Clever

Cybersecure 2024

EXPLORING THE INTERSECTION OF PEOPLE, PARTNERSHIPS, AND TECHNOLOGY IN K-12 CYBERSECURITY

Introduction

Cybersecurity across K-12 schools is facing a perfect storm. The rapid integration of digital tools in classrooms is transformative for learning but has opened the door to an escalating series of cybersecurity threats that put the personally identifiable data of millions of students and teachers at risk. It's clear the stakes are rising, but are defenses keeping pace? With insights from a survey of over 800 district leaders along with qualitative perspectives from district leaders and industry experts, this report takes a comprehensive look at the state of K-12 cybersecurity across three core pillars: people, technology, and the surrounding ecosystem, identifying gaps and opportunities to further safeguard our schools. Ultimately, cybersecurity is about more than tools—it's about people. By approaching security as a team effort spanning IT, staff, teachers and beyond, schools can ensure classrooms are safeguarded amidst growing threats.

Clever

Key Findings

53% of districts want to spend more on cybersecurity.

LEARN MORE HERE

96% of administrators see cybersecurity as a collaborative effort, yet only...

17% report their strategies truly reflect this team-based approach.

LEARN MORE HERE

#1 Ranked cybersecurity challenge in 2023:

Lack of dedicated cybersecurity personnel

LEARN MORE HERE

89% of districts are exploring new tech tools to bolster protection.

LEARN MORE HERE

1 in 2 districts have updated vendor security criteria in the past 2 years;

55% are planning more changes in the year ahead.

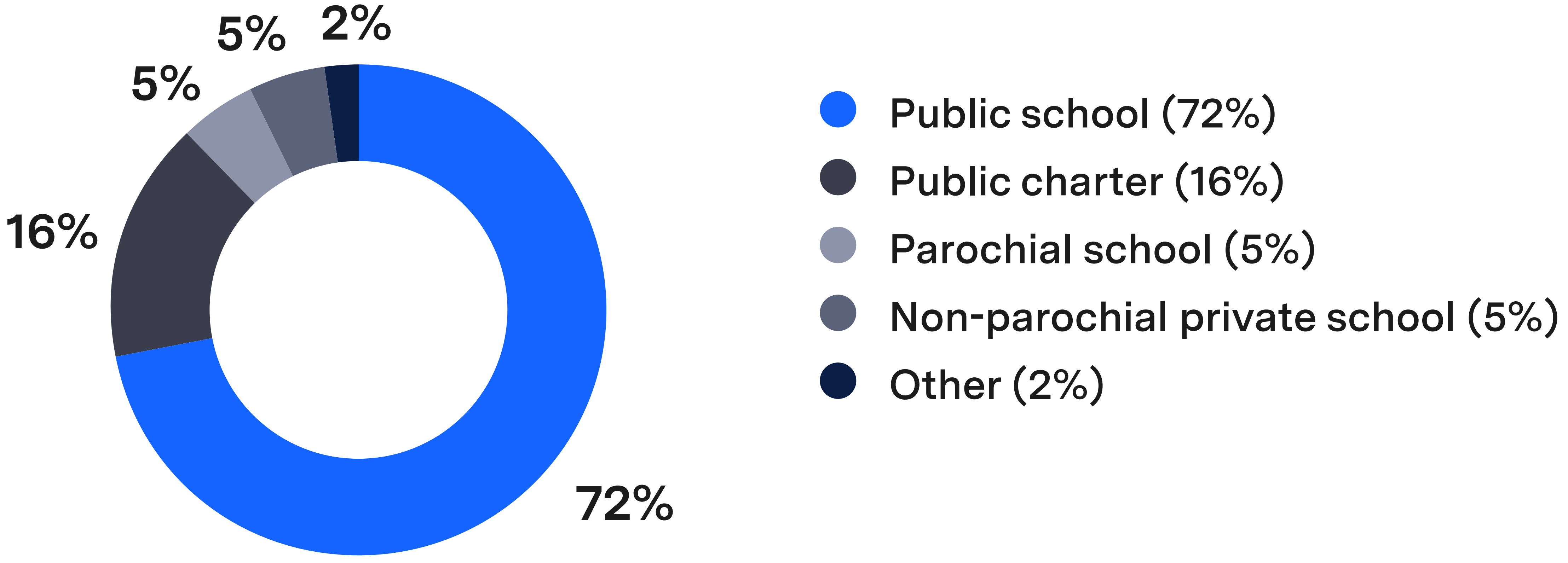
LEARN MORE HERE

Methodology

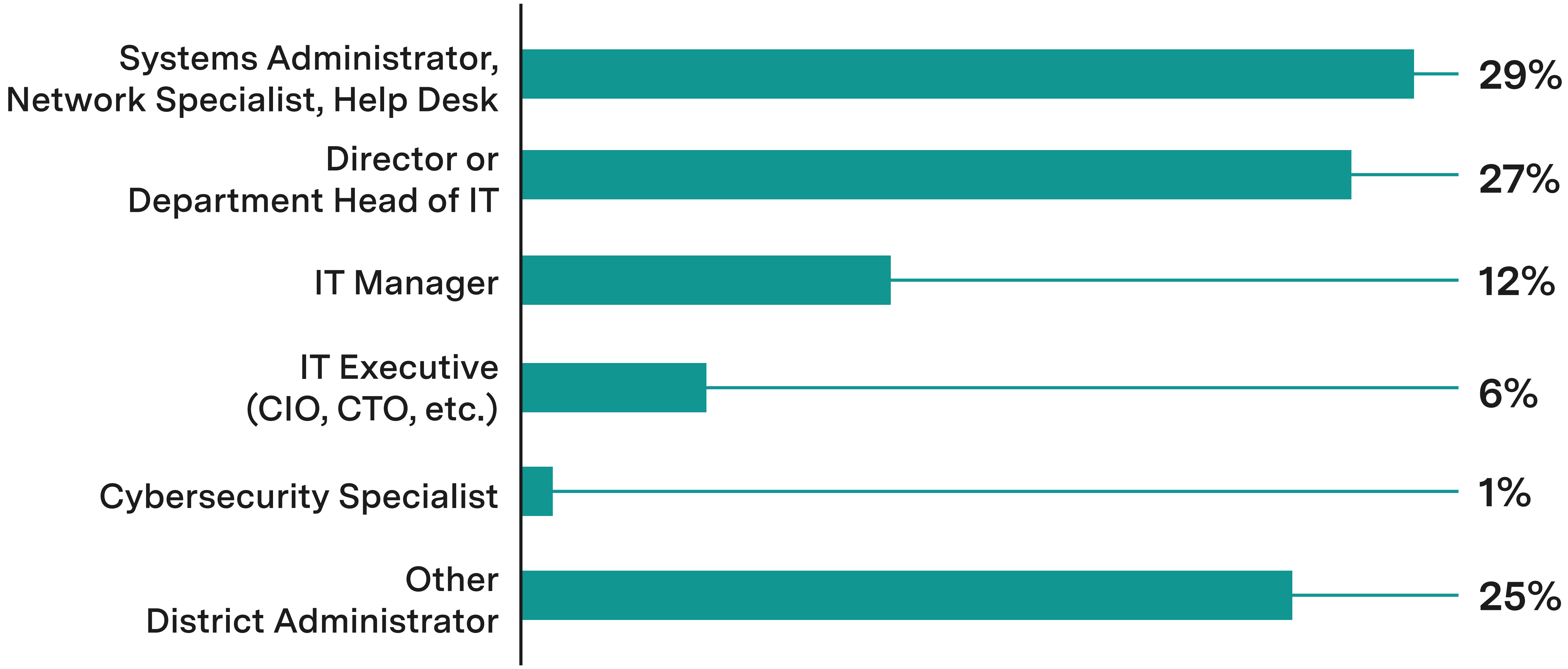
In Q4 2023, Clever conducted a survey of over 800 US-based district administrators to develop a comprehensive perspective on the state of K-12 cybersecurity. The survey pool comprised administrators from Clever's user base nationwide, 72% of which were in public schools. About 75% of administrators surveyed had roles directly related to instructional technology, including job titles such as Director of IT, Chief Information Officer, Chief Technology Officer, or IT Manager.

800+ US-based district administrators surveyed

Which of the following best describes your district or CMO?



Which of the following is closest to your role or area of work?



Acknowledgements

We collaborated with district administrators and field leaders to develop this report, incorporating their qualitative insights that influenced our key findings. We would like to express our gratitude to these forward-thinking Clever partners:

David Boxer
Chief Information Officer, The Blake School

Julia Fallon
Executive Director, SETDA

Christy Fisher
Chief Technology Officer, Norman Public Schools

Geoff Jones
Director of Technology, River Valley School

Lee Itson
District Technology Coordinator, School District of Random Lake

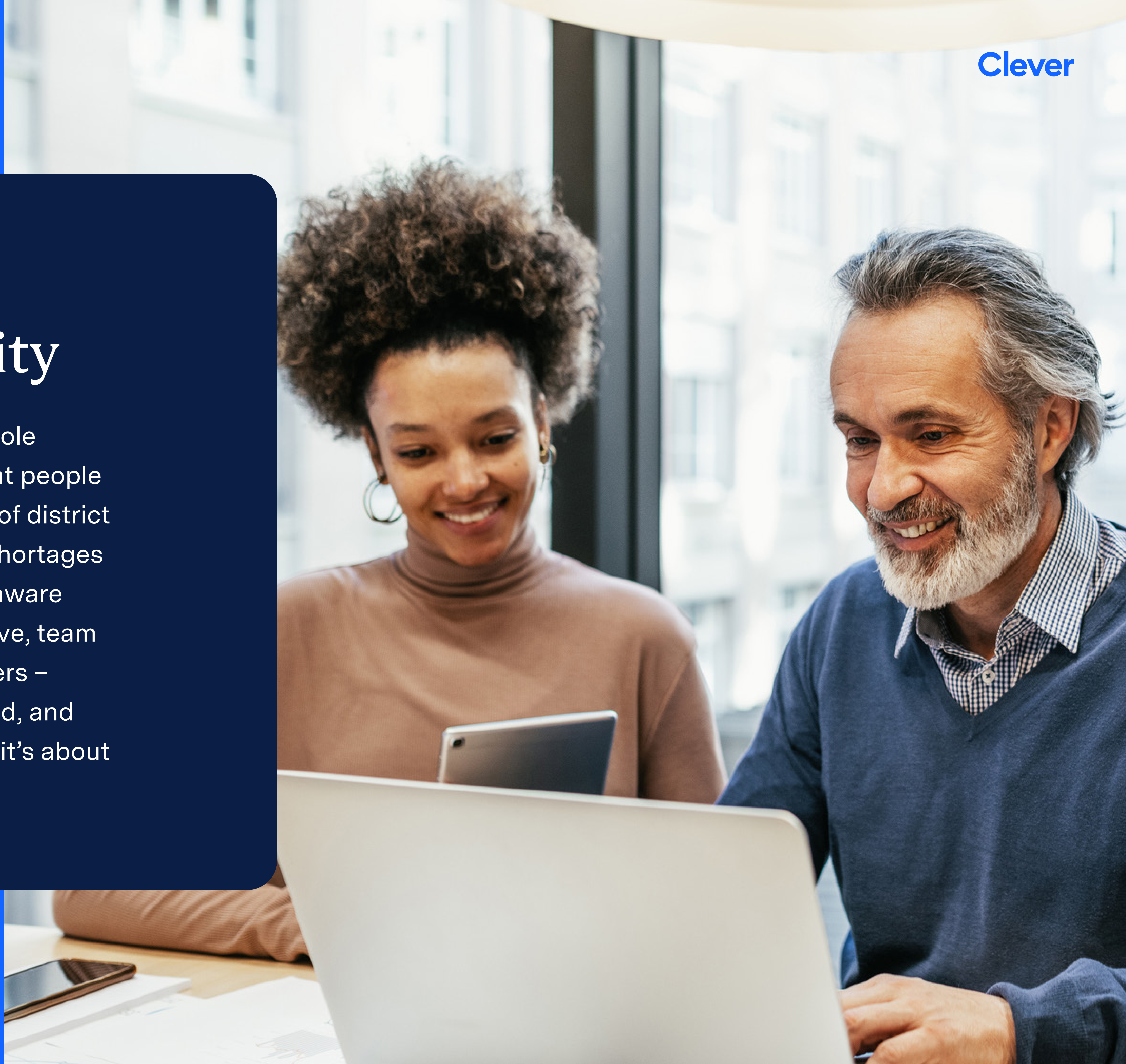
Erin Mote
Executive Director and Co-Founder, InnovateEDU

David Shulkin
Director of Learning / Information Technology, Bloomfield Hills Schools

Juwan Withers
Technology Coordinator, Chickasaw City School District

People: The Human Element of Cybersecurity

While cybersecurity tools and systems play a key role safeguarding schools, our survey results found that people remain a critical but often overlooked component of district cybersecurity. Lack of collaboration and staffing shortages create vulnerabilities against phishing and ransomware attacks, underscoring the need for a comprehensive, team approach to cybersecurity. Ensuring all stakeholders – not just the IT department – are informed, equipped, and proactive is crucial. It’s not just about technology; it’s about the people using these tools to support learning.



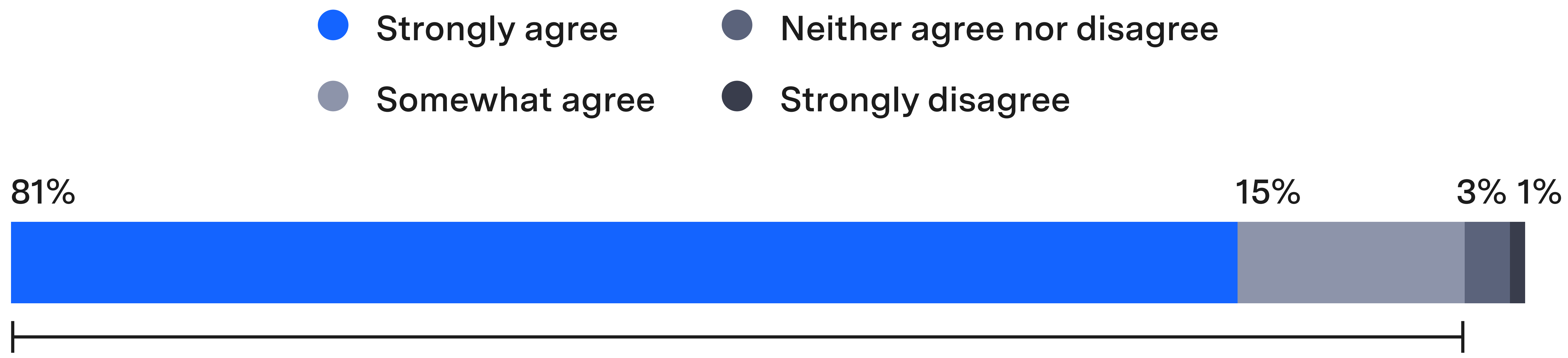
Cybersecurity Preparedness Requires More Collaboration

Cybersecurity requires team participation to secure schools, but a gap exists between expectations and reality.

96% of administrators believe cybersecurity should be a shared effort among IT, leadership, administrators, and school staff. However, only 17% of administrators describe their current cybersecurity approach this way – 55.5% of administrators report that cybersecurity is currently a sole responsibility of IT departments.

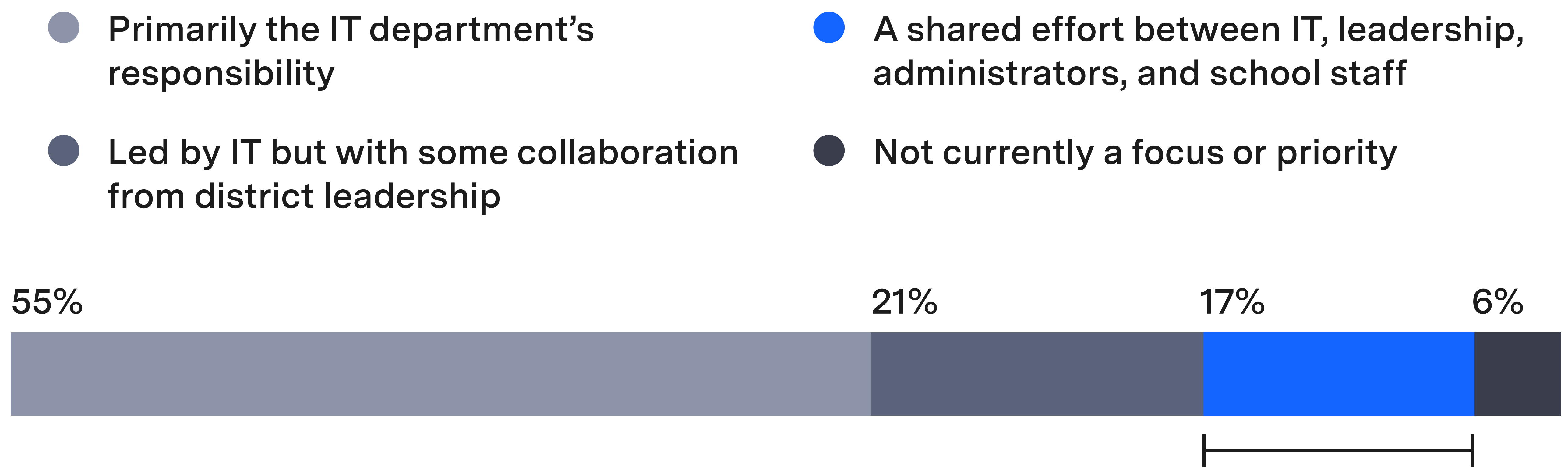
While rural district administrators most strongly agree that cybersecurity should be a collaborative effort (87%), they are also more likely to view cybersecurity as the responsibility of the IT department relative to their town, suburban and urban counterparts – often the result of limited personnel dedicated to cybersecurity.

Do you agree or disagree with the following statement: “Cybersecurity should be a shared effort between IT, leadership, administrators, and school staff.”



96% of administrators see cybersecurity as a collaborative effort...

What best describes your district’s approach to cybersecurity responsibility?



...yet only 17% report their strategies truly reflect this team-based approach.

> “ To avoid the pitfalls of compliance fatigue, we’ve adopted a strategy of integrating simple, actionable cybersecurity advice into everyday routines, making it more digestible for our staff. Our limited funding means we can’t always expand our cybersecurity team. Hence, we approach cybersecurity as a ‘team sport,’ emphasizing the need for trained staff at all levels and the critical role of funding in this endeavor.

DAVID SHULKIN | DIRECTOR OF LEARNING / INFORMATION TECHNOLOGY | BLOOMFIELD HILLS SCHOOLS

Districts Face Uphill Battle on Cybersecurity Staffing and Training

With limited dedicated cybersecurity personnel, a shared model involving all staff is essential for district cybersecurity. However, gaps persist in resources and training:

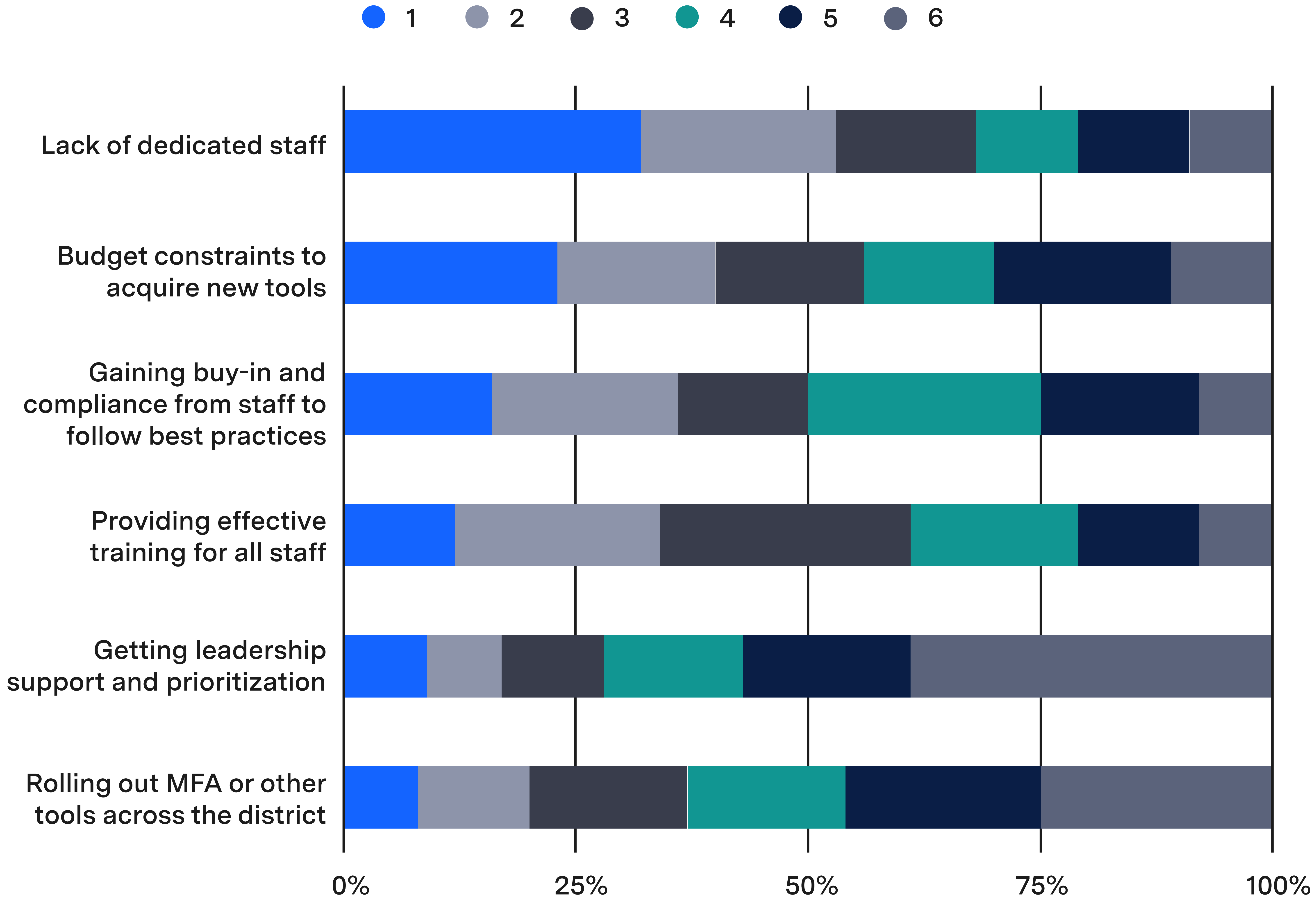
Lack of dedicated staffing to cybersecurity was ranked the #1 challenge facing districts, followed closely behind by budget constraints.

According to **CoSN,** most districts (66%) do not have a full-time cybersecurity position and with 49% still earning under $100K, lower salaries may correlate with challenges in attracting and retaining skilled cybersecurity staff, especially given competition from private industry.

While 63% of districts are actively implementing cybersecurity training for their staff, it's the second most reported challenge facing districts – right behind the lack of dedicated personnel.

Clever

Please rate the following cybersecurity challenges your district may befacing from 1 (most challenging) to 6 (least challenging):



Software Alone Can't Solve Districts' Cybersecurity Risks

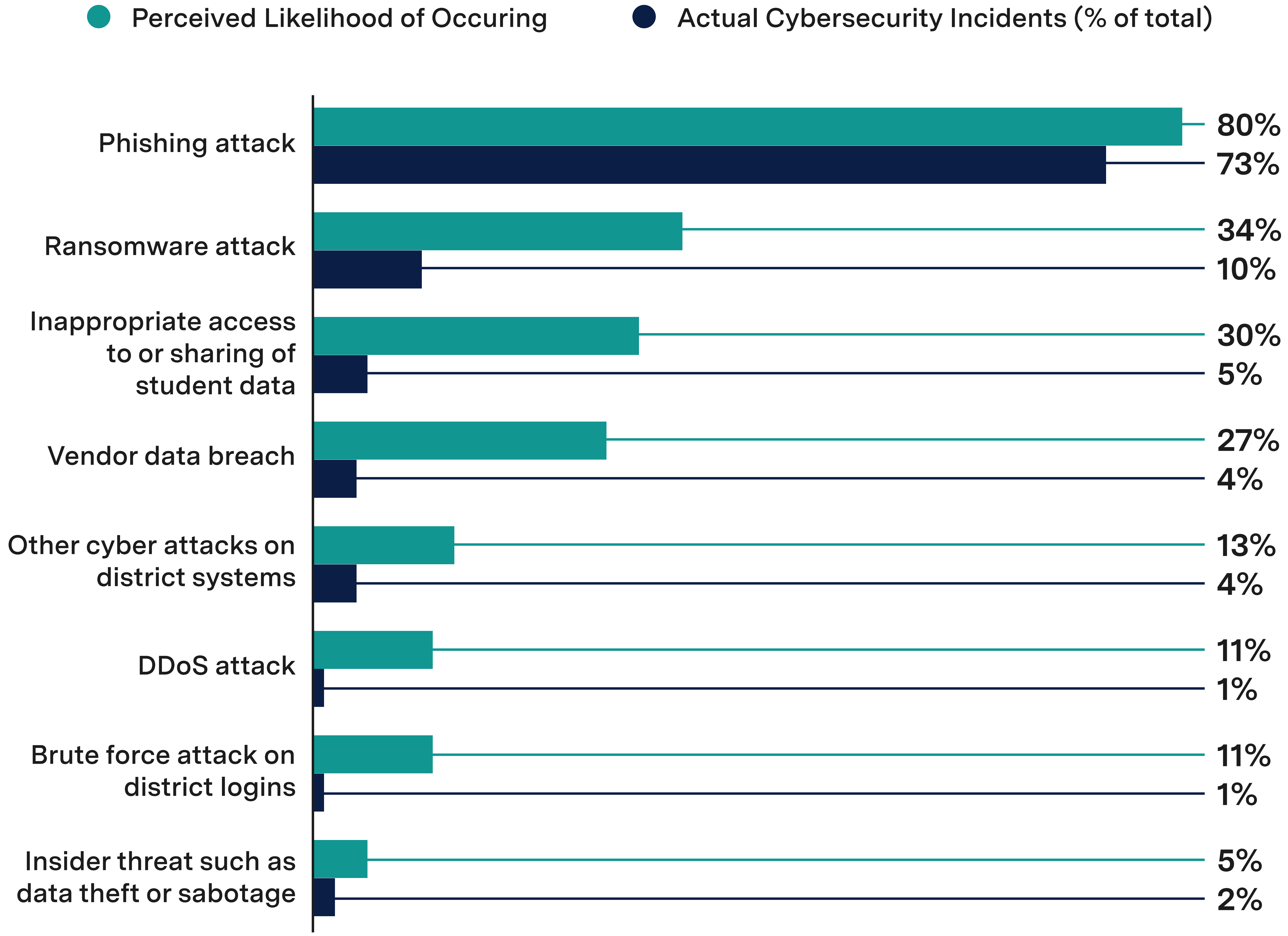
The biggest cybersecurity threats – phishing and ransomware – are caused by people, not technology gaps. This human risk underscores the need for comprehensive training and balanced tools that are easy to use, or implementation may struggle.

Phishing and ransomware attacks remain the most significant perceived threats: 80% and 34% of administrators believe they are most likely to occur, respectively. The concern is justified, as 73% of districts that had a security incident in the past year reported phishing attacks, and 10% reported ransomware.

(Continued on page 11)

Clever

Perceived likelihood of cybersecurity incidents vs actual cybersecurity incidents in the previous/next year:

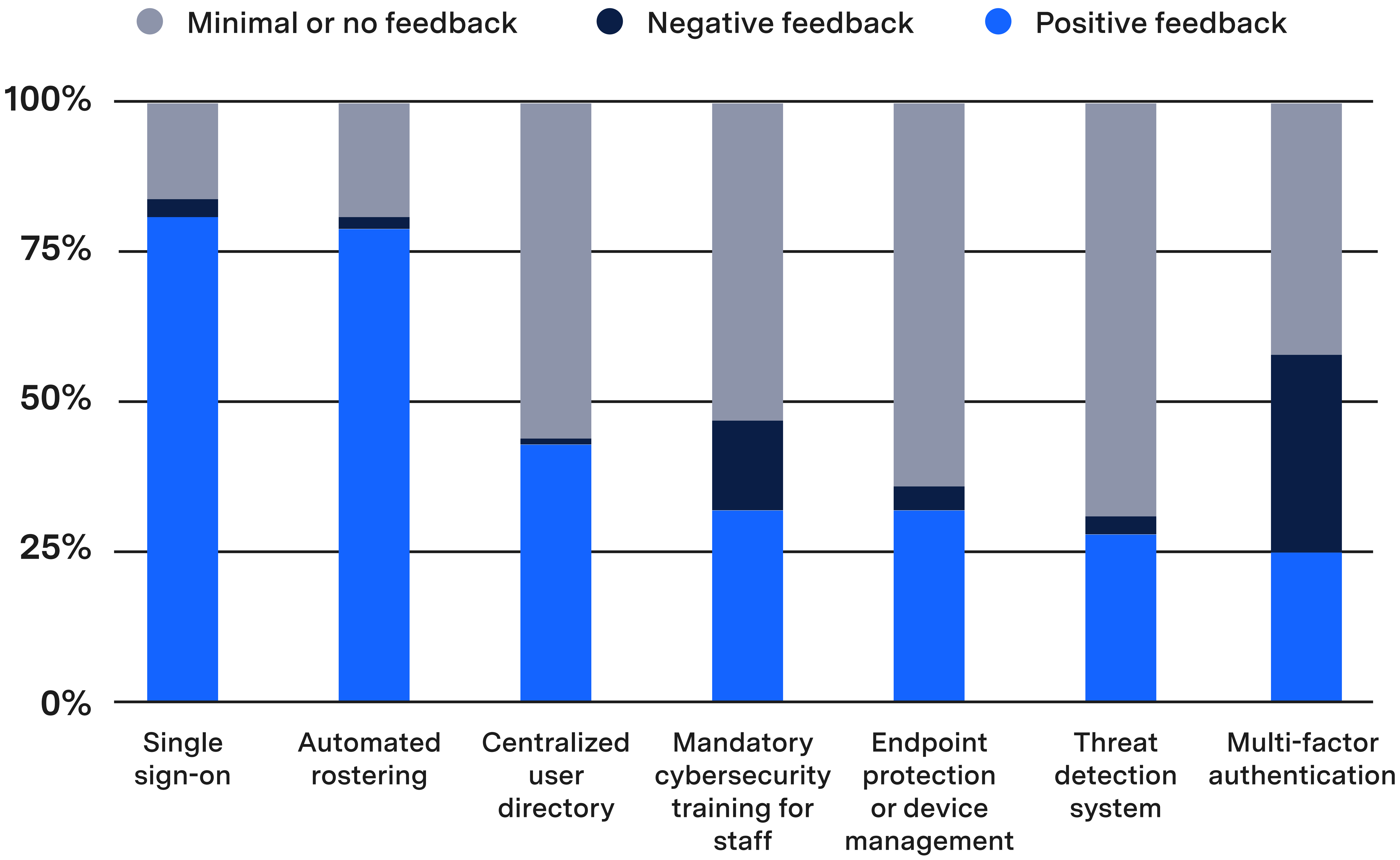


Software Alone Can't Solve Districts' Cybersecurity Risks

42% of cyber insurance policies require mandatory training for staff, emphasizing that a well-prepared and trained staff is a fundamental component of a comprehensive cybersecurity approach.

While training and balanced tools are important, key security measures like Multi-Factor Authentication (MFA) face adoption challenges due to usability issues. 33% of administrators reported negative teacher feedback on MFA, contrasting with the positive reception for more seamless tools like automated rostering (79% positive feedback) and single sign-on (81% positive feedback).

For the solutions you have implemented, what feedback have you received from teachers?



Scale your impact. Mobilize mindshare around cybersecurity by training all roles on your staff. Clever provides accessible, on-demand cybersecurity training for educators and administrators. Complete Clever Academy's cybersecurity training modules: educators | administrators. *Note: Clever login is required for access.

“An ounce of prevention goes a long way in cybersecurity efforts. Developing trainings for teachers and students alike to develop cyber-literacy can be among the most effective ways to eliminate the threat. Districts can also partner with cyber insurance providers to take advantage of discounts and free services – like risk assessments – they might offer to understand risks and develop a plan to eliminate them.

ERIN MOTE | EXECUTIVE DIRECTOR AND CO-FOUNDER | INNOVATEEDU

Technology: Tomorrow's Cybersecurity Tools to Safeguard Schools

As cyberthreats persist, administrators want to adopt more technologies to safeguard both teachers and students. However, with limited budgets and staffing shortfalls, most districts lack the resources to fund and implement these new solutions. And even when they manage to do so, usability concerns highlight the growing need for user-friendly tech.

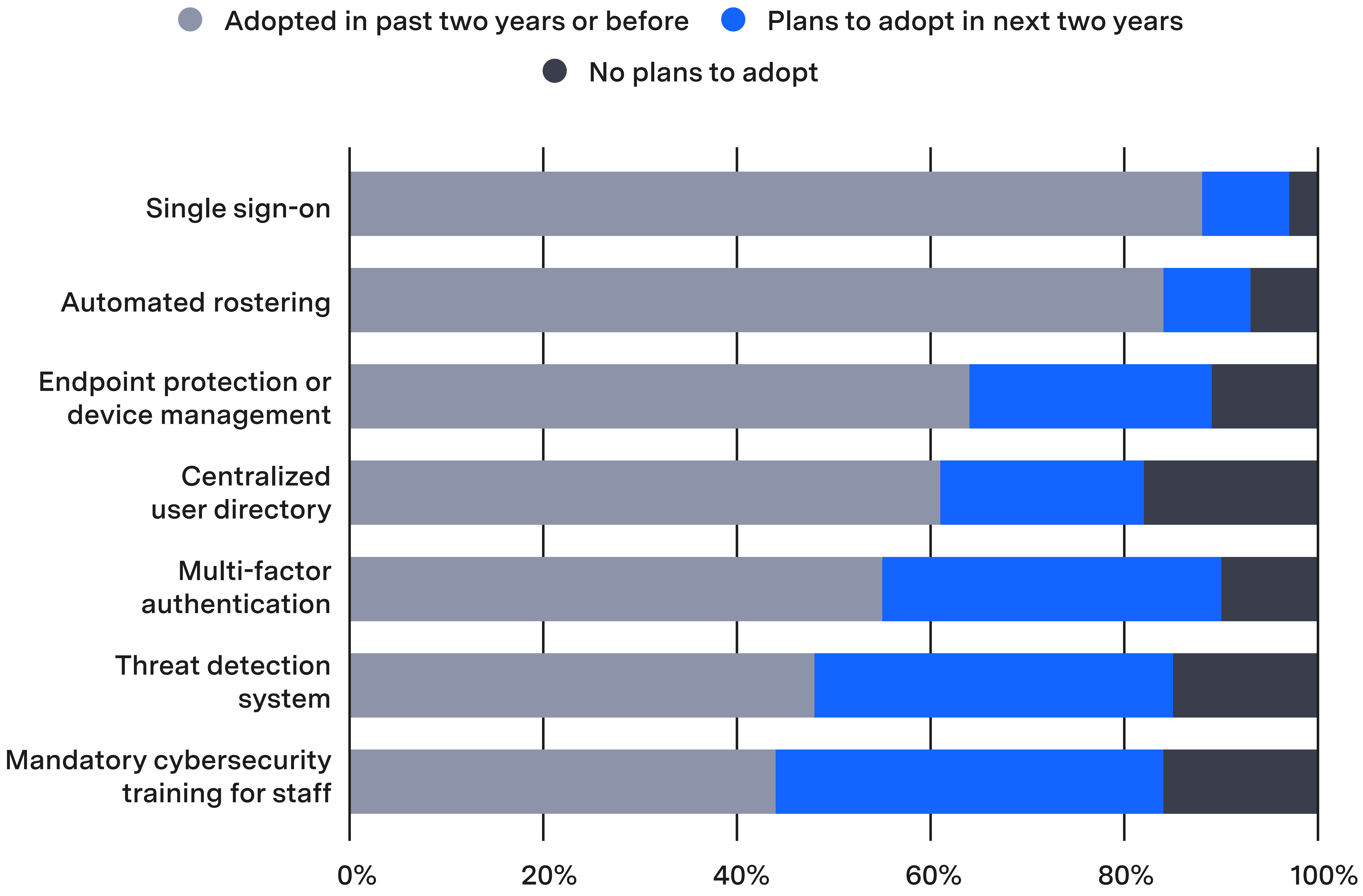
In Seeking Solutions, Most District Leaders Want New Tools

The past two years have seen an increase in adoption across many cybersecurity solutions as districts explore new approaches, while also relying on steadfast solutions – such as staff training – to bolster security.

Over 90% of surveyed districts will have adopted automated rostering and single sign-on technologies in the next two years if they have not already.

89% of districts report they are considering new technologies to address cybersecurity; top priorities include enhancing identity and access management systems (44%), stronger data encryption methods (31%), and zero trust security architecture models (26%). Not surprisingly, cybersecurity training for staff tops the list with 63% of districts reporting it as a top tactic for addressing their security concerns.

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



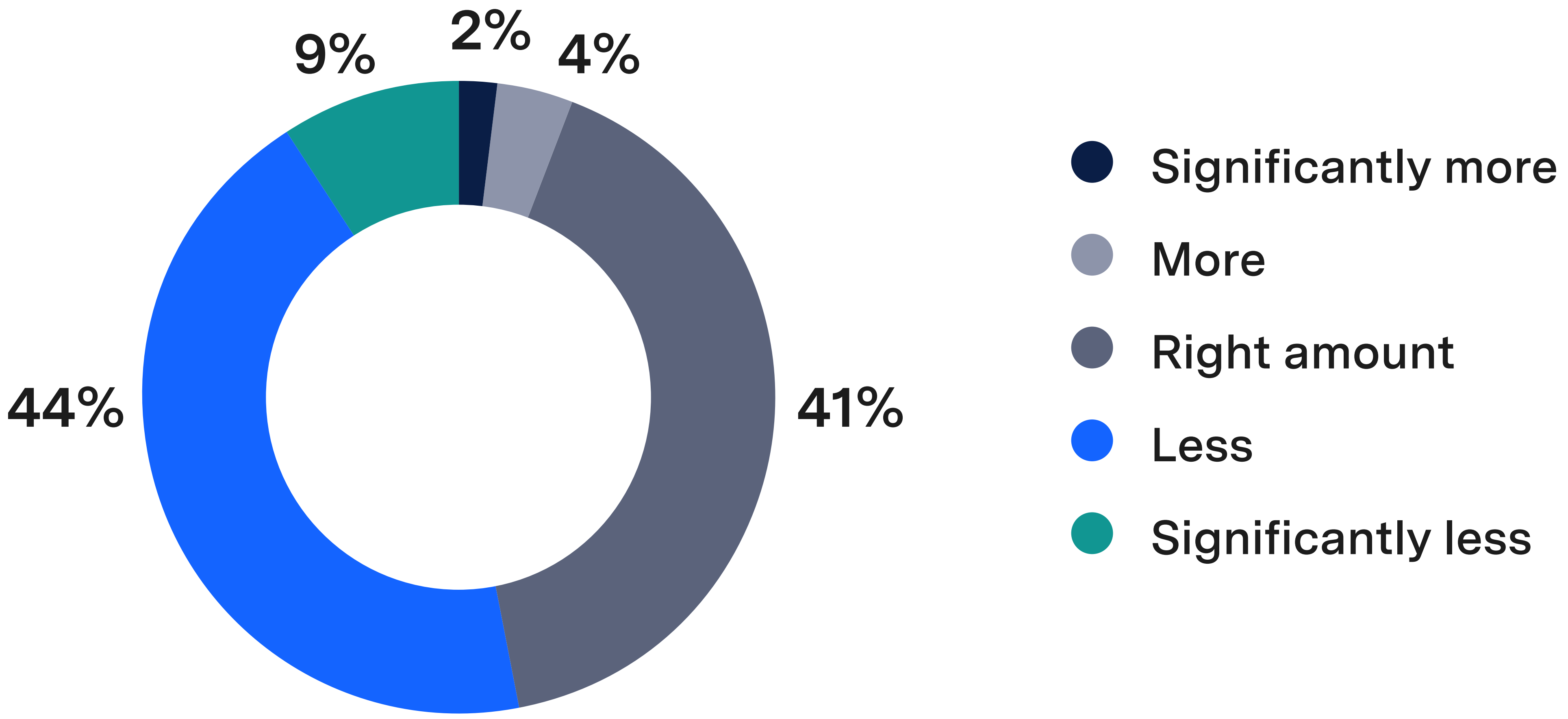
Tighter Budgets Hinder Cybersecurity Purchasing in Districts

While most districts expect their cybersecurity budgets to rise amid growing threats, many feel their current spending remains insufficient, highlighting potential resource and personnel gaps.

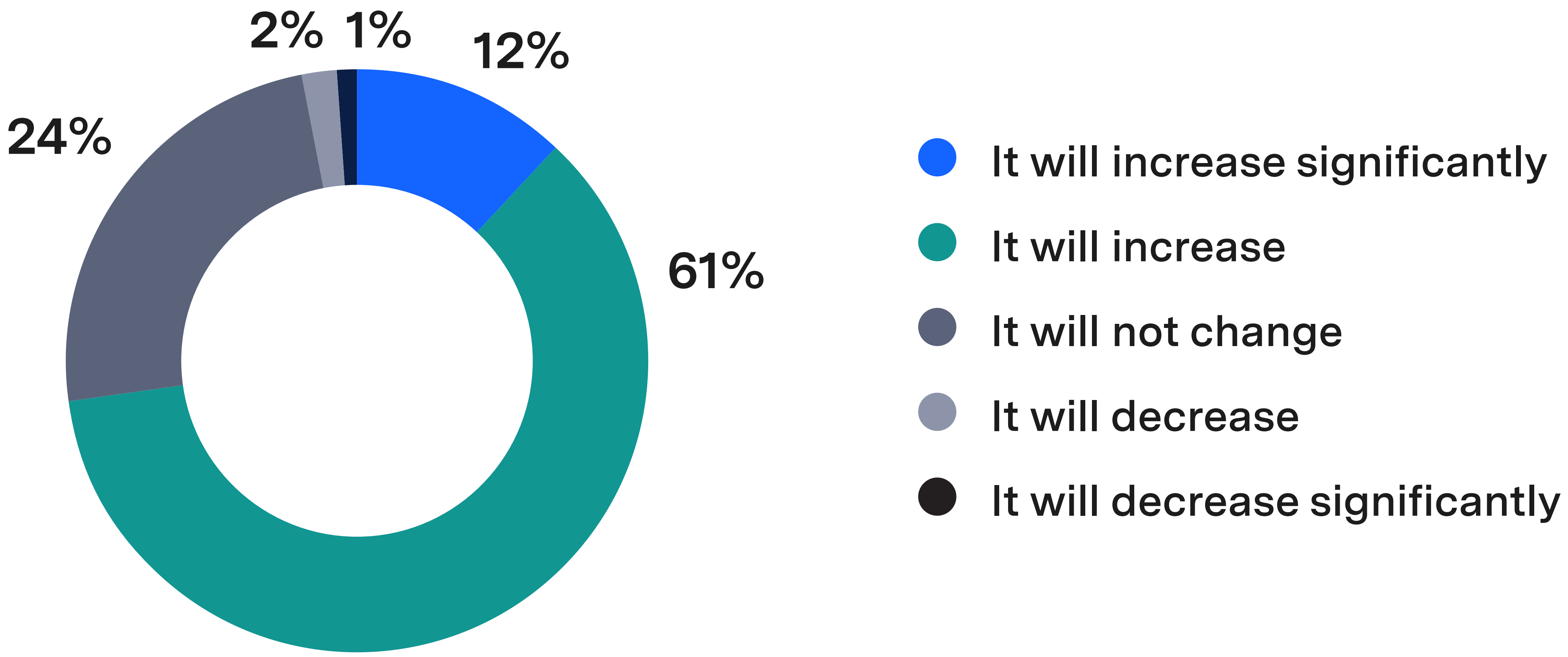
53% of administrators report their district spending less than they should on cybersecurity technology, highlighting the urgent need for increased investment. However, a promising 73% foresee their district's cybersecurity budget expanding in the next 2 to 3 years, indicating a positive trajectory towards bolstering digital defenses.

These findings track with the recent SETDA report, which found that despite cybersecurity being a top need, it is not receiving enough funding or support.

Which of the following best describes your perception of cybersecurity spending in your district/CMO?



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



Clever

> “ Districts should be able to clearly communicate the potential risks and the financial impact of cyber incidents to relevant stakeholders; and advocate and allocate funding specifically for cybersecurity initiatives in schools, enabling districts to invest in training, tools, and infrastructure.

JULIA FALLON | EXECUTIVE DIRECTOR | SETDA

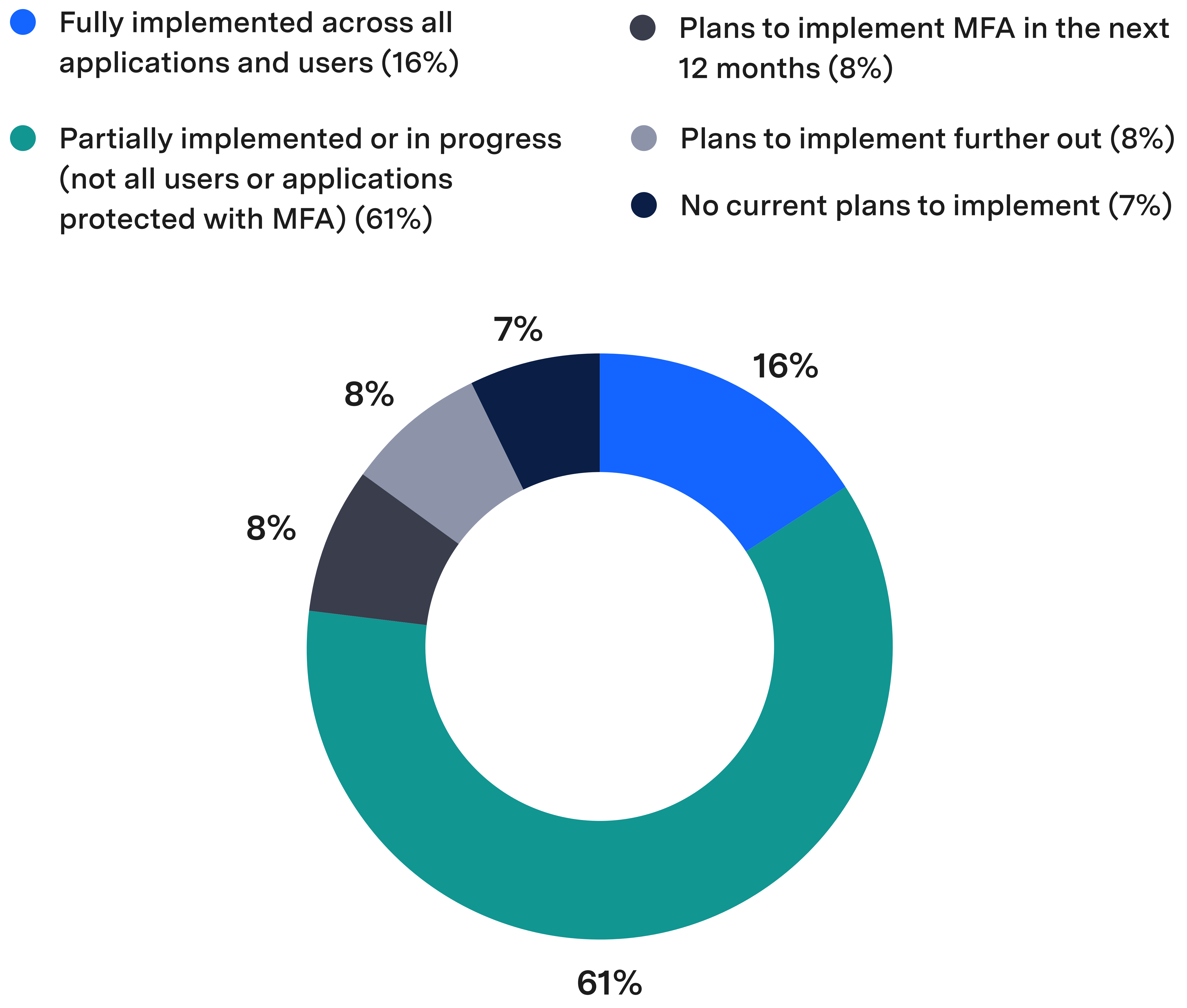
Multi-Factor Authentication Must Work for the Classroom

Despite widespread acceptance of MFA's value, district-wide deployments are scarce, stalled by friction from usability issues which complicate broad rollouts.

55% of districts have adopted MFA or plan to within the next two years. However, only 16% have fully implemented MFA across all applications and users, while 61% are in a partial or in-progress stage.

(Continued on page 18)

Which of the following reflects the implementation status of Multi-Factor Authentication (MFA) in your district?

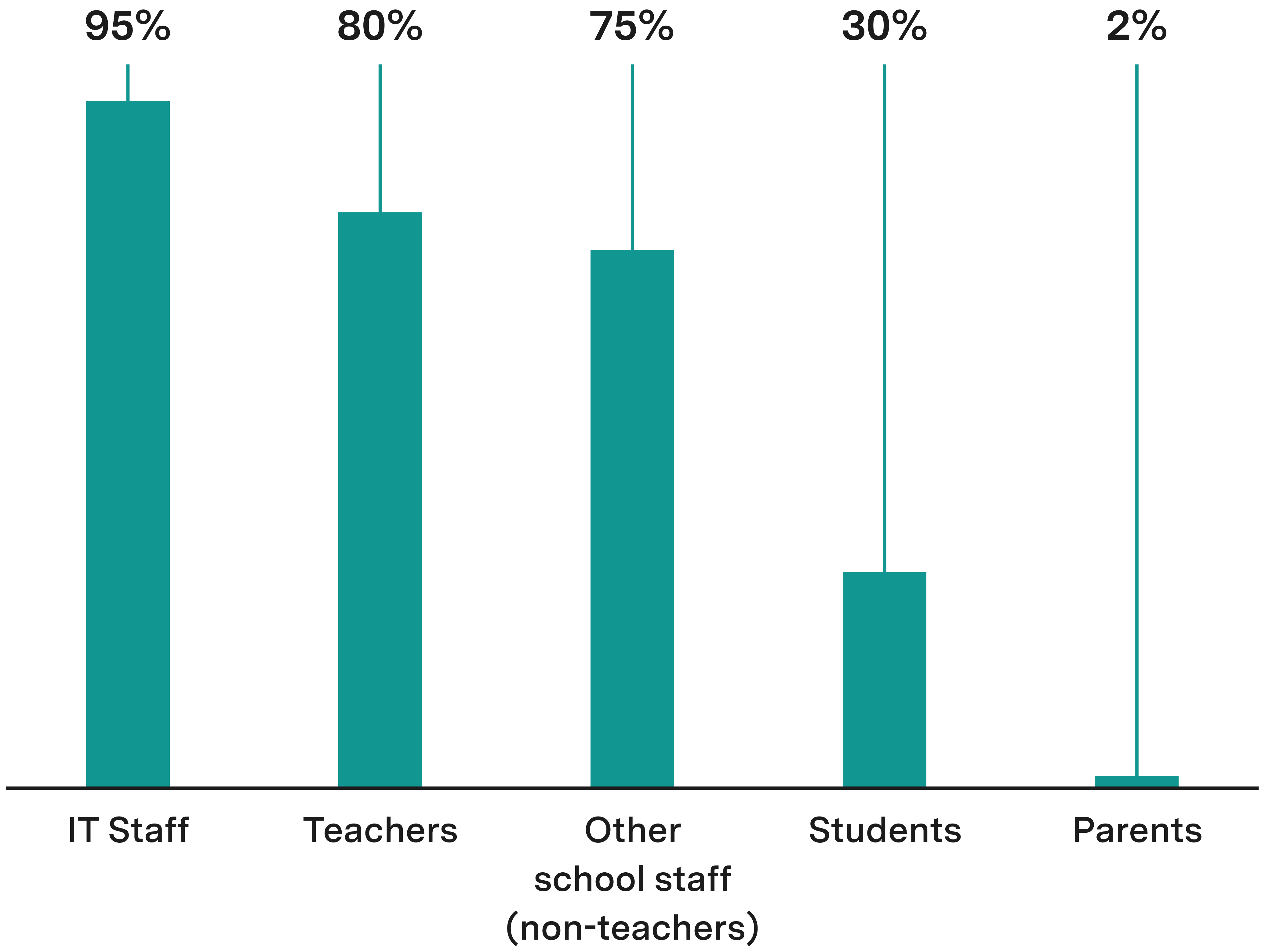


Multi-Factor Authentication Must Work for the Classroom

95% of districts are implementing (or plan to implement) MFA for IT staff, followed by 80% for teachers, and 75% for other school staff. Contrastingly, merely 30% of districts are extending MFA policies to students.

District challenges to MFA adoption include lack of current prioritization (43%), concerns on usability (30%), and resource constraints (23%). For those adopting MFA, mobile apps on personal devices (69%) and SMS text messages (65%) are the favored second-factor methods – which may prove difficult for students.

For which of the following groups is Multi-Factor Authentication (MFA) implemented or planned to be implemented in your district? (Select all that apply)



Focus on user-friendly cybersecurity. Choose tools that are straightforward and easy to use. Consult Clever's guide for MFA solutions in schools.

“Instead of just enforcing multi-factor authentication, we focused on understanding our users’ challenges. By incorporating it into their daily workflow without causing disruptions, we achieved success. Our empathetic approach was crucial in making this implementation work.

LEE ITSON | DISTRICT TECHNOLOGY COORDINATOR | SCHOOL DISTRICT OF RANDOM LAKE

Partners: The Broader Ecosystem of Cybersecurity Defense

From edtech companies ensuring robust safeguards to the evolving requirements of cybersecurity insurance policies, external factors play a critical role role in supporting a district's comprehensive approach to digital security.

Vendors' Cybersecurity Efforts Facing Increasing Scrutiny

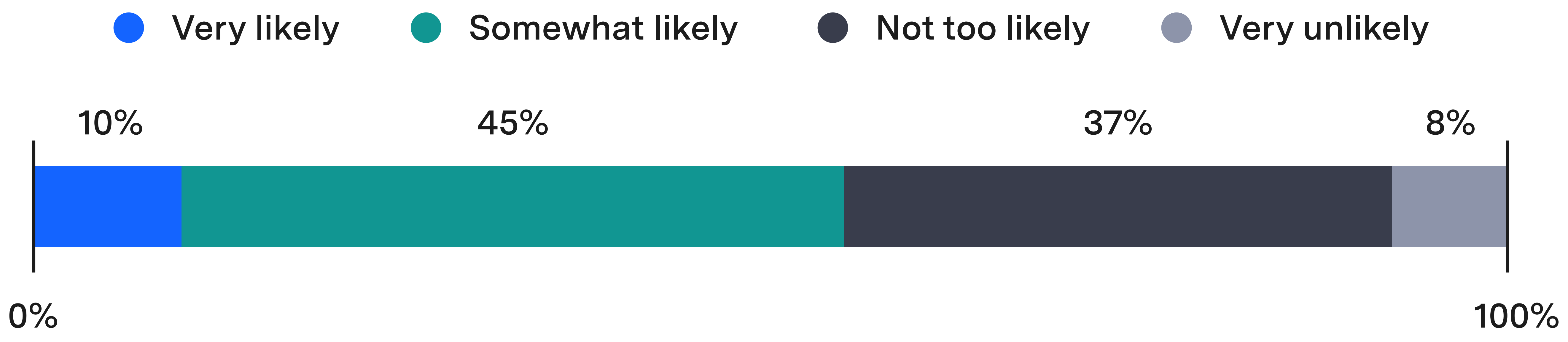
Vendor security is an integral part of layered security. Regular audits and vendor reports contribute to a comprehensive cybersecurity strategy that bolsters classroom experiences as districts continue to expect the utmost security from the tools they use.

More than half of districts (55%) have updated their vendor security requirements in the past two years, reflecting an evolving approach to vendor security.

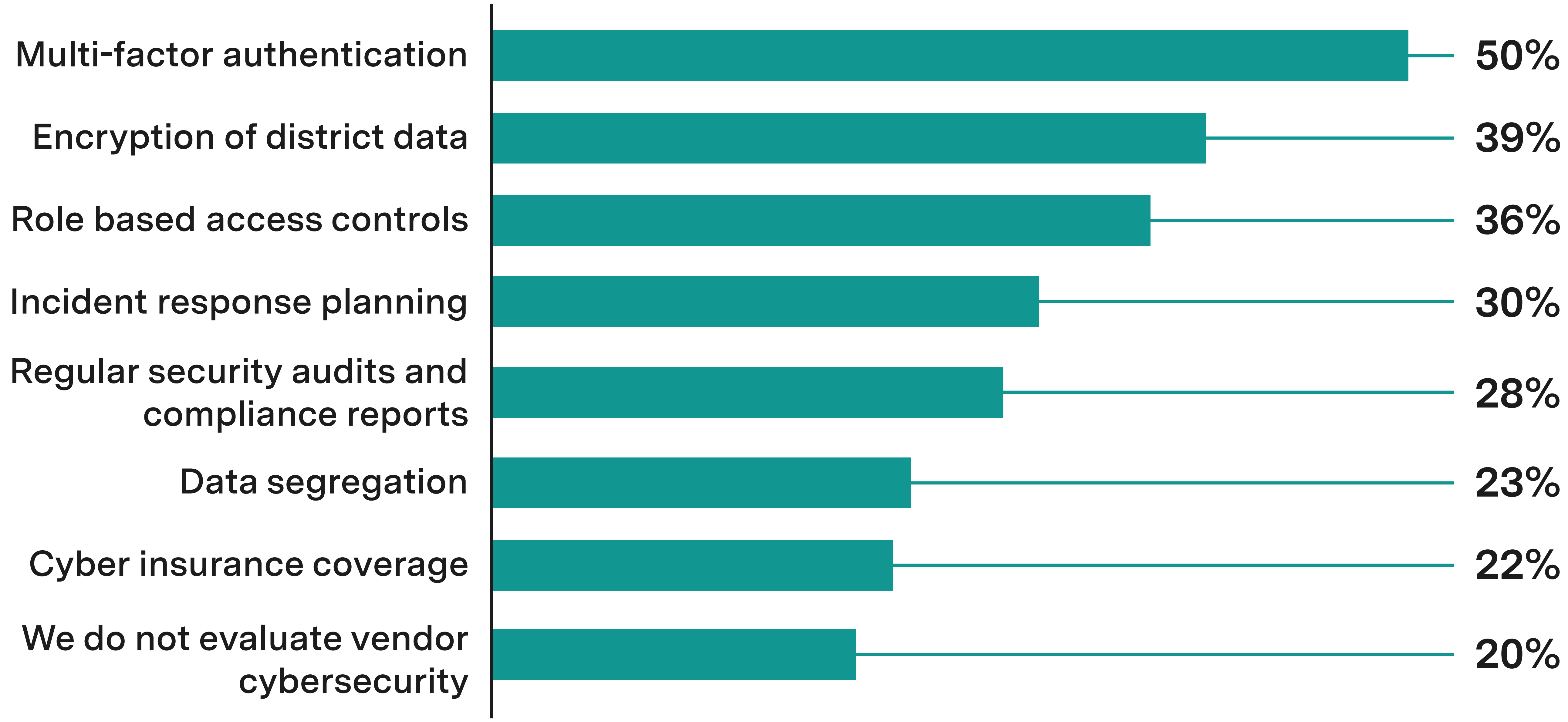
Scrutiny will continue as 55% of districts expect requirements to change in the next year.

The most common cybersecurity practices evaluated or required by districts (of vendors) include MFA (50%), data encryption (39%), and role-based access controls (36%).

In light of increasing cybersecurity risks, how likely is your district to change vendor selection requirements in the next year?



Which of the following vendor cybersecurity practices does your district evaluate or require (select all that apply)?



> “Vetting vendors for data security has proven difficult, as many don’t understand our requirements and we struggle to get clear answers about encryption and where data is kept. Vendors need to simplify this information rather than hide it in lengthy policies. It’s time for edtech companies to step up and share the responsibility for protecting student data.

GEOFF JONES | DIRECTOR OF TECHNOLOGY | RIVER VALLEY SCHOOL

Cybersecurity Insurance Becoming an Essential District Purchase

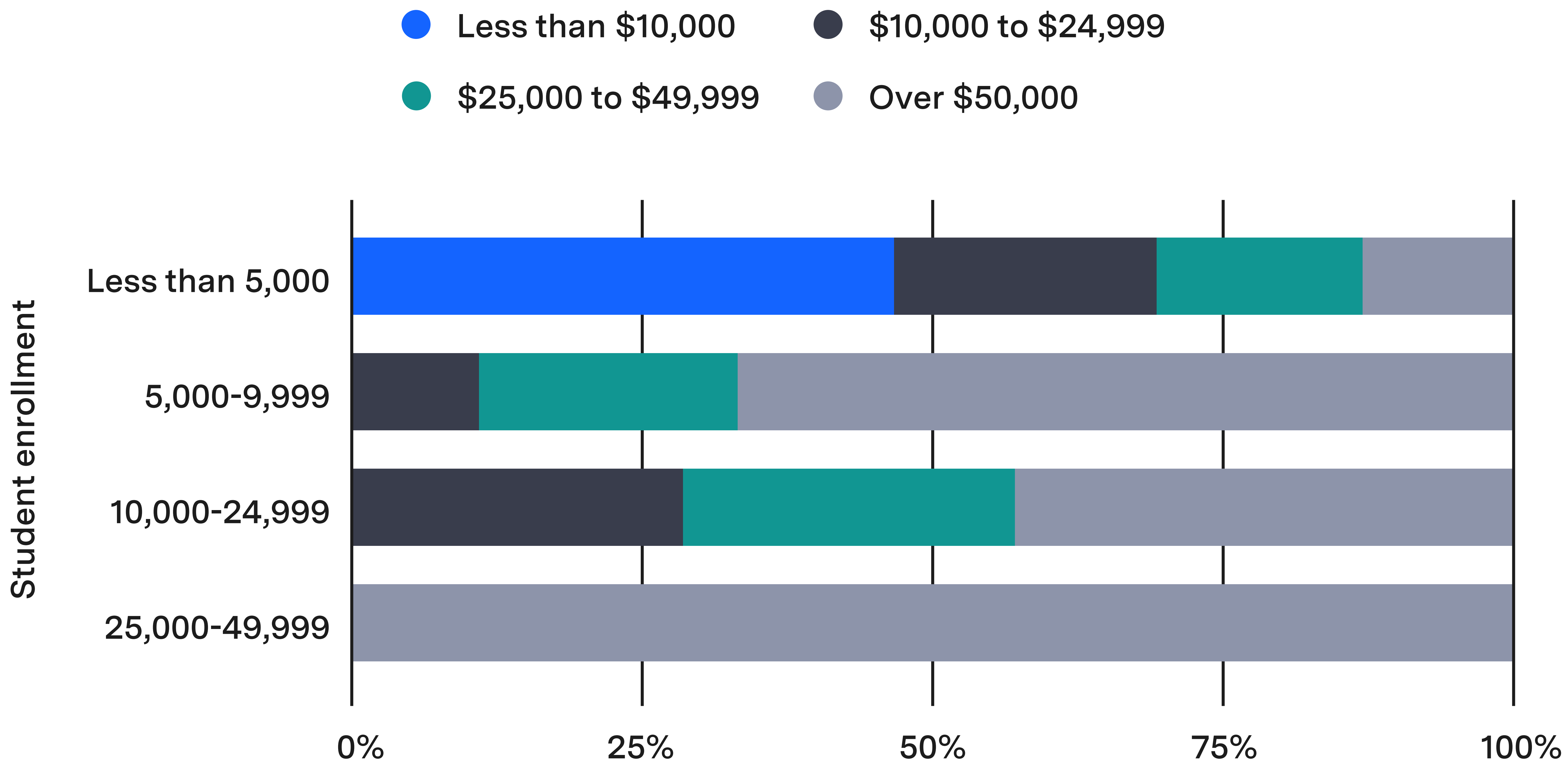
As cybersecurity attacks continue to increase, insurance is commonplace for districts across the U.S.

82% of surveyed districts have cybersecurity insurance or are planning to acquire it. Of note, 86% of rural districts have full or limited coverage compared to 71% of urban districts.

For districts with cybersecurity insurance, premium costs vary by district size and student enrollment.

(Continued on page 24)

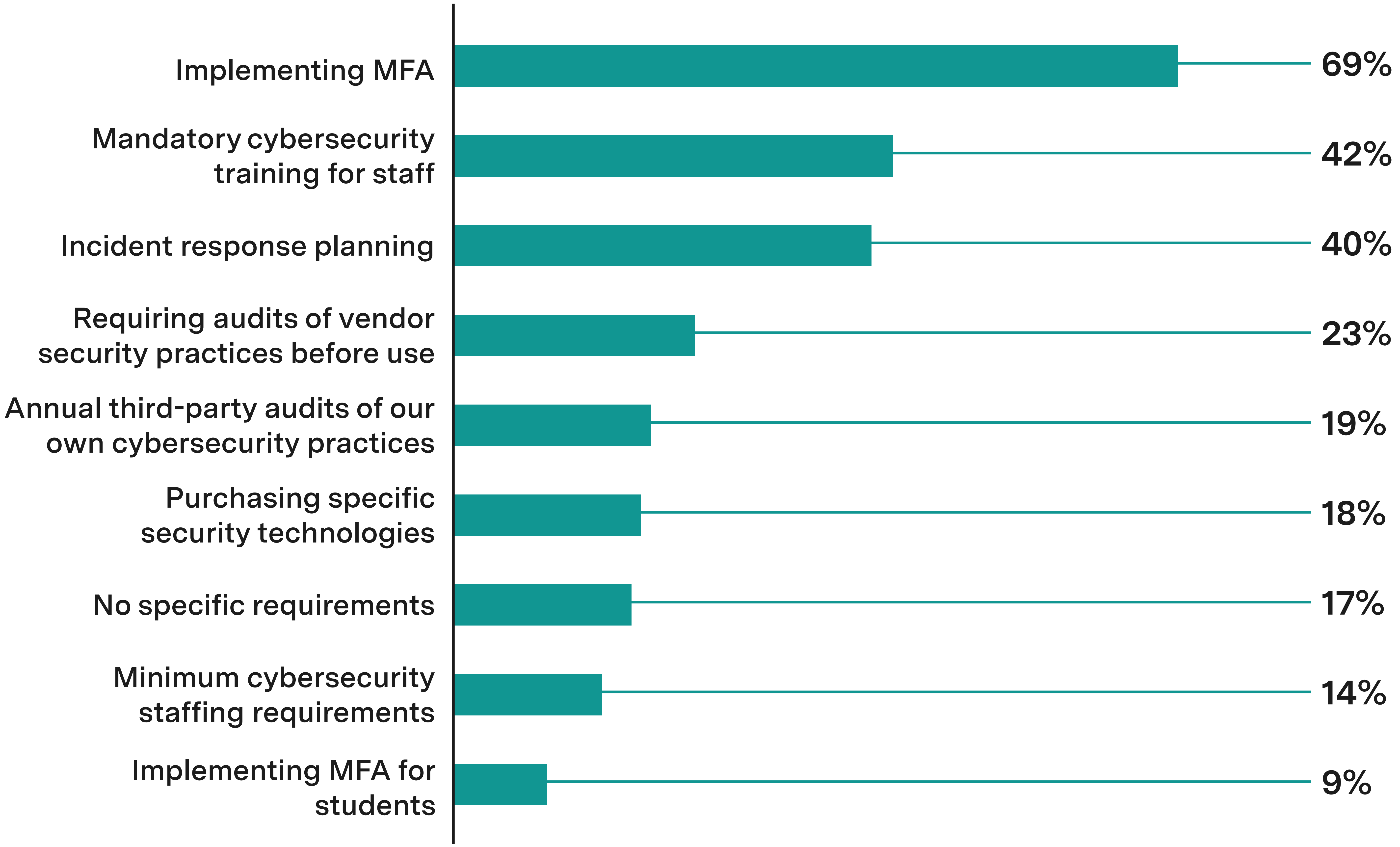
Annual premium cost of cybersecurity insurance policy by district enrollment:



Cybersecurity Insurance Becoming an Essential District Purchase

Most cybersecurity insurance policies include requirements to enhance security measures. Implementing multi-factor authentication (MFA) is the most common, with 69% of policies mandating it. Cybersecurity training (42%) and incident response planning (40%) are also reported as common requirements of insurance policies.

Which of the following requirements, if any, are included in your district's cyber insurance policy (select all that apply)?



Establish clear criteria for vendor selection. Establish clear criteria for evaluating and selecting edtech vendors and partners as outlined in Clever's blog.

> “Our collaborative stance on cybersecurity was strengthened by experiencing a major ransomware attack. It emphasized the need for cybersecurity insurance and the critical role of cross-departmental cooperation in negotiating and understanding the financial aspects of cyber risk.

CHRISTY FISHER | CHIEF TECHNOLOGY OFFICER | NORMAN PUBLIC SCHOOLS

Clever

Clever is on a mission to connect every student to a world of learning. More than 75% of U.S. K-12 schools now use Clever to power secure digital learning experiences. With our platform for schools and a network of leading application providers, we're committed to advance education with technology that works for students everywhere. Clever, a Kahoot! company, has an office in San Francisco, CA, but you can visit us at clever.com anytime.

W/A Whiteboard Advisors

Whiteboard Advisors is a mission-driven communications, research, and consulting firm that supports organizations working to advance educational equity and economic mobility. Our clients include the nation's most respected philanthropies, companies, nonprofit organizations, and investors. Our work is truly multidisciplinary, sitting at the intersection of business, policy, practice, and the media.

Clever