**SPOTLIGHT**

*Sponsored by: Cisco*

**Security is an ongoing priority at education institutions as they seek to enhance their IT maturity for the future of education. Cybersecurity is now the top priority of ongoing digital transformation efforts in education.**

# *Securing the Future of Education: Focusing on Cybersecurity*

*January 2022*

**Written by:** Matthew Leger, Research Manager, IDC Worldwide Education Digital Transformation Strategies

## *Introduction*

While the COVID-19 pandemic had a significant impact on the education security landscape, many security issues predated the virus. Cybersecurity incidents such as phishing and ransomware are still on the rise, as are the incidences of the loss of personal student data. As more devices proliferate in the classroom and education leaders navigate the future of distance and hybrid learning models, the size and scope of the attack surface that schools and universities need to protect will continue to expand and evolve.

For education institutions, a future defined by digital, distance, and hybrid learning – and where faculty, staff, and students will continue to shift back and forth between physical and digital classrooms – will create additional security vulnerabilities, driving the need for end-to-end security and, in some cases, sparking investments to help schools close the cybersecurity gap. There is still significant work to be done.

While the education sector made significant strides to boost security capabilities, not all mitigation strategies were sufficient and many institutions are still struggling to protect their IT systems and data. Many police organizations globally continue to receive reports from primary and secondary education institutions about the disruption of distance and hybrid learning efforts by hackers, including ransomware and theft of private information. Institutions must educate everyone — students, parents, teachers, and staff — about security best practices and how to use safe log-in procedures. Security education also means helping all users understand how to recognize suspicious links and dangerous attachments. In primary and secondary schools, educating parents about what is expected for security compliance, how privacy will be protected, and how the school might be involved in helping with end-user device management and security are critical practices. Most importantly, security investments may include upgrades to school network monitoring and security platforms and

## *AT A GLANCE*

### *KEY TAKEAWAYS*

» COVID-19 exposed the security vulnerabilities of education IT systems that predated the pandemic.

» According to IDC, 60% of education institutions agree that they must do more to protect student data.

» Security is now the leading priority for education institutions when evaluating technology vendors and solutions.

» While the pandemic has had an ongoing impact on education institutions, many have moved beyond the crisis to make strategic technology investments for the future.

» Education institutions need the capabilities to prevent intruders from entering online learning systems, enable secure collaboration, and protect critical student and institutional data. Education institutions are focusing investments in these areas more than ever before.

launching awareness campaigns to help all stakeholders understand how security is being addressed and what their part in that process will be.

## Industry Definition and Core Attributes

The education industry encompasses private and public as well as nonprofit and for-profit elementary, secondary, and post-secondary/tertiary educational institutions of all sizes. These organizations provide formal learning toward the award of academic degrees, accreditations, and/or certifications, such as a high school diploma or a baccalaureate or university degree. Many institutions of higher education (IHEs) also conduct research and develop products and services for eventual commercial use.

Schools, colleges, and universities are influential members of their communities. Schools for younger children not only teach academic courses but also educate students about cultural and behavioral norms including national or regional songs, games, expressions, foods, language, and social behaviors. They can be community centers for parents, shelters in emergencies, and hosts to many extracurricular activities. IHEs have a social impact and a financial impact on surrounding communities, not only via students as consumers but also through partnerships and work with local businesses, government organizations, and community groups.

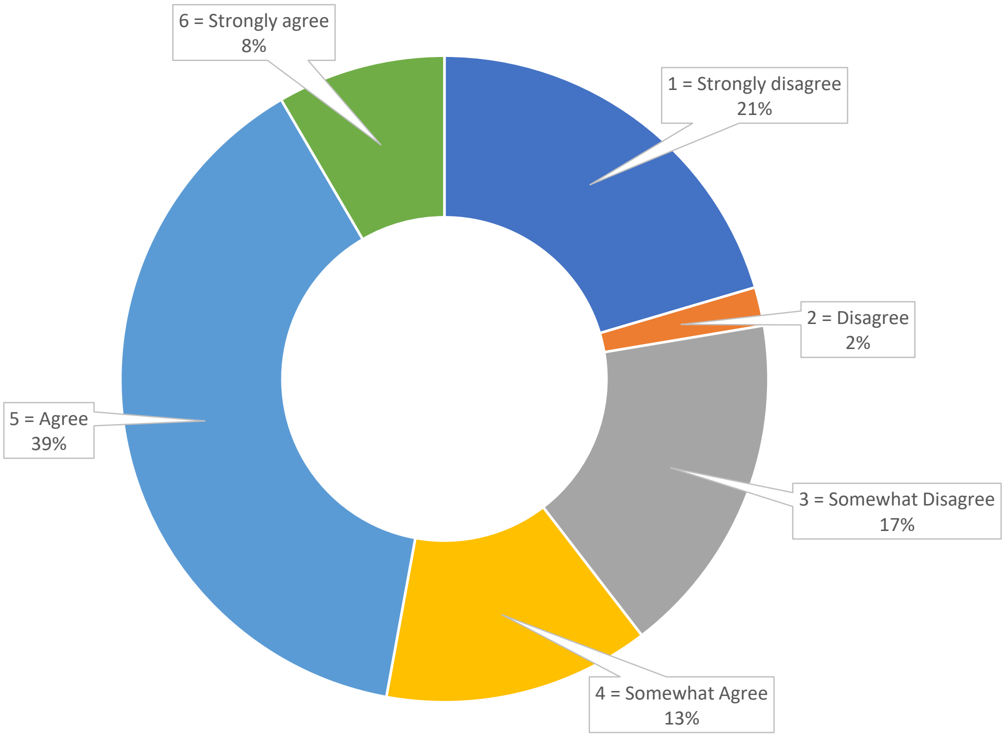
## Key Business Priorities

The shift to remote learning and operations during COVID-19 exposed the security vulnerabilities of education IT systems that predated the pandemic. A 2018 study by SecurityScorecard ranked the education sector worst among 17 major industries in implementing cybersecurity measures. When the pandemic shuttered school doors, the sector rose to the top of the target listed for cybercriminals, particularly for ransomware attacks. To make matters worse, the education sector also sits at the top of the rankings for highest ransomware recovery costs of any industry, with an average recovery cost of $2.7 million, according to a study by Sophos. An October 2021 report from the U.S. Government Accountability Office's Cybersecurity Resource Center reported that the nation's K-12 cybersecurity plans have not been updated since 2010 and called for a major overhaul to help institutions adapt to changing threats. The report cited a significant increase in cyberattacks on education institutions during the pandemic as cause to revamp cyberdefenses to protect institutions and their students.

Although the broad security and systems update measures that education institutions took during the past two years are admirable, they have proven insufficient. As many education institutions adapt their capabilities for the future, cyberthreats and vulnerabilities for institutions will only grow and evolve, requiring additional investments in security solutions. As shown in Figure 1, 60% of education leaders agree that they must do more to strengthen cybersecurity to protect student data.

FIGURE 1. ***Student Data Requires Additional Protection***

**Q** ***Please rate your level of agreement to the following: Should your institution do more to strengthen the security of protecting student data?***



*n = 48 in education*

*Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2021*

Many institutions have made key changes to their IT investment priorities, including new investments in cybersecurity. Among the changes are the following:

- **Prioritizing security in IT investments.** As education leaders evaluate technology vendors and solutions, they are prioritizing security above all else. In IDC's 2021 *Industry CloudPath* and *AIPath* surveys, education respondents noted that built-in security capabilities and data privacy were their top priorities when evaluating new solutions. Security is no longer an afterthought for education leaders as they recognize that the threat landscape is evolving beyond their capacity to defend against it.
- **Investing in cyberinsurance policies.** In recognition of the evolving cyberthreat landscape and the cybersecurity risks education institutions are exposed to, cyberinsurance companies are raising the price of policy premiums.

However, they are implementing incentives, including premium discounts, if institutions can validate that specific protection techniques or solutions are in place and maintained, monitored, and upgraded over time. While the up-front costs of acquiring cybersecurity insurance and implementing required tactics can be costly for institutions, these policies come at a fraction of cyberincident recovery costs and are designed to incentivize enhanced security measures that serve to decrease the risk of a cyberattack on IT systems, networks, devices, and applications.

» **Boosting security capabilities to enable trust and reputation resiliency.** Institutional IT systems house significant data on students, faculty, and staff including personally identifiable information, academic and behavioral data, and health records. It is imperative that such information be tightly protected. The rush toward digital transformation has encountered some speed bumps and, in some cases, poorly planned implementations that expose vulnerabilities and lead to cybersecurity breaches. Such breaches, in turn, can destroy trust. Top priorities now, for many educational institutions, are to address cybercrime, limit malware, block ransomware attempts, stop ID theft, and monitor and harden networks against network attacks. At the same time, there is broad acknowledgment that insider threats are real and that edge computing, while increasingly necessary, pushes security to the brink and raises the need for new types of monitoring, remote access control, and protection.

To boost protection, more educational institutions are supporting unified threat management platforms and moving toward enterprisewide SD-WAN technologies. In some cases, where multiple devices are attached to the network each day, zero trust environments are becoming commonplace. A move toward distance learning sparked exploitation that boosted ransomware incidents. IDC believes 2022 will bring an increase in organized ransomware and other cyberattacks that will result in 70% of schools turning to multifactor authentication for a zero trust approach to cybersecurity and 50% of institutions leveraging managed security services to deal with increased security workloads (see *IDC FutureScape: Worldwide Education 2022 Predictions,* IDC #US47242621, October 2021).

Continuity of operations and service are still weighing on educators' minds, but many have moved beyond the crisis to think about the future. In the six months from October 2020 to March 2021, the percentage of respondents noting their institutions were focused on cost optimization dropped from 23% to 8% and the percentage focused on resiliency dropped from 28% to 0%, while the percentage of respondents that noted their organizations were making targeted investments more than tripled, from 11% to 37% (see *More Than a Year After COVID-19 First Disrupted Business Operations for Education Institutions, How Have They Adapted*?, IDC #US47725121, May 2021). This supports the hypothesis that digital transformation in education has been accelerated and that more education institutions are investing in key technologies to remedy gaps in digital resiliency.

Extending endpoint security solutions to help students attend classes from anywhere can soften the operational strain and limit many types of hacking. This extension also helps improve overall cyber-resiliency and network security. By using secure applications and integrating system identity and access control, schools and universities can boost security management, authentication, malware protection, encryption, data loss prevention, intrusion detection and prevention, vulnerability assessment, and perimeter defense.

## Trends

The impact of COVID-19 on education providers cannot be overstated. The pandemic changed the very nature of classrooms, and it expanded the scope of both internal and external networking to support displaced classrooms and broader education initiatives. When it comes to cybersecurity, schools have coped admirably, but more work still needs to be done.

A shift to long-term remote and hybrid work and learning from home or while mobile for educators and students means that groups need to enhance collaboration capabilities to share applications, whiteboards, and presentations. In IDC's *Future Enterprise Resiliency and Spending Survey* from December 2021, education respondents indicated that they intend to increasingly leverage technology in physical and digital classrooms to create intelligent and connected workspaces and enable hybrid work and learning models. This increased leverage will result in more network connections and more data traffic. The personal devices and home networks used by students and educators may not be well secured, so schools, colleges, and universities must rely on zero trust connections. In addition, there's an increase in the use of deception to fool individuals into divulging confidential information or system access details. Institutions need to ramp up their efforts to educate staff and students on when it is not okay to share information. This should extend beyond the eschool environment, so they are aware of threats related to social media, suspicious websites, and shady applications.

Increased demand for client devices to support digital learning in classrooms, as well as distance and hybrid learning, creates additional security vulnerability pathways. Schools need to anticipate threats, develop scenarios for handling threats, and find ways to test their responses. Doing so before a major breach occurs can protect privacy, establish safe learning environments, and keep institutions out of the news for potential high-profile failures. But beyond this approach, new system penetration technologies continue to emerge and the geopolitical landscape is increasingly complex. Thus school leaders need to rethink cybersecurity. Because of the sprawling nature of today's education networks, this can mean finding the right partners for establishing best-of-breed technologies, security-as-a service solutions, and top-level access control.

The pandemic has accelerated the transformation of the education sector, and it has further increased the use of a wide range of client devices by primary and middle school students. Thin-client and virtualized desktops are growing in popularity. Though these solutions are usually less powerful, only have a web browser function requiring internet connectivity at all times, and bring their own security needs, they tend to be less complicated to configure than common home computers. IDC believes that the security industry needs to seize this opportunity to enhance its capabilities of providing multiple device solutions for home education.

Edge devices are proliferating across all industries, including education. The trend can help educators leverage a range of Internet of Things (IoT) devices, including sensors used for science lessons, weather data collection systems, and cameras that track eye movements to measure student engagement. Schools also are starting to invest in augmented reality. These "low end" network-connected devices have been shown to become internal vectors for security attacks. Being able to monitor such connected devices for proper security settings is a growing part of network security management.

As applications proliferate on mobile devices, it becomes obvious that edge users often need more computing power and resources than they have on their mobile devices — for example, collecting digital video versus doing in-depth video analytics.

## Considering Cisco

Cisco technology can help providers address not only the security challenges imposed by COVID-19 but also the longer-term evolution of security threats within education environments. Cisco provides holistic security that is built into its portfolio from the ground up.

- **Secure Remote Worker:**
  - Cisco understands the vulnerabilities of educators and administrators who are working from home and often access sensitive information. This is especially important as recent events have shown that remote devices have been used by bad actors for ransomware attacks and other hacking attempts. Cisco provides secure remote access via **Cisco Secure Remote Worker,** which offers an integrated set of solutions that provide secure access from any connection. **Cisco Duo** uses multifactor authentication to verify user identity, and the device must satisfy security requirements before the user is granted access to IT systems and sensitive student, faculty, and administrative information. **Cisco AnyConnect** enables virtual private network access from any device, at any time or place, to ensure secure access to critical IT resources.
- **Cisco Secure:**
  - **Network security:** As the network perimeter evolves and new challenges come into play, Cisco delivers threat intelligence, zero trust security, consistent protections, contextual visibility, predictive analytics, and automated responses to enable secure access and stay ahead of increasingly complex threats.
  - **User and endpoint protection:** Cisco unifies user access and endpoint protection with zero trust security for faculty and students, comprehensive threat protection, threat intelligence, and visibility across the institution's security architecture.
  - **Cloud edge:** As applications and networking infrastructure transition to the cloud, enabling students, faculty, researchers, and endpoints to connect directly to data, Cisco delivers a broad set of visibility, control, and security functions at the cloud edge. Cisco secures access to the internet and cloud app usage and detects external or internal public cloud threats.
  - **Application security:** As dynamic multicloud environments, containers, and serverless computing become the norm, Cisco brings continuous, adaptive, zero trust security closer to the application for greater insight and control. Cisco offers cloud workload protection to reduce the attack surface with automated micro-segmentation based on recommended policies tailored to an institution's applications and complete visibility of application behaviors, dependencies, and vulnerabilities.
  - **Cisco SecureX:** SecureX is a cloud-native, built-in platform experience that connects the Cisco Secure portfolio and an education institution's infrastructure. It is integrated and open for simplicity as well as unified in one location for visibility, and it maximizes operational efficiency with automated workflows — empowering institutions to reduce threat dwell time and human-powered tasks to stay compliant and counter attacks.

- **Webex by Cisco:**
  - Webex has security and privacy built into its core practices. In fact, all of Cisco's products and services are built using the Cisco Secure Development Lifecycle (CSDL) and are verified to meet strict security and privacy standards.
  - Cisco's Security and Trust Organization is responsible for standards and ensures that the company's Webex products are adequate for remote learning for all students, including those in primary and secondary environments.
  - Webex is committed to respecting the privacy of all users and their data, with secure default settings out of the box. Cisco Webex helps educators keep remote learning secure and student data private in accordance with FERPA and COPPA, in addition to education institutions' own privacy and security policies. Cisco publishes privacy and security FAQs for parents and guardians as well as school administrators.
  - Schools are in the best position to decide how to implement Webex for their specific teaching needs.
  - With Webex, individual schools or districts may decide how students access the platform and whether to utilize Cisco-provided integration with several learning management systems.

## *Market Opportunities and Challenges*

The market challenges that providers face also present opportunities for a vendor such as Cisco, which delivers a broad portfolio of technologies that enable transformation.

The rapid pace of change means new technologies must be rolled out while adhering to security standards. Schools may need to establish strict rules on how this is done, with a security partner that is adept at working with new and emerging technologies. Security can't wait, but budgets are limited. Given intense financial cost pressures, schools, colleges, and universities need solutions that are affordable, powerful, and flexible and able to handle future expansion. Security must be able to adapt to the rapid deployment of technology when service priorities shift, along with locations.

The right security and technology partner can fully enable remote workers and teachers while providing virtual instruction and shared resource services. Cybercriminals are evolving their attacks to exploit changes in education related to COVID-19 and to look for future opportunities. Knowing what is coming down the road is a key attribute for the right security partner. Further, security providers need a full and highly competitive portfolio of solutions. Education institutions need to know their needs can be met and that they will not have to switch their approach to security every few years.

While education institutions are under pressure from regulators, government agencies, parents, and students to enhance cybersecurity, it is important to remember that the free flow of information between people is critical to teaching and learning and is part of what makes education effective and enjoyable. Education institutions and the vendors that support them must work to balance the need for security with the need to enable institutions to be collaborative and innovative.

## Takeaways

With distance and hybrid-first work and learning models becoming increasingly permanent, end-user device management and security have surged to the forefront. Education institutions need the capabilities to prevent intruders from entering online learning systems, enable secure collaboration, and protect critical student and institutional data. Education institutions are focusing investments in these areas more than ever before.

Cybercriminals are exploiting the vulnerability of education institutions by taking advantage of distance and hybrid learning models through efforts including phishing and social engineering (the use of deception to fool individuals into divulging confidential information or system access details), which allows them to exploit institution-provided and/or personal devices. Both technology investments and educational outreach efforts are needed to counter these concerning trends.

Cybercriminals are exploiting education institutions by taking advantage of distance and hybrid learning models through efforts including phishing and social engineering.

Education institutions must make security a priority and develop a strategy to address vulnerabilities. The stakes are high for system breaches in education. Student privacy and the ongoing operations of institutional networks are at stake. The amount spent on security often more than pays for the cost of a high-profile security breach.

There can be differences between security in primary and secondary schools and higher education. In the lower grades, students often do not know how to utilize digital resources securely, and they need guidance from teachers and parents to do so. In school laptop environments, ransomware detection and mitigation are especially important for school-owned desktops/laptops for teachers and students. In colleges and universities, students often own their devices and have freer rein on their security and usage practices, and institutions may need to invest more in malware and ransomware protection, in addition to multifactor authentication because of the more open nature of what takes place on their networks.

Important investment points include highly secure access control systems, remote configuration management solutions, network monitoring tools, security as a service, and ongoing system updates and patches. In addition, institutions must comply with local, regional, and national cybersecurity standards for compliance and privacy. Some institutions build monitoring and compliance solutions to make sure their organizations keep pace.

Emerging cybersecurity trends will mean new investments for schools, including tools to monitor the growing attack surface. Schools must work toward zero trust environments that can promise security while allowing student usability and system expansion. Schools must also extend detection and response capabilities and enable secure access service edge solutions.

# About the Analyst

***Matthew Leger,*** *Research Manager, IDC Worldwide Education DX Strategies*

Matthew Leger is Research Manager for IDC Government Insights responsible for the Worldwide Education Digital Transformation Strategies practice. Mr. Leger's research focuses on key IT and digital transformation trends, as well as emerging solutions impacting how primary, secondary, and higher education and related services are delivered.

## MESSAGE FROM THE SPONSOR

**Between reacting to change and reimagining education, there's a bridge.**

Ever since two professors started Cisco in 1984, education has been in our blood. Cisco partners with education institutions to support educators, administrators, researchers, and students inside and outside the classroom with collaboration, security, mobility, networking, and data center technologies. We work with tens of thousands of schools, colleges, and universities around the world, and have trained 12.6M students through the Cisco Networking Academy.

As the world changes and continues to change, we're here to help. Cisco is and will continue to be an education company and your trusted technology partner supporting education, and we believe it is critical to continue educating the leaders, dreamers, scientists, artists, researchers, caretakers, and doctors of tomorrow, without compromising trust, security, or privacy today. **CTA**: ***Learn more.***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

**This publication was produced by IDC Custom Solutions.** The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.