CYBERSECURE 2023:

The state of data security and privacy in K-12 schools

Clever

Introduction

In the wake of remote learning, schools and their students are using more apps, devices, and digital platforms than ever before, leading to greater flexibility, personalization, and insights. But with expanded access to learning resources comes greater responsibility for schools and their edtech partners to protect the sensitive information these tools may collect.

As the district tech stack grows, so does the risk of a cyberattack or data breach. The FBI **warned districts** in September 2022 that ransomware syndicates were targeting the education sector, and that they expect attacks to increase during the 2022–2023 school year. The report was released in the same week LAUSD was hit with a ransomware attack. In 2021, nearly a million students were impacted by **67 ransomware attacks** against schools, with costs of over $3.5 billion in downtime.

Today, more than 70% of U.S. K–12 schools rely on Clever to simplify and secure access to digital learning. To better understand how administrators and educators alike are thinking about privacy and security, Clever surveyed almost 4,000 teachers and administrators, asking about their experiences and where there was room for improvement. Here's what we found.

Key Findings

Teachers may be insulated from understanding cyberattack risk.

Only 11% of teachers surveyed said they thought a cyberattack on a school near them would be “very likely,” while 25% of administrators said that their district had already experienced a cyberattack in the past year.

Because of their different roles, teachers and administrators perceive different vulnerabilities. We can learn from both.

Teachers were acutely aware of the potential vulnerabilities caused by students and teachers, while administrators saw a wider range of risks. Administrators were three times more likely than teachers to say administrators were a security vulnerability and five times more likely to say administrators were a privacy vulnerability.

Schools aren’t starting from scratch when it comes to privacy and security.

More than half of administrators (63%) and teachers (53%) believed that their districts were prepared to take on digital security challenges. And training to date has been effective: Teachers were very confident in their knowledge of their schools’ acceptable use policy (91%), student data confidentiality practices (90%) and the importance of good password management (89%).

Teachers and administrators agree that more can be done.

Both teachers and administrators said the top three things districts can do to improve digital security are more educator training, more or better technology solutions, and more staff focused on technology. But one in four teachers reported that they had never received training on privacy or security.

Increased security needs mean increased spending.

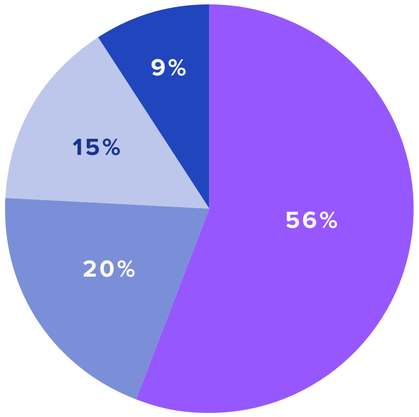
Three out of four districts said they would increase their spending on security and privacy in the next 2-3 years. The majority said they had used federal stimulus funds to make investments in security and privacy.

Teachers and administrators are already taking steps to embed new technology and practices to bolster their digital defenses. Cybersecurity is a big responsibility, but districts and teachers are up to the challenge.

Methodology

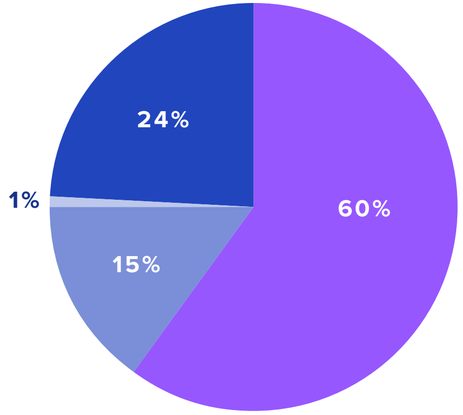
In October 2022, we surveyed over 800 US-based school administrators and over 3,000 US-based educators who used Clever on questions related to digital security and data privacy. About half (56%) of the teachers surveyed taught at an elementary school, 20% taught middle school (grades 6-8), and about 15% taught in a high school. The remainder taught in other types of schools (e.g., a K–8 school). The survey was conducted by Whiteboard Advisors.

Of the teachers, 98% were public school educators (including 8% from public charter schools). About 60% of the administrators had roles in education technology or instructional technology, 15% had roles in curriculum and instruction, and 24% had other roles within the district.



Demographics of Teachers

- Elementary
- Middle school
- High school
- Other (i.e., K-8)



Demographics of Administrators

- Education/instructional technology
- Curriculum and instruction
- Assessment and special education
- Other

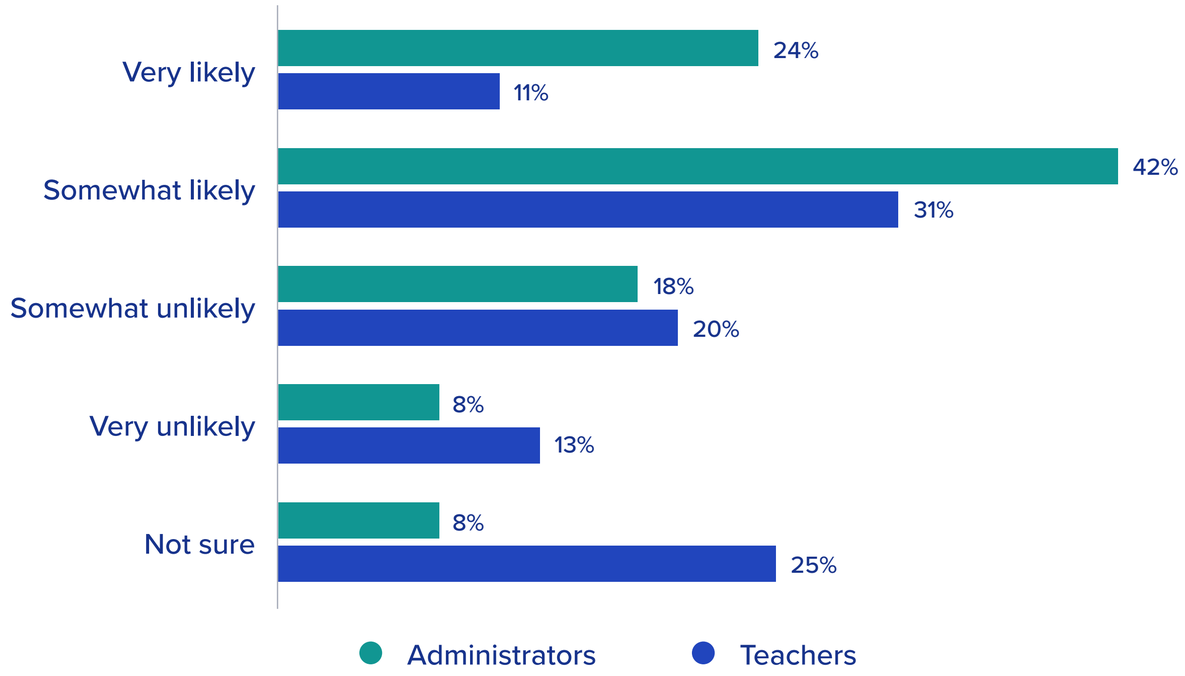
Detailed Insights

01 Administrators are highly aware of cybersecurity threats; teachers less so

Not every cyberattack disrupts teaching and learning or makes headlines. And some incidents are caught or deflected before they have any impact. It's not surprising, then, that administrators in our survey (most of whom had responsibility for technology in the district) were well aware of the potential risks, while teachers were somewhat insulated from some of those concerns. Two-thirds of administrators said it was very or somewhat likely that a school or district near them would be impacted by a security incident, compared to 42% of teachers.

Only 11% of teachers said an incident would be very likely, but one in four administrators said their district had already experienced a hack, phishing incident, data breach, or other cyberattack in the past year.

How likely do you think it is that a school near you will be impacted by a security incident (e.g. cyberattack, ransomware) in the next year?

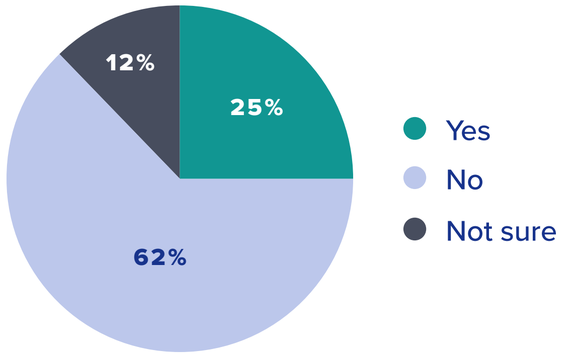


2/3 **of administrators think an attack is very or somewhat likely**

01 Administrators are highly aware of cybersecurity threats; teachers less so

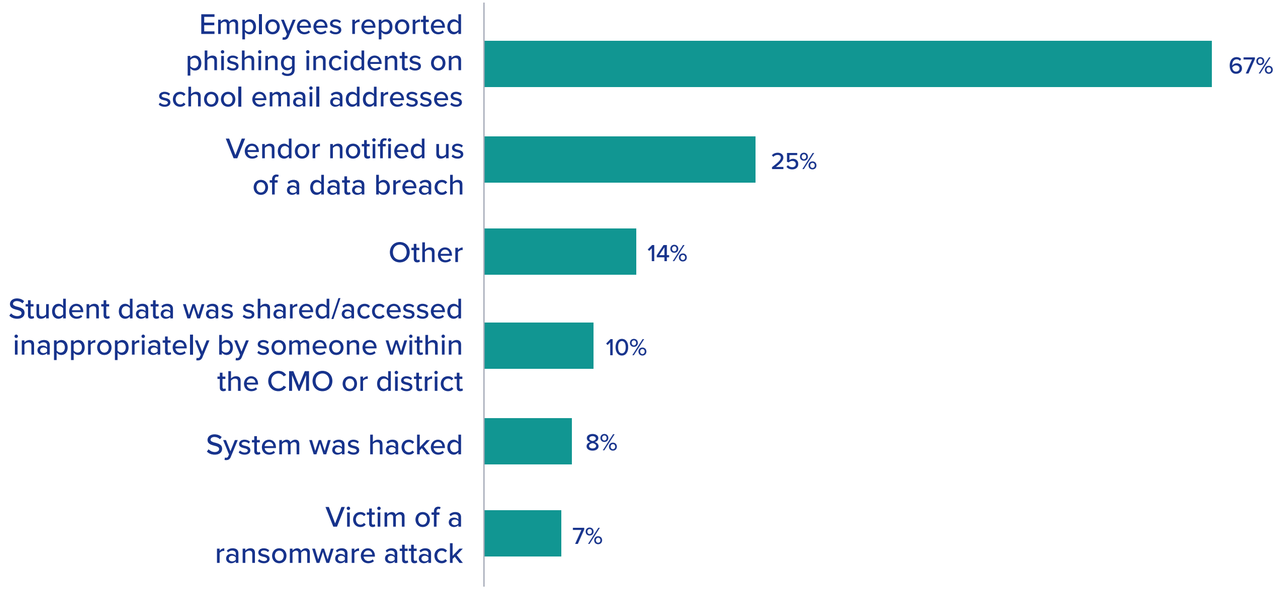
Has your CMO or district experienced a hack, phishing incident, data breach or other cyber attack in the past year?

Administrators only



What kind of incident?

Administrators only



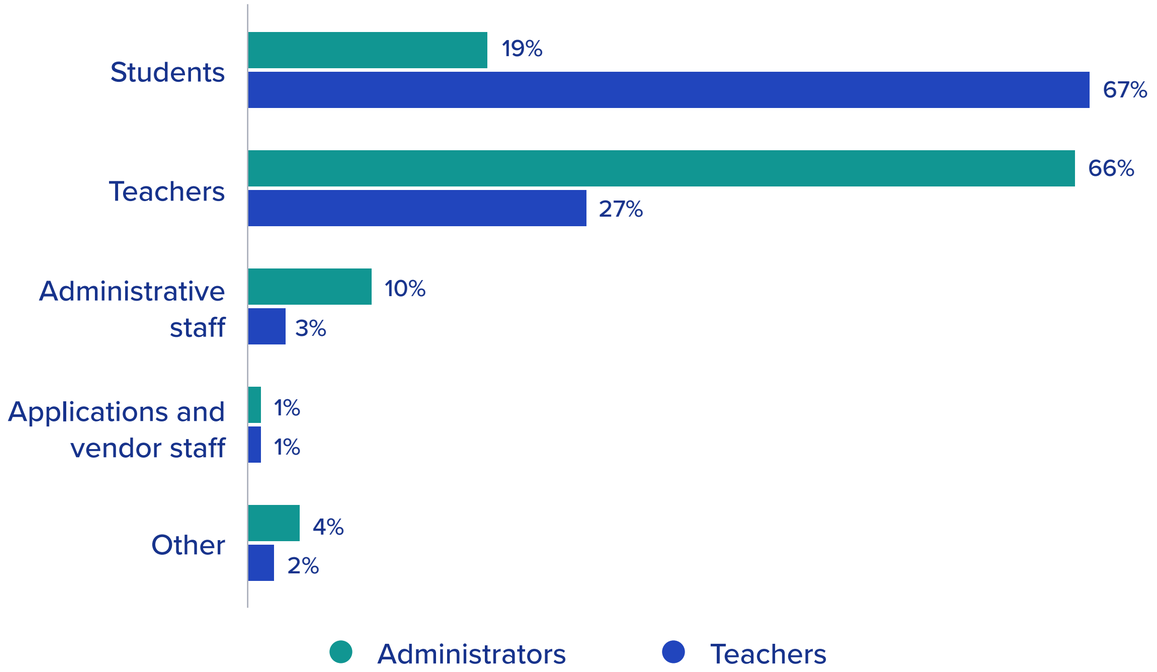
67% of administrators who responded cited phishing attacks on staff email

02 Human vulnerabilities are security vulnerabilities

Both teachers and administrators saw users of technology as a potential source of security vulnerability, but their perceptions of risk differed, reflecting their own roles. Teachers, responsible for their own safe use of technology and appropriate use by their students, saw students (67%) as the biggest risk for a security incident, followed by teachers (27%). Only 6% of teachers said the biggest risk came from administrators, edtech staff, or others.

Administrators, who are responsible for a wider range of stakeholders, had a more diffuse sense of the potential risk. They were three times more likely than teachers to say administrators were a vulnerability. This may suggest that, among administrators surveyed, there was greater awareness in general of the risks and likelihood of security issues, and an understanding that anyone can fall for phishing or other cyberattacks.

When it comes to digital security in your district or CMO, who or what is the biggest vulnerability?

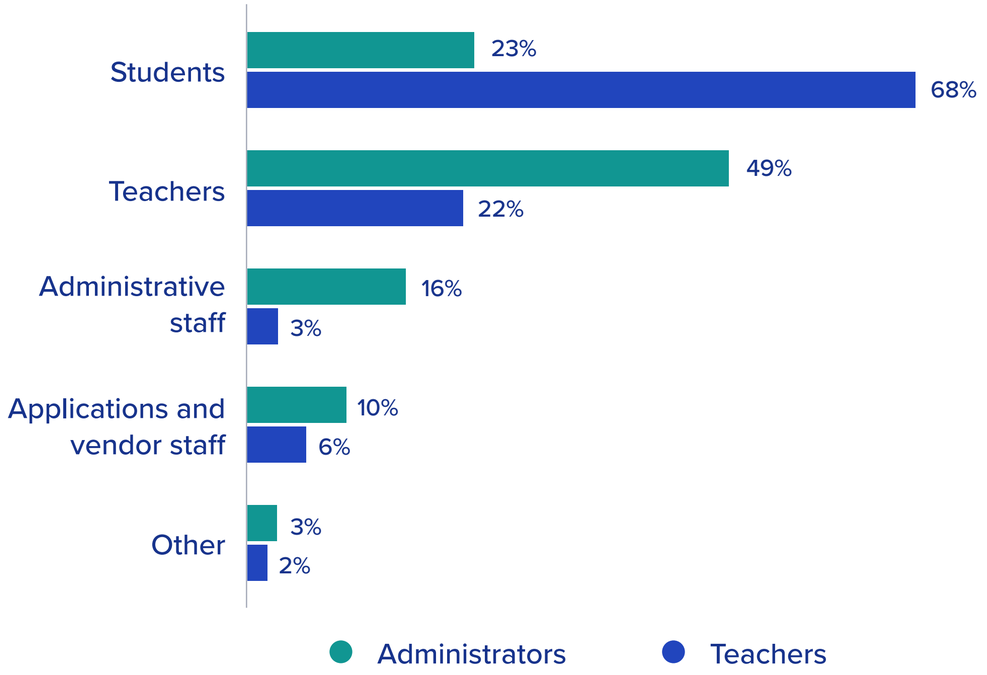


02 Human vulnerabilities are security vulnerabilities

When it comes to data privacy (rather than security), the trends are similar, but more pronounced.

Administrators are five times more likely than teachers to believe their peers in administration are the biggest vulnerability. They are also nearly twice as likely as teachers to view technology partners as a likely source of vulnerability.

When it comes to data privacy in your district or CMO, who or what is the biggest vulnerability?



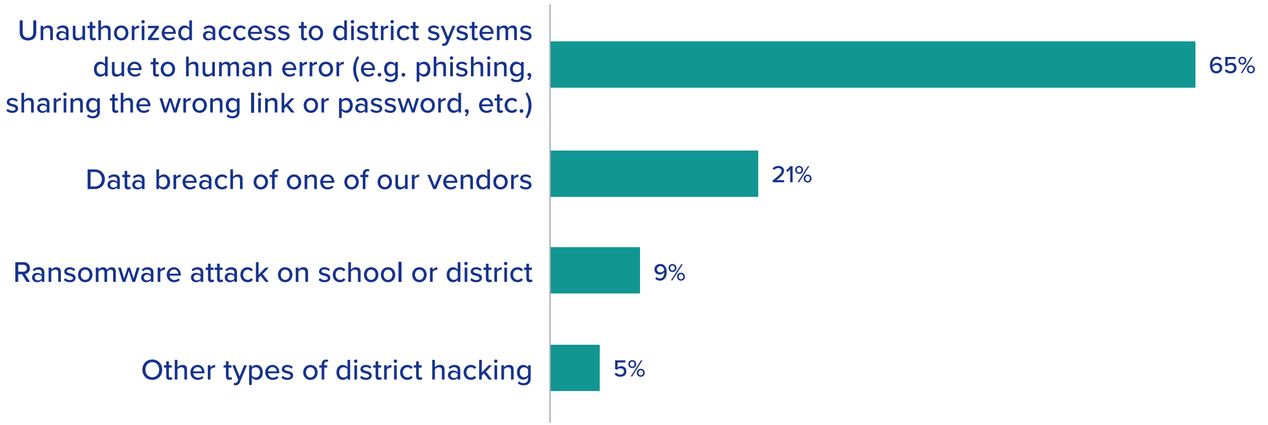
02 Human vulnerabilities are security vulnerabilities

Administrators recognize that technology is only as secure as the humans who use it. It's no surprise, then, that two out of three administrators say that they think the most likely security incident would be unauthorized access to systems due to human error.

In addition to being seen as most likely to happen, this is also the security concern administrators are most worried about. 42% of administrators reported being most worried about unauthorized access of systems due to human error, followed by 41% who were most concerned about a ransomware attack. 13% of administrators were most worried about a vendor data breach.

Which of the following do you think is most likely to occur?

Administrators only



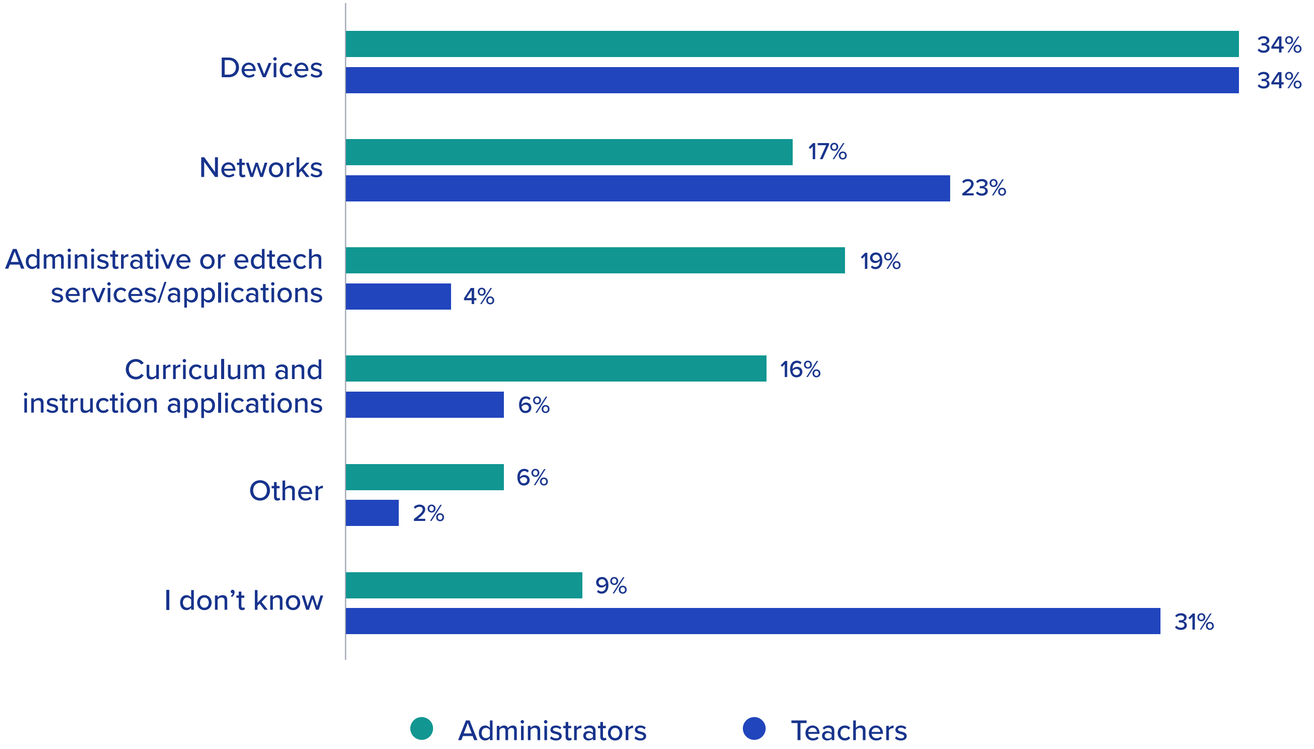
“Cybersecurity is a team sport, and the differences highlighted in the survey offer us a path forward to address vulnerabilities in our schools. While both groups differ on where the risks exist, both agree on what can be done: more training for educators, the use of security tools, and increased specialized staff.”

MOHIT GUPTA | GROUP PRODUCT MANAGER, SECURITY | CLEVER

03 When it comes to security in the tech stack, devices don't stack up

Teachers and administrators alike believed that devices were the most vulnerable part of their technology infrastructure, but administrators were more aware of potential risks elsewhere as well: They were twice as concerned about vulnerabilities from tools used for curriculum and instruction, and four times more concerned about vulnerabilities from administrative platforms like an LMS or SIS.

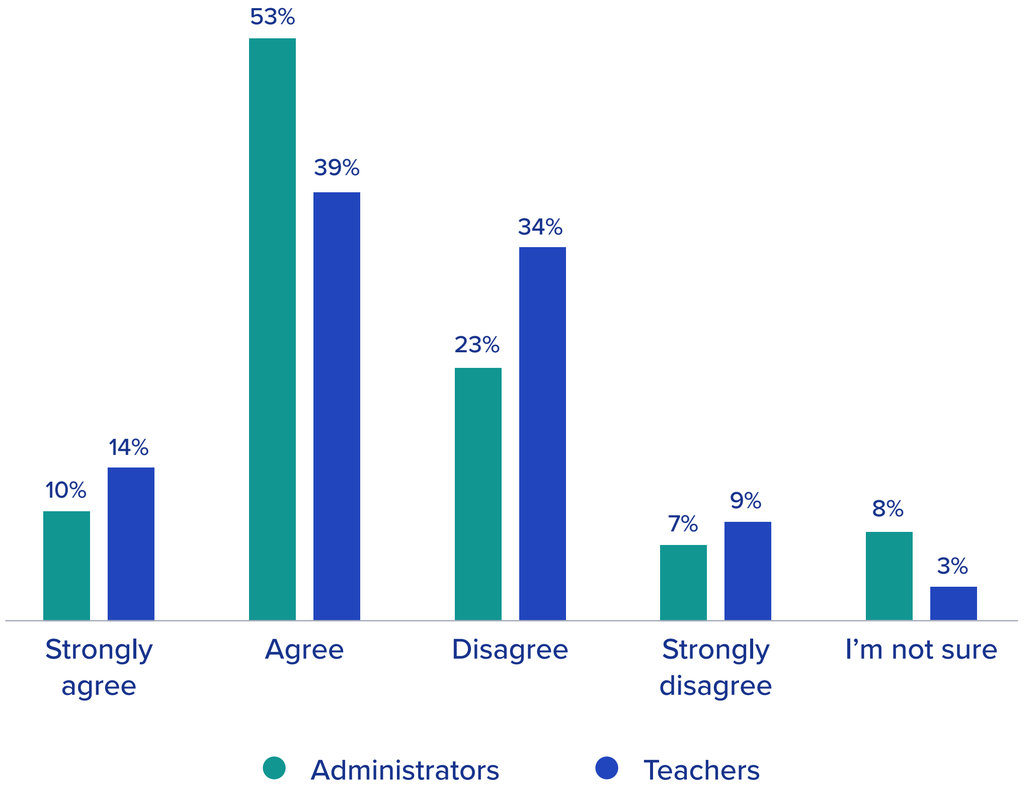
When it comes to data security, what part of your technology infrastructure are you most concerned could be a vulnerability (e.g., most likely to lead to a security incident through phishing, malware, or technical vulnerabilities)?



04 Schools aren't strangers to security dangers

While the challenges are changing (and bad actors are growing more sophisticated), security and privacy aren't new for districts. Districts have long had acceptable use policies and training for teachers on student data confidentiality to help support data security and privacy. As a result, teachers were confident in their knowledge of their schools' acceptable use policy (91%), student data confidentiality practices (90%), and the importance of good password management (89%). Most teachers and administrators said that their district had the right resources in place to prepare for digital security challenges.

To what extent do you agree or disagree with the following statement: My district or CMO has the right resources to appropriately prepare for or handle digital security challenges?

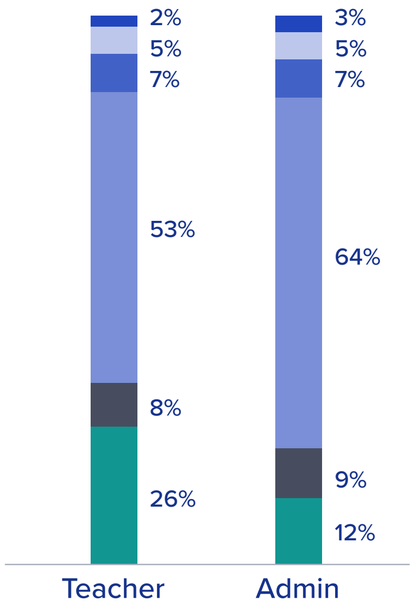


05

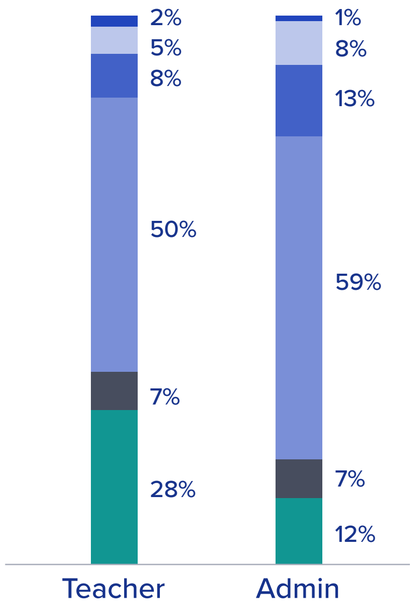
One in four teachers say cybersecurity training is missing altogether in their district

While the majority of administrators and educators reported that privacy and security training happened in their district, a surprising 26% of teachers said they had never received training on privacy or security, representing a big opportunity for districts to shore up their practices.

How often do you provide formal or informal training about student data privacy for your teachers?



How often do you provide formal or informal training about digital security for your teachers?

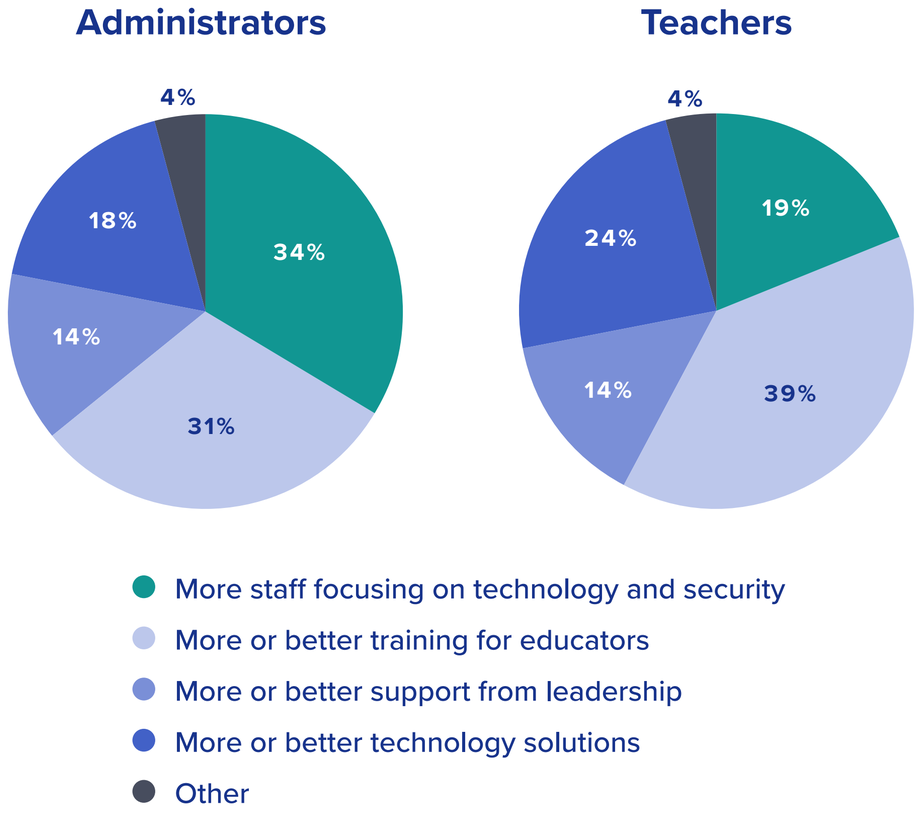


06

Improving security takes staff, training, and technology

There's no silver bullet for improving security, but administrators and teachers agreed on the components that matter: staff, training, and technology. Teachers were more likely to say that more or better training for teachers would help most, while administrators put additional staff as their top choice.

Which of the following would most help your district or CMO improve its digital security efforts?



“We don’t have enough time on professional development calendars to address technology in general, whether that be on instructional technology or cybersecurity. Teachers’ plates are already so full with compliance pieces and other priorities for the district, so we get very little time for cybersecurity training.”

BRADLEY HILTON | TECHNOLOGY SUPERVISOR | BERKELEY UNIFIED SCHOOL DISTRICT | BERKELEY, CALIFORNIA

07

Security training and interest have increased since COVID

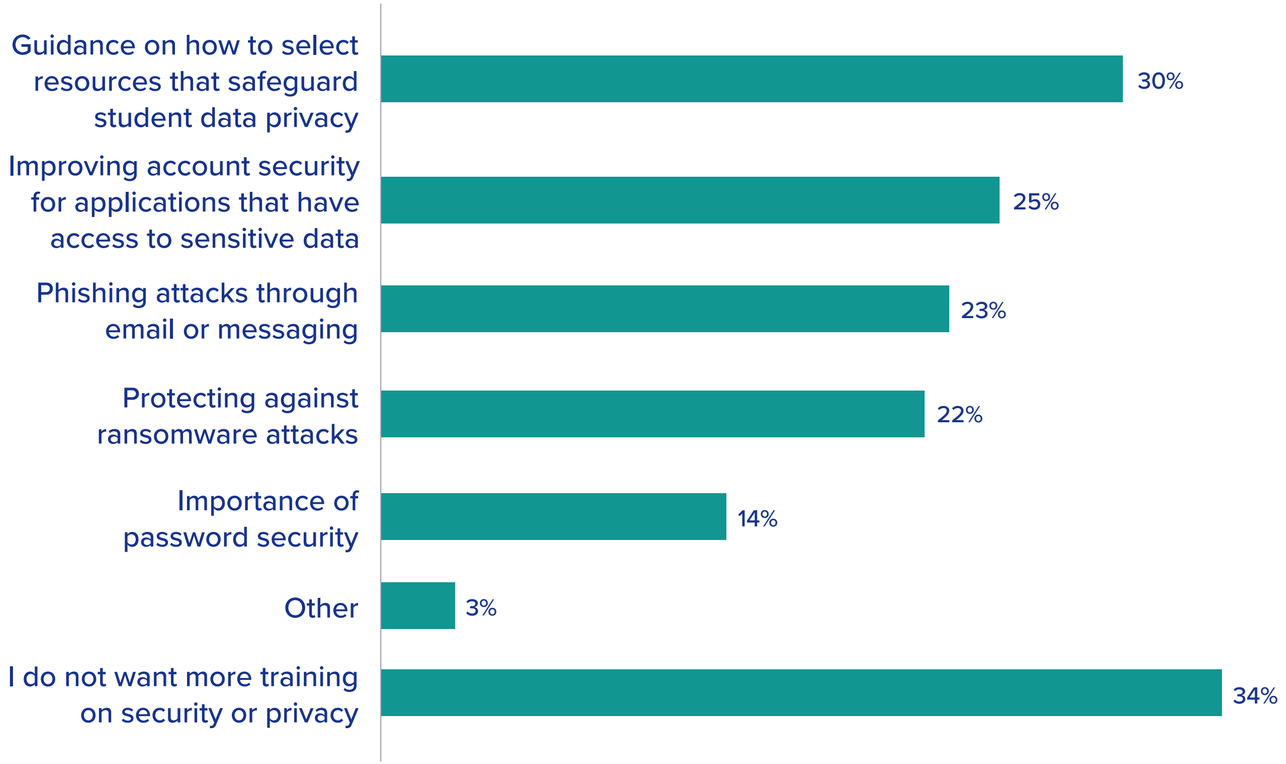
With the massive shift to digital learning precipitated by the pandemic, more than half of administrators said that training and informal conversations about digital security had stepped up. However, only a quarter of the teachers had experienced more frequent security education. Teachers said they were interested in more training: two-thirds indicated they wanted to learn more about topics related to data privacy and security. A third of teachers said they didn't want more training, which likely reflects a critical situation in which teacher burnout and stress are, understandably, at an all-time high.

2/3
OF TEACHERS

want to learn more about data privacy and security

What security or data privacy topics, if any, do you want more training about?

Teachers only

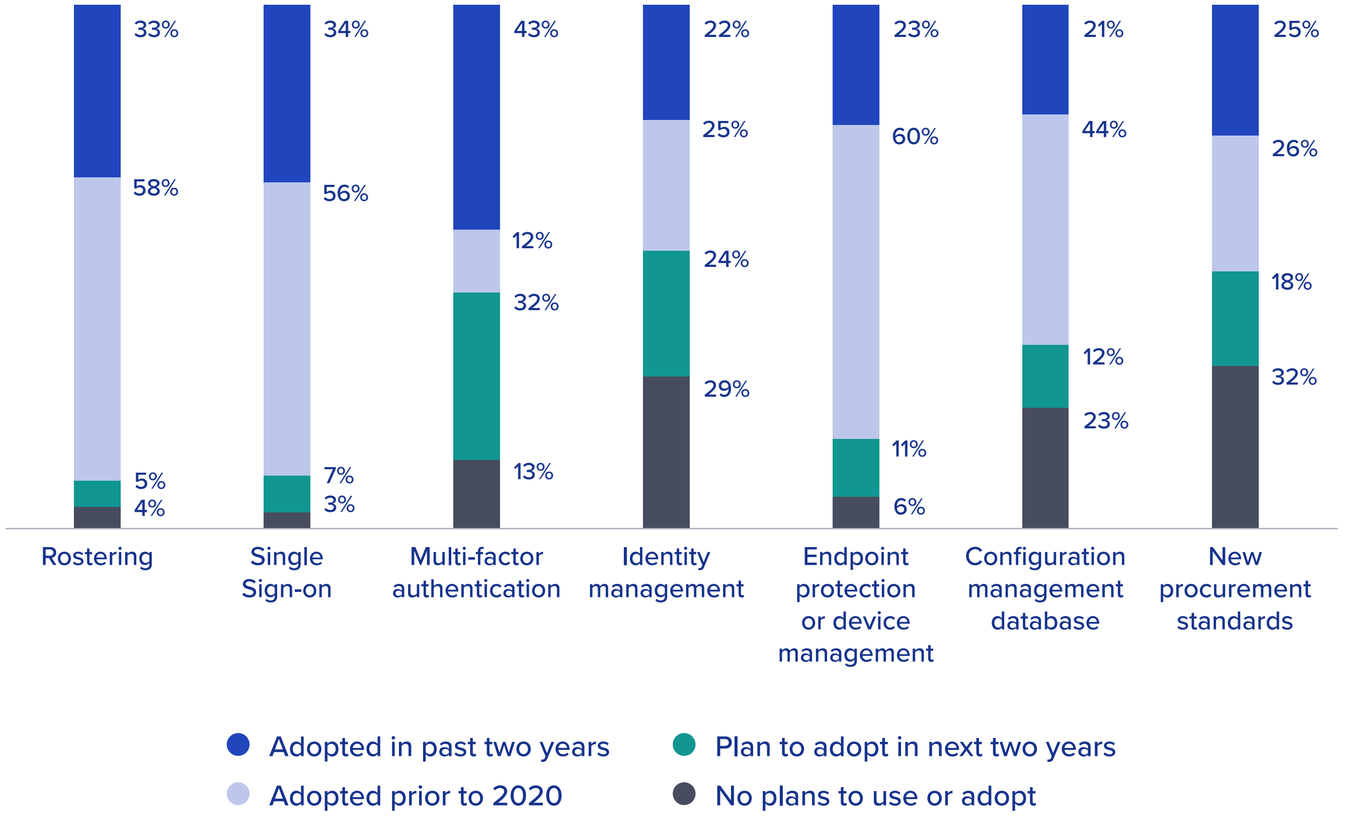


08 Districts are adopting systems that can reduce human error

Training is important, but technology can also help by making passwords more secure or reducing the number of times students and staff need to enter their passwords. Many districts adopted new practices during the pandemic, and many are planning to adopt others in the coming years. These tools and practices are in different stages of adoption and maturity. Some, like single sign-on and rostering, were adopted by most districts prior to 2020. Others, like multi-factor authentication or identity management, are growing in adoption now, but still face growing pains.

Which of the following have you implemented or do you plan to implement in the next school year, if any?

Administrators only



09

Increasing challenges means increased spending

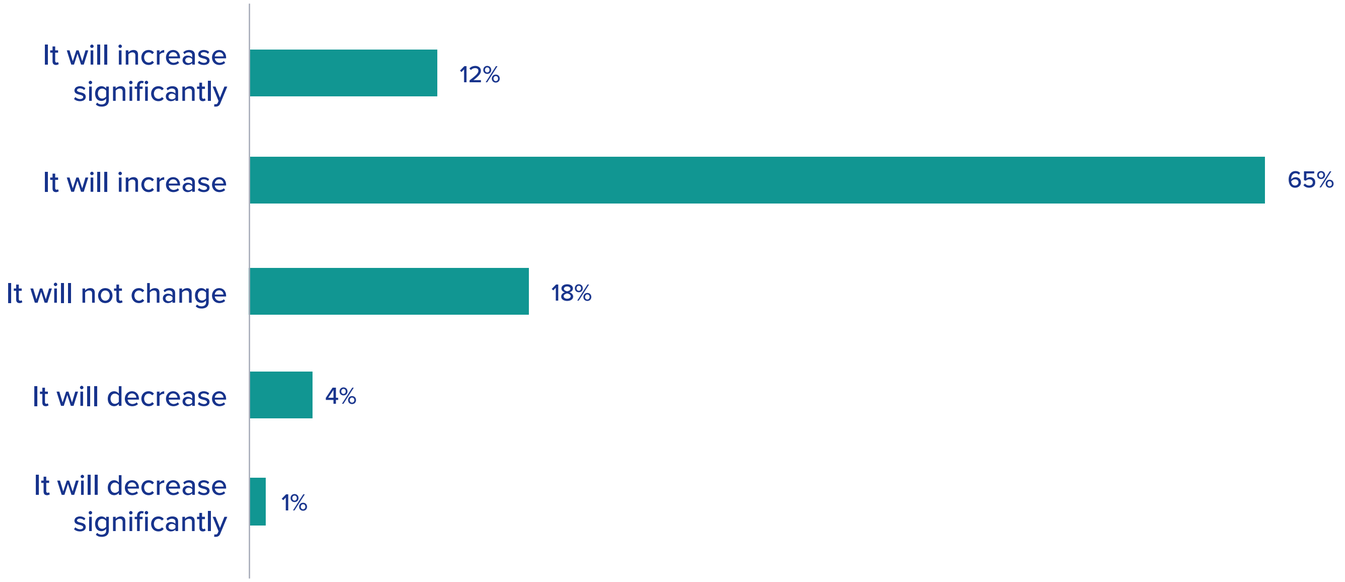
Districts are upping their spending to keep pace with the emerging security challenges: 65% say their spending will increase, with another 12% saying it will increase significantly. The majority said that federal stimulus dollars were helping to support their efforts.

51%
OF DISTRICTS

used federal stimulus funding to support student data privacy and/or security during the pandemic.

How, if at all, do you think your CMO or district's spending on digital security will change over the next 2 to 3 years?

Administrators only



“Our investment in cybersecurity has increased compared to previous years. In trying to improve our posture and reduce risk, our district secured a full-time employee focused on cybersecurity. After receiving a list of best practices provided by the state, we’ve now implemented an EDP to reduce a lot of vulnerabilities, and we’re making changes so that personal devices can no longer access internal resources.”

MARK SALZER | DIRECTOR OF TECHNOLOGY | PLYMOUTH-CANTON COMMUNITY SCHOOLS | PLYMOUTH, MICHIGAN

About Clever

Clever is on a mission to unlock new ways to learn for all students. More than 65% of U.S. K-12 schools now use Clever to simplify access and improve engagement with digital learning. With our free platform for schools and a network of leading application providers, we're committed to advancing educational equity. Clever, a Kahoot! company, has offices in San Francisco, CA and Durham, NC, but you can visit us at clever.com anytime.


Clever