Building an Identity and Access Management Solution That Can Keep Up with the Demands of Higher Education

How Baylor University and Fischer Identity created a better, more secure access experience for students, employees, and guests by using the AWS cloud architecture

FISCHER IDENTITY

powered by aws

Many higher-education leaders recognize the rising stakes of cybersecurity.

Attackers frequently target higher-education institutions because these institutions serve so many personas, including faculty, students, staff, and guests — and because these institutions capture so much data across these personas. Government bodies have recognized this threat too: Title IV funding requires colleges to implement a range of cybersecurity measures, and due to a 2018 policy mandate, every single data breach must be reported to the U.S. Department of Education.

However, the higher education sector remains a popular target, and the costs of data breaches continue to rise. IBM research shows that the average data breach at a higher-education institution in 2023 costs $4.5 million — an increase of 15.3 percent from 2020.

According to Jon Allen, chief information officer (CIO) and chief information security officer (CISO) at Baylor University, in Waco, Texas, a potentially pivotal change is sweeping through many technical leaders: A reconsideration of identity and its centrality in cybersecurity.

Allen says identity was not a hot topic in higher education a decade ago. But higher-education leaders increasingly recognize that "Identity is really the matrix interconnecting it all."

People touch an institution's identity system whenever a prospective student applies, a faculty member is hired, or a visiting researcher needs a guest account. They make contact frequently as they create accounts, reset passwords, and request access to a website, file, or application. And every time a student graduates or a professor departs, the identity system must take all that access back.

That's why Allen partnered with Fischer Identity, a leading provider of Identity & Access Management (IAM) solutions, to build an identity system that could manage all the personas Baylor served and, in the process, provide a system that could scale as Baylor grows. In addition, the Fischer suite of products is based on ease-of-use configuration rather than complicated custom code development to enable long-term sustainability.

In 12 weeks, Baylor went from a statement of work to a fully-executed solution that saved staff effort and secured sensitive information. The Baylor and Fischer teams — supported by Amazon Web Services (AWS) infrastructure and a range of AWS services — built an identity system that now manages and supports over several hundred thousand identities and accounts.

People touch an institution's identity system whenever a prospective student applies, a faculty member is hired, or a visiting researcher needs a guest account. They make contact frequently as they create accounts, reset passwords, and request access to a website, file, or application.

WITH ACCESS DEMANDS RISING, A HOMEGROWN SOLUTION WASN'T SUSTAINABLE

Identity begins with applicants and Baylor receives tens of thousands of applications every year. A sustainable identity system for the university needed to carry each student profile — from the moment a student applies to Baylor to the day students step on campus and to the day they eventually graduate.

Bryan Leber, vice president of product and service delivery at Fischer Identity, says, "Higher education faces the same cybersecurity threats that others do," but these institutions are often more vulnerable than others because the variety of personas and access needs in play exposes such a large surface area of attack.

Like many colleges and universities, however, Baylor relied on an identity system that was built in-house. These systems are primarily scripts — sequences of instructions running against a database that return results bit by bit. At scale, these layers and layers of scripts can prove fragile and managing them becomes laborious. "Many businesses operated that way for many, many, many years," Allen says.

Every time a business rule changed, Allen says, his team would have to manually fix a script and ensure that the rest of the system could handle that change. Every update required his team to rewrite a script. At that point, Allen says, "It's not configuration; it's programming."

Faced with an aging homegrown system and limited internal resources, the risk of cybersecurity attacks made an important issue an urgent one. The scale of the challenge was enormous, but so was the scale of the opportunity. So, Baylor looked for help.

FOR HIGHER EDUCATION, THE VENDOR SELECTION PROCESS HAS TO BE CAREFULLY CONSIDERED

Few off-the-shelf identity solutions can handle the demands of the higher education sector.

In a corporate environment, identity problems tend to follow patterns that vendors can solve out-of-the-box: A company hires an employee, creates an account to give that employee access to the basics (email, Slack, etc.), and adds role-specific resources to that account as necessary (GitHub access for a software developer, for example). The patterns are reliable and the exceptions are rare.

But in a higher-education context, exceptions can dominate. As Allen says, for many higher-education institutions, "identity is driven by exceptions."

A professor who's helping students with research, thesis projects, and dissertations,

for example, might leave the university at any time. Colleges might need to deprecate the professor's access to some systems when they depart but maintain email access so that the professor can keep communicating with students who have ongoing research.

In a corporate context, a departing employee would hardly be a problem. Simply de-provision the employee's account and shut off access to any internal systems. In a higher-education institution, exceptions arise. The departing professor can't retain access to sensitive internal resources, but they still need email access — at least temporarily — to communicate with students working on dissertations or theses.

How, then, can an education institution build an identity system that can provision accounts and de-provision them piece-by-piece, such that some access disappears immediately and other access continues?

Baylor needed a partner — a vendor that could provide them with the building blocks they needed to build a system for the unique needs of higher education. They needed a partner who could manage the system's infrastructure in the cloud too so the system could remain scalable long into the future. But, despite the maturity of the identity solutions market, few vendors have a readymade solution.

"Getting the right provider of that infrastructure is critical," Allen explains, "because this is the absolute glue of the fabric and plumbing of your entire IT infrastructure."

Baylor needed a partner — a vendor that could provide them with the building blocks they needed to build a system for the unique needs of higher education. They needed a partner who could manage the system's infrastructure in the cloud too so the system could remain scalable long into the future.

Fischer Identity quickly became a leader in Baylor's search. Not only could Fischer execute identity, but the company has built a unique expertise in higher education. "When we first started developing our product, the first clients we engaged were in higher education," Leber explains.

"During those engagements, we noticed that they have some complex use cases that would require more advanced features to meet their needs. As we expanded into more and more higher-education institutions, there were new use cases and features that they needed in almost every case," Leber says.

Fischer has developed a range of configurations that takes care of colleges' needs. And when new requirements arise, Fischer has a toolbox they could use to build new workflows. "To date," Leber says, "there has not been a technical requirement that the Fischer Identity product has not been able to meet, due to its vast configurability built within the product."

IDENTITY AT BAYLOR TODAY

With the help of Fischer Identity, Baylor University built a robust identity system that extends and expands the identity lifecycle. The new system offers a better user experience, a stronger security posture, and a more efficient, hands-off workflow.

With several hundred thousand identities within the system, Baylor can provision more identities faster and with much less effort than it could before. Users can self-register and manage their profiles without help and without delay.

A longer and wider identity lifecycle

The "identity lifecycle" describes the process that encompasses each and every identity, from account creation to account deletion. In between, any given account might need access to specific resources, and the system might need to authenticate that identity by request, update credentials and attributes, and de-provision that account when the lifecycle ends.

Within higher education, the identity lifecycle has an almost fractal complexity. Take a long enough look at any persona; its unique needs will keep multiplying.

A guest on campus might need to create an account, get access to a specific resource, and be able to depart — all on a short schedule. A prospective student might create an account to apply, come to campus and need access to more resources, choose a major and need even more resources, and eventually graduate, requiring all those lines of access to disappear. A graduate may decide to return as a full time employee years after their graduation and will need to match to their previous account and request a name change.

Brittle, script-driven identity systems tend to struggle with this complexity. But

as Baylor worked with Fischer, Allen's team built an identity system that was longer — extending to prospective students and departing faculty — and wider — expanding across various parties, including students, teachers, guests, and staff.

In 2017, Baylor implemented a new feature where prospective students could self-register as Baylor users. No hands-on work was necessary for these prospective students and as a result, this established an automated process that is still in use today.

Greater security and better audits

Many identity systems haven't caught up to the major risks that seemingly small cyberattacks pose.

Phishing, for example, doesn't appear to be the most dangerous of attacks at first glance. An attacker sends an email that seems legitimate, but inside is a link that, once clicked, allows the attacker to hijack that person's account credentials. Even a single stolen account, however, can lead to extensive damage.

Once an attacker has one set of credentials, they can do what cybersecurity experts call a "lateral attack," leaping from one account to the next and from one system to another. A small mistake by one person can result in a data breach affecting an entire institution. According to Proofpoint Research, 15 percent of all successful phishing attacks affect educational institutions, leading to the firm's conclusion that "the education sector is the most vulnerable to phishing-related attacks."

Identity, as Allen says, is the "matrix interconnecting it all." When colleges build identity systems, they need to be able to trace attack attempts, halt attacks in progress, and improve their systems over time.

The potential of a small mistake leading to a large breach shows why identity has come to the foreground in security conversations. Identity, as Allen says, is the "matrix interconnecting it all." When colleges build identity systems, they need to be able to trace attack attempts, halt attacks in progress, and improve their systems over time.

The ability to audit and iterate was a key goal for Baylor when Allen and his team started working with Fischer. Allen saw the previous system's weaknesses and wanted to improve it. "When you run scripts," Allen explains, "You get an output from the script, but it's not really what I would call an audit log."

"With Fischer," Allen explains, Baylor now has a "hub that is actually a ledger of what's

happening with identity." Leber explains further, saying, "Anything that happens within the system or into a target system is automatically audited." Afterward, clients can generate reports whenever they need to and can focus on whichever user or group of users they want.

Automation and user experience

In many organizations, a key responsibility of the IT help desk is to receive access requests — say, a student requesting access to a department's research database — and approve or refuse. Over time, however, Baylor discovered that the growth in user personas created an uptick in access requests that no help desk could efficiently manage.

Before Fischer, most access requests at Baylor went to the help desk, but frequently, the help desk didn't have the permissions they needed to help. Even though the help desk could receive requests as fast as people could make them, the help desk had to triangulate with other departments – human resources key among them – to check who could have access to what. With the new identity system, Baylor and Fischer automated the vast majority of access requests.

By giving up some control, the help desk can actually offer more help. "The help desk has been empowered a lot from where they were traditionally," Allen says. "They're able to go into the platform to see the status of the users to do a lot of things that maybe took two or three steps in the past."

WITH FISCHER AND AWS, BAYLOR IS READY TO ITERATE

Fischer has proven to be an ideal collaborator for Baylor's IT department, and Amazon Web Services (AWS) has provided the support both teams need to succeed and iterate.

A member of the AWS Partner Network (APN), Fischer Identity uses over twenty AWS services to support its identity systems, including Amazon Elastic Cloud Computing (EC2), Amazon Relational Database Service (RDS), Amazon S3, and AWS CloudFormation. Leber trusts AWS as a partner because of its current offerings and how fast AWS responds to feedback and develops new features. "AWS is always coming out with new offerings that can enhance what we do for clients," Leber says, "so it gives us an upper hand on deploying future releases with the support we get as a partner."

That upper hand extends to Baylor too. Allen and his team praise the combined offerings and the experience of working with Fischer.

Mary Gonzales, a member of Allen's team at Baylor, commended Fischer's ability to collaborate and pivot. "We'll input some tickets," Gonzales says, "and if there's a repetitive pattern, we'll look into the logic." Fischer is there and ready, willing to fine-tune their system to suit Baylor's developing needs. "It's always evolving and that collaboration is what's really helpful," Gonzales says.

By working with a vendor that provides managed cloud services, Baylor doesn't need to worry about managing all the infrastructure that would typically be necessary for an enterprise-level product. Fischer handles all the patching and monitors the service daily to ensure it runs smoothly and without interruption.

That support means Baylor can actually save on maintenance costs while fretting less about the system itself, and having Fischer run and manage the cloud infrastructure costs Baylor only a fraction of what it would cost if the team tried to run it themselves.

"CIOs and CISOs are always concerned and often lose sleep when they have a homegrown solution," says Chuck Donnelly, vice president of field operations at Fischer Identity. Leaders often feel like the next issue is always around the corner, and leaders never know whether it will be an isolated issue or whether it will be one domino to fall among many. "Moving to the Fischer cloud allows the C-level to focus on other areas of their many responsibilities," Donnelly explains, and hopefully, "they can sleep a little better."

By working with a vendor that provides managed cloud services, Baylor doesn't need to worry about managing all the infrastructure that would typically be necessary for an enterprise-level product.

Fischer Identity, a visionary leader in Identity and Access Management (IAM), is dedicated to empowering organizations with cutting-edge solutions that fortify security, streamline operations, and simplify administration. Our mission is clear: immediate value through IAM excellence. Our vision propels us to be the global IAM leader, pioneering cybersecurity's future. We're committed to a world where organizations navigate the digital realm with confidence, fortified by our innovative, Zero Trustbased solutions. Join us in safeguarding data, elevating user experiences, and achieving operational excellence.

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments.