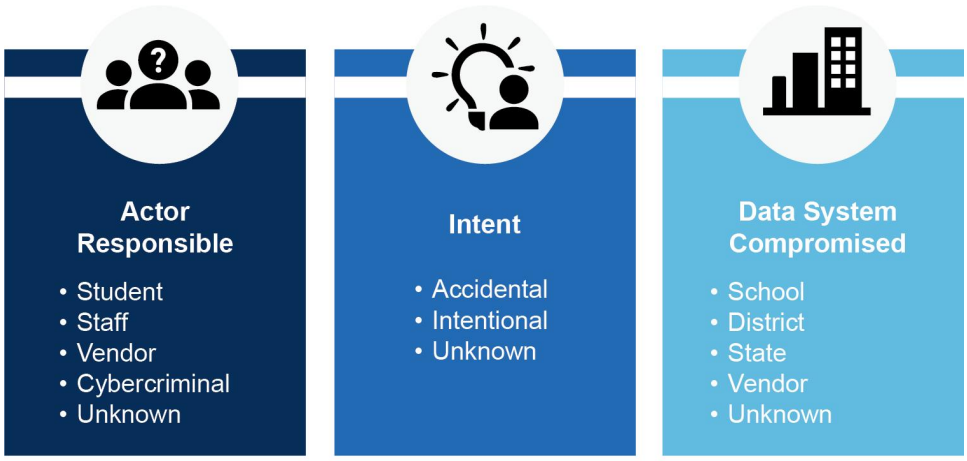
Background

K-12 Student Data Breaches

Schools, districts, states, and educational technology vendors collect and store a range of information about their students in various data systems, from grades, tests, and SAT or ACT scores, to addresses, telephone numbers, and emails, to Social Security numbers and medical information. A student data breach occurs when the confidentiality, integrity, or availability of these student data are compromised.

As figure 1 shows, the actor responsible for the breach, their intent, and the data system compromised can help in describing and understanding the nature and breadth of student data breaches. Depending on these three characteristics, a student data breach might affect a few students or all of the students in a school district.

Figure 1: Characteristics of K-12 Student Data Breaches



Source: GAO analysis. | GAO-20-644

Note: Other actors not indicated above may be responsible for student data breaches. The actors in the figure represent those identified in the breaches analyzed by GAO.

Various ways and reasons one might improperly gain access to student data include:

- Unauthorized access: an attempt to access, modify, or acquire data without consent. In a school district, this can range from students accessing a teacher's computer to change a grade to cybercriminals stealing thousands of students' personal information.
- Phishing: an attempt to acquire data or other resources through a fraudulent solicitation in email or on a website in which the actor pretends to be a reputable person or business.
- Ransomware: an attempt to block access to a data system until a fee is paid. In some instances, the attacker may gain access to the data, resulting in a data breach. They may also sell access to valuable student data to another malicious actor.

Federal Laws Governing Student Data Privacy and Data Security

Data privacy and data security are connected concepts. Data privacy is the process of appropriately limiting the collection, use, and handling of students' information and data security is the process of maintaining the confidentiality, integrity, and availability of student data by an

organization, such as a school district.[9] Federal privacy laws may address both data privacy and data security, or focus on either one. Two relevant federal laws pertain to protecting information about students and children: the Family Educational Rights and Privacy Act of 1974 (FERPA),[10] which focuses on data privacy, and the Children's Online Privacy Protection Act of 1998 (COPPA),[11] which addresses both privacy and data security.

- Education is responsible for enforcing FERPA, which addresses the privacy of PII in student education records and applies to all schools that receive funds under an applicable program administered by Education. If parents or eligible students believe that their rights under FERPA have been violated, they may file a formal complaint with Education. In response, Education is required to take appropriate actions to enforce and deal with violations of FERPA. However, because the department's authority under FERPA is directly related to the privacy of education records, Education's security role is limited to incidents involving potential violations under FERPA. Further, FERPA amendments have not directly addressed educational technology use.
- COPPA requires the FTC to issue and enforce regulations concerning children's privacy. The COPPA Rule, which took effect in 2000 and was later amended in 2013,[12] requires operators of covered websites or online services that collect personal information from children under age 13 to provide notice and obtain parental consent, among other things. COPPA generally applies to the vendors who provide educational technology, rather than to schools directly. However, according to FTC guidance, schools can consent on behalf of parents to the collection of students' personal information if such information is used for a

[9]This process is to be conducted in a manner consistent with the organization's risk strategy. Further, preventing unauthorized access, data corruption, and denial of service attacks are all important tenets of data security. For more information, see National Cybersecurity Center of Excellence, National Institute of Standards and Technology, *Data Security*, accessed June 12, 2020, https://www.nccoe.nist.gov/projects/building-blocks/data-security.

[10]20 U.S.C. § 1232g.

[11]15 U.S.C. §§ 6501-6506.

[12]The COPPA Rule is codified at 16 C.F.R. Part 312.

school-authorized educational purpose and for no other commercial purpose.[13]

Federal Resources Supporting Student Data Security

Several federal agencies provide resources to schools, districts, or education technology vendors that may help them prevent and respond to student data breaches.[14] For example, Education's Student Privacy Policy Office, through its Privacy Technical Assistance Center, offers resources focused on privacy protections under FERPA and promoting data security best practices. These resources include a series of case studies to illustrate how specific provisions of FERPA may be implemented. One case study provides best practices for minimizing access to sensitive information, including data minimization. Data minimization is the practice of collecting only PII that is directly relevant and necessary to accomplish the specified purpose, retaining it just for as long as necessary, and restricting its access to those with a legitimate need.[15]

In addition, Education offers a series of tabletop exercises designed to help educational organizations train staff about data incidents and breaches.[16] One training simulates an incident in which a teacher leaves log-in information on his desk, and students discover the note and access the system to change grades. These case studies and exercises may help highlight for district management the need to properly plan for protection of PII and avoid a data breach, and to illustrate the processes, procedures, and skills needed to respond (see fig. 2).

[13]When schools provide consent on behalf of parents under COPPA, there may be FERPA implications as well. However, an exception to FERPA, known as the "school official exception," generally applies. This exception permits the disclosure of PII from education records, without parental consent, to vendors with whom schools have outsourced institutional services or functions. The exemption also includes restrictions on vendors' use and disclosure of PII.

[14]In addition to Education, FTC, DHS and FBI also provide resources to education stakeholders. Within DHS, the Cybersecurity and Infrastructure Security Agency is the lead agency addressing cybersecurity issues.

[15]Privacy Technical Assistance Center, U.S. Department of Education, *Case Study #5: Minimizing Access to PII: Best Practices for Access Controls and Disclosure Avoidance Techniques* (Washington, D.C.: revised July 2015).

[16]Privacy Technical Assistance Center, U.S. Department of Education, *Data Breach Scenario Trainings* (Washington, D.C.: January 2020).

Figure 2: Examples of Federal Resources That May Help Education Stakeholders Address Vulnerabilities and Ensure Data Security

Vulnerability	Example of an available resource
Staff inadvertently disclose sensitive data or personally identifiable information (PII) in an email.	The **Department of Education's** best practices for raising data security awareness and its trainings detail how those who have access to PII should be trained to protect data confidentiality and preserve system security. For example, the best practices suggest trainings could cover good email practices for keeping data secure. They also suggest minimizing the amount of student data retained and destroying them when no longer needed to lessen the potential harms in the event of a data breach.
Vendors misconfigure systems.	The **Federal Trade Commission's** "Start with Security" guide includes discussion and examples of proper configuration of systems, as well as other strategies that can help ensure the security of information systems and other applications.
A school district is uncertain about how effective its cybersecurity programs and initiatives are and what could be done to strengthen them.	The **Cybersecurity and Infrastructure Security Agency**, which is within the Department of Homeland Security, sponsors the Nationwide Cyber Security Review (NCSR). The NCSR is offered by both the Multi-State Information Sharing and Analysis Center (ISAC) and the Elections Infrastructure ISAC, which the Department of Homeland Security funds as part of a cooperative agreement. It is a no-cost, annual self-assessment that helps school districts, as well as other state and local entities, assess the effectiveness and measure gaps of their cybersecurity programs and initiatives.
School districts and educational technology vendors, among others, are unaware of a growing cybersecurity threat.	The **Federal Bureau of Investigation** (FBI) issues occasional notices to warn education stakeholders about specific cybersecurity threats. For example, in September 2018, the FBI issued a notice for school districts and the education industry on cybersecurity threats and considerations to protect students and their data. Additionally, the FBI investigates cyber incidents, when deemed appropriate.

Source: GAO analysis of federal documents, interviews with federal agency officials, and K-12 Cybersecurity Resource Center data. | GAO-20-644

Note: The examples of resources provided are not exhaustive, and other federal resources may help address data security vulnerabilities.

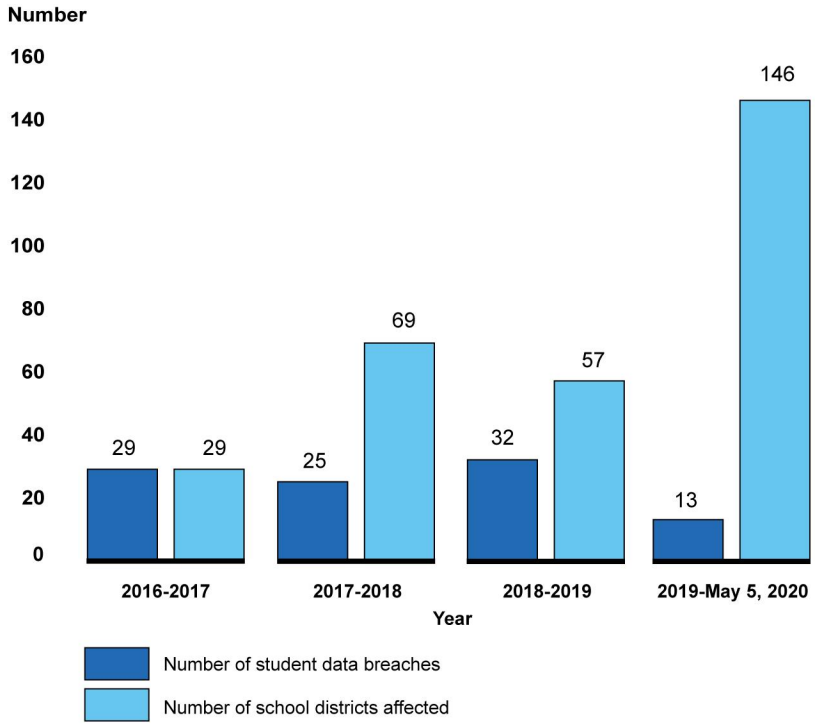
Known K-12 Student Data Breaches Compromised a Range of Information and Exposed Students to Harm

Ninety-Nine Reported K-12 Student Data Breaches Affected Thousands of Students across 287 School Districts

Ninety-nine student data breaches reported from July 1, 2016 through May 5, 2020 compromised the data of students in 287 school districts across the country, according to our analysis of CRC data (see fig. 3).[17] Some breaches involved a single school district, while others involved multiple districts. For example, an attack on a vendor system in the 2019-2020 school year affected 135 districts. While information about the number of students affected was not available for every reported breach, examples show that some breaches affected thousands of students, for instance, when a cybercriminal accessed 14,000 current and former students' PII in one district.

[17]The details of a breach, like whether and what kind of student data were compromised or the actor responsible, might not be included in public reports of the incident, either because they are unknown or a district has chosen not to disclose some information.

Figure 3: Reported K-12 Student Data Breaches and the Number of School Districts Affected, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Notes: The school years in the figure start July 1 and end June 30 with the exception of 2019-2020, which reflects reported breaches through May 5, 2020, 2 months less than the other years.

The jump in the number of school districts affected by breaches in the 2019-2020 school year is due to one breach that affected 135 districts.

The total number of school districts in the figure exceeds 287, as 14 experienced a breach in more than one school year.

The 99 reported student data breaches likely understate the number of breaches that occurred, for different reasons. Reported incidents sometimes do not include sufficient information to discern whether data were breached. We identified 15 additional incidents in our analysis of CRC data in which student data might have been compromised, but the available information was not definitive. In addition, breaches can go undetected for some time. In one example, the personal information of hundreds of thousands of current and former students in one district was publicly posted for 2 years before the breach was discovered.

More recently, as almost all schools and districts transitioned to online learning to slow the spread of COVID-19, reports of student data breaches have continued and additional cybersecurity challenges

emerged in April and May 2020 (see text box). CRC reported at least one incident in May involving distance learning technology that may have resulted in student data being compromised. In the incident, a teacher shared an image with her students that inadvertently included her login and password for a data management tool, and a student used it to gain unauthorized access to the system.

CRC reports of other kinds of cybersecurity incidents, for example, phishing, declined during this time period. One explanation provided by experts is that while at home, some students and teachers do not have their laptops, tablets, or other devices connected to school networks as they usually do when physically present at school. This provides some level of protection as phishing and other risks are confined to an individual's device. Experts warn that when devices are reconnected to school networks, they could introduce risks to school and district systems that could result in data breaches.

COVID-19 and the Transition to Distance Learning Have Presented Additional Cybersecurity Challenges for School Districts

The K-12 Cybersecurity Resource Center (CRC) identified 28 incidents involving videoconferences from April 1, 2020 through May 5, 2020, some of which disrupted learning and exposed students to harm. In one incident, 50 elementary school students were exposed to pornography during a virtual class. In another incident in a different district, high school students were targeted with hate speech during a class, resulting in the cancellation that day of all classes using the videoconferencing software. These incidents also raise concerns about the potential for violating students' privacy. For example, one district is reported to have instructed teachers to record their class sessions. Teachers said that students' full names were visible to anyone viewing the recording.

Some federal agencies have established resources to help districts address evolving cybersecurity challenges related to distance learning. For example, in May 2020, the Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security, issued recommendations for schools using videoconferencing and other online platforms.[a] These recommendations included adopting practices to limit the number of authorized collaboration tools to reduce overall vulnerability; reviewing and updating security settings continuously; and preventing use of collaboration tools while logged on with administrative privileges. The Federal Bureau of Investigation (FBI) also issued a statement in March 2020 on cyber threat issues due to increased use of virtual environments, including for education.[b]

Source: GAO analysis of K-12 Cybersecurity Resource Center data, CISA recommendations, and FBI statements. | GAO-20-644

[a]Cybersecurity and Infrastructure Security Agency, Cybersecurity Recommendations for K-12 Schools Using Video Conferencing Tools and Online Platforms (Washington, D.C.: May 13, 2020).

[b]Federal Bureau of Investigation. FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic (Boston, MA: March 30, 2020).

Reported K-12 Student Data Breaches Compromised Various Types of Student Data and Were Both Intentional and Accidental

Types of Student Data Breached

Student data breaches compromised a range of student data collected by schools, districts, vendors, and states, according to our analysis of CRC data (see table 1). Academic records, like assessment scores and special education records, were the most common type of data compromised (58 breaches) followed by student PII, such as Social Security numbers and birthdates (36 breaches). Nineteen breaches are known to have compromised student data, but specifics about the types of data compromised are unknown, either because this was unclear to the district, public reports did not include this information, or districts decided not to share it in reports.

Table 1: Types of Student Data Compromised in Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020

Type of student data[a]	Information included in type	Number of breaches (out of 99 reported breaches)[b]
Academic records	Grades, test or assessment results, student identification number, special education record, discipline record, suspension record, bullying incident information, reasons for absences, English Language Learner status, attendance record, assigned counselor, legal notices, schools attended, transfer information, digital images and videos, teacher assignments	58
Student personally identifiable information	Name, birthdate, Social Security number, partial Social Security number, driver's license number, other government identification number	36
Directory/other personal information	Nickname, email address, address, phone number, grade level, parent name, parent email address, parent address, parent phone number	35
Unknown[c]		19
Logins, passwords, or other restricted information	Login information, locker combination, lunch accounts, financial account information	11
Health or medical information[d]	Medical records, vaccination records, insurance information	8
Information related to physical location	Schedule, physical school information, bus stop times, bus pickup location, bus dropoff location	7
Demographic information	Gender, ethnicity, race, languages, housing status, other	7
Other	Other information or records	6

Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

[a]GAO created these categories for the purposes of our analysis. They are distinct from the Family Educational Rights and Privacy Act (FERPA) definition of an "education record."

[b]Student data breaches do not sum to 99. Some breaches compromised more than one kind of student data, so the totals exceed 99. Not every data element listed under information included in type w as compromised in each breach involving the type.

[c]These include incidents in w hich the district is unsure of the exact data that w ere breached, public reports did not include this information, or districts decided not to share it in reports.

[d]We did not analyze the extent to w hich these breaches exposed data protected by the Health Insurance Portability and Accountability Act.

Access to or disclosure of some of the types of data collected by K-12 institutions can harm students, including their financial well-being. According to our analysis of CRC data, 22 of the 36 reported breaches that exposed students' PII included full or partial Social Security numbers, or names and birthdates. Financial and cybersecurity experts say this kind of information can be sold on the black market and can cause significant financial harm to students who typically have clean credit histories and often do not inquire about their financial status until adulthood. Data breaches can also cause students physical and emotional harm (see text box). For example, for students with an Individualized Education Program (IEP), disclosure of special education status, annual goals, or medical diagnoses contained in these records could lead to embarrassment or stigmatization.[18]

Disclosures of Data Can Harm Students' Physical and Emotional Well-Being

When a high school survey that asked students to identify bullies or their victims was inadvertently shared by staff in one data breach, students and teachers feared becoming targets of reprisals. In another breach, cybercriminals targeted several district servers and accessed student data, including phone numbers, which were used to send text messages that threatened physical violence. One targeted district was very small, and students' locations could have been easily determined.

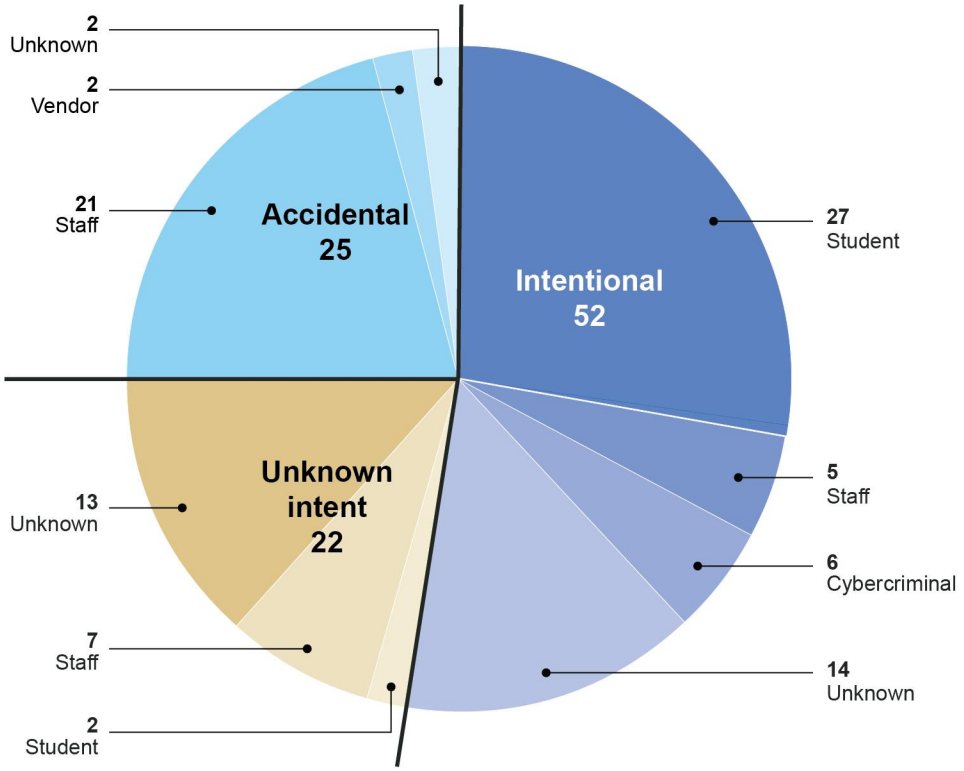
Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Intent and Actors Responsible

Breaches were perpetrated by different actors, some with nefarious intent and some who did so accidentally. More than half of the reported breaches were intentional and a quarter were accidental (see fig. 4).

[18]An Individualized Education Program (IEP), which is required for certain students under the Individuals with Disabilities Act, is a written statement developed by a team composed of a student's teachers, parents, school district officials, the student (if appropria te), and, at the discretion of the parent or district, other individuals who have knowledge or special expertise regarding the student. The IEP includes, among other information, a statement of the child's present levels of academic achievement and functio nal performance, annual goals, and a statement of the special education and related services and supplementary aids and services needed to attain those goals. 20 U.S.C. § 1414(d).

Figure 4: Reported Number of K-12 Cybersecurity Student Data Breaches by Actor and Intent, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Notes: The actor responsible for a breach or the intent may be unknown from the details provided in public reports.

For this analysis, a cybercriminal is defined as an actor external to the school district who breaches a data system for malicious reasons.

When the breach was intentional, students were more often responsible (27 of 52 breaches), with grade changes the most common motive (16 breaches). When the breach was accidental, staff were more often responsible (21 of 25 breaches). There were a variety of ways students gained access to grading systems and staff accidentally disclosed student data (see text box).

Students and Staff are Most Commonly Responsible for K-12 Student Data Breaches

Students used a variety of methods to gain access to grading systems, including exploiting vulnerabilities, gaining access to teachers' login information, and sending phishing emails to staff. In one breach, high school students hacked into the school system and changed their grades, attendance records, and lunch account balances. In another, a high school student raised his own grades and lowered those of other students.

Staff accidentally disclosed student data in different ways, including by emailing it to the wrong recipients and posting private data to public files or websites. In one breach, 2,000 homeless students' names, birthdates, housing status, and eligibility for special education or English Language Learner services were mistakenly posted on a public website for 6 months. In another accidental breach, a district inadvertently emailed the addresses, phone numbers, state identification numbers, and locker combinations of over 1,000 high school students to the wrong recipients.

Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Though reports of breaches by cybercriminals or by vendor error were rare, those breaches affected large numbers of students, sometimes across multiple districts, and some cybercriminals targeted students in attempts to steal PII (see text box). Cybercriminals were responsible for six of the 99 reported breaches, all of which were intentional, and educational technology vendors were responsible for two reported breaches, both accidental.

Thousands of Students Can Be Harmed by Breaches Caused by Cybercriminals or by Vendor Errors

In one reported breach, a cybercriminal accessed the personally identifiable information (PII) and test scores of 14,000 current and former students. In another, international cybercriminals targeted at least four school districts, including one of the largest districts in the country, to try and steal personal information. It is unknown what student data they were able to access. In one accidental vendor disclosure caused by incorrectly configured settings, the PII of high school students in at least 27 school districts was exposed, including names, birthdates, partial Social Security numbers, email addresses, and addresses.

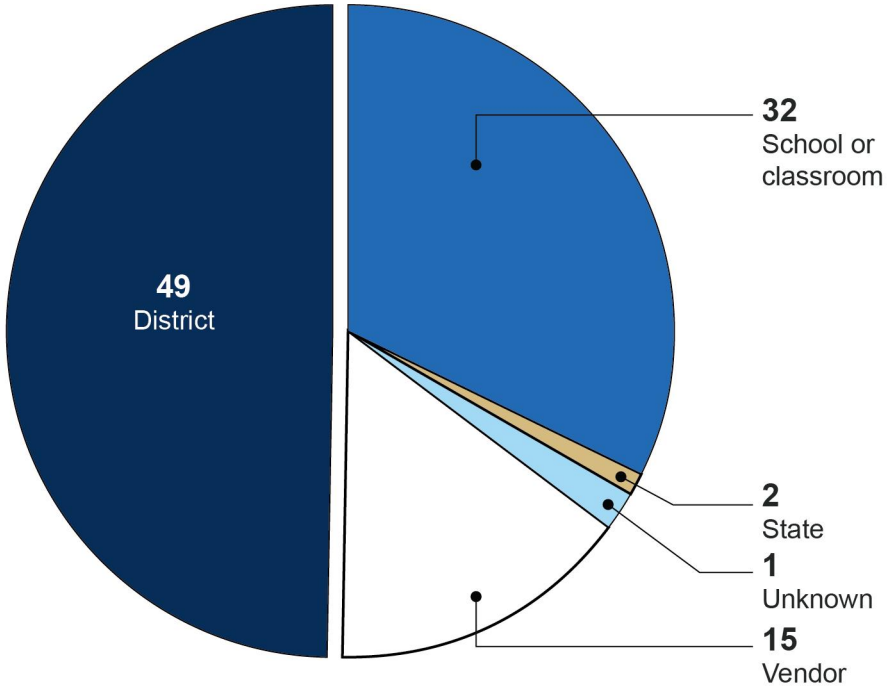
Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

In about one-quarter of the 99 known breaches (22) the intent was unknown, as was the actor in almost one-third (29). This may have been because districts do not have this information or decided not to publicly share these details.

Data System Compromised

Breaches of district and school or classroom data systems were the most common, followed by vendor systems (see fig. 5).[19] Nearly half of student data breaches (49) involved district data systems, and a third (32) involved school or classroom data systems. Vendor systems were involved in 15 breaches.

Figure 5: Data System Involved in Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Note: For GAO's analysis, the data system involved is defined as the level at which the vulnerability exploited in the breach needs to be corrected to prevent further breaches.

While data breaches involving vendor or state data systems were fairly rare, the impact can be severe. For example, five of the 15 breaches that involved vendor systems affected more than one district, with one

[19]Identifying the data system involved in a breach can be ambiguous, for example, when the breach occurs in one classroom but involves educational technology provided by a vendor. For GAO's analysis, the data system involved is defined as the level at which the vulnerability exploited in the breach needs to be corrected to prevent further breaches.

potentially compromising the PII of students in at least 135 school districts (see text box).

Breaches of Vendor and State Data Systems Can Expose the Information of Large Numbers of Students

Educational technology vendors typically have many school districts using their products. As a result, a vulnerability in the technology that leads to a data breach can affect thousands of students. In one breach by an unknown actor, a learning assessment platform exposed the personally identifiable information (PII) of students with accounts, including their names and birthdates. The incident is estimated to have affected 13,000 K-12 school districts and universities; the K-12 Cybersecurity Resource Center identified 135 K-12 school districts affected by this breach.

State data systems similarly store the data of students from many school districts. A ransomware attack that affected a state employee's laptop compromised the data of students in at least 35 school districts. PII, including names, birthdates, and Social Security numbers, were among the data accessed by the unknown perpetrator of the attack. The information of at least 700 students is believed to have been exposed.

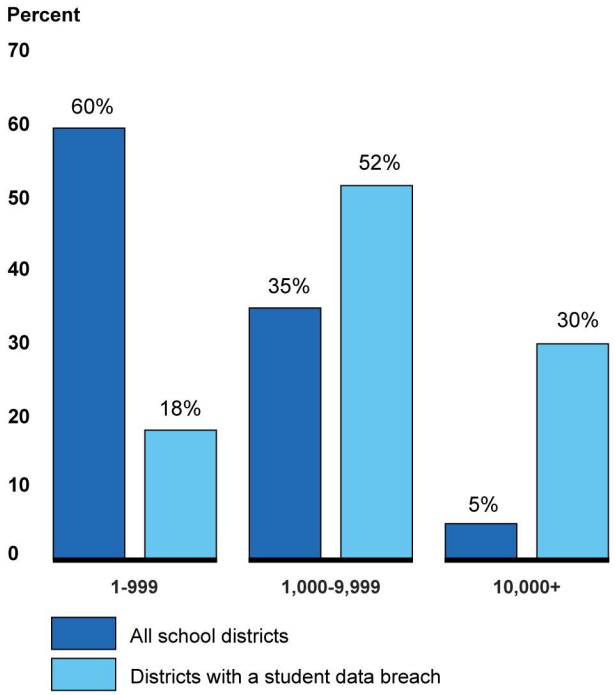
Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Certain School Districts Disproportionately Experienced Reported Student Data Breaches

Of the 287 school districts with reported student data breaches from July 1, 2016 through May 5, 2020, larger, wealthier, and suburban school districts were disproportionately represented, according to our analysis of CRC data that was matched to school district characteristics in the CCD.

Larger districts had disproportionately more reported data breaches than smaller districts (see fig. 6). Further, schools with over 2,500 students accounted for 66 percent of all breaches and four of the five largest school districts in the country (all with over 100,000 students) reported a breach during our time frame.

Figure 6: Student Enrollment in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020



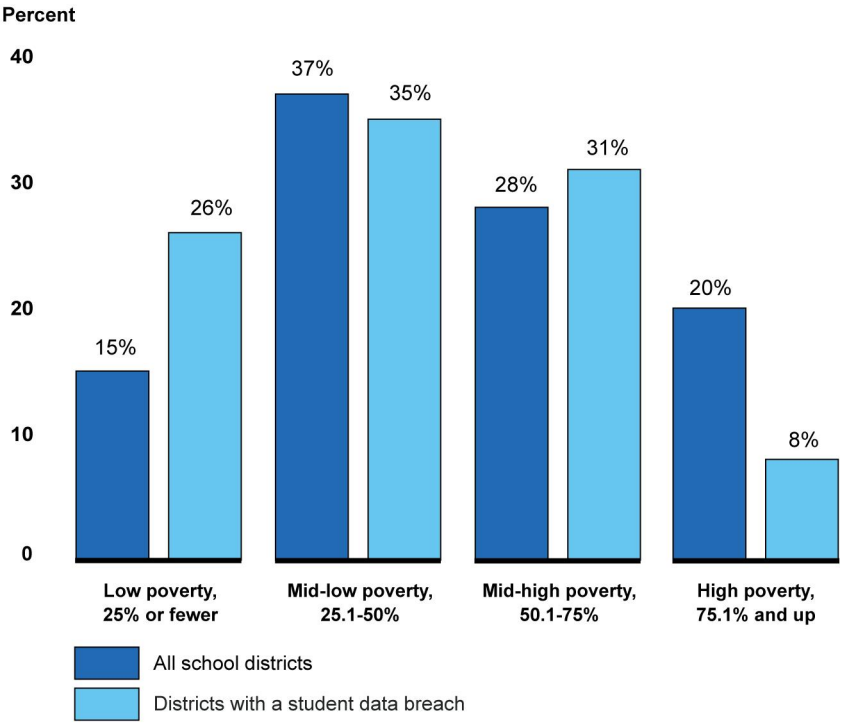
Source: GAO analysis of K-12 Cybersecurity Resource Center data and the Department of Education's Common Core of Data. | GAO-20-644

Note: Enrollment data were not available for six of the 287 school districts with reported data breaches. For districts with a student data breach, enrollment data are from the year the breach was reported; for all other school districts, the most recent year of data are used.

Wealthier districts had disproportionately more reported data breaches (see fig. 7). These districts—those with 25 percent or fewer students eligible for free or reduced-price lunch (FRPL)—accounted for 26 percent of reported breaches, although they made up 15 percent of all districts nationwide.[20]

[20]CRC analyzes the poverty status of school districts using a different measure, the U.S. Census Bureau's Small Area Income and Poverty Estimates.

Figure 7: Poverty Status in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020

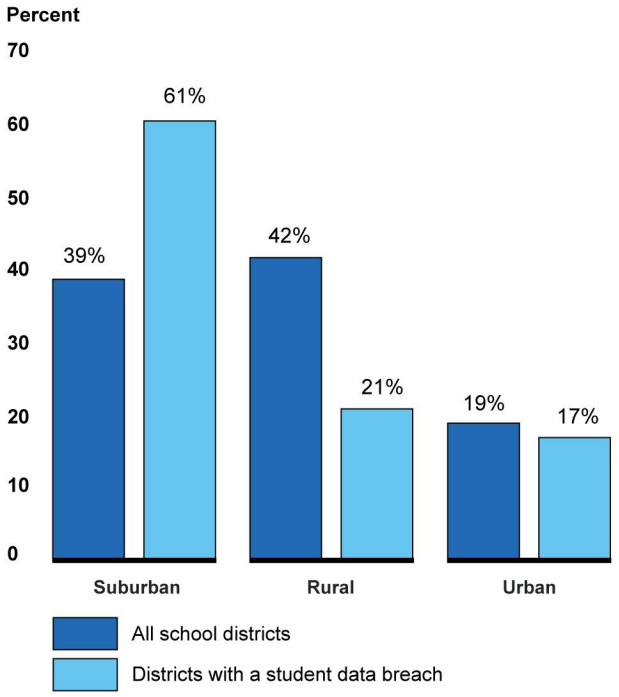


Source: GAO analysis of K-12 Cybersecurity Resource Center data and the Department of Education's Common Core of Data. | GAO-20-644

Note: Poverty status is measured by the percentage of students eligible for free or reduced-price lunch (FRPL). FRPL data were not available for 15 of the 287 school districts with reported data breaches. For districts with a student data breach, FRPL data are from the year the breach was reported; for all other school districts, the most recent year of data are used.

Suburban districts also had disproportionately more reported data breaches, comprising 61 percent of districts with breaches, although they made up 39 percent of all school districts (see fig. 8). Conversely, rural districts comprised 21 percent of districts with reported breaches although they made up 42 percent of all school districts.

Figure 8: Locale of K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020



Source: GAO analysis of K-12 Cybersecurity Resource Center data and the Department of Education's Common Core of Data. | GAO-20-644

Note: Locale data were not available for four of the 287 school districts with reported data breaches. For districts with a student data breach, locale data are from the year the breach was reported; for all other school districts, the most recent year of data are used.

Experts we spoke to provided potential explanations for why larger, wealthier, and suburban school districts had disproportionately more reported data breaches. One expert said that larger school districts are typically a more advantageous target than smaller ones: a school district with 500 staff has 500 potential targets for a breach, whereas a district with 50 staff has 50 potential targets. It is more likely that 1 of 500 people who receive a malicious link in a phishing email will click on it than 1 of 50. Similarly, experts said that wealthier and suburban districts tend to use more technology in schools, providing more opportunities for breaches to occur.

Reporting bias also emerged as a potential explanation from experts for higher reported incidents in these kinds of school districts. Overall, districts with the resources to identify breaches may more commonly report them. Two experts said larger districts are also more likely to have dedicated staff, such as a Chief Technology Officer, monitoring and

reporting breaches. Experts also said wealthier and suburban districts might have parents more engaged in technology and data practices who help identify and publicly report breaches. These communities might also have local news media more likely to report on K-12 data security.[21]

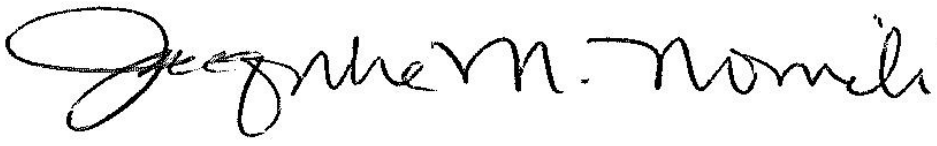
Agency Comments

We provided a draft of this report for review and comment to the Departments of Education, Homeland Security, and Justice and to the Federal Trade Commission. The Department of Homeland Security provided technical comments, which we incorporated as appropriate. The Departments of Education and Justice and the Federal Trade Commission provided no comments.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Education, the Acting Secretary of Homeland Security, the Attorney General, and the Chairman of the Federal Trade Commission. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (617) 788-0580 or nowickij@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix I.

Sincerely yours,



[21]There can be overlap between the three district characteristics that were disproportionately represented in districts with breaches, compared to all school districts, particularly poverty status and locale. Our analysis of CCD data indicates that 52 percent of wealthier districts in the U.S. with 25 percent or fewer of students eligible for free or reduced-price lunch are also classified as suburban.

Jacqueline M. Nowicki, Director
Education, Workforce, and Income Security Issues

Appendix I: GAO Contact and Staff Acknowledgments

GAO Contact

Jacqueline M. Nowicki, Director, (617) 788-0580 or nowickij@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Sherri Doughty (Assistant Director), Jennifer Gregory (Analyst in Charge), and Jessica Mausner made key contributions to this report. Susan Aschoff, Elizabeth Calderon, John de Ferrari, Sheila R. McCoy, John Mingus, Jr., Almeta Spencer, Curtia Taylor, and Walter Vance provided additional support.

Appendix II: Accessible Data

Data Tables

Accessible Data for Responsible Actor and Intent of Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020

Category	Cybercriminal	Staff	Student	Vendor	Unknown
Accidental	0	21	0	2	2
Intentional	6	5	27	0	14
Unknown intent	0	7	2	0	13

Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Accessible Data for Figure 1: Characteristics of K-12 Student Data Breaches

Actor Responsible

- Student
- Staff
- Vendor
- Cybercriminal
- Unknown

Intent

- Accidental
- Intentional
- Unknown

Data System Compromised

- School
- District
- State
- Vendor
- Unknown

Source: GAO analysis. | GAO-20-644

Accessible Data for Figure 2: Examples of Federal Resources That May Help Education Stakeholders Address Vulnerabilities and Ensure Data Security

Vulnerability	Example of an available resource
Staff inadvertently disclose sensitive data or personally identifiable information (PII) in an email.	The Department of Education's best practices for raising data security awareness and its trainings detail how those who have access to PII should be trained to protect data confidentiality and preserve system security. For example, the best practices suggest trainings could cover good email practices for keeping data secure. They also suggest minimizing the amount of student data retained and destroying them when no longer needed to lessen the potential harms in the event of a data breach.
Vendors misconfigure systems.	The Federal Trade Commission's "Start with Security" guide includes discussion and examples of proper configuration of systems, as well as other strategies that can help ensure the security of information systems and other applications.
A school district is uncertain about how effective its cybersecurity programs and initiatives are and what could be done to strengthen them.	The Cybersecurity and Infrastructure Security Agency, which is within the Department of Homeland Security, sponsors the Nationwide Cyber Security Review (NCSR). The NCSR is offered by both the Multi-State Information Sharing and Analysis Center (ISAC) and the Elections Infrastructure ISAC, which the Department of Homeland Security funds as part of a cooperative agreement. It is a no-cost, annual self-assessment that helps school districts, as well as other state and local entities, assess the effectiveness and measure gaps of their cybersecurity programs and initiatives.
School districts and educational technology vendors, among others, are unaware of a growing cybersecurity threat.	The Federal Bureau of Investigation (FBI) issues occasional notices to warn education stakeholders about specific cybersecurity threats. For example, in September 2018, the FBI issued a notice for school districts and the education industry on cybersecurity threats and considerations to protect students and their data. Additionally, the FBI investigates cyber incidents, when deemed appropriate.

Source: GAO analysis of federal documents, interviews with federal agency officials, and K-12 Cybersecurity Resource Center data. | GAO-20-644

Accessible Data for Figure 3: Reported K-12 Student Data Breaches and the Number of School Districts Affected, July 1, 2016-May 5, 2020

Year	Number of student data breaches	Number of school districts affected
2016-2017	29	29
2017-2018	25	69
2018-2019	32	57
2019-May 5, 2020	13	146

Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Accessible Data for Figure 4: Reported Number of K-12 Cybersecurity Student Data Breaches by Actor and Intent, July 1, 2016-May 5, 2020

Intentional, 52

- Student, 27
- Staff, 5
- Cybercriminal, 6
- Unknown, 14

Unknown intent, 22

- Student, 2
- Staff, 7
- Unknown, 13

Accidental, 25

- Staff, 21
- Vendor, 2
- Unknown, 2

Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Accessible Data for Figure 5: Data System Involved in Reported K-12 Student Data Breaches, July 1, 2016-May 5, 2020

- School or classroom, 32
- State, 2
- Unknown, 1
- Vendor, 15
- District, 49

Source: GAO analysis of K-12 Cybersecurity Resource Center data. | GAO-20-644

Accessible Data for Figure 6: Student Enrollment in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020

Category	All school districts	District with a student data breach
1-999	60%	18%
1,000-9,999	35%	52%
10,000+	5%	30%

Source: GAO analysis of K-12 Cybersecurity Resource Center data and the Department of Education's Common Core of Data. | GAO-20-644

Accessible Data for Figure 7: Poverty Status in K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020

Category	All school districts	Districts with a student data breach
Low poverty, 25% or fewer	15%	26%
Mid-low poverty, 25.1-50%	37%	35%
Mid-high poverty, 50.1-75%	28%	31%
High poverty, 75.1% and up	20%	8%

Source: GAO analysis of K-12 Cybersecurity Resource Center data and the Department of Education's Common Core of Data. | GAO-20-644

Accessible Data for Figure 8: Locale of K-12 School Districts with Reported Student Data Breaches Compared to all U.S. School Districts, July 1, 2016-May 5, 2020

Category	All school districts	Districts with a student data breach
Suburban	39%	61%
Rural	42%	21%
Urban	19%	17%

Source: GAO analysis of K-12 Cybersecurity Resource Center data and the Department of Education's Commo

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548