FOLLOW-UP REPORT

Denver International Airport *Cybersecurity Operations*

JUNE 2021

TIMOTHY M. O'BRIEN, CPA
DENVER AUDITOR

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

Audit Team

Jared Miller, CISA, CFE, CDPSE, Information Systems Audit Manager
Nick Jimroglou, CISA, CDPSE, Information Systems Audit Lead
Rob Farol, CIA, CGAP, Senior Auditor
Dave Hancock, MURP, Senior Auditor

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

June 3, 2021

In keeping with generally accepted government auditing standards and Auditor's Office policy, as authorized by city ordinance, the Audit Services Division has a responsibility to monitor and follow up on audit recommendations to ensure city agencies address audit findings through appropriate corrective action and to aid us in planning future audits.

In our follow-up effort for the "Cybersecurity Operations" audit report issued in September 2019, we determined that Denver International Airport fully implemented four, but did not implement two, of the six recommendations it agreed to in the original audit report. Despite the airport's Business Technologies department efforts, we determined the risks associated with the audit team's initial findings have not been fully mitigated. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure the city takes appropriate corrective action.

The Highlights page in this report provides background and summary information about the original audit and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation.

I would like to express our sincere appreciation to the personnel in the Business Technologies department who assisted us throughout the audit and the follow-up process. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

ORIGINAL REPORT HIGHLIGHTS

Cybersecurity Operations

JUNE 2021

Objective

The objective of our audit of cybersecurity operations at Denver International Airport was to determine the effectiveness of the airport's cybersecurity processes, policies, and governance. We assessed how well the airport's Business Technologies department and cybersecurity operations team were prepared to identify, protect, detect, respond, and recover from cybersecurity incidents.

Background

Denver International Airport's Business Technologies department is responsible for managing and safeguarding the airport's network and technology equipment, including data and infrastructure. This department also provides cybersecurity services to protect the airport from threats and vulnerabilities.

During our audit of cybersecurity operations at Denver International Airport, we determined that the Security Operations Center needs to improve communication and collaboration within its cybersecurity operations.

The Airport's Security Operations Center Needs To Improve Communication and Collaboration with Internal and External Stakeholders

- There is limited collaboration between the airport's Security Operations Center and its key stakeholders.
  - Meetings between Security Operations Center staff and other information technology officials at the airport focus largely on business goals, rather than processes and tool-sharing for cybersecurity purposes.
  - The Security Operations Center does not communicate with airport personnel who manage vendors.
  - Security Operations Center personnel do not formally communicate with other airport divisions on actions such as network scans, which has caused system disruptions at times.
- The Security Operations Center uses unapproved and ineffective policies and procedures.
  - There is no evidence of a signed nondisclosure agreement for one information technology security contractor.
  - The Security Operations Center uses policies and procedures that have not been signed by executive management.
  - The Security Operations Center should improve its lessons-learned process following a security incident.

Why This Matters

Denver International Airport depends on its Business Technologies department to protect its systems against cyberattacks as well as to ensure the security of the people who use its network. Without a well-honed security operations center, the airport is susceptible to threats and vulnerabilities.

✓ 4	●●● 0	✗ 2
FULLY IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED

June 3, 2021

Action Since Audit Report

Cybersecurity Operations

6 recommendations proposed in September 2019

● ● ● ●

● ●

✓ **FULLY IMPLEMENTED** 4

••• **PARTIALLY IMPLEMENTED** 0

✕ **NOT IMPLEMENTED** 2

Business Technologies fully implemented four recommendations made in our original audit report, but two have yet to be fully implemented or acted upon.

We found Business Technologies developed collaboration opportunities with the city's Technology Services agency and created presentations on a weekly basis for Business Technologies' management. However, the airport did not improve communication practices with vendors or with airport employees who manage third-party information technology contracts.

Because Business Technologies does not have a formal process for communicating with vendor managers, the Security Operations Center is limited in its ability to resolve third-party conflicts, which reduces the security of the airport's network. Additionally, without a documented lessons-learned process, the Security Operations Center has fewer opportunities for improvement.

FINDING | The Airport's Security Operations Center Needs To Improve Communication and Collaboration with Internal and External Stakeholders

Recommendation 1.1

SHARE INFORMATION – The airport's chief information officer should share information, such as successful processes, identified risks, cybersecurity tools, and other data that could be integrated with the city's or Business Technologies' cybersecurity operations on a semiannual basis with the city's information security team.

✓

FULLY IMPLEMENTED

AGENCY ACTION

Original target date for completion: November 2019

In response to our recommendation, we found that Denver International Airport's Business Technologies department is sharing information and collaborating with the city's Technology Services agency. We reviewed communications and meeting minutes provided by Business Technologies. For example, from August 2019 through November 2020, there was a series of collaboration meetings that occurred between the two agencies that have helped to improve information technology and cybersecurity.

We found documentation of the airport's Business Technologies staff collaborating and communicating with the city's Technology Services staff to develop shared goals, partnership opportunities, and inclusion of security awareness training. After evaluating the evidence provided and after interviewing Business Technologies personnel, we were informed that collaboration has been extremely helpful for Business Technologies to understand how the city's Security Operations Center operates.

Based on our analysis, we consider this recommendation fully implemented.

Recommendation 1.2

IMPROVE COMMUNICATION WITH AIRPORT VENDOR MANAGERS – The airport's chief information officer should formalize and document Information Security Team involvement and processes for communicating with airport managers who monitor third-party contracts. This involvement could include:

- Monitoring vendor access to the airport's systems.
- Facilitating communication between vendor managers and airport information security teams.

- Communication of identified risks and risk remediation activities from vendor managers to airport security teams.

NOT IMPLEMENTED

AGENCY ACTION

Original target date for completion: November 2019

Business Technologies staff said they have not made much progress on this recommendation's implementation but that they have a vendor contacts list and a process to contact vendor managers on incidents occurring within their technology ecosystems. However, they also indicated they have had some difficulty in moving the effort forward during the COVID-19 pandemic. When our team asked for a copy of the documented process, they told us they had not made much progress. According to the department, vendor communication is strictly done through cybersecurity incident management. This means that the only communication occurring with vendors regarding cybersecurity happens when an incident occurs, which impacts the vendor systems. The intent of the recommendation was for the airport to formalize and document its role in communicating with airport managers who monitor third-party contracts; however we found that the airport has not formalized, documented, or established a process to do so. Therefore, we consider this recommendation not implemented.

Recommendation 1.3

FORMALIZE COMMUNICATION WITH BUSINESS TECHNOLOGIES TEAMS – The airport's chief information officer should formalize cybersecurity operations communication on a weekly basis between managers of the airport's Business Technologies teams.

FULLY IMPLEMENTED

AGENCY ACTION

Original target date for completion: October 2019

In response to our recommendation, we found that Business Technologies has formalized cybersecurity operations communications between its managers on a weekly basis through comprehensive PowerPoint presentations. For example, these presentations detail the number of security events that have occurred and trending statistics on the frequency of events during the previous week. The presentations also include information on weekly events that impact the information technology systems and networks at the airport.

Based on this information, we consider this recommendation fully implemented.

Recommendation 1.4

SIGN NONDISCLOSURE AGREEMENTS – The airport's chief information officer should establish a process to ensure Security Operations Center contractors with access to sensitive data sign a nondisclosure agreement upon hire.

✓

FULLY IMPLEMENTED

AGENCY ACTION

Original target date for completion: September 2019

In response to our recommendation, Business Technologies staff said that the onboarding process documentation was updated requiring contracted employees in the Security Operations Center to sign a nondisclosure agreement. The new onboarding procedure requires a form to be completed that indicates a signed and completed nondisclosure agreement is on file.

Business Technologies staff told us the Security Operations Center has only two full-time contracted employees. We verified this through inspection of their organizational chart and confirmed that the two full-time contractors signed nondisclosure agreements.

Business Technologies provided a new on- and offboarding policy and procedure dated April 16, 2021, which includes an onboarding form requiring a nondisclosure agreement for contracted employees. With both the evidence of a new procedure form and the signed nondisclosure agreements for current contracted employees completed, we consider this recommendation fully implemented.

Recommendation 1.5

ESTABLISH PROCESS TO APPROVE DOCUMENTS – The airport's chief information officer should establish a process to ensure all Security Operations Center policies and procedures are approved and updated annually.

✓

FULLY IMPLEMENTED

AGENCY ACTION

Original target date for completion: December 2019

In response to our recommendation, Business Technologies staff told us they would implement a process to review, update, communicate, and approve all policies and procedures annually. The department created a policy titled Business Technology Documents Standards, which requires all documents to have an annual review.

We verified that the "data cassification and handling" policy, which was missing approval in the original assessment, now includes the approval of the chief information security officer. This review was completed in June 2020, and the next expected review date is June 2021.

Therefore, we consider this recommendation fully implemented.

Recommendation 1.6

FORMALIZE LESSONS LEARNED – The airport's chief information officer should improve the lessons-learned step in the Security Operations Center incident response process that formally documents how an incident occurred, where it originated from, whether the incident has spread to other devices in the network, and how it could be avoided in the future.

✖

NOT IMPLEMENTED

AGENCY ACTION

Original target date for completion: October 2019

Business Technologies staff intended to review and update their lessons-learned steps in the incident response process to include language on how an incident occurred, where it originated from, whether the incident spread to other devices in the network, and how the incident could be avoided in the future. However, during our follow-up, the department provided us with the 2018 incident management process policy, which does not show that it has been reviewed or updated since that time and does not include the addition of the recommended items. We therefore consider this recommendation not implemented.

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.