Implementing Identity and Access Management

Project Impact Report

Issue/Problem

With cyber-attacks becoming more common and more sophisticated, Illinois Institute of Technology needed better defenses and new policies surrounding access and security, and a tool to help us establish "zero trust architecture," meaning an identity is not trusted for access until it meets specific acceptance critera. Additionally, multi-factor authrenticaion is now required by many cybersecurity insurance companies, ours included.

Response

The Office of Technology Services (OTS) selected a premier identity and access management solution, Okta, to provide the services we needed. We knew its implementation would mean a multi-year, large scale change, and involve all departments that manage university data, so we conducted project work in several phases. These included: enrolling our community in Okta, setting up multifactor authentication, launching a massive data clean-up effort required to enable a data integration, moving key applications behind the Okta platflorm with single sign-on, and enabling self-service password resets. A senior developer built out an extensive data integration to connect our data to Okta. We also engaged a third-party vendor called Cirrus Bridge to extend Okta single sign-on to applications that still rely on outdated technology protocols that woud not otherwise conform with Okta.

Participants

Project Manager:	Molly McDermott
Business Champions:	Sejal Vaishnav, Louis McHugh, Ibukun Oyewole, Eric Breese
Project Team Members:	Brian Hogan, Kristin Lennert, Christopher Hines, Fred Eichhorst, Ian Hernandez, Shadi Beidas, Adrian Bucurica, David Rose, Matthew DeChant
Key Departments:	Office of Technology Services, Registrar, Enrollment, Human Resources

Impact

The implementation of Okta allowed us to evaluate and centrally manage access to almost 200 applications used daily by students, faculty, and staff, including email, Google, Microsoft, Blackboard, financial systems, and many more. We now require multi-factor authentication (MFA) through Okta as a gateway to these systems, provide a single sign-on experience to most of our applications, and enabled self-service password management. We also mitigated major risks to our operations and external funding by meeting cybersecurity insurance MFA mandates. Regarding security improvements, we developed better technology access requirements, and utilized Okta to identify and remove accounts that did not meet them.

- 88, 496 inactive university email accounts were suspended
- 117,644 Active Directory accounts were disabled, revoking unneeded access to wifi and workstations

Illinois Tech is much better positioned for automating technology access for staff, faculty, and students so that they have what they need when they join our community, and lose access when they leave.

The Measure	Value	Context
Number of grant fund opportunities retained	$33 million	By retaining our cyber-security insurance, we mitigate the risk of losing grant funds that require it, upwards of 33 million dollars.