Gigamon®

Higher Education Must Do More with Less While Accelerating Technology-Powered Learning

The New Tomorrow for Colleges and Universities

Executive Summary

The learn-from-home requirement for education has had profound effects on students, teachers, administrators and educational institutions. While many higher education institutions pivoted to some form of a distance learning model to cope during the immediate crisis, just how the learning environment will look for the coming academic year and the ones to follow remains less certain.

This white paper discusses the impact on the network of accelerating technology-powered learning and how NetOps and InfoSec can use network visibility, analytics and automation to manage security, performance and reliability, while doing more with existing network, staff and tools.

Welcome to the New Tomorrow in Higher Education

For the immediate future, the likelihood of repeated shutdowns and interruptions of in-person, classroom-based learning remains significant. Schools and universities will have to change their operating model to comply with social distancing and quarantine policies and support a mix of on-campus and distance learning. Distance learning will likely include distinct components — recorded core curriculum classes and testing, interactive class discussion sessions, small group tuition and one-on-one counseling services.

In a poll of 155 institutions in late April 2020, 66 percent reported that for the fall term their institution would offer some version of face-to-face learning with social distancing that can also accommodate those who prefer to stay off-campus. Almost one-quarter (23 percent) reported that they plan to offer fully distance/online classes, research and operations. Only 3 percent plan to fully resume face-to-face operations.[1]

Some institutions will take the opportunity to reimagine the operating and learning model and embrace innovative new ways to enrich learning, both in person and distance. Artificial intelligence (AI), virtual reality, holographic wearables and many other technological advances can dramatically improve access to and quality of education for today's generation of digital natives while keeping higher education institutions relevant and financially healthy.

A critical component underpinning the success of these endeavors is the resilience, agility and security of the network. That makes network operations (NetOps) and information security (InfoSec) professionals the unsung heroes of higher education.

These two teams must keep the network running fast and secure as the campus turns inside out and colleges and universities prepare to broadly adopt distance-learning models and new technologies. These professionals must accomplish their tasks while being asked to do more with less because of declining revenue and IT budgets.

From Disruption to Technology-Powered Learning

As university and college operating models evolve in response to the various stages of the global crisis, the learning experience may never be the same — but it can be better for both students and institutions. Distance learning may just be the beginning of the new tomorrow for education. Sudden disruption of the norm can be a powerful catalyst for innovation, spurring new interest, funding and creativity in using technology to enhance access to learning, engage students and make education more efficient and valuable to more people. Higher education institutions that take bold steps towards distance learning and greater adoption of technology learning models can better:

+ Adapt to the new realities of the world to minimize learning disruptions
+ Maintain or improve school rankings, student population and revenue
+ Justify tuition in a more/full virtual educational environment
+ Attract new generations of digital-native students and reengage with international students
+ Differentiate the institution compared to all-online universities

The Foundation for Reinventing Higher Education

Even before the crisis, some universities had already begun thinking outside of the proverbial box — the traditional classroom — and had launched projects that test new ideas for using increasingly sophisticated technology to improve learning and reduce costs. Some of the exciting new ways that colleges and universities are looking at incorporating technology for a technology-powered education include:

+ Augmented reality: Medical students at Case Western Reserve University have been using Microsoft HoloLens to replace cadavers in anatomy classes by superimposing digital content, including hologram-like images, onto a user's view of the real world. The augmented reality technology is combined with voice instruction for a successful distance-learning model for hands-on or lab-based learning.[2]
+ Virtual assistants: Georgia Tech has been experimenting with an artificial intelligence (AI)-based virtual teaching assistant called Jill Watson (in homage to the IBM Watson supercomputer). The virtual assistant answers student questions in a discussion forum alongside human teaching assistants.[3]
+ Immersive, AI-powered virtual reality: At Rensselaer Polytechnic Institute, students master Mandarin Chinese twice as fast using an immersive language lab with a 360-degree projection system. Students converse with AI avatars within a computer-generated backdrop of Chinese street markets, restaurants and other locations.[3]

It's not only models of learning that can benefit from an injection of new technology. Administrative systems — many of them legacy, on-premises systems — are ripe for being replaced with more modern software that supports capabilities needed to handle the current crisis and beyond, including: remote access to support work-from-home models; expanded access to digital self-service tools for students; and support for new business models like subscription-based classes instead of semester- and course-based tuition.

While opportunities abound to reinvent higher education for the better, the introduction of new technology and the greater use of technology for distance learning and teaching creates a set of new challenges for an institution's network.

Network Bandwidth, Security and Data Privacy Issues

University and college networks are among the heaviest trafficked. Now, with a greater shift to distance learning, these already-stretched networks must handle enormous and growing amounts of traffic. As bandwidth issues proliferate, higher education institutions that haven't already upgraded to 100GB networks will find that they must do so in the near future or find ways to get more out of existing network investments to keep up with traffic demands and performance requirements, as new technology is deployed and more learning takes place in virtual classrooms.

In the rush to move to distance learning, existing vulnerabilities, new risks and the attack surface have all increased. As a case in point, universities and K–12 schools have endured hackers disrupting remote classes with pornography and other unwelcome activities.

Financially Motivated Cyberattacks

Cybercriminals increasingly target educational institutions with malicious cyberattacks, including data theft and ransomware.

+ A data breach at Georgia Tech exposed the records of 1.3 million faculty and staff[4]
+ Regis University, a private university in Denver, had its internet, email, phones and website shut down due to a cyberattack as the school year was starting[5]
+ The Stevens Institute of Technology, a private university in New Jersey, was the victim of a "very severe and sophisticated" cyberattack, causing it to remain offline for a week[5]
+ Monroe College, a for-profit institution in New York City, was asked to pay a ransom of $2 million in bitcoin to restore access to the college's website, learning management system and email[5]

State-Sponsored Cyberattacks

Research universities have long been the target of state-sponsored hackers, with the intention of stealing intellectual property, gaining access to sensitive information or disrupting research.

+ Chinese hackers attempted to steal military research secrets from 27 U.S. institutions, including: MIT, University of Hawaii, Penn State, Duke University and University of Washington[6]
+ During the COVID-19 pandemic, U.S. intelligence agencies issued warnings that China is sponsoring widespread cyberattacks intended to steal vaccine research[7]

Data Privacy Issues

Finally, from the data privacy perspective, the shift to digital is creating more opportunity for violations of student privacy laws such as the Family Educational Rights and Privacy Act (FERPA). For instance, new technology being put into place could create what could be considered private education records, and then inadvertently allow disclosure of those records to unauthorized parties.

THE STATE OF CYBERSECURITY IN EDUCATION

The education sector was ranked last among 17 industries in cybersecurity preparedness[8]

819 **Cybersecurity incidents in education** reported in 2019, of which 228 had confirmed data disclosure[9]

114% **Increase in cybersecurity incidents** compared to 2018, which saw 382 incidents[10]

348 **Cyberattacks on K–12 school systems** in 2019, which represent three times as many publicly disclosed cyber incidents as in 2018[11]

500 **U.S. schools and colleges** that were hit with ransomware attacks in the first nine months of 2019[12]

Budget Uncertainty: A Mandate to Do More with Less

Most IT organizations are facing budget uncertainty, and higher education is no exception. In a poll of higher education institutions, almost three-quarters of respondents are preparing for budget cuts in the institutional IT budget for the next academic year. Four in ten respondents are preparing for cuts of 5–25 percent.[1]

In the same poll, more than 90 percent of respondents indicate that their institutions are implementing or intending to implement (47 percent) or are considering (45 percent) digital transformation as a way of reducing institutional costs.[1]

Tasked to accelerate digital initiatives such as technology-powered learning despite having less overall budget to do so, IT organizations within higher education must find ways to do more with less and get more out of existing investments to free up additional discretionary budget in the short term.

The Burden on NetOps and InfoSec Teams

Given the criticality of the network for distance learning and other technology-powered learning initiatives, NetOps and InfoSec teams must do more with less while preventing disruptions, enabling the security and performance of new technologies, thwarting cyberattacks and preventing theft of private student information or intellectual property. To do so, these two teams must overcome the following challenges.

To address their respective challenges and enable new learning and operational models, NetOps and InfoSec teams need the following capabilities:

+ Real-time visibility into all network traffic to understand and optimize performance of existing investments and improve security
+ Analytics to optimize and manage network performance to accommodate and secure increasing volumes of data/traffic

+ A single pane of glass that simplifies network and security operations across physical, virtual and cloud environments, while extending security and network tool life
+ Threat detection and response to find and remediate threats on the network faster and minimize disruption
+ Automation to free up staff and allow them to do more, faster

NetOps Challenges	InfoSec Challenges
Assure the constant resilience, performance and security of IT networks	Identify security vulnerabilities in the network and mitigate them
Identify and eliminate potential bottlenecks that impact performance and cause disruption	Detect and respond to cyberthreats on the network
Scale networks quickly to support increased traffic and data volume	Manage security across an increasingly complex network environment
Manage increasingly complex network environments	Gain visibility into threats originating from connected devices such as wearables for virtual reality-based learning
Do more, faster to keep up with technology additions and changes, and do so with reduced budgets	Support security efforts with reduced budgets and limited staff

University of Wisconsin–Madison Upgrades Its Network and Maintains Visibility and Security

> [Gigamon] enabled multiple teams to have visibility into the traffic on our 100GB links and across the network. We got this so we could have UW–Madison traffic analyzed by our security monitoring systems."
>
> *—Jeff Savoy, Campus Information Security Officer, University of Wisconsin–Madison*

By implementing the Gigamon Visibility and Analytics Fabric™, the university, one of the most prolific research institutions in the world, gained:

+ Renewed visibility and security after a network upgrade
+ Reliable data access for tools and teams
+ Improved network troubleshooting
+ Accelerated testing of new tools

Final Thoughts

As higher education institutions adapt to the challenges of physical distancing and distance learning, network security, performance and reliability will be imperative to prevent further disruption to the college and university experience. NetOps and InfoSec professionals need visibility, analytics and automation as their building blocks for delivering an optimized, secure network that accelerates technology-powered learning initiatives while getting more out of existing investments.

The Gigamon Visibility and Analytics Fabric delivers visibility, availability, and security solutions that power the highest levels of innovation. It provides a unified visibility architecture across physical, virtual, cloud and multi-cloud environments to power the digital transformation process and optimize the entire network, enabling institutions to run fast, stay secure and emerge stronger in the New Tomorrow.

About Gigamon

Gigamon provides network visibility and analytics on all traffic across your physical, virtual and cloud networks to solve critical security, performance and business continuity needs. The Gigamon Visibility and Analytics Fabric delivers optimized network and security performance, simplified management and accelerated troubleshooting while increasing your tools' return on investment. Trusted by 83 percent of the Fortune 100 and 4,000 organizations worldwide, Gigamon enables higher education institutions to do more with their existing resources and accelerate critical technology-powered learning initiatives.

For the full story on how Gigamon can help you, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95954 USA
+1 (408) 831-4000 | www.gigamon.com

Resources

[1] Susan Grajeck. "EDUCAUSE COVID-19 QuickPoll Results: IT Budgets 2020-2021." EDUCAUSE. May 6, 2020. https://er.educause.edu/blogs/2020/5/educause-covid-19-quickpoll-results-it-budgets-2020-2021.

[2] Agam Shah. "Universities Get Creative with Technology Due to Coronavirus Closures." The Wall Street Journal. April 3, 2020. https://www.wsj.com/articles/universities-get-creative-with-technology-due-to-coronavirus-closures-11585918801.

[3] Jon Marcus. "Subscribing to College and Other Visions of Higher Education's Future." The Hechinger Report. February 20, 2020. https://hechingerreport.org/subscribing-to-college-and-other-visions-of-higher-educations-future.

[4] Scott Ikeda. "Recent Hacks Show That Even Tech-Savvy Universities Are Still Very Vulnerable to Cyber Attacks." CPO Magazine. April 17, 2019. https://www.cpomagazine.com/cyber-security/recent-hacks-show-that-even-tech-savvy-universities-are-still-very-vulnerable-to-cyber-attacks/.

[5] Lindsay McKenzie. "Cyberattacks Mar Start of Academic Year." Inside Higher Ed. August 27, 2019. https://www.insidehighered.com/news/2019/08/27/two-universities-targeted-hackers-just-new-school-year.

[6] Lindsay McKenzie. "On Red Alert." Inside Higher Ed. March 6, 2019. https://www.insidehighered.com/news/2019/03/06/report-top-universities-us-targeted-chinese-hackers.

[7] Gordon Lubold and Dustin Volz. "U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research." The Wall Street Journal. May 14, 2020. https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205.

[8] "2018 Education Cybersecurity Report." Security Scorecard, December 2018.

[9] "2020 Data Breach Investigations Report." Verizon, 2020.

[10] "2019 Data Breach Investigations Report." Verizon. 2019.

[11] "Ransomware Attacks and Data Breaches on U.S. Schools and Colleges Triple in 2019." CISO Magazine, February 2020. https://cisomag.eccouncil.org/ransomware-attacks-and-data-breaches-on-u-s-schools-and-colleges-triple-in-2019.

[12] Catalin Cimpanu. "Over 500 US Schools Were Hit by Ransomware in 2019." ZDNet. October 1, 2019. https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019.