

ASSESSMENT REPORT

Cybersecurity: Password Hygiene

SEPTEMBER 2021



TIMOTHY M. O'BRIEN, CPA
DENVER AUDITOR

OFFICE OF THE AUDITOR
AUDIT SERVICES DIVISION, CITY AND COUNTY OF DENVER

Assessment Team

Jared Miller, CISA, CFE, CDPSE, Information Systems Audit Manager

Nick Jimroglou, CISA, CDPSE, Information Systems Audit Lead

Contractors

CP Cyber

Bill Evert, Partner

Donald McLaughlin, Lead Consultant

Brian Cather, Lead Consultant

Tristan Neate, Associate Consultant

Audit Management

Timothy M. O'Brien, CPA, Auditor

Valerie Walling, CPA, CMC, Deputy Auditor

Dawn Wiseman, CRMA, Audit Director

Audit Committee

Timothy M. O'Brien, CPA, Chairman

Rudolfo Payan, Vice Chairman

Jack Blumenthal

Leslie Mitchell

Florine Nath

Charles Scheibe

Ed Scholz

You can obtain
copies of this
report by
contacting us:



Office of the Auditor

201 West Colfax Avenue, #705

Denver CO, 80202

(720) 913-5000 | Fax (720) 913-5253

Or download and view
an electronic copy by
visiting our website at:
www.denverauditor.org.

Cover illustration by Denver Auditor's Office staff.

City and County of Denver



TIMOTHY M. O'BRIEN, CPA
AUDITOR

201 West Colfax Avenue, #705, Denver, Colorado 80202
(720) 913-5000 | Fax (720) 913-5253 | www.denverauditor.org

AUDITOR'S LETTER

September 16, 2021

On behalf of the Auditor's Office, CP Cyber conducted a cybersecurity assessment of an agency within the City and County of Denver. This assessment found some areas of strength and some areas that need improvement. Because of the information security sensitivities involved with this assessment, these issues have been communicated separately to the relevant city agency for its remediation.

This assessment is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, "General Powers and Duties of Auditor."

We extend our appreciation to the city personnel who assisted and cooperated with us and CP Cyber during the assessment. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

A handwritten signature in black ink, appearing to read "Timothy M. O'Brien".

Timothy M. O'Brien, CPA
Auditor

BACKGROUND

Multifactor Authentication

The Threat

Compromised credentials pose a risk to most organizations. One of the easiest ways for an attacker to gain access to an organization’s sensitive data is to use credentials provided by willing or, more commonly, unwitting employees.

To reduce these risks, organizations should implement mitigating controls such as multifactor authentication where possible and increase the password strength of services and accounts with elevated access.

“Multifactor authentication” is a method in which a user is granted access to a website or application only after successfully presenting two or more pieces of identifying evidence. This evidence could be:

- Something the person knows, like a password.
- Something they have, like a smart card.
- Something tied to that person specifically, like a fingerprint.

City and County of Denver

Technology Services is the City and County of Denver’s lead agency for information technology. It provides information technology-related infrastructure and services to city agencies.

Technology Services has implemented multifactor authentication, also known as “two-factor authentication,” across many of the city’s information systems and applications. This is a great step in ensuring security best practices throughout the management of the city’s technology-related infrastructure.

The main advantage of multifactor authentication is that, without additional verification (e.g., a code sent via text message), a cybercriminal cannot use compromised credentials to gain unauthorized access to information systems and sensitive data. Multifactor authentication reduces the risk of a breach when an attacker successfully collects a user’s credentials or gains internal access to a network, account, or application.

Multifactor authentication has other benefits that are less obvious, such as making it much more difficult for users to share accounts.

Access controls rely on the principle of “least privilege” access — meaning users of a system should be granted only the level of access necessary to perform their work. Accounts should be used by specific individuals with specific roles. Traditionally, multifactor authentication can be set

up on only one device per account. Therefore, multifactor authentication increases the likelihood that account access will be limited to the individual who configured it.

Additionally, if multifactor authentication is set up by the user to receive a secondary code or pop-up on their phone, this can aid in notifying the user or organization of credentials that have been potentially compromised.

Residual Security Risks

Once multifactor authentication has been implemented, attackers have to work harder and be more creative to gain access to an information technology environment. For example, an attacker will try to find a public-facing application that does not require multifactor authentication but is configured to use only basic credentials (i.e., a username and password) for authentication.

Often applications do not require multifactor authentication because of the complexity and cost of implementing it across an entire information technology environment. Attackers will target these applications to test credentials and gain access to sensitive information.

Another risk can be service accounts or user accounts that have exceptions to the multifactor authentication requirement.

A “service account” is an account that is usually not logged into directly but is created explicitly to provide security context for services or applications. Traditionally, service accounts do not have a requirement for changing the password as this could disrupt services. Therefore, these credentials must be more complex to reduce the likelihood of credentials being compromised over time.

Most modern applications mitigate this risk by authorizing service accounts with a key and by not allowing those accounts to authenticate using the application’s login form.

Cybersecurity Frameworks

The National Institute of Standards and Technology recommends the “use of alternative security mechanisms [that support] system resiliency, contingency planning, and continuity of operations.”¹

The federal agency goes on to say:

“To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. The mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ alternative or supplemental mechanisms enhances mission and business continuity that might

¹ National Institute of Standards and Technology, Special Publication 800-53 (Revision 5), accessed July 6, 2021, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, the alternative or supplemental mechanisms are only applied to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue one-time pads to senior executives, officials, and system administrators if multi-factor tokens—the standard means for achieving secure authentication—are compromised.”²

The National Institute of Standards and Technology also says using multifactor authentication is one of the top three things security experts can do to protect their security while online. This tool should be used whenever possible, especially when involving the most sensitive data.

As a result, using multifactor approaches adds necessary layers of security and truly makes it harder for cybercriminals to access certain information.³

² National Institute of Standards and Technology, Special Publication 800-53 (Revision 5).

³ National Institute of Standards and Technology, “Back to Basics: Multi-factor Authentication (MFA),” June 28, 2016, accessed July 21, 2021, <https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication>.

Office of the Auditor

The **Auditor** of the City and County of Denver is independently elected by the residents of Denver. He is responsible for examining and evaluating the operations of city agencies and contractors for the purpose of ensuring the proper and efficient use of city resources. He also provides other audit services and information to City Council, the mayor, and the public to improve all aspects of Denver's government.

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the city's finances and operations, including the reliability of the city's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of city operations, thereby enhancing residents' confidence and avoiding any appearance of a conflict of interest.



201 West Colfax Avenue #705

Denver CO, 80202

(720) 913-5000 | Fax (720) 913-5253

www.denverauditor.org

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public's investment in the City and County of Denver. Our work is performed on behalf of everyone who cares about the city, including its residents, workers, and decision-makers.
