A technology plan for an uncertain world

Four pillars to help you shape the future of higher education

Most well-run educational institutions spend considerable time and effort building and updating five-year plans. Yours is probably among them. You know the exercise: deciding what you want your university to look like, five years from now, and drawing a plan for how you mean to get there.

How is that five-year playbook you drew up in 2020 looking today? Chances are that all the projections for fundraising, instruction, research, facilities, IT, and classroom activity you made back then have turned to mincemeat. In fact, it's hard to think of any part of your institution that's running the way it was in early 2020.

But wallowing in busted plans doesn't help you move forward. The question is no longer, "How can we adapt quickly until things get back to normal?" The better questions are, "How can we move forward into a future where no one really knows what 'education' will look like?" and "How is it possible to plan for a future that's so uncertain?"

The reality is that you need a whole new kind of plan—not one that attempts to dictate a fixed future but one that prepares your institution to thrive in an era of uncertainty.

The four pillars of a successful plan

It's possible to create an effective plan even in an environment where the day's news headlines can shift your current strategy. Five-year planning may be obsolete; even a two-year horizon often seems ambitious. But adhering to core principles will never fail you, whether you work in education, business, or some other realm. Even though educational institutions and educators have unique issues to solve, there are important lessons to be learned from business and other leaders who struggle with similar planning issues.

"I never believed in five years," says Ken Lamar, who ran the data and statistics function of the Federal Reserve Bank of New York and now is the principal partner for Lamar Associates LLC. "I thought you could plan 24 months out and then have aspirational goals after that. What you planned this year, it's going to change by next year anyway. I think you have to show a lot of flexibility."[1]

These four pillars can help you prepare a blueprint for whatever the world throws your way:

Stay secure
Maintain peace of mind

Stay connected
Take location out of the equation

Stay productive
Give the right gear to the right people

Stay flexible
Avoid operational interruption

Stay secure

"People are more worried about what someone will do once they get [into a network]. Stop worrying so much about what's going to happen once they get in: Do everything you can to prevent them from getting in. This is the starting point."

Dr. Rois Ni Thuama

Wherever and however people work, they have to stay secure. That means giving people the tools to protect themselves and to detect and recover from attacks.

Look to see what the intelligence communities are saying are the biggest problems, advises Dr. Rois Ni Thuama, head of cyber governance with the security firm Red Sift. "They're the only problems that you need to worry about. Do not get distracted.... Then you look to the solutions that are recommended, including but not limited to multifactor authentication and endpoint detection. You need encryption, you need DMARC [email authentication], you need good, strong passwords. Find the biggest problems [and] address only those...."[2]

That means ensuring endpoints have built-in protection against the biggest threats, along with a mechanism to keep those endpoints up to date, wherever they may be. Badly secured endpoints are how ransomware frequently gets into networks; one study found that while ransoms cost educational institutions an average of more than $100,000, the additional cost of network outages averages $2.73 million.[3]

35% of ransomware-attacked schools handed over money to their attackers, but only 68% of those had their data restored.[3]

Whatever your security plan is, ensure it acknowledges the very real threats that are already occurring and are likely to become more intense.

HP Wolf Security helps keep endpoints safe, ⟶ wherever they are.

Stay connected

The heartbeat of academia is collaboration, and finding the means to do that when people are separated became Job One in early 2020. The hard part in creating this new era, particularly for blended classroom environments, turned out to be making sure that everyone felt heard, emotionally connected, and part of a unified group.

Lynne Labrador spent much of her 40-year career managing remote teams around the world. "To me," says Labrador, now a global product head at Equifax, "the pandemic was sort of a 'gotcha' moment." Many institutions were uncomfortable allowing people to do their jobs away from campus, but Labrador points out, "I believe if you want people to act like grownups, treat them like grownups. If people have kids or a long commute, and they would rather work from home a couple days, let them do that."[4]

The right technology can also foster the casual interactions that so often power the academy and help define an institution's culture. Well-designed casual meeting places can make collaboration with remote staff simple and effective.

Technology that fosters collaboration and equity is especially important for academic institutions.

Ensure employees are in the room from any room with HP Presence. ⟶

Stay productive

Just as it's always been, having the right gear and systems in place is vital to give your institution the flexibility it needs. Legacy systems often don't lend themselves to cloud adaptation. What sometimes holds up dispersed work isn't so much the available technology as it is the determination or necessity to deploy it.

When the early days of the pandemic made distributed work necessary, educational institutions found the discipline to make it happen. Now that people are embracing the new era of work, it's smart to renew the decision to make it work better.

If the old style of plan embodied a top-down structure offering little room to maneuver, the new style must embrace change and put people at the center. Give everyone the tools they need or let them use the tools they already like, whether that's a laptop, a tablet, or a workstation.

The world is fortunate that the pandemic didn't come a decade ago, when online services weren't as sophisticated, high-speed bandwidth wasn't as common, and desktop systems weren't so powerful. Remote work was possible then, but it was much harder to pull off on a mass scale.

"It's a complicated world. Integration is tough, and I'm not sure people know exactly what they're buying all the time."[1]

Ken Lamar

Learn more about how HP Elite PCs and Ecosystems keep teams productive. ⟶

Stay flexible

Nothing is more important than making sure that your institution can keep operating, whatever challenges arise. Over the past two years, your IT department's mission has changed from being a vendor to internal clients to becoming a full strategic partner in keeping the campus operating.

"For a CIO, one of our primary conversations is how do we get that seat at the table? Well, now we've got that seat at the table. And I feel as if it's expanded."

Paige Francis, former CIO, University of Tulsa[5]

And it is possible to plan—or at least contemplate—the worst. "I did a lot of business continuity planning when I was at the Fed," says Lamar. "We planned out all these things. I remember [drawing up plans for] the 'bird flu' [pandemic of 2006]. If you didn't have the infrastructure we have, you wouldn't be able to do this. It would've been a much different story, I believe."

"I think a five-year plan is dangerous. What's missing in those plans is the feedback loop and the agility to pivot as new things are learned. What's key is, how quick are you to fail fast and pivot based on new information?"[4]

Lynne Labrador

Lamar says the pandemic and the urgency it introduced to IT departments are helping shift in favor of outside services where possible. "I think the rate of change and the expectations about your ability to adapt...are going to require [IT] people to find innovative ways" to work, he said. A large part of that is finding trusted partners that can relieve the stress on overburdened IT departments.

Learn more about how HP can help with managed services. →

The new plan

⟶

[HP logo]

No rational five-year plan was ever static, but the challenges that education faces in these immensely uncertain times are particularly daunting. Academia needs to find a new type of path forward—one that emphasizes flexibility and empowerment rather than top-down decrees.

Focus on the things that make you successful:

Help ensure endpoints and data stay secure with
HP Wolf Security[6] ↗

Be in the room from any room with HP Presence[7] ↗

Equip people to thrive with HP Elite PCs and Ecosystems ↗

Solve problems before they happen with HP Services[8] ↗

Ask how HP can help.

[1] Ken Lamar, in discussion with the authors, 2021.

[2] Dr. Rois Ni Thuama, in discussion with the authors, 2021.

[3] Insight Into Diversity, "Cyberattacks Pose Huge Financial Threat to Struggling Colleges and Universities," December 21, 2021, http://www.insightintodiversity.com/cyberattacks-pose-huge-financial-threat-to-struggling-colleges-and-universities/

[4] Lynne Labrador, in discussion with the authors, 2021.

[5] EdScoop, "University IT department's 'seat at the table' expanded during pandemic," April 13, 2021, https://edscoop.com/radio/it-departments-had-to-fill-in-the-gaps-during-pandemic/

[6] HP Wolf Security for Business requires Windows 10 or 11 Pro and higher, includes various HP security features and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.

[7] Select HP Products are enhanced with HP Presence. Features vary by platform.

[8] HP Services are sold separately and are are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.