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.

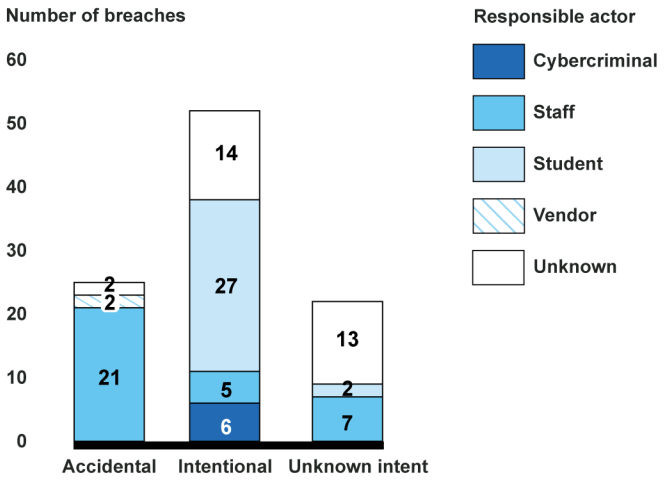
GAO analyzed data from July 1, 2016 to May 5, 2020 from CRC (the most complete source of information on K-12 data breaches). CRC is a non-federal resource sponsored by an educational technology organization that has tracked reported K-12 cybersecurity incidents since 2016. GAO also analyzed 2016-2019 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.