Malwarebytes

Lessons in cybersecurity

How education coped in the shift to distance learning

Contents

1 | Executive summary

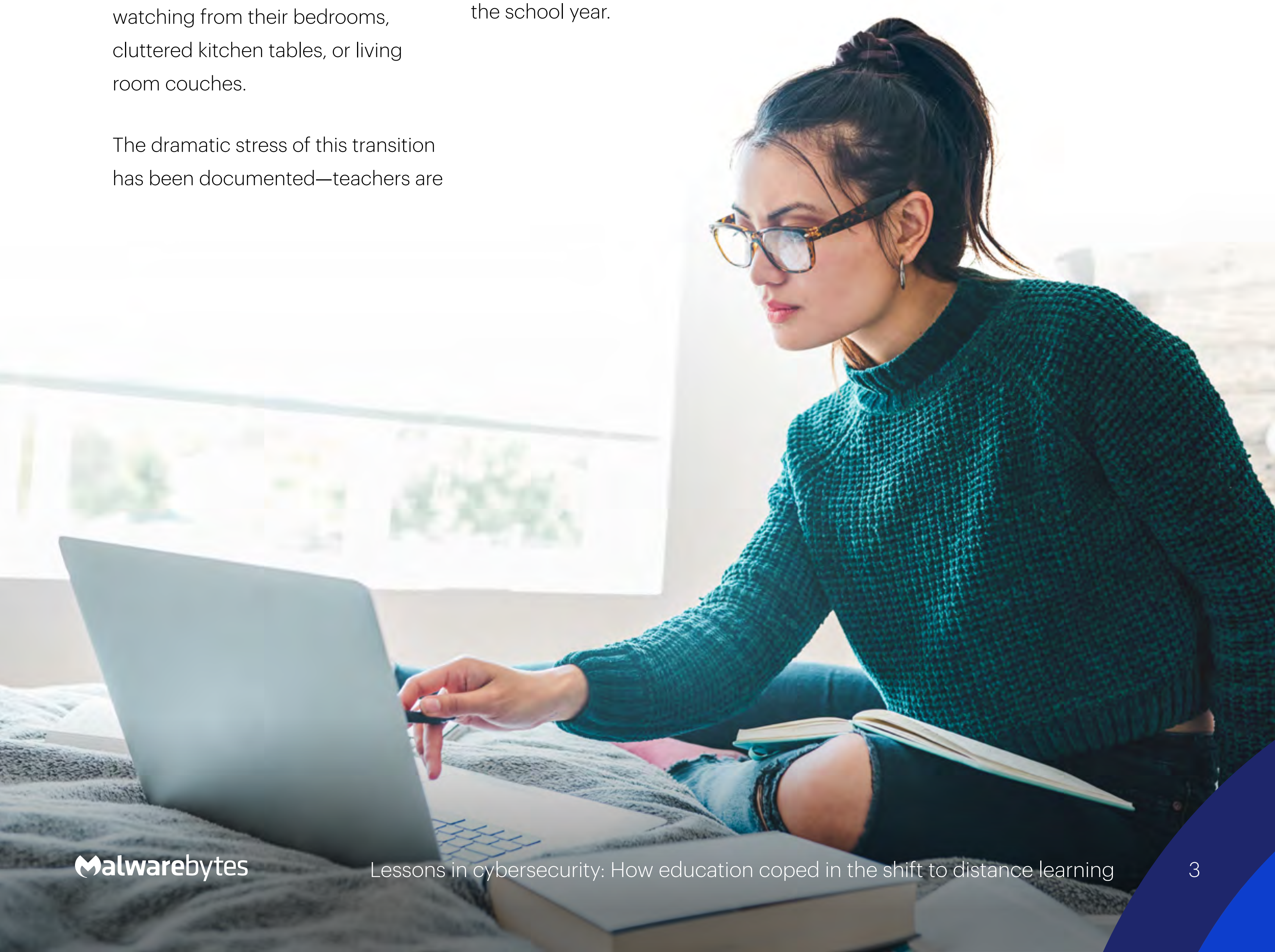
Education in the United States faced a crisis this year. The looming threat of the coronavirus—which spreads easily in highly-populated, enclosed rooms—forced schools across the country to develop new strategies for education.

No longer safe in hallways and classrooms, many teachers, administrators, and students moved their jobs and their routines online. "Hybrid" models of education emerged. Some students returned to their classroom, but many met only in Zoom conference rooms. Some teachers utilized their classroom space to at least broadcast their lessons to students who were watching from their bedrooms, cluttered kitchen tables, or living room couches.

The dramatic stress of this transition has been documented—teachers are working more hours than ever and parents are pulled between work and 24/7 childcare—but perhaps for the first time, Malwarebytes has revealed how this transition has stressed the cybersecurity posture of schools and school districts.

In short, schools need to do a lot of catch up to stave off any potential cyberattacks in the second half of the school year.

Schools need to do a lot of catch up to stave off any potential cyberattacks in the second half of the school year.



Methodology

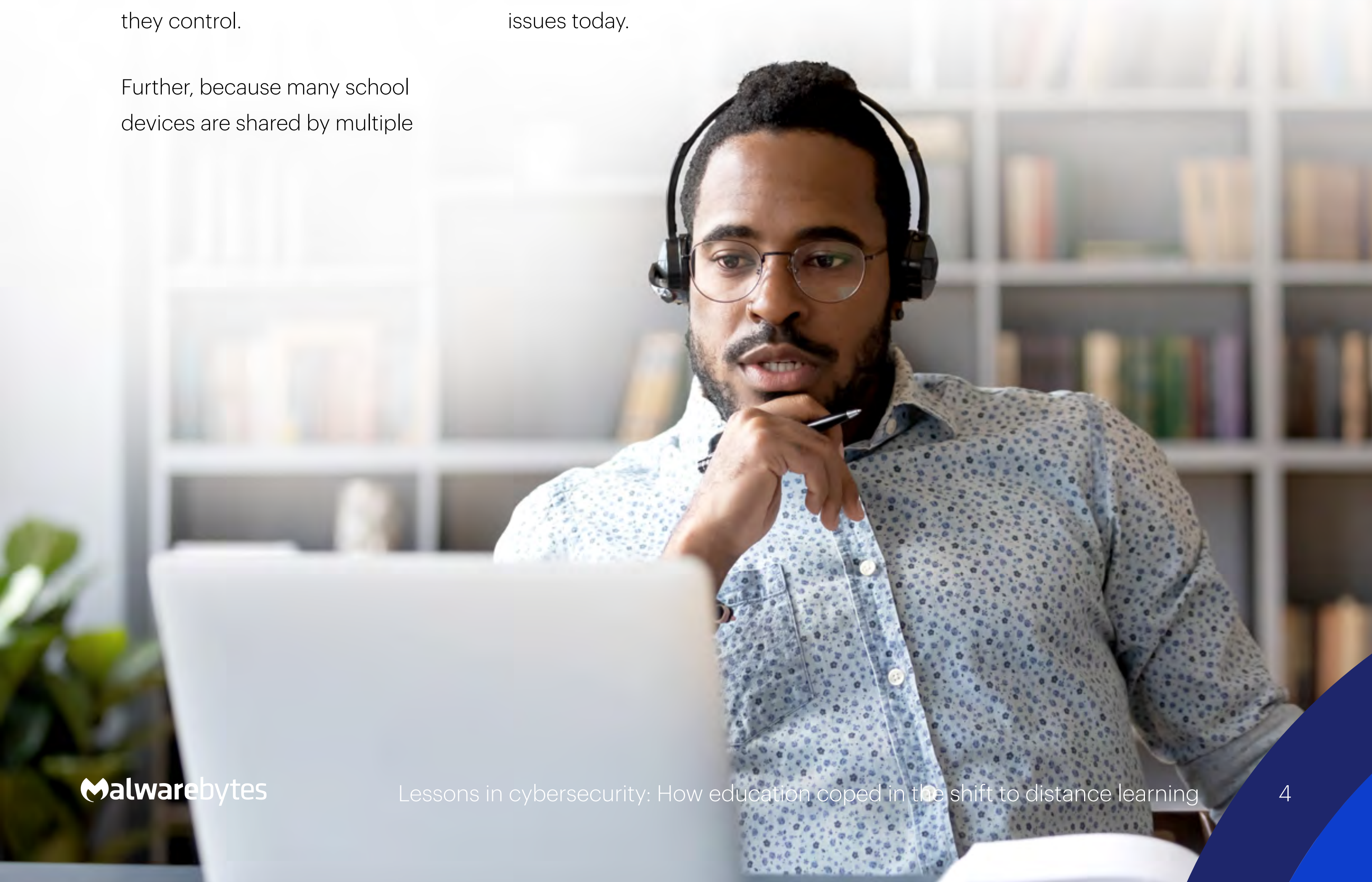
To determine an accurate reading of the situation that many schools face, we went straight to the source. This is because schools and school districts present unique challenges in data interpretation.

For instance, we cannot guarantee that malware detections always signal the work of malicious threat actors. Plainly, students like to experiment with their devices, whether they're trying to cause trouble or not. And with far fewer years—read, probably zero—of cybersecurity training to rely on, students may be more likely to click on malicious ads, fall for basic phishing scams, download fraudulent email attachments, and test the boundaries of the devices they control.

Further, because many school devices are shared by multiple students, we cannot assume that one device equals one user. This complicates any data analysis when trying to find iron-clad trends.

For our report, we conducted two, parallel surveys. The first survey targeted IT decision-makers at schools across the United States. The second survey targeted students enrolled in K–12; students working on obtaining a bachelor's degree, associate's degree, or attending trade school; and students enrolled in any post-graduate program. Our IT decision-maker survey received data from 75 respondents, and our student survey received data from 500 respondents, offering a unique look into how schools and their students view cybersecurity issues today.

We conducted two, parallel surveys, polling 75 IT decision-makers and 500 students



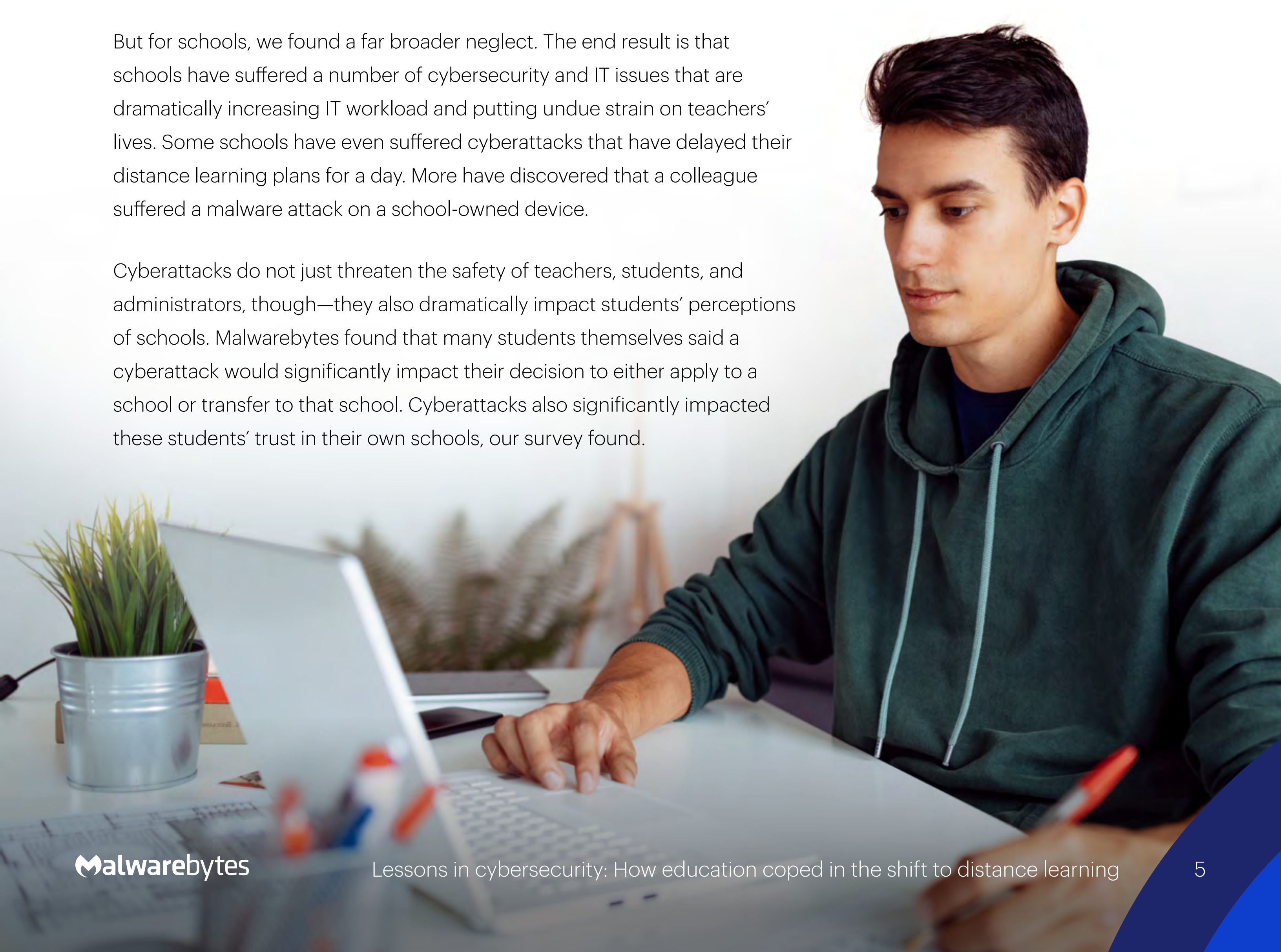
Key takeaways

Our surveys showed that, for many schools, there are some untaught lessons.

Broadly, while schools admirably attempted to provide teachers, students, and parents with extra tools and software to teach and learn—which is their primary mandate—many schools failed to do this safely.

Nearly half of all schools simply did not change anything about their cybersecurity preparations in transitioning to distance learning. Earlier this year, we saw the detrimental impacts that companies suffered after their individual failures to, for instance, install antivirus software on work-issued machines or review new, required software for privacy and cybersecurity vulnerabilities.

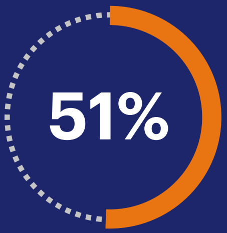
> **Cyberattacks do not just threaten the safety of teachers, students, and administrators, they also dramatically impact students' perceptions of schools.**



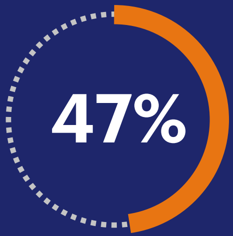
But for schools, we found a far broader neglect. The end result is that schools have suffered a number of cybersecurity and IT issues that are dramatically increasing IT workload and putting undue strain on teachers' lives. Some schools have even suffered cyberattacks that have delayed their distance learning plans for a day. More have discovered that a colleague suffered a malware attack on a school-owned device.

Cyberattacks do not just threaten the safety of teachers, students, and administrators, though—they also dramatically impact students' perceptions of schools. Malwarebytes found that many students themselves said a cyberattack would significantly impact their decision to either apply to a school or transfer to that school. Cyberattacks also significantly impacted these students' trust in their own schools, our survey found.

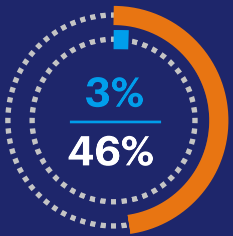
Here are some of the key takeaways we found from both IT decision-makers and students:



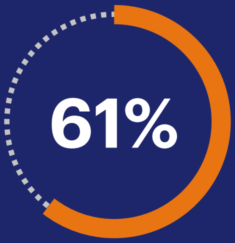
of IT decision-makers said that no one—not students, teachers, staff, or guests (including parents)—were required to enroll in cybersecurity training before the new school year began



of IT decision-makers said their schools developed “no additional requirements”—no distance learning policy read-throughs, no cybersecurity training, no antivirus tool installations—for the students, faculty, or staff who connected to the school’s network

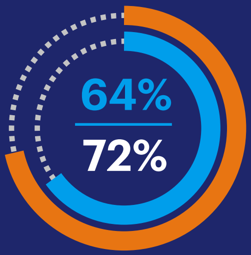


A remarkably low number of IT decision-makers said their schools suffered a cyberattack—just 2.7%—and, yet, 46.2% of students said their schools suffered a cyberattack

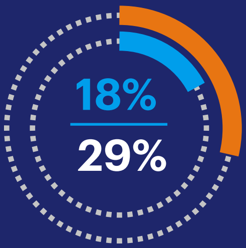


of students said a cyberattack resulted in a significant or strong impact on their trust in their school

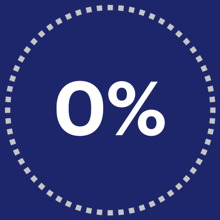
Cybersecurity preparation matters deeply—for respondents who engaged in a variety of cybersecurity best practices before transitioning to a distance learning model, **none suffered a cyberattack**, and **none canceled a single day of distance learning** because of a cyberattack:



63.6% of these well-prepared respondents said they suffered “sustained, excess IT workload” compared to the 72% of all respondents

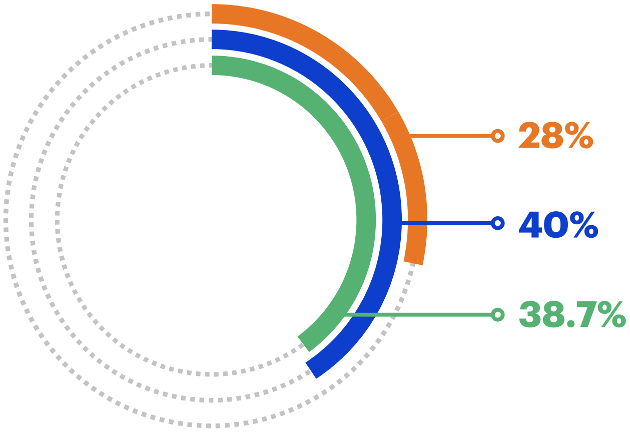


18.2% of these well-prepared respondents said “teachers or students have suffered a Zoombombing attack” compared to the 29.3% of all respondents



Zero well-prepared respondents said they suffered a school-wide cyberattack

With distance learning in full swing, concerns remain with device shortages:



28% of IT respondents said their schools are missing laptops, computers or tablets for teachers

40% are missing those tools for parents and students

38.7% worry that teachers or students are too quickly using up the data on school-provided WiFi hotspots

Despite the harmful impacts, schools should not receive all of the blame. They often work with limited staff and limited budgets. In fact, 20% of IT decision-makers said they had trouble convincing their schools to "invest in cybersecurity protections (including purchasing new antivirus software, hosting cybersecurity training, providing up-to-date devices, etc.)"

We wish that better funds did not correlate with better cybersecurity, but when looking at our IT decision-makers who suffered the fewest cybersecurity and IT impacts, none reported facing any budget limits in actually deploying cybersecurity protections.

In the end, we're halfway through the school year for many, but it is never too late. As we found, there is no silver bullet to school cybersecurity. Instead, there is a series of best practices that can protect a school from a cybersecurity incident. Not only that, but some of those same practices can help a school's faculty focus on what matters most—educating students.

2 | Bulking up for immediate need

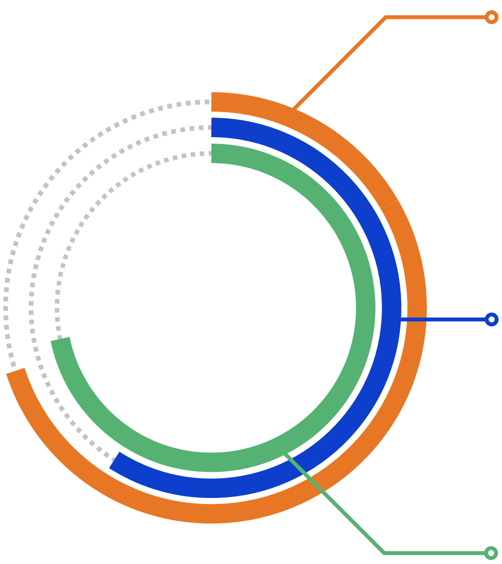
In transitioning to several distance learning models, schools across the US worked fast to get their teachers and students online in order for classes to resume as quickly as possible.

But before the educating could begin, schools had to ensure that teachers and students had the right equipment to get started.

Schools distributed thousands of Chromebooks, tablets, and hotspots to student families (72%) and devices such as external microphones, webcams, and laptops to teachers (58.7%). Nearly three quarters (70.7%) of schools deployed new software needed for distance learning, such as Zoom, Remind, and Google Classroom. It's clear that most schools were trying hard to support both staff and students in what was a completely unprecedented and challenging time.

IT decision-makers acted well to supply teachers and students with tools and software.

How did distance learning change your schools' issuance of devices and software?



70.7%
We deployed new software tools to provide distance learning (video communication software like Zoom, communication software like Remind, collaboration and document sharing software like Google Classroom, etc.)

58.7%
We deployed new devices to teachers to provide distance learning to students (laptops with built-in webcams, external microphones, external webcams, WiFi hotspots, etc.)

72%
We deployed new software tools to provide distance learning (video communication software like Zoom, communication software like Remind, collaboration and document sharing software like Google Classroom, etc.)

But that wasn't an easy feat. And, as many schools returned after the summer break, they faced several challenges for the new academic year—and a new normal set about by the current global pandemic. Perhaps obviously, it's been a steep learning curve for teachers and students to understand and become proficient with the new tools they must use for online learning (80%).

While it's true that most schools were able to deploy devices to students and teachers, not everyone received one and, thus, a digital divide remains. We found that, in preparing for the new school year, 30.7% of schools admitted to not being able to provide for all teachers, administrators, and staff members to work remotely, while 45.3% of schools could not provide all the devices needed for every student to attain an equal quality of education.

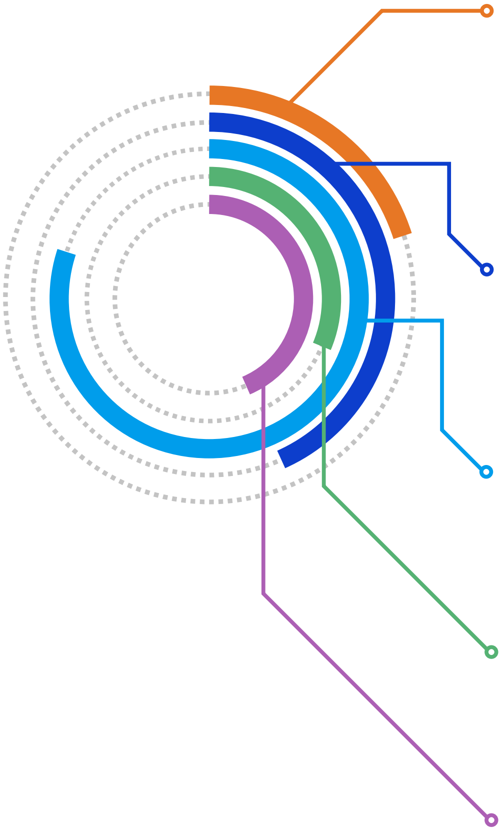
In terms of keeping devices and their users safe, 44% of schools revealed that device management had been a challenge, due to the sudden increase in the number of devices connecting to the network. On a somewhat positive note, what IT teams found the least challenging (20%) in their shift to the new normal was convincing the school or school district to invest in cybersecurity protection, such as purchasing antivirus software, conducting cybersecurity training, and more.

With that last bit in mind, we looked at how well these schools fared in preparing for the new academic year, cybersecurity-wise.

The verdict: Not very well.

IT decision-makers supported a steep learning curve for students and teachers.

What challenges did you face in preparing for the new school year?



20%
Convincing the school/school district to invest in cybersecurity protections (including purchasing new antivirus software, hosting cybersecurity trainings, providing up-to-date devices, etc.)

44%
Managing sudden increase in the number of devices either offered to teachers or connected to the school's network for the first time

80%
Steep learning curve for teachers and or students to understand and become proficient in new online learning tools

30.7%
Lacking the necessary devices for every teacher, administrator, and staff member to perform their roles

45.3%
Lacking the necessary devices for every student to obtain an equal quality of education from teachers

3 | A worrying lack of cybersecurity preparation

Many businesses had both time and resources available to prepare for the pandemic. Transitioning to remote work is fairly smooth when many tools in daily use can be used whether in the office or not.

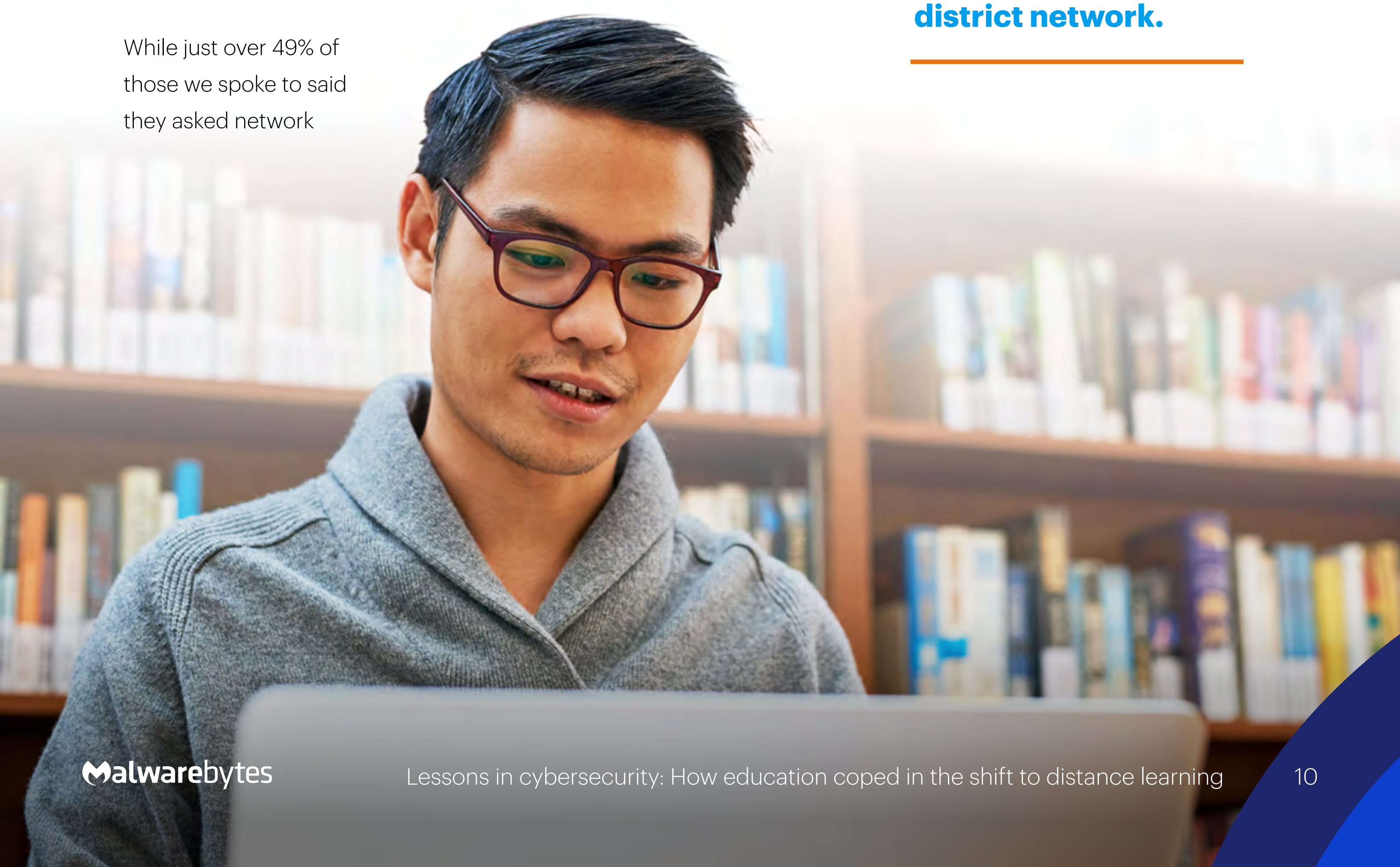
In education, where the general expectation is that everything will be on-site, there were more mixed results.

Throwing distance learning suddenly into the mix presented many challenges for staff, students, parents, and IT departments. We surveyed IT decision-makers on how their pandemic plans had taken shape, what proactive steps they took, and where they perhaps may have done better.

While just over 49% of those we spoke to said they asked network users to read through new distance learning guides or policies, proactive steps to keep things secure were somewhat thin on the ground.

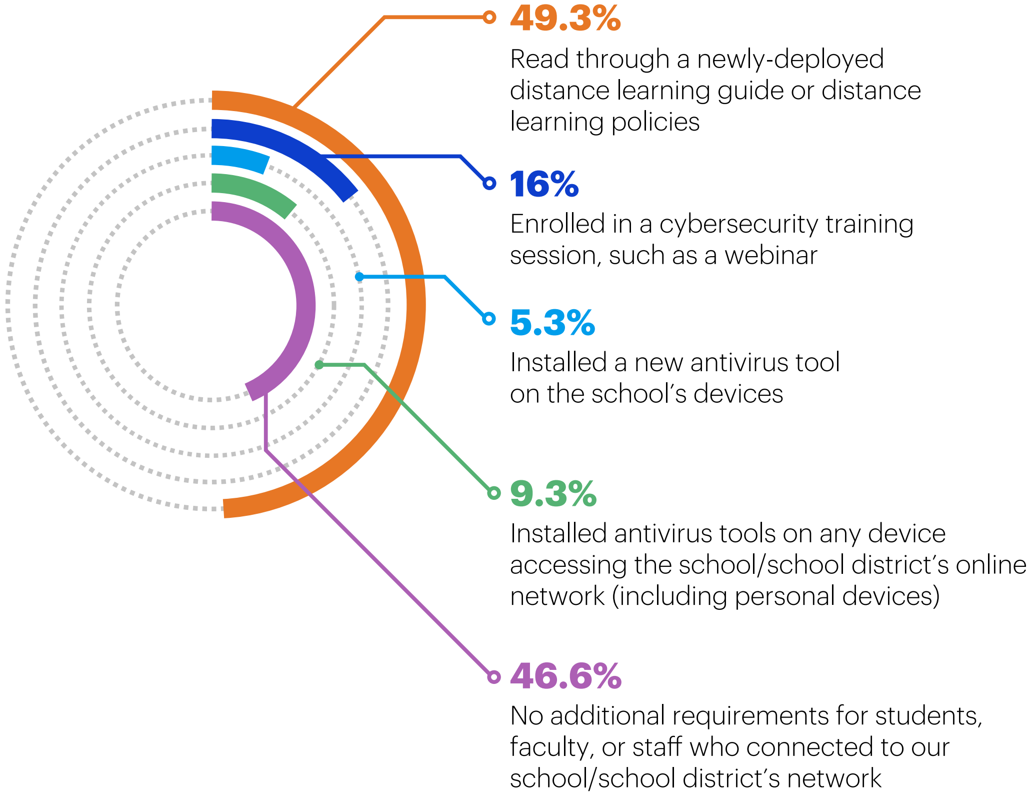
A worrying 46.7% said they developed no additional requirements for students, faculty, or staff connecting to their school or district network. Just 16% enrolled in a cybersecurity training session, such as a webinar.

A worrying 46.7% said IT decision-makers developed no additional cybersecurity requirements for students, faculty, or staff connecting to their school or district network.



IT decision-makers said their schools took few actions to stay cybersecure in the transition to distance learning.

In restarting the school year, what steps did you or your school district require for all students, faculty, or staff who connected to your school network? (Check all that apply)



Perhaps most alarming were the answers we received when we asked which groups were required to engage in new cybersecurity training. Our respondents were requested to tick all options that apply.

Before we look at the results, let's briefly explain the importance here.

As we've seen with other organizations, cybercriminals have adapted their attack techniques since the shift to remote work. Students are often vulnerable to scams and fraud, especially if they're international students. This risk is potentially made worse if students are left to fend for themselves with no advice, secure devices, or training. While staff may be prime targets, their reliance on and direct line to IT is surely a boon. For students learning from home, this is not a good situation to be in.

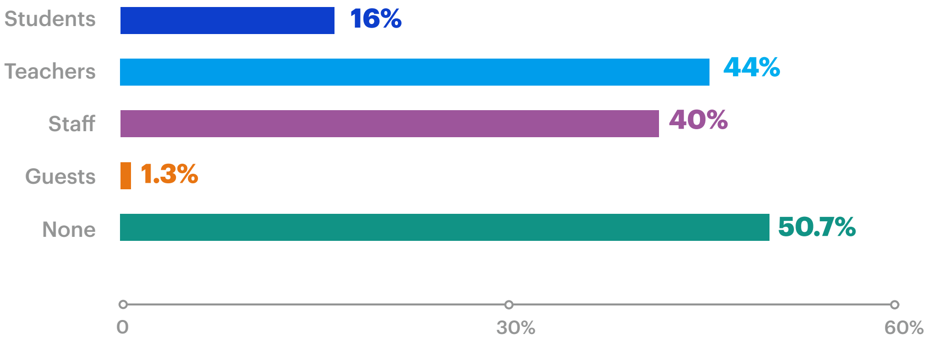
Knowing these risks, how did our respondents do?

Just 16% of students had to receive new training, versus 44% of teachers and 40% of staff (administration, janitorial, and so on).

"None" weighed in at 50.7%, which means that more than half of our respondents said no one was required take any cybersecurity training in the transition to distance learning. This is a deeply alarming result, and a stark reminder that security simply isn't high on the priority list while knee deep in a pandemic crunch. **This isn't to lay blame at the door of the schools. The various lockdowns have taken almost everybody by surprise, and it's challenging enough to suddenly move everything online at short notice, much less in a worldwide pandemic where nothing is certain.**

More than half of respondents said no one was required to take cybersecurity training before starting distance learning.

Which of the following audiences were required to engage in new cybersecurity training? (Check all that apply)



When we surveyed students, the results were similarly lower than one may have hoped. Nearly a third—29%—had to both take part in training and make use of a security tool. A little more than a fifth—22%—had to attend some form of training only, and 30.6% were not required to attend training or install security tools when connecting to their school's network.

This lack of security readiness can only contribute to network intrusions, phishing attack successes, data being compromised and/or ransomed, and students ending up in a less safe position than they would be on campus.

4 | Why cybersecurity preparation matters

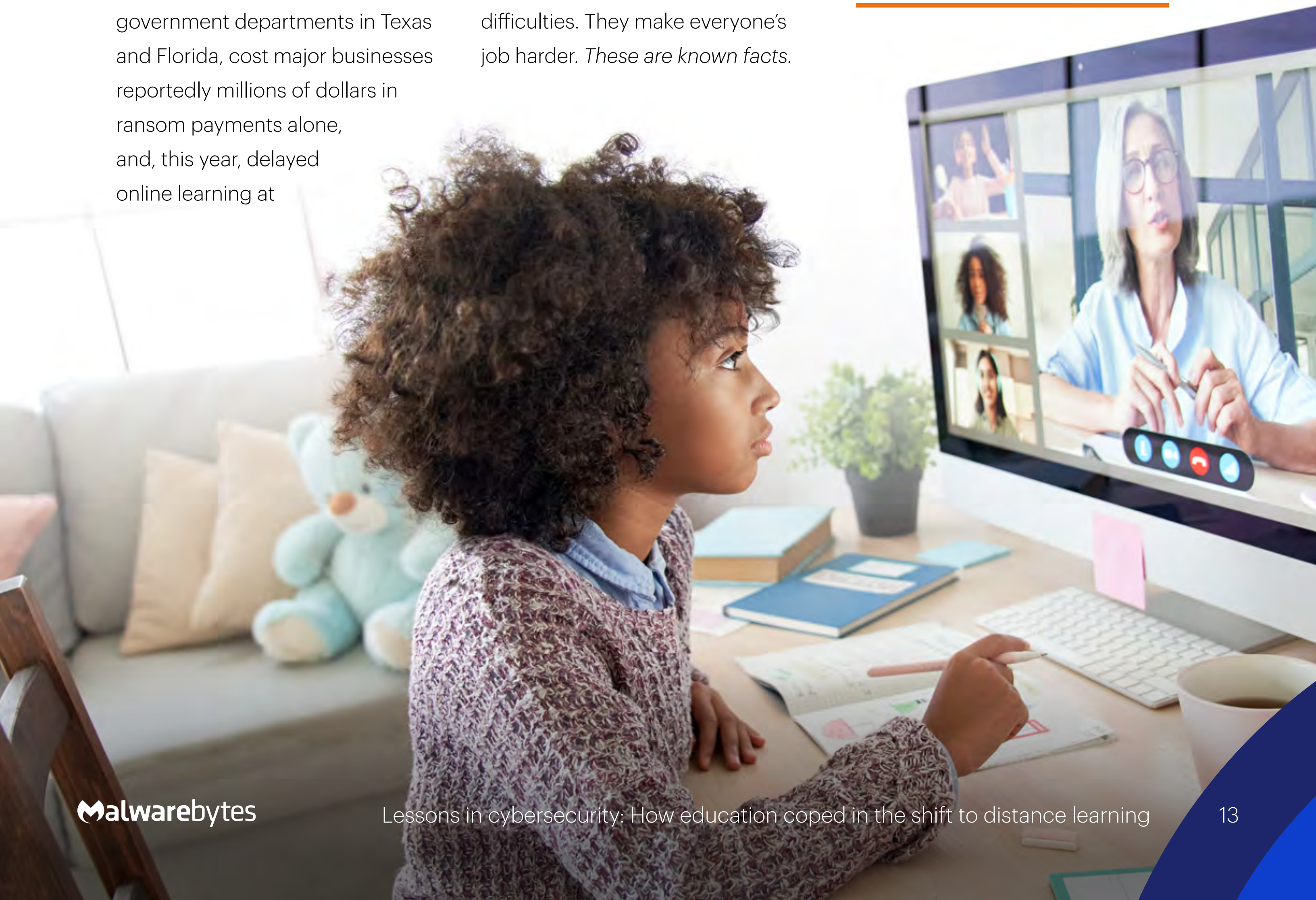
Across every sector—from healthcare to government to education—cybersecurity best practices often overlap.

Despite this, we see individuals, corporate enterprises, nonprofit organizations, and schools miss the mark every year on one of the most basic rules: The best cybersecurity defense is one that stops an attack before it happens, not one that simply cleans up a mess after it's too late.

This is because a malware attack is not just a single day of disrupted servers or one IT administrator's ruined schedule. Malware attacks have derailed entire city government departments in Texas and Florida, cost major businesses reportedly millions of dollars in ransom payments alone, and, this year, delayed online learning at schools in Rialto, California and Hartford, Connecticut.

Malware attacks that target schools today threaten students' stable access to education in an already turbulent year. They threaten to put unexpected workloads on already-stressed IT departments. They threaten to exacerbate the unfortunate trend today in which teachers are expected to not just teach, but to serve as on-call IT administrators for students and parents experiencing technical difficulties. They make everyone's job harder. *These are known facts.*

The best cybersecurity defense is one that stops an attack before it happens, not one that simply cleans up a mess after it's too late.



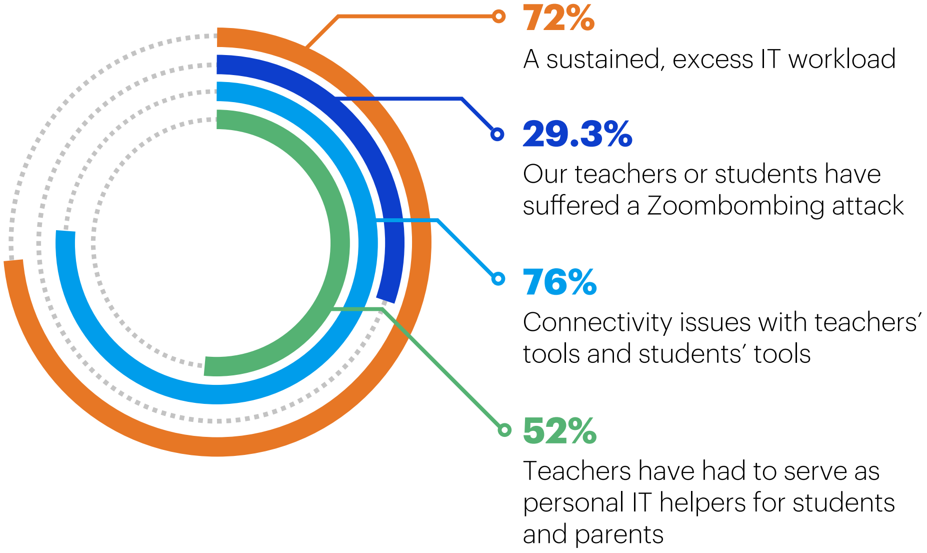
And yet, as we learned above, schools did not require cybersecurity preparations for distance learning models this year that could have helped their teachers, students, and administrators. The end result is that teachers are being stretched thin, IT staff are feeling overworked, students are suffering classroom disruptions, and schools have cancelled classes directly as the result of a cyberattack.

When we asked IT decision-makers what "impacts" their schools or school districts had suffered since the beginning of the school year, the most common response—at 76%—was "connectivity issues with teachers' tools and students' tools."

No school should be blamed for this, as this impact is often beyond a school's control. Connectivity issues rely on an enormous number of variables, from a home network's stability, to the routers that a family uses, or an Internet Service Provider's coverage.

With few cybersecurity preparations, schools suffered major consequences.

Since your school/district restarted the school year, what impacts have you suffered so far? (Check all that apply)



That said, some of our results showed serious problems that schools can work to solve with the right preparations.

We found that 72% of respondents said they suffered a "sustained, excess IT workload," 52% said that "teachers have had to serve as personal IT helpers for students and parents," and 29.3% said their teachers or students had suffered "a Zoombombing attack."

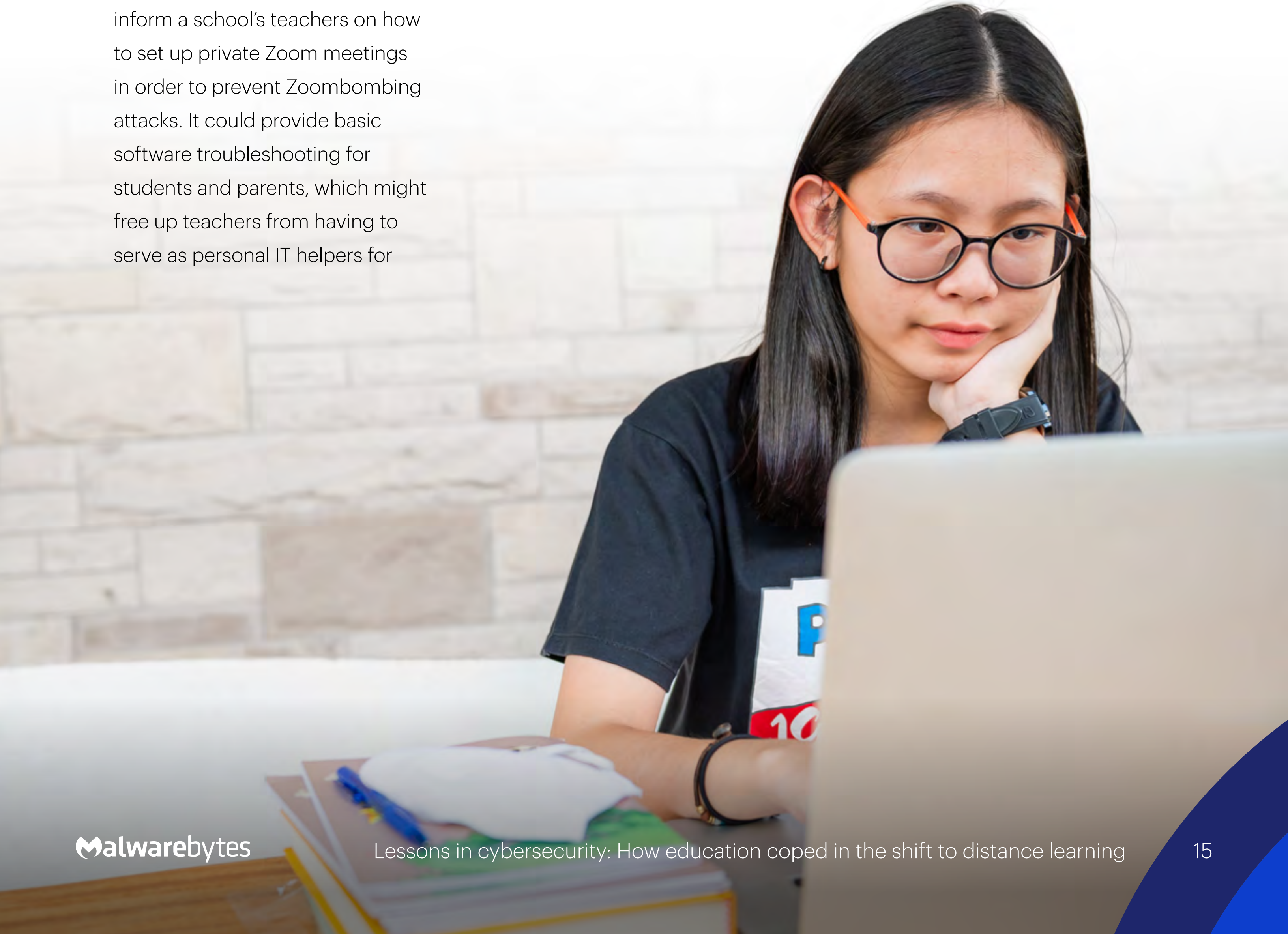
These are unfortunate impacts that schools should not have to grapple with while also attempting to offer every child an equal, strong education. Which is why it's important to describe some of these impacts for what they are—somewhat preventable.

Recall that 50.7% of respondents said that not one audience—not teachers, not students, not staff, not parents or other guests—was required to take any cybersecurity training before starting the new school year.

Cybersecurity training can help prevent these impacts. A good cybersecurity training program could inform a school's teachers on how to set up private Zoom meetings in order to prevent Zoombombing attacks. It could provide basic software troubleshooting for students and parents, which might free up teachers from having to serve as personal IT helpers for their classrooms. And it could teach everyone, from students to teachers to staff to guests, how to responsibly manage and use the new devices and software tools used by the school, so as to remove some of the excess burden now placed on IT workers.

Year after year, organizations in the United States report difficulties in finding skilled workers in cybersecurity and information technology, and while larger enterprises can pay their way out of those difficulties—the median Google employee salary two years ago was $246,804—few schools can take the same route.

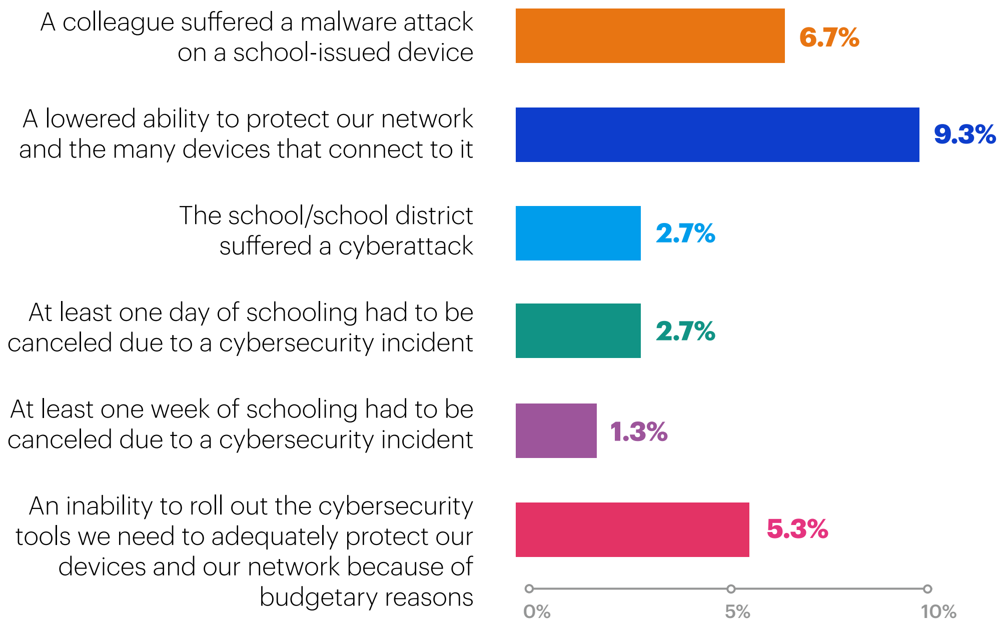
50.7% of respondents said that not one audience—not teachers, not students, not staff, not parents or other guests—was required to take any cybersecurity training before starting the new school year.



Separate from workload issues and increased stressors and distractions, our respondents also said they rarely suffered malware attacks. Our data found that 6.7% of respondents said that "a colleague suffered a malware attack on a school-issued device" and 2.7% of respondents said that the "school/school district suffered a cyberattack." Those cyberattacks sometimes proved disruptive enough to cancel classes for a day—2.7%—or even a week—1.3%.

Thankfully, far fewer schools reported actual cyberattacks that disrupted their distance learning models.

Since your school/district restarted the school year, what impacts have you suffered so far? (Check all that apply)



On first impression, the reported, low rate of malware attacks is reassuring. This hopefully suggests that the kinds of malware attacks not just in Rialto, California and Hartford, Connecticut, but also in Athens, Texas; Haywood County, North Carolina; Ponca City, Oklahoma; and King George County in Virginia, are rarities.

However, the low number of reported cyberattacks does not immediately absolve schools and school districts. First, the number simply does not coincide in any way with separate data that we gathered from students (which we'll discuss further below). Second, remember again that in restarting the school year, just 5.3% of respondents said that, for anyone connecting to a school network, the school required the installation of a "new antivirus tool on the school's devices."

Strong antivirus tools are a part of best cybersecurity practices, as they can catch and prevent attacks before they happen. With our data, we have a rare opportunity to prove this. We also have the opportunity to show the benefits of separate types of cybersecurity protections—not just antivirus tools.

The Unprepared, the Well-Trained, and the Best Practiced

Rather than relying on single case studies within the data, we separated our respondents into three categories to try to find any data trends within. These are what we are calling "group studies."

These groups were categorized by the distinct, separate cybersecurity preparations that schools and school districts required of teachers, students, administrators, and parents. By analyzing the data, we found that different cybersecurity preparations sometimes correlated with better or worse cybersecurity and IT impacts.

While correlation does not imply causation, the trends within the data deserve a look.

Strong antivirus tools are a part of best cybersecurity practices, as they can catch and prevent attacks before they happen.

Here are our three groups:

The Unprepared

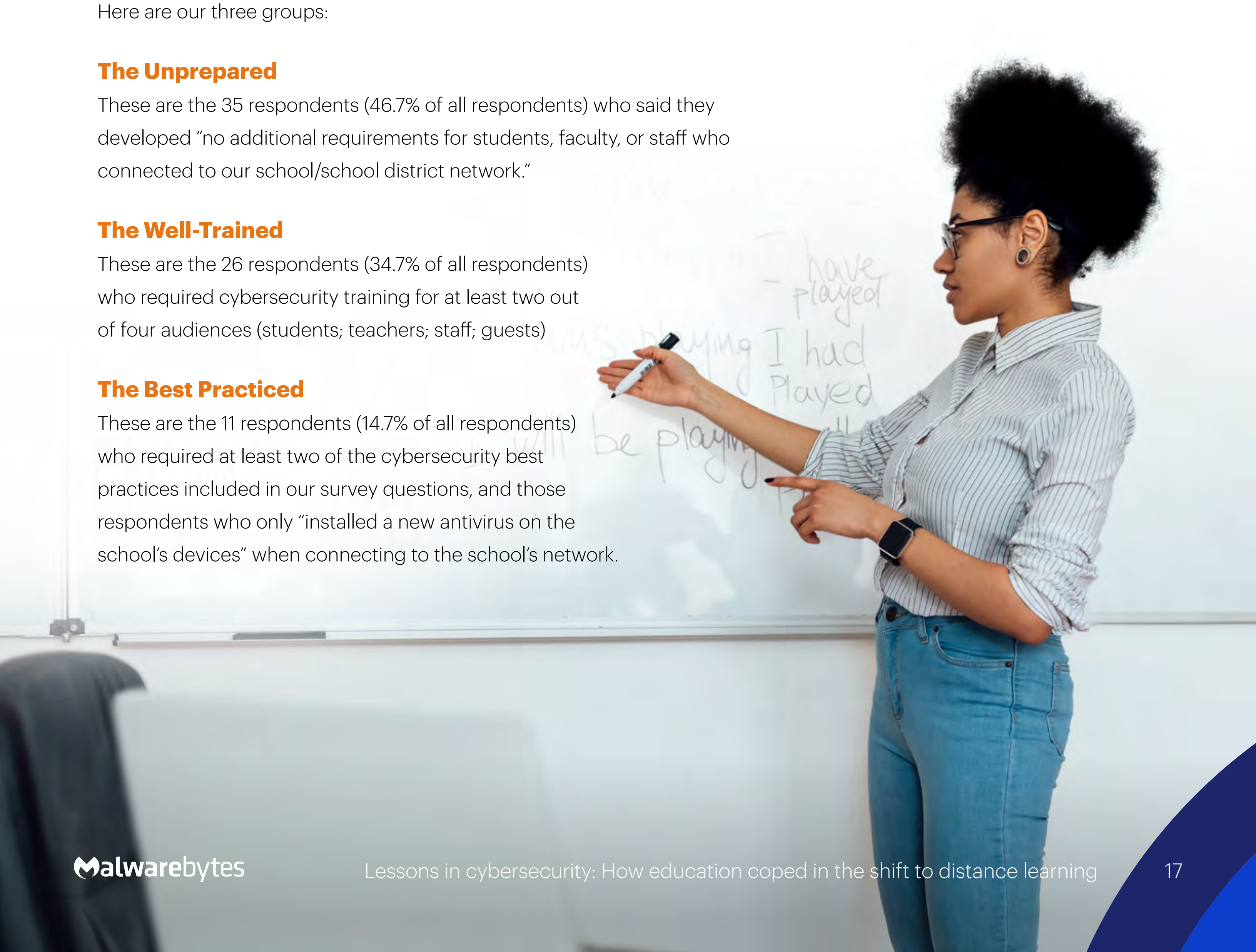
These are the 35 respondents (46.7% of all respondents) who said they developed "no additional requirements for students, faculty, or staff who connected to our school/school district network."

The Well-Trained

These are the 26 respondents (34.7% of all respondents) who required cybersecurity training for at least two out of four audiences (students; teachers; staff; guests)

The Best Practiced

These are the 11 respondents (14.7% of all respondents) who required at least two of the cybersecurity best practices included in our survey questions, and those respondents who only "installed a new antivirus on the school's devices" when connecting to the school's network.



Here are the group study results:

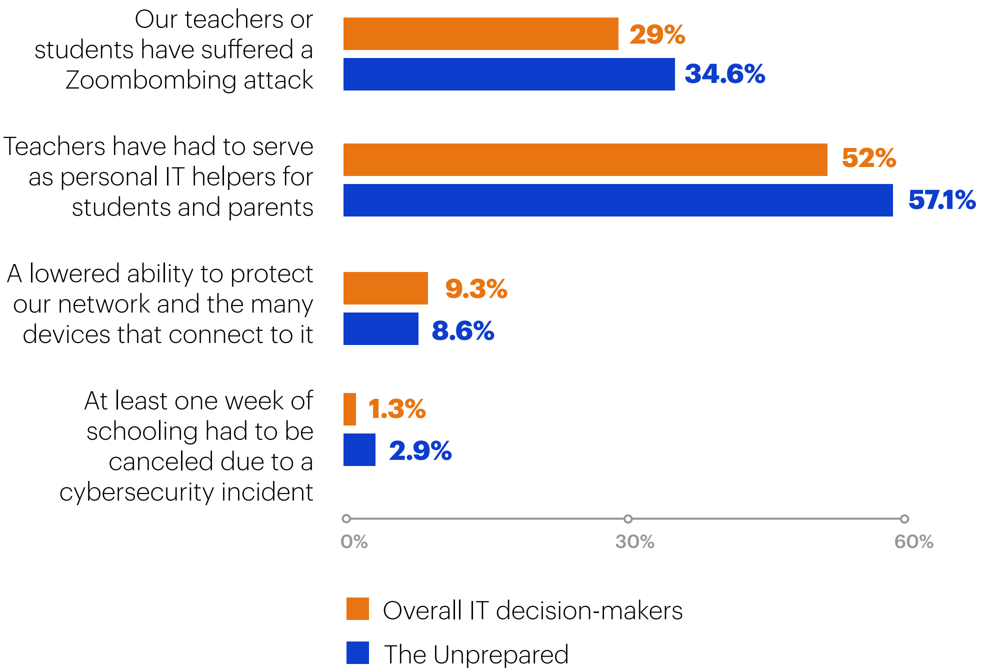
The Unprepared group suffered a small number of cybersecurity and IT issues at a higher rate than the average respondent. For instance, 34.6% of the Unprepared respondents' teachers or students suffered a Zoombombing attack, compared to 29.3% of overall respondents, and 57.1% of the Unprepared respondents' teachers have had to serve as personal IT helpers for students and parents, compared to the 52% of overall respondents.

Curiously, just 8.6% of the Unprepared group said it suffered from a "lowered ability to protect our network and the many devices that connect to it"—which is marginally lower than the 9.3% reported by all respondents. If those respondents had no problem protecting their network, then one might assume they reported no cyberattacks at all, right?

Not quite. The only respondent in our entire data set to suffer a cyberattack that delayed classes for an entire week fell into our Unprepared group.

IT decision-makers who said their schools required no cybersecurity protections sometimes suffered harsher consequences.

Overall IT decision-makers compared to Unprepared group



When we analyzed the Well-Trained group, we found few, marked improvements compared to the overall respondents. For example, 65.4% of Well-Trained respondents suffered "connectivity issues with teachers' tools and students' tools," compared to the 76% of overall respondents.

But in just as many areas, Well-Trained respondents faced similar rates of cybersecurity and IT issues as the broader group of all IT decision-makers. For instance, 76.9% of Well-Trained respondents said they experienced a "sustained, excess IT workload"—close to the 72% of all respondents—and Well-Trained respondents reported a higher rate of Zoombombing incidents: 46.2% compared to 29.3% of all respondents.

So, what's happening here?

By looking at the data, we can see that most organizations that roll out just one type of cybersecurity preparation—whether that is deploying new distance learning policies or requiring students to attend cybersecurity training—are not insulated entirely from cybersecurity and IT consequences. Essentially, there is no silver bullet to cybersecurity.

This makes sense.

A strong cybersecurity plan understands that vulnerabilities come in many shapes and sizes. A vulnerability can be a school administrator who accidentally opens an email attachment containing malware, a teacher who falls for a spearphishing campaign, or simply the many, many students goofing around on school devices, browsing potentially unsafe websites, or downloading suspicious software. Vulnerabilities are multifaceted, and cybersecurity must be, too.

There is no silver bullet to cybersecurity ... A strong cybersecurity plan understands that vulnerabilities come in many shapes and sizes.

Still, we wanted to test these ideas in the data by finding respondents who deployed a variety of cybersecurity preparations. When looking through the data, we decided to group together all respondents who met one of the following two requirements:

- They required at least two of the suggested cybersecurity preparations that our survey asked for regarding how schools protected who and what devices connected to the school's network, which included:
    - Reading through a newly-deployed distance learning guide or distance learning policies
    - Enrolling in a cybersecurity training session, such as a webinar
    - Installing a new antivirus tool on the school's devices
    - Installing antivirus tools on any device accessing the school/school district's online network (including personal devices)

- They required just one of the suggested cybersecurity preparations that our survey asked for, so long as that one preparation was only "installing a new antivirus tool on the school's devices" that connected to the school network

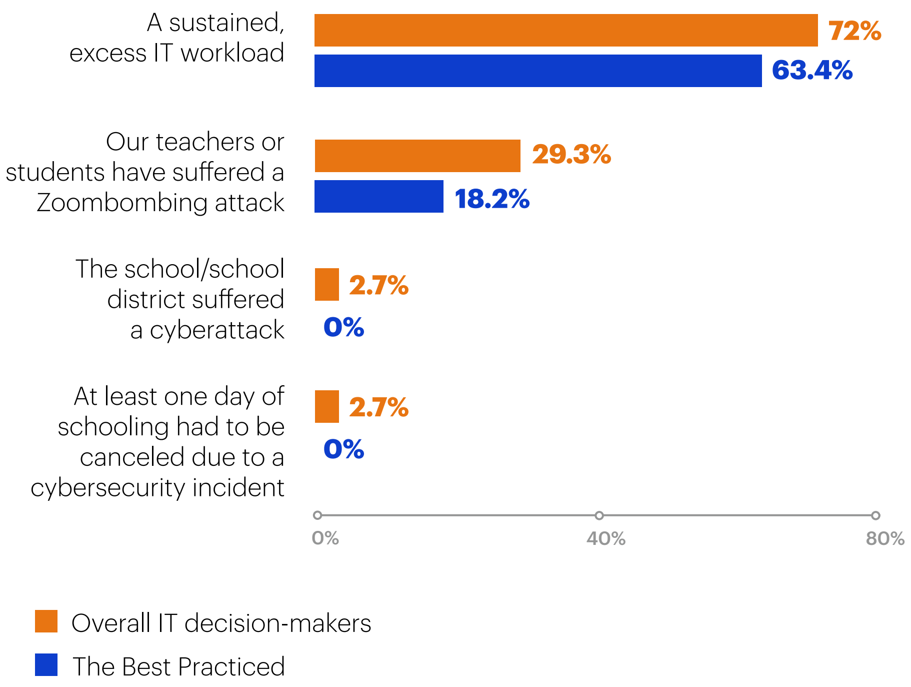
This metric for cybersecurity preparations produced just 11 respondents.
Here is what we found.

Far and above, the Best Practiced group proved to be the most resilient to cybersecurity and IT issues. For example, 63.6% of the Best Practiced group reported a "sustained, excess IT workload" compared to the 72% of all respondents. Also, 18.2% reported that their "teachers or students have suffered a Zoombombing attack" compared to the 29.3% of all respondents.

Most importantly, no Best Practiced respondents said their school or school district suffered a cyberattack, and not a single day of online schooling was canceled because of a cyberattack. While IT decision-makers already reported a low rate of cyberattacks, the Best Practiced group wiped that rate down to zero.

Schools with more cybersecurity preparations sometimes fared better than others.

Overall IT decision-makers compared to Best Practiced group



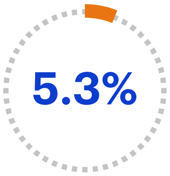
The above trends look good, but one response casts shadow on our Best Practiced group. Nearly triple the rate of respondents in the Best Practiced group—18.2% compared to 6.7% of overall respondents—said that a colleague suffered a malware attack on a school-owned device.

Finally, buried deeper in the data is one possible trend that showcases the importance of a healthy budget.

Only 5.3% of overall respondents said that they faced "an inability to roll out the cybersecurity tools we need to adequately protect our devices and our network because of budgetary reasons." This is a small number and its significance should not be overinflated; however, it is interesting to note that, of the Best Practiced group, not a single respondent said they encountered the same budgetary problems. Adding to the intrigue here is that, in getting ready to provide distance learning before the school year started, more than half of those same respondents said they had earlier challenges in "convincing the school/school district to invest in cybersecurity protections."

Perhaps those IT decision-makers effectively made their case to their schools or school districts, and perhaps those funds led to the stronger rollout of cybersecurity preparations. If so, that's good news for the entire school, including its IT decision-makers, teachers, students, administrators, and parents.

And, as we found out in the next section, it's a great result for a school's reputation.



Only 5.3% of overall respondents said that they faced "an inability to roll out the cybersecurity tools we need to adequately protect our devices and our network because of budgetary reasons."

5 Why cybersecurity preparation matters, part two

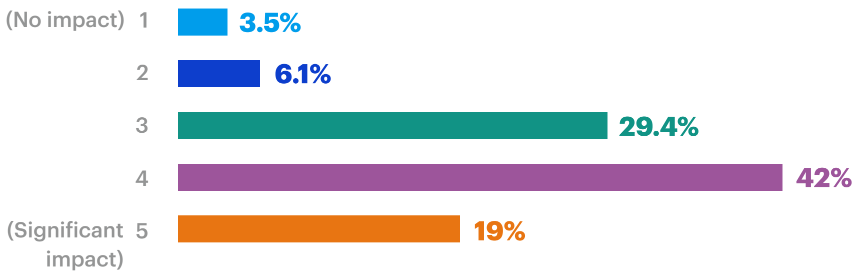
As in any industry, school security is not just about protecting users—whether they're teachers, students, parents or admin staff—but also about protecting the reputation of the school itself. The level of security provided to students and staff has an influence on how attractive it is to work or study in that environment.

We learned that students care deeply about whether a school has suffered a cyberattack, impacting both their trust and their decision to attend that school in the future, whether through a college application or a transfer.

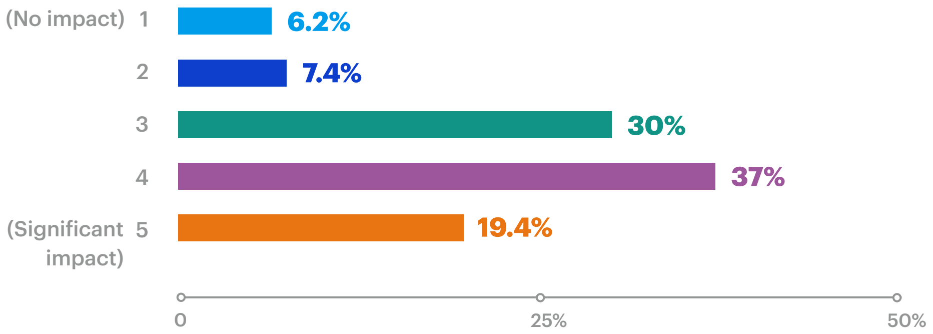
For those students whose school had already suffered a cyberattack, 61% of the students said it had an impact in their trust on the school. For those considering applying for a place at school, 56.4% said a cyberattack would impact their decision to attend a school in future.

Students clearly care about whether a school they are attending or thinking about attending suffers a cyberattack.

On a scale from 1 – 5, with 1 representing "No impact" and 5 representing a "Significant impact," what effect did this cyberattack have on your trust in your school?

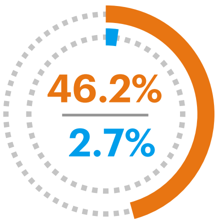


How heavily would a cybersecurity incident impact your decision to attend a school (applying for college, obtaining a transfer from one school to another, etc.)



This shows that lack of investment in cybersecurity could result in a lower revenue in the future caused by students that were scared away by a cyberattack. Interestingly, those who say it would have little to no impact on their choice of school is much lower for those at the undergraduate level (6%) as it is for those at the graduate level (13%). But for every level of education, it’s clear that smart security funding can help make sure educational institutions remain functional, safe places for students to learn.

Interestingly, our survey appears to show a disparity in perception between students and IT teams about what constitutes a cyberattack. A surprising 46.2% of students said their school had suffered a cyberattack, while only 2.7% of IT decision-makers said their school had. One could argue that IT decision-makers are inclined not to count unsuccessful attacks, but how would students even know about them? Given that one of the most common attacks on schools are DDoS attacks (sometimes performed by resident students), it could be that IT decision-makers see them as disruptions rather than actual cyberattacks. The decision-makers are likely to be significantly more afraid of data breaches or ransomware, for example.



A surprising 46.2% of students said their school had suffered a cyberattack, while only 2.7% of IT decision-makers said their school had.

6 | What are schools doing now?

Every public and private organization, regardless of size, has been affected by the many statewide and sometimes nationwide lockdowns put into place to limit the spread of COVID-19.

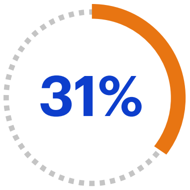
These lockdowns created dramatic impacts for businesses big and small, as Malwarebytes proved earlier this year, often leading to more layoffs, fewer pay raises, and somehow, higher productivity.

Schools, however, are in a unique situation.

The cybersecurity challenges they struggled and attempted to address, pre-pandemic, have been further compounded by new concerns that arose from making distance learning possible for every staff member, teacher, and student.

Admittedly, a bulk of the concerns are not specific to cybersecurity, but to broader connectivity issues (80%). Teachers and students have been apt to complain about not being able to connect to a congested school network, further hampering their ability to successfully participate in online classes. IT departments are also anxious about not being able to see all devices connected to the network (30.7%), making it next to impossible to monitor them all.

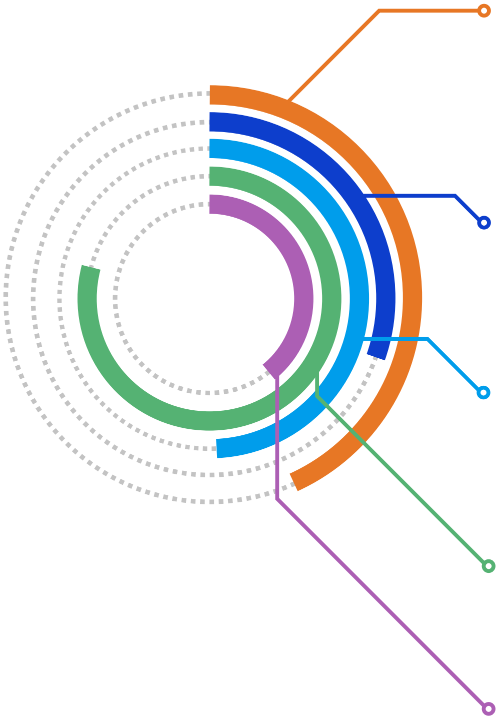
Both of these concerns are due to the dramatic increase of devices now being used by those involved in distance learning and other school staff. With that in mind, it's interesting to note how our IT decision-makers responded when asked what tools their schools are lacking right now.



IT departments are also anxious about not being able to see all devices connected to the network (30.7%), making it next to impossible to monitor them all.

Distance learning may be several months in, but IT decision-makers still have unaddressed concerns.

With distance learning in full effect now, what IT/cybersecurity concerns do you have today?



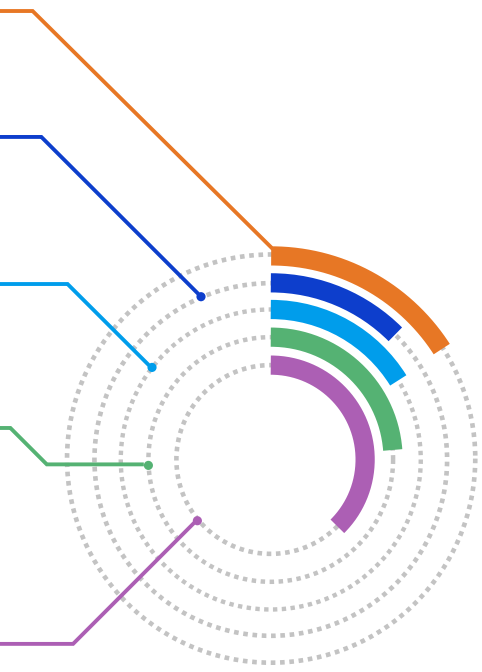
42.7%
Teachers, administration, and/or staff members will not have the time to manage cybersecurity on top of new, daily responsibilities

30.7%
Increased gaps in visibility due to the increased device count beyond our traditional security perimeter

49.3%
Teachers or students will suffer "Zoombombing," or similar video conferencing attacks

80%
Teachers or students having repeated connectivity issues

40%
Teachers or students lacking the devices or software they need to accomplish distance learning



18.7%
Teachers or students lacking the antivirus protection to prevent or endure the damage of a malware attack

12%
Teachers or students purposefully launching a malware attack

18.7%
A malware attack shutting down distance learning for at least a day

24%
Running several software platforms that we did not review for regulatory compliance (Family Educational Rights and Privacy Act)

38.7%
Teachers or students quickly using the data on WiFi hotspots provided by the school at a rate that the school cannot afford

First, remember that schools confidently said that they already provided devices (72%) and new software tools (70.7%) for use in distance learning to students. However, at the same time, schools noted that they still don't have enough devices for students (40%) and teachers (28%) alike. IT decision-makers also said that they still lack the necessary software needed for teachers to manage online classes (34.7%), along with endpoint protection tools like antivirus software (18.7%) that would keep students and teachers safe from online threats and vulnerabilities.

Complicating matters is that, while IT decision-makers said they provided WiFi hotspots for both teachers and students to use for distance learning, those WiFi hotspots sometimes have a data cap. More than a third of IT decision-makers (38.7%) said that they were concerned about "teachers or students quickly using the data on WiFi hotspots provided by the school at a rate that the school cannot afford."

This problem is more difficult to track than it seems. Even if parents, students, and teachers are responsibly using school-provided WiFi hotspots only for distance learning, the schools may be relying on a bevy of school management software that requires constant micro-updates, which could eat through a WiFi hotspot's data allowance without its owner even realizing it.

These are real causes for worry, since our survey also reveals almost half of IT departments (42.7%) fear that teachers, administrators, and/or school staff simply wouldn't have the time to manage cybersecurity on top of their new, daily duties. If the IT team has no visibility on all devices connected to the school's network, not only can they not know when an endpoint is at risk, but they also can't manage cybersecurity tasks on behalf of the teachers and staff.

With online classes in full swing, it's always possible that an outsider can barge into private rooms in Zoom and other video conferencing software to conduct mischief. After all, "Zoombombing" (also known as "Zoomraiding") has happened before and on multiple occasions—not just in schools. Such incidents have become so prevalent that even the FBI released a statement about it and provided steps on how one can mitigate teleconferences getting hijacked. These external statements represent a valid

If the IT team has no visibility on all devices connected to the school's network, not only can they not know when an endpoint is at risk, but they also can't manage cybersecurity tasks on behalf of the teachers and staff.

response to the internal numbers we found: 49.3% of schools fear that teachers and students would get bombed on Zoom or experience similar video conferencing attacks.

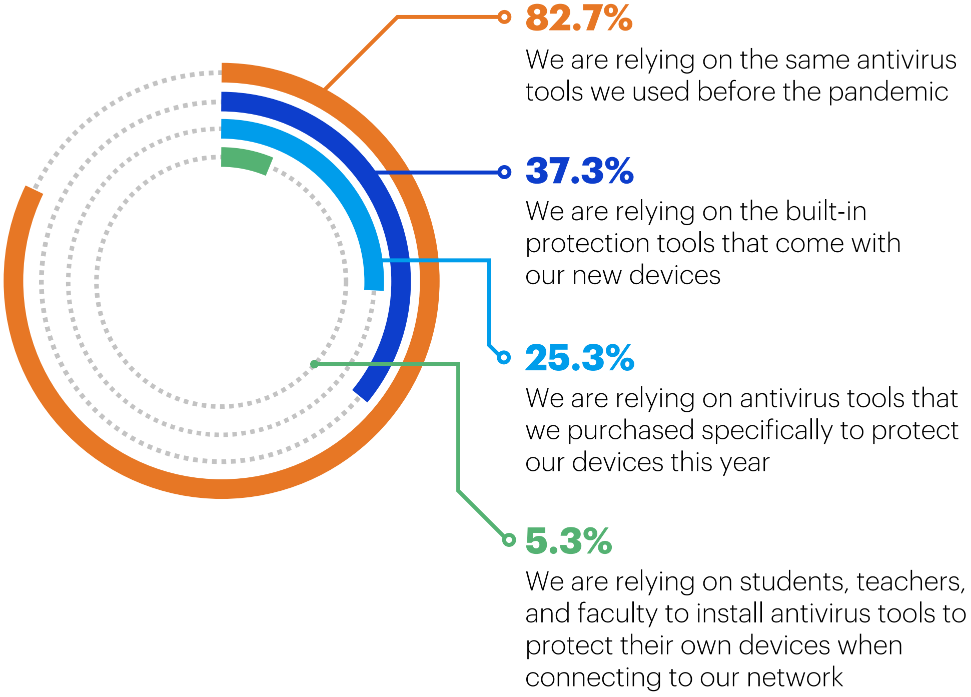
When it comes to what schools or school districts are doing to protect their networks and the endpoints that connect to them, considering there are new cybersecurity challenges and concerns in sight, it's noteworthy that not much has changed with how they have been handling cybersecurity today compared to pre-pandemic times.

A substantial majority (82.7%) admitted to using the same antivirus tools, while some rely on built-in protection tools that came with the new devices they bought (37.3%). A quarter of schools we surveyed (25.3%) bought new antivirus tools specifically to protect the new devices they distributed for distance learning.

The unfortunate truth here is that, for the schools that have not changed their approach to cybersecurity this year, the same old routine is not enough.

Many schools are relying on the same antivirus tools that they did before transitioning to distance learning.

How is your school/school district protecting its network and the devices that connect to that network today? (Check all that apply)



7 | Moving forward: Lessons learned

Cybersecurity protection is multi-faceted. It's more than just cybersecurity training, antivirus software, or strong password creation. Importantly, the more individual actions that schools take to improve their cybersecurity posture, the better prepared they are for the future.

Understandably, this is easier said than done. Schools face constant budget and time constraints often beyond their control, and even when the budget is there, it can be hard for IT and cybersecurity staff to convince school boards to put those funds into cybersecurity.

Schools that doubt the importance of these investments should heed the consequences.

As our report showed, better-prepared schools reported a lower rate of overworked IT administrators and a lower rate of teachers forced to serve as on-call IT helpers for students and parents. Better cybersecurity preparations can translate into better working experiences for everyone—not just IT staff.

Those same schools also reported a lower rate of school-wide cyberattacks and a lower rate of disrupted classes because of school-wide cyberattacks. These types of attacks have increasingly appeared in news stories this year and there's little reason to believe that threat actors will stop targeting schools as the pandemic continues.

For schools wondering what steps they should take, there are many.

Schools should consider writing and training teachers and administrators on cybersecurity policies for distance learning. Teachers and administrators should know who to report

Better-prepared schools reported a lower rate of overworked IT administrators and a lower rate of teachers forced to serve as on-call IT helpers for students and parents.

Teachers should be able to teach, students should be able to learn, staff should be able to keep a school running, and parents should be able to trust that their kids are getting an education.

issues to that they can't solve themselves, and there should be rules for safely connecting to the school's network and the many online applications that a school uses in daily operations. That could include, for instance, requirements to use a VPN when accessing a school's online resources, or requirements to use a password manager and strong, non-repeated passwords for school-associated accounts.

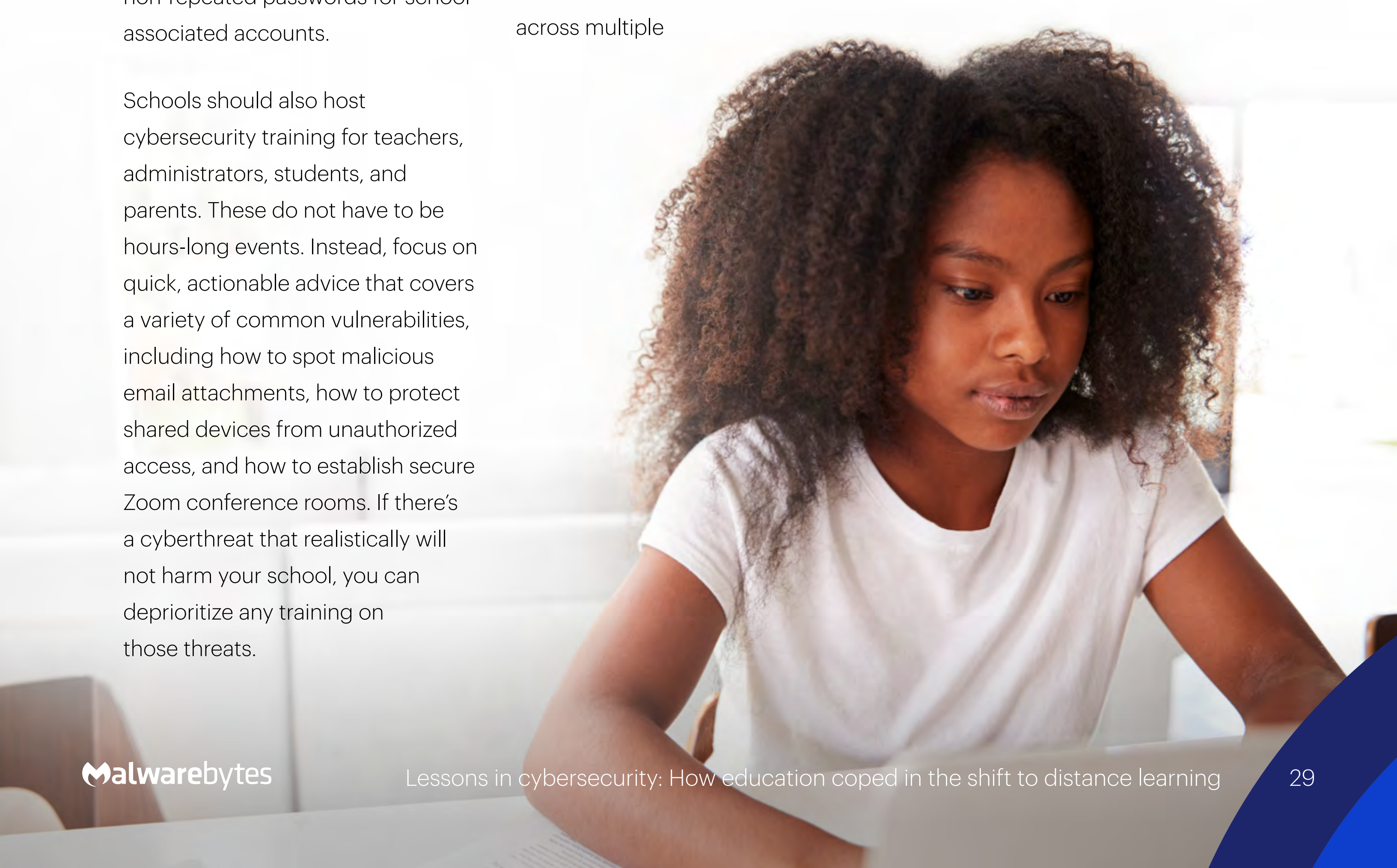
Schools should also host cybersecurity training for teachers, administrators, students, and parents. These do not have to be hours-long events. Instead, focus on quick, actionable advice that covers a variety of common vulnerabilities, including how to spot malicious email attachments, how to protect shared devices from unauthorized access, and how to establish secure Zoom conference rooms. If there's a cyberthreat that realistically will not harm your school, you can deprioritize any training on those threats.

Also, because the school year is reaching its halfway mark, schools should ask teachers, students, and parents about their most common cybersecurity and IT issues so far. If these issues can be quickly addressed through basic troubleshooting guides, focus on writing those guides and sending them out. If even a small percentage of the intended audiences learn how to fix these issues on their own, IT staff and teachers might find more time for their primary responsibilities.

Finally, we must stress the importance of installing antivirus software on school-issued devices. We understand that many schools rely on a variety of devices, from tablets to Chromebooks to laptops. Consider an antivirus solution that works across multiple devices and provides 24/7 endpoint protection—which means school devices are safe from malware, and will continue to stay safe, even from a student's risky click.

This year is easy for no one, and the cybersecurity issues taking place now only compound the stress. Teachers should be able to teach, students should be able to learn, staff should be able to keep a school running, and parents should be able to trust that their kids are getting an education. The more Zoombombing disruptions, the more canceled classes due to malware attacks, the more strain put on teachers, the harder it is for everyone.

Stay safe out there.
Education depends on it.



Contents

Contributors

David Ruiz
Senior Content Writer, Malwarebytes Labs

Adam Kujawa
Director of Malwarebytes Labs

Anna Brading
Editor-in-Chief, Malwarebytes Labs

Jovi Umawing
Senior Content Writer, Malwarebytes Labs

Chris Boyd
Senior Threat Intelligence Analyst, Malwarebytes Labs

Pieter Arntz
Senior Threat Intelligence Analyst, Malwarebytes Labs

Malwarebytes

Malwarebytes Inc.

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

USA

+1-800-520-2796