TECH TACTICS

Modernizing Identity Is Vital to More Efficient, More Effective Campus IT

Any IT initiative really starts with identity. Without a cohesive identity strategy, you put security at risk and users have a much harder time maneuvering through campus systems. Here's how to put an identity plan and solution in place.

AS COLLEGES AND UNIVERSITIES REMAKE themselves to deliver value in a new era of higher education, there's one modernization priority that forms the foundation of every project in the works: Identity. Identity and access management (IAM) underpin other major aspects of IT: infrastructure, data and security. To manage and safeguard these areas appropriately, IT must be able to see, manage and protect user identities, and connect the right people to the right technologies at the right time.

While almost every institution — be it a small community college, a Research 1 institution or schools in between — addresses IAM problems in some way today, the technology in place may not be doing enough. Take one of the country's largest universities. "Their lead administrator for the identity management program was going to be spending the next six weeks upgrading directory services authentication servers," said Rob Forbes, senior solutions architect for **Okta**, a company that provides a trusted cloud identity platform. "That meant the 15 projects other departments were coming to him for had to wait."

As Forbes put it, "The care and feeding and testing of old systems means the IT organization doesn't have time to undertake the projects that are really important."

By virtue of his role, Forbes works with a lot of organizations to assess the state of their IAM setups. The ones that need help have a few characteristics in common:

- Adding new students requires following a process that has been cobbled together involving manual tasks and numerous applications. “We send these files around to these 10 people and they each do one piece of the job,” Forbes gave as an example of common feedback he receives from universities.
- Some servers can never “be touched” because “a student or programmer wrote the source code five years ago, nobody else understands it, and if that server goes down, we’re in big trouble,” another common sentiment Forbes noted.
- LDAP server maintenance requires a disproportionate amount of effort. Oftentimes, Forbes explained, new servers will need to replace the old ones, one-by-one, with all of the accompanying effort, including testing of every single application and workflow that relies on that instance of LDAP.

Even schools using more modern platforms often find themselves supporting a “high-touch infrastructure” with an army of machines to support: workload servers, database servers, LDAP servers and load balancers.

“A lot of education customers end up behind because they can’t keep up with patching,” noted Forbes. “I can’t upgrade your database because this application over here is using it and it doesn’t support that new version.” As a result, IT gets “into this cycle of chasing upgrades and patches, and it’s a lot of effort.”

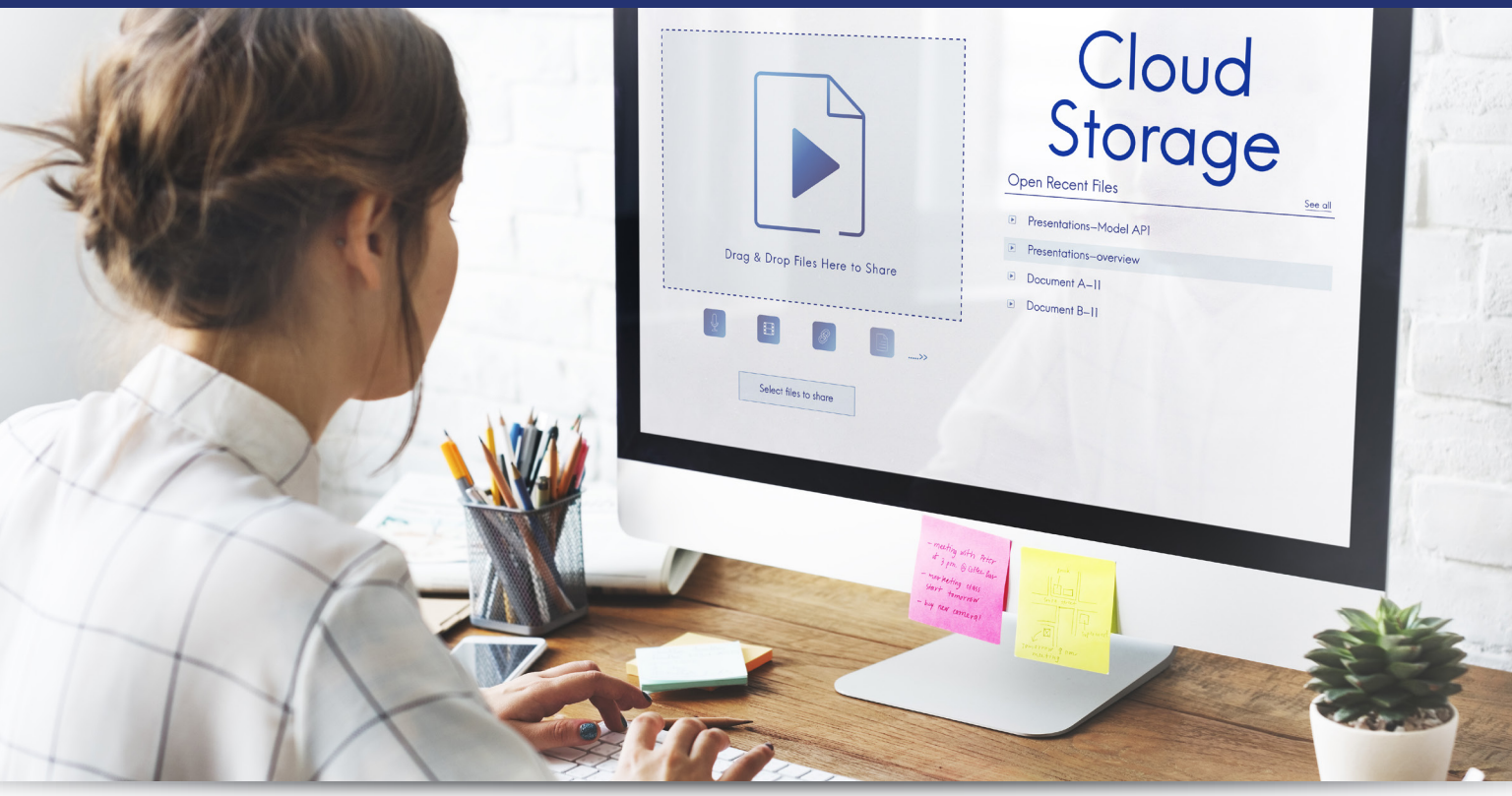
Removing Roadblocks

When IAM is done properly, the campus community enjoys a “frictionless day,” Forbes asserted. “As users are interacting with the university or college, whether they’re coming to a lab as a student, logging into a virtual meeting as a faculty member or logging in to get tickets for the game as an alumnus, it’s very simple and easy for them to do it. It’s secure and seamless to users, even if they’re going across three or four different platforms on the back side to get something done.”

When these roadblocks are removed, “my day is not spent putting my password or multi-factor authentication in over and over again — or calling the help desk because I don’t have the right access.”

As a result, the volume of help desk calls and tickets related to access issues and password resets shrinks “and the level of effort by your system administrators is going to drop drastically,” Forbes added.

Achieving that starts with development of a cohesive identity strategy. And that’s where a cloud approach excels. An independent cloud identity solution connects the right people to the right technologies at the right time, serving as a *lingua franca* that bridges an



institution's various directory sources with its many login mechanisms — SSO, MFA, YubiKeys and biometrics — to provide users with efficient and secure access to a variety of applications.

As a result, IT worries less about availability, scalability or security. And it spends less time patching servers, adding new hardware or managing one-off IAM integrations.

How Okta Does Identity

The **Okta Identity Cloud** serves as an independent and neutral platform that securely connects the right people to the right technologies at the right time, reducing the effort required by IT to balance the needs of access and security. The Okta Identity Cloud incorporates **Single Sign-On**, **Adaptive MFA** and **API Access Management**. But the magic ingredient is really the architecture, which empowers organizations to unify service across disparate organizations through a hub-and-spoke model that serves as a centralized identity layer:

- The *hub* acts as the centralized identity provider, using standards such as security assertion markup language (SAML) and OpenID to integrate with numerous downstream applications, whether those are in the cloud or on premise, to provide access and provisioning capabilities across the network.
- Each *spoke* represents a unique campus, school or department, whether part of the same institutional system or a separate university or college. The spokes tap Okta's **Universal Directory** for storing information about the user profile and group. The **Org2Org** connector enables spokes to share user profiles with the hub or other spokes, allowing for SSO and **multi-factor authentication** to work across numerous shared applications.

Each campus can marry its own Active Directory repository on one side of the hub with the advantages of SSO, MFA and provisioning on the other side, giving users efficient and secure access to college or university applications — both their own and those of their institutional partners.

According to Forbes, a first use of Okta can be set up rapidly, in a quarter to half of the time that is required for deploying legacy IAM programs. "We can have an Okta instance up in weeks, talking to your key sources, whether that's Active Directory, LDAP servers, HR systems, the student information system, Workday or Peoplesoft instance, and putting them through a central platform. We do this in a very rapid fashion because you won't have to set up and provision a bunch of servers. Time-to-value is critical with us."

Also important: the maturation process itself. The work often begins with one directory service and grows from there. The route to success is "configurable based on what capabilities the university has and its identity maturity."

Modernizing IAM: Do's and Don'ts

10 expert tips to effectively manage and protect user identities.

DO watch for the signals of a lagging approach to IAM.

For a lot of institutions, a big clue they're behind on the identity curve is this: A majority of help desk requests have to do with password resets.

Maybe the user needs access to a legacy program that isn't part of the portal he or she normally logs into. Or perhaps some aspect of the user's status has changed and he or she doesn't have the right access to a new set of applications because there's a lag between the time the change was made and when the other systems get updated.

Or there could be deeper problems with provisioning overall, suggested Forbes. An institutional audit might reveal that people have moved around in the organization and still have access they shouldn't: "Hey, Robert doesn't even work here anymore but he can still get into this system. Or, Robert now works in the finance office, but he's got access to all these IT systems for the department where he used to work."

Then again, it may just be challenging for the identity team to keep up. A school can tell that it's time to upgrade IAM, said Forbes, "when people go to IT and ask for a new application or request a new parent portal or want to bring on a new mobile app to help the students, and the response is, 'Can't get to it. Don't have the cycles because I'm over here doing these patches and all this care and feeding.'"

DO expect to "mature" your IAM processes over time.

When an institution undertakes an IAM transformation, it often begins with the "low-hanging, high-touch problems." Often, that entails getting the school moved away "from the manual processes involved in creating and removing and moving users," said Forbes.

The biggest pain point could be managing user identities through the entire lifecycle, from applying to the university through donating as alumni, or becoming a graduate student, teaching assistant or faculty member. At each milestone, the user requires access to different resources. On the faculty side, a quick win might be helping instructors who teach at a myriad of locations, each requiring a separate login and password. Or the main challenge could involve rescuing researchers who suddenly have a new government contract that requires use of multi-factor authentication in front of the research applications they'll use.

Once those kinds of problems are resolved, Forbes said, the next stage might entail looking for opportunities to create a "closed loop business process," such as tying in IT service management (ITSM) and help desk systems. That involves finding ways to automate the process of provisioning access to resources following an authorized request — such as an instructor requesting access to a necessary application for students before a new class begins. When IAM is architected properly, he noted, the request will "just automatically reach into the identity platform, update the attribute that's used to give the access, and then that access is granted." Automating requests that way "closes the loop on that process and eliminates human error," he said. "And it makes it faster and creates less friction for the end user to get access to the things they need."

From there, Forbes suggested, the institution can "start working on things like federation and Shibboleth and the central authentication service and other legacy identity systems that the university has to deal with and manage and maintain."

What's important to remember, he added, is that this won't all happen on day one. "This might be something that

we say we're going to grow into over 12 or 18 months. But that first phase can be accomplished in 12 to 16 weeks."

DO start with the birthright of the lifecycle, where user satisfaction gets made or waylaid.

Forbes advised starting modernization of IAM with the "birthright of the lifecycle of the employee or student." That means automating the process of getting them into the systems initially.

As he asserted, "There should be no sending an e-mail to IT to make sure they're adding the new person to a file. It should be that the user gets an e-mail saying, 'Here's your account and this is where you go to claim it. This is how you're going to log in, and once you do — with one click — you'll be able to access everything you're going to need.'"

While most employees will suffer silently as the crank of user access gets turned, students aren't as patient, Forbes added. "If students aren't happy, they're going to tell people on social media. So, you want to make sure that that flow and process is complete."

What needs to happen is that as a flag on a user changes — they've been admitted, graduated, hired, fired, transferred, promoted or whatever — the IAM system is alerted and kicks into action, without waiting for human intervention. Okta, for example, can be configured to "see those changes," said Forbes, and then "those actions just flow seamlessly," reducing the risk of human error, delay and dissatisfaction.

DO clean up the data.

Cleanup is always a part of initial conversations when Okta begins a new engagement, said Forbes. "If you've got old, orphaned accounts in there, you don't want to bring them into your Okta instance and have your auditor say, 'Wow. You've just brought up a brand-new identity management platform, and you still have a professor listed over here who hasn't been part of the school in five years.'"

Undertaking an IAM refresh is a great time to jettison the flotsam. The big question is, who does the work? As Forbes explained, "We can do it; partners can do it; or universities can go do it themselves."

Oftentimes, third-party providers will build "fuzzy logic" tools that make it easy to look across data stores and perform cleanup activities. That doesn't just include deleting duplicates or removing outdated information. It could mean recognizing the need to develop new roles, such as a group of faculty or students who are part of the newest college on campus.

DO provide IT with visibility.

When IT is troubleshooting incidents or dealing with audits, it needs to be able to see who logged in where, when and how. Frequently, this results in information overflow, with a number of different SEM, SIM and SIEM systems pouring out their log data. Ideally, IT should have visibility in one place that also empowers it to act on the data , without a complex configuration/integration exercise to get all downstream applications to feed accurate data into the central repository.

"There's great value in being able to pull that information and have that visibility coming from one source," said Forbes. He offered a couple of examples. Say a user is all of a sudden being phished a lot. "Why not drop that user into a group that requires multi-factor authentication all the time" as a temporary security measure, he suggested.

Or why couldn't the staffers handling incident response and root cause analysis send a message to a user whose status indicates he or she is on vacation, asking, "Are you doing this huge transfer of data?" This level of visibility enables IT to proactively spot and remediate security threats.

"Leveraging the power of identity, you can improve not just the identity program but also other processes, like incident response, creating a greater maturity over your IT infrastructure as a whole," said Forbes.

DON'T ignore user satisfaction or customer experience.

Users rely on their digital systems for nearly everything now — learning, teaching, working, collaboration,

communication. Figuring out how to get to any given resource might require cruising through a list of bookmarks, searching e-mails for login information, or navigating a website to find out who to contact when access is needed but has not yet been provisioned.

Ideally, schools would offer a single place to go where users log in using multi-factor authentication and immediately have a list of the applications they'll need laid out and ready to use with a single click. While portals have been with us for a long time, they haven't always worked as seamlessly as they ought to. Nor have they been customizable and expandable with additional resources the user wants at hand, such as their calendar or a link to the next virtual meeting.

Nor have those portals been adaptable. If you've just logged in, why should you have to repeat that process again and again? Yes, maybe when you're getting into payroll, another explicit confirmation is a good idea; but just because you're suddenly joining a new project, the systems involved should know that you belong because HR has already been notified.

Forbes referred to it as the "art of the possible — making it much easier for users to go do stuff.

He offered the example of an IT support request. "I should be able to open up a help desk ticket for access to a new application and, as it flows through that chain, be able to see where it's at and know when it'll be done — without having to wait on a follow-up e-mail from somebody."

When that's how the process unfolds, users are happy because the experience is so easy. "They know they'll get the right access at the right time without having to worry about it, without having to chase the status down."

DON'T rely on batch processing. It poses a security risk.

While batch processing is doable in IAM activities, it's not advised. "Initially, we'll leverage the CSV format to get things rolling," said Forbes. "That is a great way to get things done and shrink time-to-value. But in the long term, the more real-time an institution can make identity, the less friction they impose on users and the less risk the universities incur."

Forbes offered the example of a CSV file listing the people who have been terminated during the last 24 hours. A person who has been let go at 5 p.m. may continue to have access to work resources until midnight. The batch updates "create time windows for exposures to occur until the next update," he noted.

Similarly, the reverse can happen. When people's jobs change in the middle of the day, they may have to wait until the next day to get access to the new roles' resources.

"The more real-time you can make it, the better you are from a user satisfaction standpoint and from a vulnerability standpoint," said Forbes.

DON'T wait for your Shibboleth expert to leave before you act.

The Shibboleth system for single sign-on has been a boon for higher ed for nearly two decades. But, as Forbes observed, setting up federation inside Shibboleth "is a very technical thing." The XML files used to manage the implementations "can be three plus pages long and full of very detailed information that you have to edit manually." Hammering out connections between data sources and applications can take SAML experts "two or three days."

Ideally, schools would offer a single place to go where users log in using multi-factor authentication and immediately have a list of the applications they'll need laid out and ready to use with a single click. While portals have been with us for a long time, they haven't always worked as seamlessly as they ought to.

That's worrisome to Forbes. "It's mind-boggling, the number of universities I've talked to that tell me, 'We've got Joe. He's our Shibboleth expert. He's been here for 13 years.' What are you going to do when Joe goes?"

Forbes advised schools to consider expanding their environment along with their human resources. That's where a platform like Okta proves advantageous. "We've got 7,500-plus connections," Forbes said. "When someone needs to talk to a given application with SAML, great. Click. Five minutes, 10 minutes, 15 minutes and you have a setup."

On top of that time savings, he added, the work can be handed off to an IT administrator without specialized Shibboleth or SAML expertise, "because we have those integrations, they're documented, they're well known,

well understood, and we just walk you through it. The level and skill needed for somebody to do the integrations drops drastically."

And the Shibboleth expert? "That's a really smart person" who can now go work on all those other "higher value" projects waiting in the wings, Forbes pointed out.

DON'T delay identity work until your data governance structure is in place.

Forbes said it's *atypical* for institutions of higher ed to have data governance councils in place. And while education customers need data governance, setting up a council is a project in itself. "There's the whole negotiation of who owns that data, who's got the right to tag that data, who's got the right to grant access to that data," he noted.

That doesn't mean, however, that identity work should wait. It can follow a parallel process. "If we're having that conversation, I tell them they need to start since identity decisions are going to touch all these platforms that data governance is going to cover. The key players are going to be the same," Forbes pointed out. "So, you might as well start looking at data governance as part of understanding how people and applications are getting access to the resources that data governance is going to control and write the rules about. They're different trains, but they're running parallel to each other, feeding out of the same station."

DON'T settle for "free."

Oftentimes, vendors will provide IAM products as part of a larger enterprise application licensing deal. Or an institution will decide to adopt an open-source solution. Forbes urged higher-ed IT organizations in colleges and universities to be wary of those "free" deals.

Free can mean "free like a puppy," he pointed out. Just because something's free, "that doesn't mean it is going to meet your needs." A lot of times, there will be hidden costs associated: It's free, as long as you don't exceed x number of authorizations. It's free up to this many users. It's free for these 300 connectors that the company offers out of the box. For anything else, you'll have to pay professional services to create custom connections or you'll have to write your own — which the company may or may not support.

"You have to compare apples to apples, when you start thinking about some of these opportunities for a free identity solution," he advised. "Identity has become a foundational piece of IT that pervades pretty much everything else. If someone says, 'I can give you some great land over here and it's free,' but it's quicksand, would you want to build your house on that?"

Identity Is Complicated

Universities and colleges present some of the most complicated environments in the world because they have an ever-changing set of users. Every semester a huge share of students departs while another cohort enrolls. Visiting faculty are invited on campus for a period and adjuncts are shuffled. Researchers pair up with experts in other institutions for the terms of their projects. University hospitals see an influx and outflux of patients. And even within each of those roles, there's a fluidity that other organizations outside of the education sector don't face. While a company CEO may also be a board member, a student may be a learner, a worker, an intern, a teaching assistant, a graduate, a patient at the campus clinic, and a donor, all in the same year.

"This constant ebb and flow of users is complex, which makes identity difficult to understand," said Forbes. "Streamlining your identity approach with the right identity and access management platform can free up hard working resources from manual efforts and allow them to go do the other things you need to do to modernize your campus and solve a lot of other problems."

At the same time, he added, "user satisfaction, employee satisfaction, student satisfaction will go up because you're giving them access to things they need. They can badge into the building and get into their research projects. And when a department comes to them and says, 'We're going to spin up this research project and we need this new application integrated and set up to be able to provision folks to,' they'll have the capability to help because identity integration becomes easier and faster."

This article is based on contributions and commentary provided by Rob Forbes, senior solutions architect at Okta, Inc. The views, thoughts and opinions expressed in this article are his own based on his professional and personal experience and do not necessarily represent the official views of Okta. This article is provided for informational purposes only. Okta makes no representations, warranties or other assurances regarding the content of this article. Information regarding Okta's contractual assurances to its customers can be found at ***okta.com/agreements****.*