



MORPHISEC
**EDUCATION
CYBERSECURITY**
THREAT INDEX

Overview 3

Key Findings..... 4

Education Cyber Attacks Before & After COVID-19 5

Balancing Teaching,Technology and Security in the New Normal 7

Ransomware Dangers Aren't Being Addressed 9

Conclusion 11

About MORPHISEC..... 11

OVERVIEW

COVID-19 has had significant cybersecurity implications for almost every industry globally, and education is certainly no exception. Under immense pressure to rapidly adapt to remote learning environments while depending on third-party technology tools like Zoom – with widely reported security vulnerabilities – educators are scrambling to safely implement online teaching plans at scale for the fall.

Of the 20 largest K-12 school districts in the U.S., 17 plan to begin the school year fully remote this fall. Many of these districts had little if any online learning programs before the onset of COVID-19 and, to make matters worse, plans continue to change every day. As the first students have gone back to school in certain areas of the country in recent weeks, we've already seen how in-person and hybrid schooling plans shifted overnight to remote-only plans with positive COVID-19 cases.

The same fluctuation in planning can be seen across U.S. colleges and universities. According to the College Crisis Initiative (C2i), which tracks back-to-school plans for higher education institutions across the country, over 1,000 of the 3,000 institutions it follows are planning school reopenings that include either fully online, primarily online, or hybrid set-ups. This widespread shift to online learning, which necessitates the use of new technologies, has the education industry's attack surface stretched and firmly in cyber attackers' crosshairs.

Microsoft's Global Threat Activity tracker recently found 5 million malware incidents detected in the education sector in July alone – making it the most targeted industry. It accounted for more than 60% of all enterprise malware encounters. For context, the business and professional services industry came in second with just under 1 million incidents in that timespan.

One such incident that made headlines over the summer was a June attack on the University of California, San Francisco. The attack hit UCSF's School of Medicine with NetWalker malware that encrypted data and rendered it inaccessible. The school was forced to pay \$1.14 million in ransom to the hackers to get access back. This is the same ransomware threat responsible for similar attacks against Michigan State University and Columbia College, Chicago, in late May and early June.

Ransomware is also the number one threat facing K-12 schools and, by some accounts, more than 1,000 individual K-12 schools in at least 72 districts nationwide were the victims of ransomware attacks in 2019. The threat has increased during the COVID-19 crisis as both teachers and IT teams have been forced into remote environments. The increase in distance learning over the last several months on account of COVID-19 prompted the FBI to warn that cyberattackers are increasingly eyeing K-12's remote learning setups as an opportunistic target.

KEY FINDINGS

As Morphisec continues to assist K-12 and higher education institutions with improving cyber defenses against advanced threats, we commissioned the **Education Cybersecurity Threat Index** to explore how the increasing risk of cyberattacks amidst the shift to distance learning has impacted educators and whether it has increased their knowledge of common threat vectors. To do this, we **surveyed 500 educators across the United States in July 2020**. Of those we surveyed, 67% worked within K-12, 24% worked within Higher Education, and 9% worked within other education institutions (e.g., private and alternative education). The vast majority of respondents were teachers, with some administrators also included in the survey sample.

Here's what we found:

- More than a third (34%) of educators at colleges or universities, and 26% at K-12 schools, say their institution has been the target of a cybersecurity attack historically.
- Since the onset of COVID-19, 21% of higher education respondents say their school has been the target of a cybersecurity attack, more than double that of K-12 respondents (9%). Meanwhile, 29% of educators are unsure if their school or education institution has ever been the target of a cyber attack.
- One-third of educators note that COVID-19 has mandated more dialogue on cybersecurity with parents and students, while 31% admit it has created new cybersecurity vulnerabilities at their institution.
- Despite ransomware attacks increasing in number and sophistication, over half of K-12 educators (52%) say their institution has not warned them about the specific dangers of ransomware. In fact, across both K-12 and higher ed institutions, just 13% of educators say they feel ransomware poses the most significant security risk as they move to distance learning environments.
- Likely influenced by the recent [Twitter attack](#) and government warnings, educators recognize the substantial threat phishing attacks pose to their schools. A third of educators said these types of threats represent the most danger as they scale online learning, while 28% say spyware is the most dangerous threat.

EDUCATION CYBER ATTACKS BEFORE & AFTER COVID-19

While it took until 2018 for the Department of Education to mandate that all Title IV education institutions have to report data breaches regardless of their size, recent findings have illustrated the impact of cyberattacks against the education industry over the last decade. [Comparitech](#), for instance, found that there have been more than 1,300 breaches since 2005 and more than 24 million records lost. According to the study, public schools and universities suffered more breaches than their private counterparts, hinting at the struggle faced by many educators and IT professionals working within limited budgets and tight resources.

Since Onset of Covid-19: Higher Ed Remains in Crosshairs of Cyber Attackers

VICTIM OF HISTORICAL ATTACK



VICTIM OF ATTACK SINCE COVID-19 ONSET



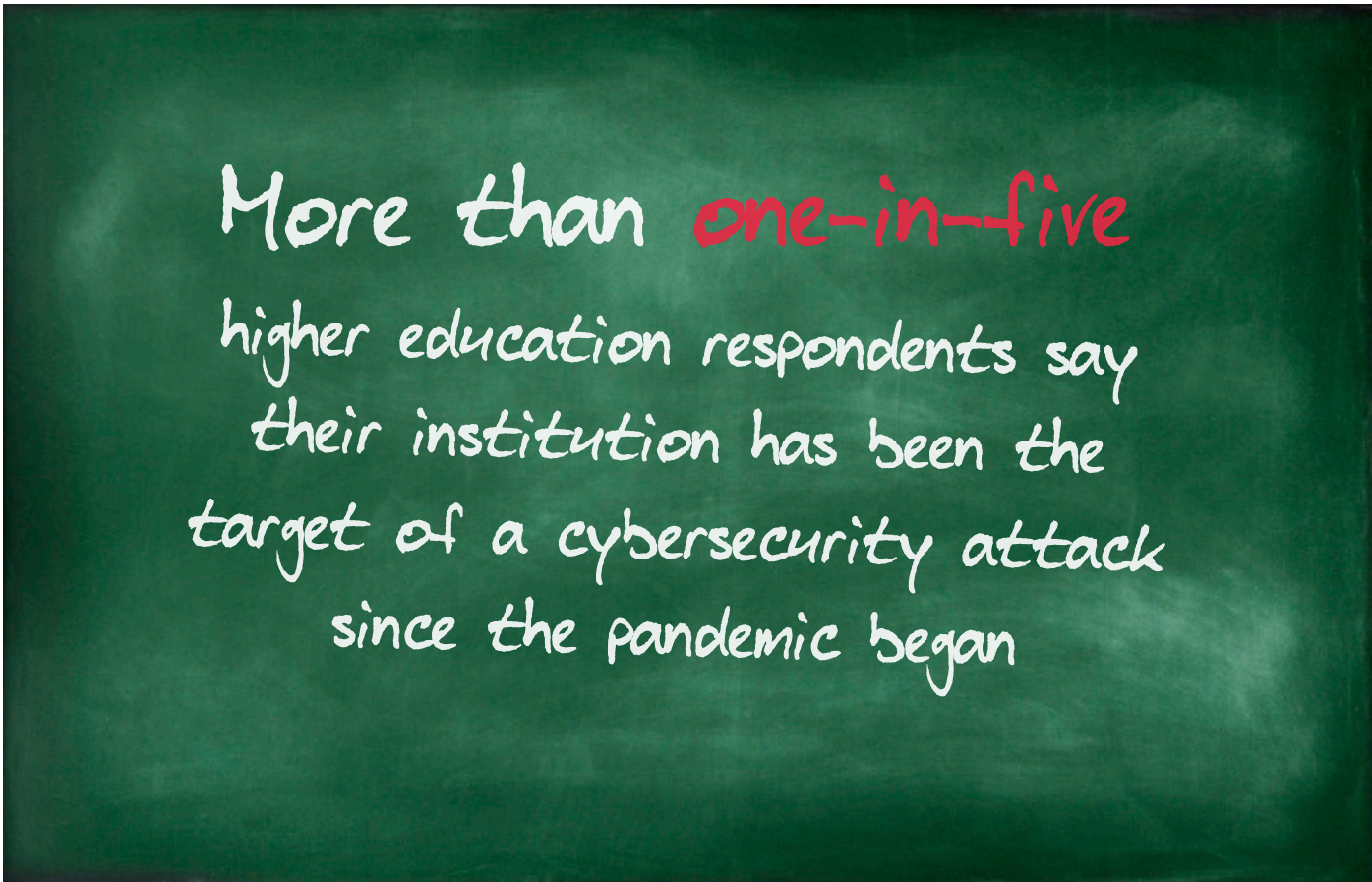
Our survey found that **34%** of higher-ed respondents say their institution has historically experienced a cybersecurity attack, while **26%** of K-12 educators report the same. When you consider how successful attacks on education institutions have been, it's hardly surprising that such a large proportion of educators within the system are aware of attacks against their institution, school, or even school district. COVID-19 is only exacerbating the cybersecurity risk within the education industry. With millions of students, teachers, and associated staff using personal computers for distance learning, attack surfaces and cybersecurity budgets are stretched. Therefore, it's becoming much easier for hackers to carry out low-risk, high-reward infiltrations.

The number of educators reporting attacks against their institutions since the onset of COVID-19 is evidence of this. **More than one-in-five (21%) higher education respondents say their institution has been the target of a cybersecurity attack since the pandemic began.** This is more than twice the number of K-12 respondents who reported their school was targeted since COVID-19 (9%).

Part of the issue is that educational institutions have flocked to learning apps and video conferencing tools in such volumes that these platforms' security issues are much higher profile than in previous years. Higher education, in particular, is far more likely to be targeted, despite having comparatively more resources and several high-profile ransom payouts hitting the news in the past few years.

This does not mean, however, that hackers are sympathetically sparing K-12. There have been more than [775 publicly disclosed cybersecurity incidents](#) targeting K-12 schools in the last four years alone, all of which interrupted learning in at least some capacity, affected staff emails, and ultimately reinforced the need for all schools to bolster their online security.

It's also worrying to consider that **29% of educators state they are unsure if their school or education institution has ever been the target of a cyberattack.** Lack of this knowledge may be simply due to many school systems having fewer dedicated cybersecurity resources in place. Baseline antivirus solutions may not identify when a sophisticated threat has breached a school system. Despite this, almost two-thirds (63%) of educators rate cybersecurity practices at their school or education institution as good or better.



More than **one-in-five**
higher education respondents say
their institution has been the
target of a cybersecurity attack
since the pandemic began

BALANCING TEACHING, TECHNOLOGY AND SECURITY IN THE NEW NORMAL

The technology challenges facing today's educators are unlike any they have experienced before. While many higher education institutions have experimented with remote learning in recent years and online classes have grown in popularity, any K-12 teacher will admit to the anxieties that arise from being suddenly thrust into full-time digital education.

Much of this anxiety is driven by their desire to ensure students are engaged and actively learning in full-time virtual learning. When we asked educators their most significant concern with shifting to teaching students entirely online, this topped their list (49%). It was followed by a concern for potentially leaving students without computers or the internet behind (26%) and trepidation over effectively utilizing technology for online instruction (14%). All of these worries topped concerns over a cyberattack shutting down their ability to teach online (7%). Educators are rightly focused on their students and learning, but this can lead to issues with balancing the online security for both their sessions and more broadly for their school.

Educators' biggest concern with moving to 100% Distance Learning

Keeping students engaged and actively learning in online settings

49%

Not leaving students behind due to lack of computers at home or ability to get online

26%

Teachers understanding and effectively using technology tools for online instructions

14%

Cybersecurity attack shutting down our ability to teach online

7%

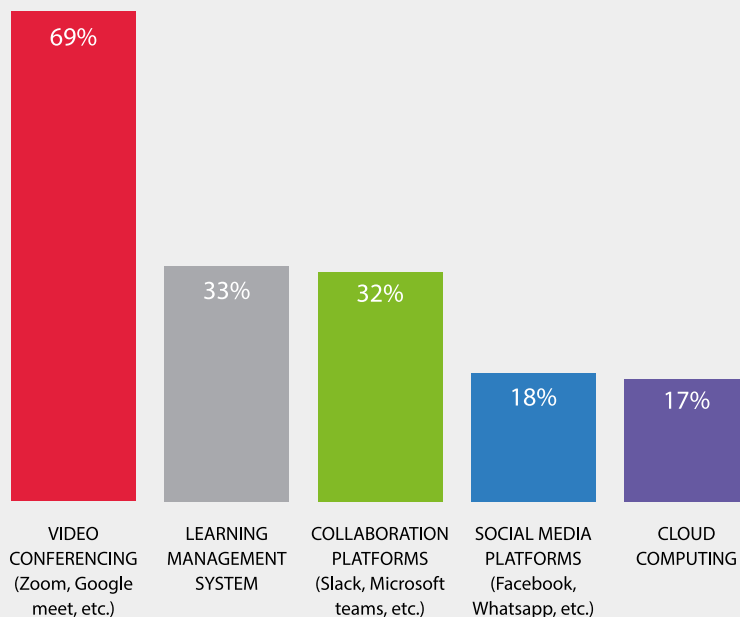
Other

4%

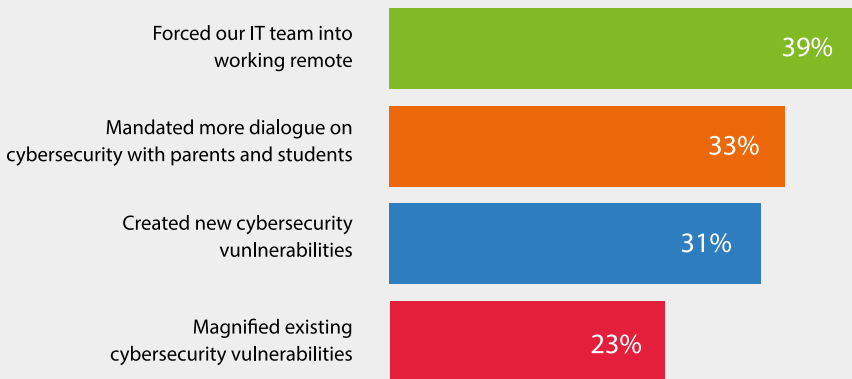
Many schools remain ill-equipped to securely migrate to a completely digital-based curriculum solely with their traditional learning management system. Therefore, they are heavily reliant on third-party video conferencing tools like Zoom and Google Meet, which contain highly publicized security gaps, to stay connected with students. Morphisec Labs researchers discovered one such flaw in the [Zoom application](#) that enables threat actors to record Zoom sessions and capture text chats without the participants' knowledge.

Our survey indicates that **69% of educators say they are using these video tools to improve their teaching and productivity**. In addition to video conferencing and leveraging their learning management systems (33%) for going remote, collaboration platforms (32%) are also being leveraged for distancing learning communication.

Tech tools educators are using to improve teaching and productivity in distance learning settings



Expected to balance online learning, new technologies, and widening security gaps resulting from the above, educators' concerns are understandably prevalent. When asked how COVID-19, online learning, and remote teaching has impacted cybersecurity at their school or institution, most respondents (39%) said the most significant impact was that it **forced their IT teams to work remotely**.



Q How has COVID-19, online learning, and remote teaching impacted cybersecurity for your school or education institution?

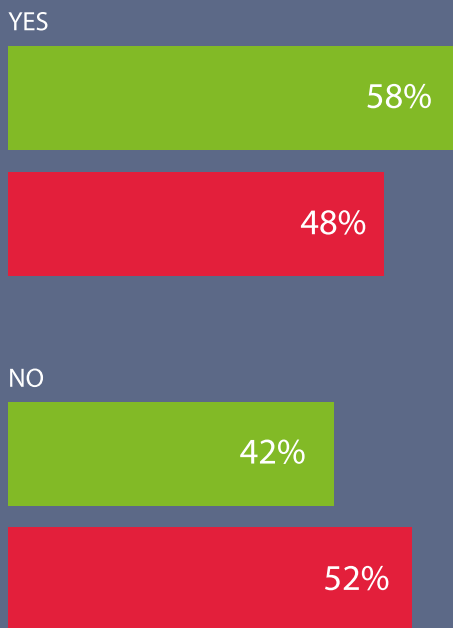
One-third of respondents note that it has mandated more dialogue on cybersecurity with parents and students, while 31% admit it has created new cybersecurity vulnerabilities for their school. Almost one-quarter (23%) recognize that the current pandemic has magnified existing cybersecurity vulnerabilities.

RANSOMWARE DANGERS AREN'T BEING ADDRESSED

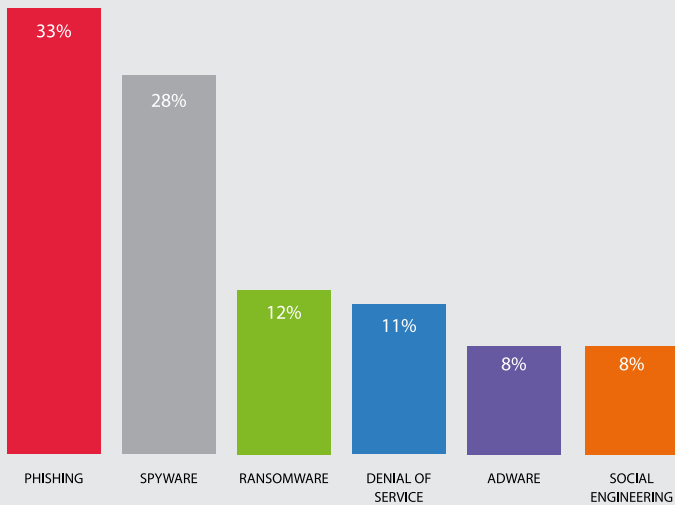
From the [WastedLocker](#) payloads that recently infiltrated Garmin to the Maze malware that cost NJ-based IT company Cognizant [up to \\$70 million](#), ransomware has terrorized organizations even more since the onset of COVID-19. Several prominent schools have already fallen victim. A month before NetWalker's June attack on UCSF, data sets from Kent State University and the University of Dayton were compromised by [ransomware attacking a third-party vendor](#). With ransomware demand costs [exceeding \\$1.4 billion](#) in the U.S. in 2020, it's clear that the growing dangers of avaricious cybercriminals are too much to ignore.

Yet, over half (**52%**) of K-12 educators say their school has not warned them about the specific dangers of ransomware attacks. In fact, across both K-12 and higher ed institutions, just 13% of educators say they feel ransomware poses the most significant risk as they move to distance learning environments. Even though ransomware has been around for three decades and is hardly an unexpected threat, these findings illustrate the rapidly escalating issue isn't being taken as seriously as it should. Many ransomware attacks begin with a bogus email, meaning one wrong decision by a staff member can put an entire organization at risk. And remote working is only increasing these risks.

Q Has your school or education institution warned you about the specific dangers of ransomware attackers?



■ HIGHER ED
■ K-12



Q Which one of these cybersecurity threats do you feel poses the most danger to your school or education institution as it scales remote?

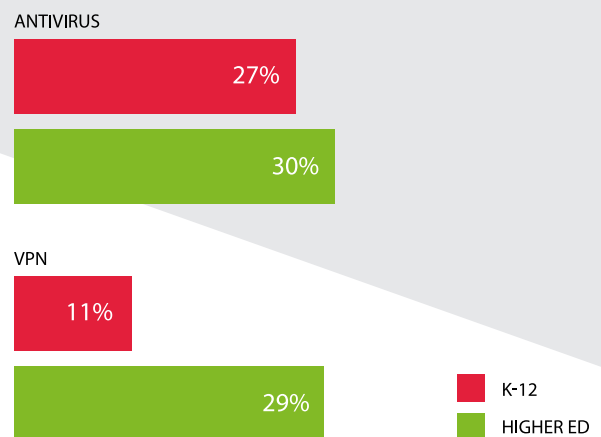
Meanwhile, **a third of educators** state they feel phishing poses the biggest danger to their school as they work on scaling remote learning. As bad actors continue to leverage COVID-19 as an access tool, phishing attacks are becoming more creative — and damaging (even leveraged to deliver ransomware) — by the day. This is illustrated by [Twitter's](#) high-profile phishing incident in July. Likely helped by [government warnings](#) about such attacks, it is promising that a significant number of educators understand the severity of phishing threats.

The second biggest cybersecurity threat, according to educators, is spyware (28%), which was followed by the aforementioned ransomware (15%), denial-of-service (11%), adware (8%), and social engineering (8%).

It was also slightly worrying that just **27% of K-12 educators are using antivirus software** to protect themselves from attacks. Meanwhile, only **11% say they are currently using a VPN in their distance learning environment**. With more IT resources, educators in higher education are slightly more likely to use some of these baseline security measures, with 30% using antivirus and 29% using VPN.



Security tools being used in shift to Distance Learning



While VPN usage won't ensure protection from ransomware for educators, it will ensure that their online activities are encrypted, and IP addresses masked. Therefore, it becomes more difficult for attackers to obtain their personal and login information. Furthermore, while traditional, and even Next Generation Antivirus (NGAV), can't thwart sophisticated and targeted ransomware attacks from cybercrime groups on their own, end-to-end endpoint protection solutions utilizing application memory morphing alongside antivirus can be effective in protecting against these types of advanced threats.

CONCLUSION

As school districts continue to commit to distance learning for the foreseeable future, how to keep student and teacher data secure from cybercriminals is just one issue fueling their anxieties. Even before classes were moved entirely online, many K-12 schools were dealing with a lack of dedicated funding and resources to help them vet and improve their cybersecurity defenses. And as a result, many failed to employ even the most basic security protocols and left gaping vulnerabilities unpatched. Now they're increasingly exposed to third-party technology vendors with security vulnerabilities and IT teams operating remotely.

With the current pandemic amplifying these security threats, now is the time for both K-12 schools and higher ed institutions to address their cybersecurity defenses. With ransomware increasingly targeting the education sector, the costs of falling victim to an attack are too hefty to ignore — from both a monetary and downtime standpoint. Therefore education IT teams must reassess the expanding size of their attack surface within distance learning environments and determine a security stack that can be successful within our new normal environment. These steps will enable them to protect both educators and students as they progress through the stages of remote learning and finally, in their return to the classroom.

ABOUT MORPHISEC

FUNDAMENTALLY ALTERING THE CYBERSECURITY LANDSCAPE

Morphisec is transforming endpoint security with our pioneering Moving Target Defense. Our solutions deliver operationally simple, proactive prevention unbound by the limits of detection and prediction. We protect businesses around the globe from the most dangerous and sophisticated cyberattacks immediately, efficiently and absolutely.

