Washington Community & Technical Colleges
Strategic Technology Advisory Committee

ISSUE BRIEF

ctcLink and Multi-factor Authentication

July 21, 2020

Issue background

In today's online environment, the fundamental “username and password” approach to account security can be easily breached by cyber criminals. Many log-ins can be compromised in a matter of minutes, and private data; such as personal and financial details, is under increasing threat. A strong multi-factor authentication (MFA) method is now the industry standard for secure access to systems, and required for security compliance to protect sensitive data. MFA typically requires that users provide something that they “know” and something that they “have.” For example, the use of a pass code sent to a user’s cell phone at the time of log-in, or a biometric scan to assure there is an actual person logging in.

> *“Strong web security relies on a variety of tools and policies. It’s important not to rely on any single method for comprehensive protection. Multi-factor Authentication (MFA) adds another layer of account security, supplementing the username and password model with another factor that only the specific user has access to. Whenever possible, users should get into the habit of protecting themselves with the extra layer of security that MFA provides.”* [1]

Why does the issue exist?

The introduction of ctcLink results in a new environment that everyone has to become used to operating effectively; accordingly the potential for a security breach is increased. There has also been an expectation from the colleges that a secure single sign-on (SSO) solution would be provided for ctcLink in order to provide a more seamless experience for our users. However, at the beginning of the ctcLink project there were no viable SSO or federated identity solutions identified, and this was declared to be out of scope.

Why now?

Access to ctcLink via the internet, while enabling our workforce and students to access the system wherever they are, creates a greater risk than when access to our centralized systems was limited to workstations on our campus networks. With the advent of COVID19, colleges have less control over the environment in which their employees and students work. With everyone working and studying remotely, cyber criminals are increasingly taking advantage of vulnerabilities and social engineering to gain access to credentials and sensitive information.

> *“Widespread major data breaches are occurring at an alarming rate affecting millions of people. The information that's stolen, in many cases, includes usernames and passwords that could allow cybercriminals access to user accounts. In addition, passwords alone can frequently be easily guessed or compromised through phishing or hacking. As more personal information finds its way to online applications, privacy, and the threat of identity theft is increasingly a concern.”* [1]

Who is impacted by this issue?

All students and employees of SBCTC and all WACTC colleges could be impacted by this issue.

What is the WACTC statewide significance?

ctcLink is the system of record for all student, employee and financial information. Due to the centralized nature of our administrative systems, this impacts all WACTC colleges and students. This issue also extends to the decentralized processes and systems at local colleges.

A proactive solution for multi-factor authentication is currently out of scope for the ctcLink project and project budgets are already fully allocated. A resolution to this issue will require extra funding. Conversely, the risk of not addressing this issue is very high.

What are the risks or ramifications of not resolving the issue?

The average cost of breach in Higher Education for 2019-2020 was: $4.77m *[2]*. A cyber security breach can cost an organization multi-millions of dollars, and effectively put it out of business. Loss of institutional reputation and credibility, corruption of critical data and inability to continue operations are all potential impacts of a breach.

What solution options were considered?

The primary requirements for a solution are:

- It must be implementable by all colleges in the WACTC system.
- It must have comprehensive interoperability and be platform agnostic because of the range of technologies used by colleges now and in the future.

Two possible solution paths were identified to address this issue:

- A **comprehensive enterprise access management solution** that meets ctcLink requirements for MFA and also flexible enough to meet other college needs for MFA/Security. This would be the preferred solution because it provides more long term options for integration and operability, and provides the highest return on investment system-wide.

- A **single focused access management solution** that meets only the ctcLink requirements for MFA/Security, and colleges are responsible for all other local systems. While this solution supports more autonomy for product selection at local colleges, the system-wide cost would be significantly higher than a comprehensive solution, and will require much more time (person-hours) at colleges and with SBCTC to realize benefits.

Recommendation

SBCTC completed an RFP in 2019 for an Access Management solution focused on multi-factor authentication and identifying multiple viable vendors that could provide a solution. The RFP resulted in contracts with multiple vendors for related services, and through the evaluation process, one vendor stood out with a comprehensive enterprise solution and pricing. Therefore, the Strategic Technology Advisory Committee (STAC) **recommends a system-wide purchase of Okta**, a comprehensive Access Management platform. Okta is the industry leader in Identity and Access Management as rated by both Gartner and Forrester research organizations.

The Okta solution would cover ctcLink, and a tenant for every WACTC college at no extra cost. Each school will have full control over publishing apps to branding in their tenant. You even get a sandbox Tenant and premium plus support from Okta at no additional charge. The ctclink buy covers all users in a school tenant as well.

High-Level Okta Features

- Adaptive MFA - Secure authentication for all environments, protecting identity and access to data wherever users go and wherever data lives.
- SSO (Single Sign-On)
- Self Service Password portal for a password reset, changes, and unlocks
- Unlimited users - Licensing is based on active users a month, not user count in AD or Okta. Annual cost estimates for active users were based on full student and staff counts per quarter per year for the system.

Additional benefits for local colleges and system-wide administration include: Production and sandbox tenants, universal directory, unlimited applications and custom integrations, and premium support.

Cost

System cost would be $535,000/yr, subscription cost.

Benefits of the Proposed Solution

There is a significant cost savings through an enterprise procurement (10x?), and provides an equitable service offering for all WACTC colleges to take advantage of. If procured individually, many colleges would not have sufficient budget/funding for this service. An enterprise solution encourages a community approach for sharing best practices, standards and resources across colleges. Additional benefits of a single sign-on and password management solution provided by the Okta platform will save the cost of other locally purchased tools, minimize support time and reduce student frustrations during the first weeks of every new academic term.

Timeframe for Implementation

Once purchased, the service would be implemented within 90 to 120 days for ctcLink and would be immediately available for all colleges to begin local configuration and implementation.

Communication Plan

Who needs to approve?

- Proposed by STAC and SBCTC - IT
- STAC - demo and issues
- Endorsement from SBCTC leadership
- Sponsored by WACTC-Tech - Issue Brief
- Endorsement from IT Commission - Issue Brief and Demo, Meeting
- Endorsement from the ctcLink Steering Committee - Must be implemented without negatively impacting project resources or time-line.
- Endorsement from BAC - Grant get on the BAC Agenda
- Approval by WACTC Presidents

How will the recommendation be communicated?

- Issue Brief shared with Commissions, Website
- Presentations to IT Commission, WACTC-Tech

Who needs to know?

- All the commissions need to know (STAC Representatives)
- Decisions will be communicated: WACTC decision - Kevin Brockbank, Purchase and implementation - Grant Rodeheaver to ITC.

References:

(1) Carnegie Mellon University, September 2019: https://www.cmu.edu/iso/news/mfa-article.html
(2) IBM/Ponemon report: https://digitalguardian.com/blog/whats-cost-data-breach-2019