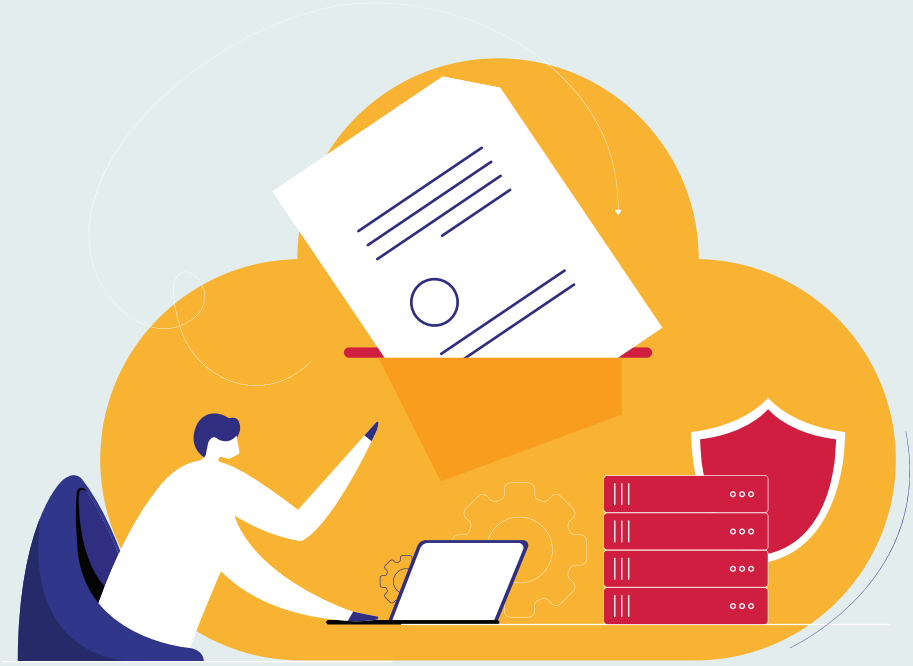
EdWeek Research Center

Managed Methods



—Getty

What You Don't Know Can Hurt You

New survey identifies gaps in K-12 cloud security

EXECUTIVE SUMMARY

The remote learning necessitated by the pandemic led to an explosion in the amount of educational technology. But results of a new survey conducted by the EdWeek Research Center and commissioned by ManagedMethods, a cloud application security and student safety monitoring platform, suggests that district-level ed-tech decision makers may lack the information and resources they need to adequately protect their data, especially when it comes to cloud collaboration and storage applications. Although the influencers expressed high levels of confidence in their cybersecurity, half either did not have a security system that protected cloud applications, or did not know whether such a system had been implemented. All of the 214 district-level administrators who responded said they had at least a medium level of influence over ed-tech decision making, raising questions about whether they have the information they need to determine the protections necessary for human resources, financial, and student learning platforms that have migrated to the cloud. Despite the pervasiveness of cloud platforms, which 94 percent of leaders said were used by their districts, the typical respondent will invest just $4,000, or 20 percent of the total cybersecurity budget, in monitoring and securing them. The survey results suggest the need for district ed-tech influencers to gather more information and reconsider the resources and methods used to protect their data and stakeholders.

Introduction

In Lodi, California, a cybersecurity attack brought school phones down for days.

A massive data breach in a school district in Toledo, Ohio resulted in the theft of personal information, which was subsequently used to take out credit cards and car loans in children's names.

And in Broward County, Florida, hackers published nearly 26,000 stolen files online because the school district did not pay $40 million in ransom.

These are just a few of the cybersecurity incidents that occurred in the past year in American schools and they are the tip of the iceberg: A 2021 report by the EdTech Strategies/K-12 Cybersecurity Resource Center and the K12 Security Information Exchange identified 408 publicly-reported incidents in 2020, which was 18 percent higher than in 2019 (additional incidents may have occurred, but were not detected or disclosed). With the coronavirus pandemic, the cybersecurity threat potential increased exponentially as schools rushed to move operations and learning online and into the cloud in an effort to limit in-person contact that could spread the disease. For instance, between March 2020 and July 2021, 53 percent of district leaders reported that their school districts had implemented 1:1 programs (one computer per student) for the first time, according to an EdWeek Research Center survey conducted for Education Week. Forty-three percent said they had introduced technology-based learning platforms such as Blackboard or Moodle. And 31 percent said their districts had started using adaptive learning software to personalize student instruction.

In the summer of 2021, ManagedMethods, a cloud application security and student safety monitoring platform designed for education, commissioned the EdWeek Research Center to conduct an online survey to explore how school districts were coping with cybersecurity, safety, and data privacy challenges while navigating their new learning environments. The respondents were 214 district-level administrators who identified themselves as having at least a medium level of influence on technology decisions.

About the Survey

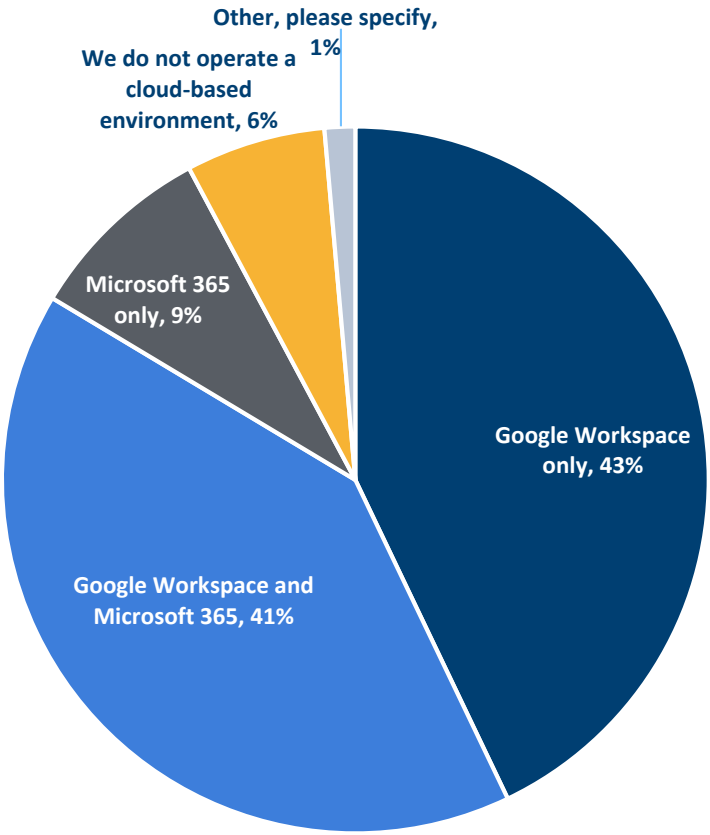
Who: 214 district-level administrators who identified themselves as having at least a medium level of influence on technology decisions, including 54 technology officers, 52 district superintendents, and 30 curriculum and instruction directors

What: A nationally representative, 31-question survey

When: July 14th-September 15th, 2021

Where: The survey was administered online

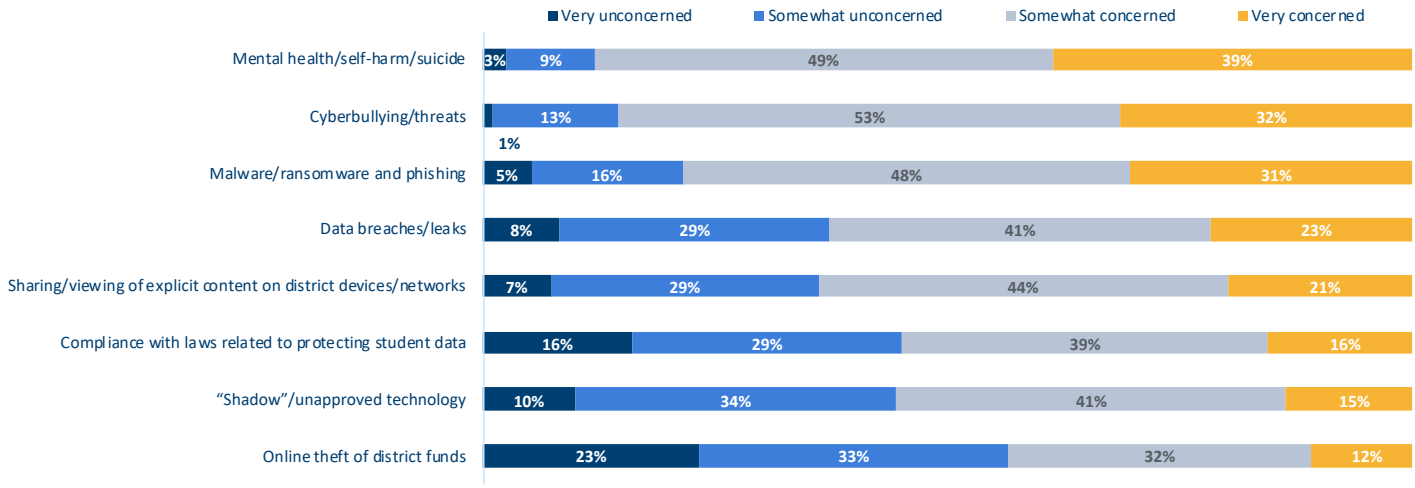
Which cloud-based environment does your district operate?



District Leaders Believe Their Data is Safe

Despite their heavy reliance on cloud systems, online privacy and safety are not major concerns for these ed-tech influencers. Just 23 percent are very concerned about data breaches and leaks. Sixteen percent are very concerned about compliance with state and federal laws that protect student data. Twenty-one percent are very concerned about the sharing or viewing of explicit content on district devices.

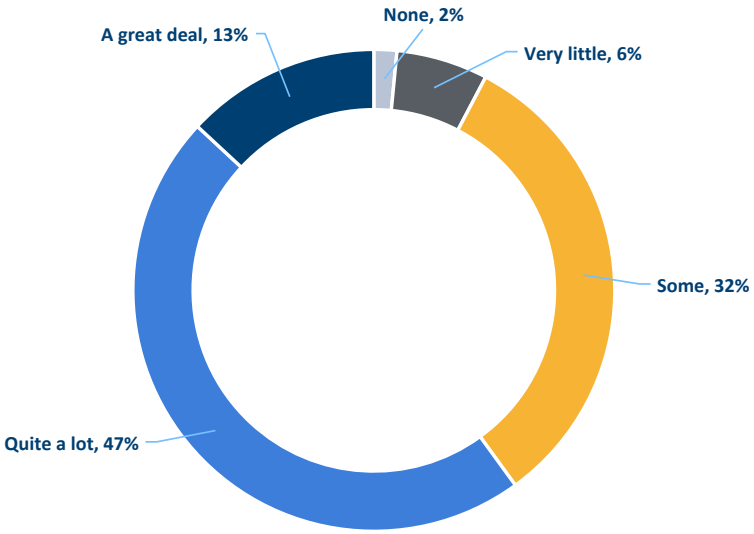
How concerned are you about the following types of cybersecurity/online safety issues in your school district?



One reason for their relative lack of concern may be that these leaders express high levels of confidence in the safety of their cloud environments. Sixty percent say they have a great deal or quite a lot of confidence in the privacy and security of data stored in their cloud applications, the most common of which are Google Workspace and Microsoft 365. Conversely, 8 percent have very little or no confidence that these environments are secure.

Google Workspace for Education Enterprise Edition is the platform leaders are most likely to use to protect the data stored in their Google Workspace domain, followed by Google Workspace for Education Standard Edition.

How much confidence do you have that your district's cloud data stored in Google Drive, Microsoft OneDrive/ SharePoint, Dropbox, Box, etc. is private and secure?



District Leaders May Be Unaware of Cloud-based Cybersecurity Threats

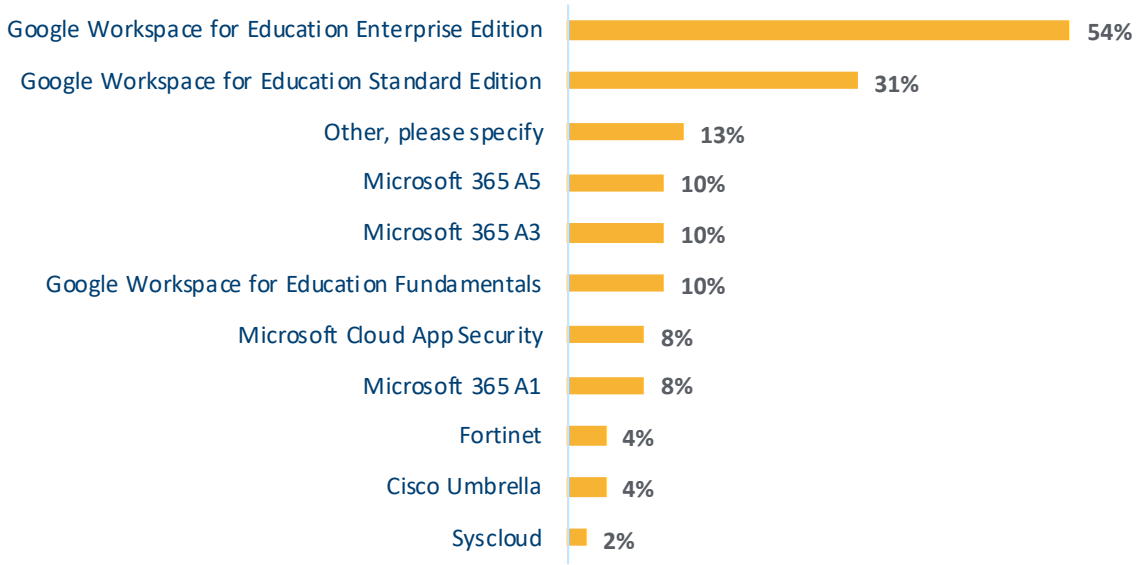
When it comes to cloud-based cybersecurity, it's possible that many of these ed-tech influencers don't know what they don't know.

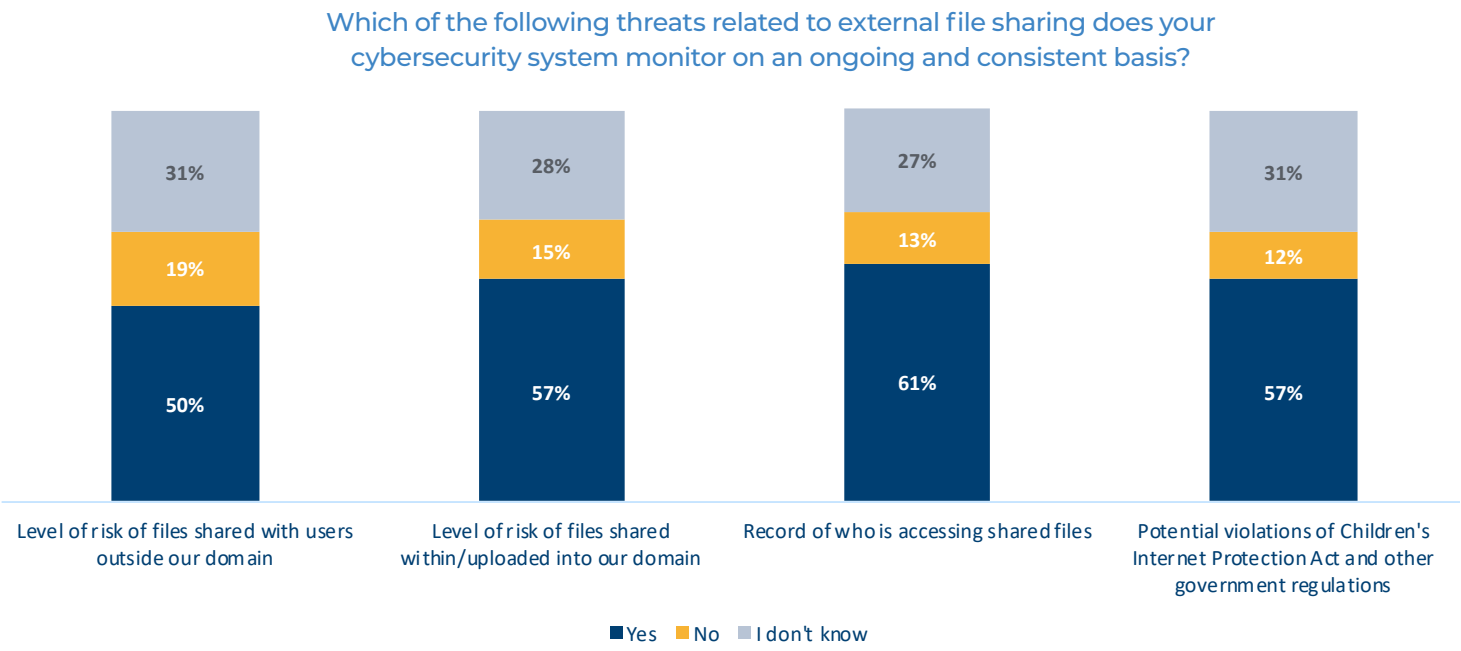
For instance, nearly a quarter of district-level tech influencers say they operate in a cloud environment, but that they do not know if they have a security system that monitors and protects them.

Nearly 1 in 3 do not know whether or not their human resources system is hosted in the cloud. Roughly 1 in 5 aren't sure if their learning management, student information, and/or financial systems are cloud-based applications.

Close to 1 in 3 are unsure if their cybersecurity systems consistently monitor the level of risk of files shared with users outside the district's domain. The same share does not know whether their systems track potential violations of the Children's Internet Protection Act and other government regulations. And more than a quarter are unsure if their cybersecurity systems keep tabs on the level of risk of files shared within/uploaded into their cloud domains or records who accesses shared files.

What platform do you use for protecting cloud collaboration and storage applications such as Google Workspace, Microsoft 365, Dropbox, Box, etc.? Select all that apply.





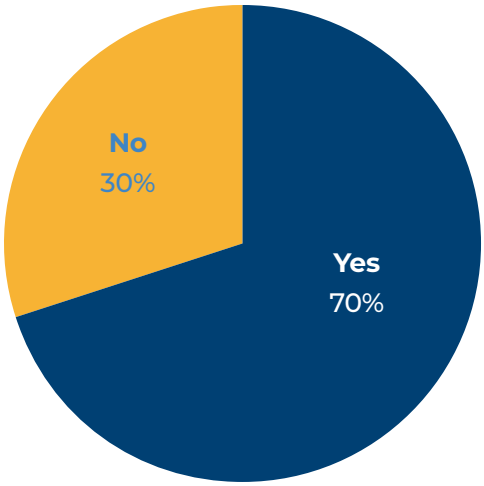
These are not classroom teachers whose professional roles do not require them to be informed about the details of their districts' technology. All survey respondents rated themselves as having at least a medium level of influence on district technology decisions.

Districts Devote Limited Resources to Securing the Cloud but Store Sensitive Information There

Even when district leaders do have knowledge of the details of their cloud security, they do not necessarily devote extensive resources to it.

Among leaders who do know whether they have a cloud security platform or system that protects cloud collaboration and storage applications, 30 percent say they lack this type of protection.

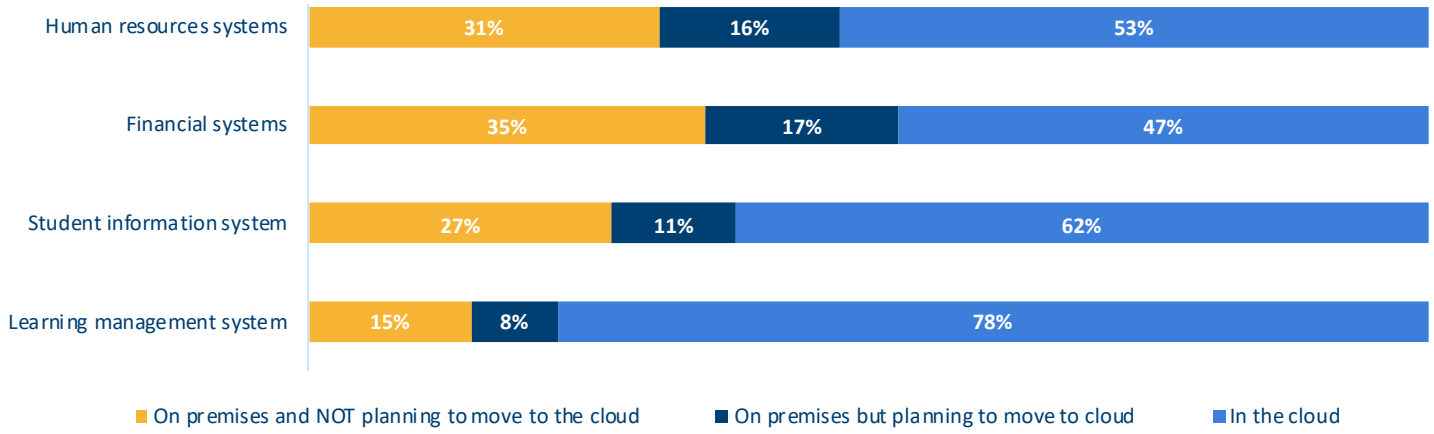
Does your district have a security platform or system that protects cloud collaboration and storage applications, such as Google Workspace, Microsoft 365, Dropbox, Box, etc.?



Twenty thousand dollars is the median amount that district leaders say they devote annually to cybersecurity. Of that amount, 20 percent ($4,000) will go toward protecting cloud applications in 2022, survey respondents report.

Yet some of districts' most sensitive information is stored in their cloud applications. Eighty-six percent of district leaders either use cloud-based learning management systems (mostly Google Classroom) or plan to move these systems to the cloud. Sixty-nine percent have moved—or plan to move—their human resources systems to the cloud. Ninety-five percent say students and/or staff collaborate using Zoom and/or Google Meet.

Where are the following systems hosted?



Conclusion

U.S. school districts have clearly committed to the cloud. Yet, their appetite for cloud applications may have outpaced their ability to protect the sensitive and important student and employee information currently stored there. The ed-tech revolution sparked by the pandemic has only made the situation more challenging by increasing the amount of software and hardware under their purview. Based on the survey results, leaders may want to consider taking the following steps.

- **Educating the educators**: Survey results suggest that too many ed-tech influencers are under-informed about the steps being taken to protect their online assets. Some are also unsure whether key systems are located in the cloud or on-site. District leaders who make technology-related decisions should make it their business to learn more about their district's current cybersecurity approach, to understand which systems are and are not currently cloud-based, and read up on best practices.

- **Rethinking resources**: Given the rapid expansion that occurred during the pandemic, district leaders should make sure they devote sufficient resources to buy new technology and protect it. Just as buyers factor in the cost of insurance to protect a new home or car, ed-tech purchasers need to make sure they set aside money to not only acquire technology but to keep it secure.

- **Custom-tailoring to the cloud**: As more and more applications move to the cloud, districts should take a fresh look at their overall approach to cybersecurity. Older approaches that worked for securing file cabinets of paperwork, or information stored on local hard drives and servers, are insufficient to protect student and employee data stored in cloud applications.

The EdWeek Research Center, a nonprofit, nonpartisan research organization, provided the content for this report. ManagedMethods was the sponsor. EdWeek Research Center publications do not necessarily reflect the opinions of its research clients and sponsors. References to sponsors in this white paper do not constitute endorsements by Education Week or Editorial Projects in Education.