The focus of technology and cybersecurity within higher education is going through a cultural shift. While higher educational institutions in the past focused on building the strongest firewalls to keep intruders from breaching their systems from the outside, it left everything inside the security perimeter vulnerable — and that unprotected attack footprint is getting even larger and moving away from the physical campus environment as remote work and distance learning become the norm in our lives.

Most colleges and universities already offered some online classes. Faced with the recent pandemic, those offerings have drastically increased with some schools opting to go fully online, or mostly online, for at least the next few semesters. Schools that rely on a perimeter security mindset are finding it difficult or impossible to scale that protection up to meet new demands.

To address these issues and plot a new and better course for cybersecurity within higher education, FedInsider hosted a webinar entitled “Identity and Access Management in Higher Education” with Director of Higher Education for Okta Kevin Bresser as the featured speaker. Bresser shared ways that higher education institutions can improve their security through implementation of Identity and Access Management (IAM) programs, along with new guidelines and best practices designed to keep students, staff and campuses safe.

Bresser stressed four key areas where new best practices could bolster security while also scaling with demand. Colleges and universities that implement them will not only be better equipped to handle the current situation, but they will become more agile and responsive to future needs.

**Adopt a Zero Trust Framework to Bolster Security**

There has been a big increase in the number of private companies adopting a zero trust security infrastructure, and for good reason. Zero trust has become increasingly important due to a growing number of advanced network threats, both internal and external. Implementing a framework where users are never granted automatic trust and must constantly prove their credentials and intentions certainly helps to eliminate insider threats as well as attacks that have already successfully breached perimeter security. In higher education, a zero trust framework will help to lockdown most schools’ sprawling internal network resources.

**Multi-Factor Authentication Allows Stronger Versatility with Network Solutions**

One thing to consider about zero trust in education is that it’s not just a single solution that helps you achieve full protection. Zero trust networking is comprised of multiple components. The good news is that because of this, they can be implemented separately as zero trust is built out across a campus environment. And one of the most critical of those components is multi-factor authentication, or MFA.

MFA works by challenging users to enter additional information instead of just their name and password. Campuses often use second factors ranging from SMS to higher assurance factors such as a push notification to a mobile app or physical token like a YubiKey as a second form of verification. Further, when MFA is tied to contextual or risk-based access, it can
both enhance security and also make it easier for users to get access to the systems they need.

“The campus IT and security teams can leverage risk signals from across security tools, such as device, email gateways, SIEMs, and more to determine the potential riskiness of a particular login attempt,” Bresser said. “When combined with factor options, campuses can set policies to either require higher assurance factors in potentially risky scenarios or for sensitive apps as well as passwordless policies when risk is low – making ease of use and security go hand-in-hand.”

Moving to a true contextual experience, the campus may take into consideration signals from other solutions (email phishing detection software, endpoint security management systems, security information and event management solutions, etc.) to determine a particular user’s MFA requirements and experience, Bresser added. “But as you build out more of these contextual sources, it’s then possible to move to a true frictionless user experience by beginning to offer passwordless logins to some users some of the time.”

**Importance of Automating the Student Lifecycle**

The majority of students attending higher education won’t travel in a straight line between admissions to graduation in four years. Students will travel through numerous experiences while on campus, including working as student employees, leaving campus for cooperative education work experiences, taking summer classes, moving from undergraduate to graduate-level courses, possibly splitting time between the university and teaching hospital, and much more. It’s important that access management tools do much more than simply provide access and help provision and deprovision users from various systems on campus. Technology now enables the campus to have the identity systems be the control point to take deeper lifecycle actions in core campus systems when the user’s roles and permissions change on campus.

“Examples of this may be to ease the onboarding process for students by having the identity systems take actions inside G Suite or Office 365 to prepare the student’s account, send welcome email messages, prepare documents and folders in Drive or Box, and much more,” Bresser said. “They can also help with partial offboarding steps when a student graduates to remove access from course registration systems retaining email access for a limited time as an alumnus.”

As schools grow their online presence, automation will become more important to improve the efficiency of the increasingly virtual educational system as well as to maintain a safe network infrastructure. Additionally, the rapid influx of more online students requires a system that can get them set up quickly. Faculty can additionally benefit by being able to adjust student accounts quickly and with less stress caused by outdated or unfriendly interfaces.

**The Higher Education Single Sign-On Evolution**

A typical student might have several passwords to access different applications or resources. Faculty and staff probably have even more since they will need to access administrative tools. As everyone already knows, it can be difficult and, more importantly, less secure to juggle passwords for multiple systems. In higher education, it’s just one more unnecessary obstacle to the learning process.

While most campuses began taking steps towards Single Sign-On (SSO) years ago, many campus systems and servers are not yet connected to those SSO services today. Some campuses have made improvements to bring their SaaS solutions under one SSO service, but are still many on-prem applications, custom applications, and administrative servers throughout the institution that aren’t connected to their SSO portal. This further presents risks for many campuses when it may take significant time and manual steps to truly deprovision a terminated staff or faculty member from all of the systems that they may have accessed outside of the core SSO solution set.

“There’s a lot of power in simplification along with modernization,” he added. Combining SSO with other technologies like MFA, Lifecycle Management automation and building a zero trust framework around it can go a long way to protecting institutions of higher education while also making them more accessible and accommodating.” As most people have learned in 2020, it’s a very different world requiring a new way of thinking about distance learning, remote work, security, user experiences, and the big picture when it comes to taking higher education into the future.