ASSESSMENT REPORT

Cybersecurity: Asset Management

JUNE 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
Karin Doughty, CISA, CDPSE, Information Systems Audit Lead
Nick Jimroglou, CISA, CDPSE, Information Systems Audit Lead

Contractors

Cornerstone Partners LLC
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

June 17, 2021

On behalf of the Auditor's Office, Cornerstone Partners LLC 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 city agency for their 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 Cornerstone Partners LLC during the assessment. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

BACKGROUND

Information Technology Asset Management

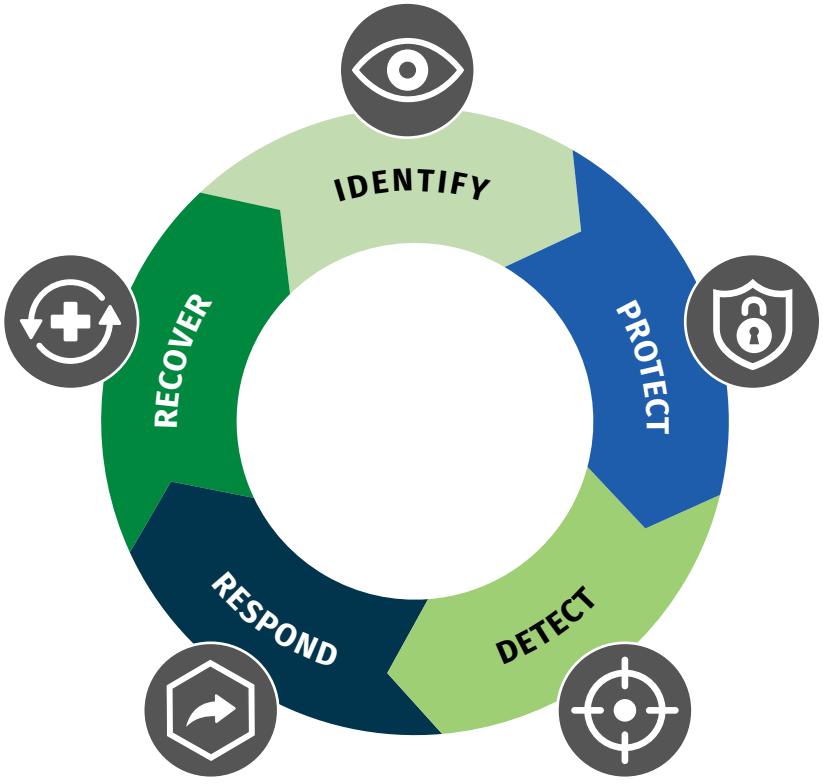
Cybersecurity begins with knowing what assets are owned and managed by an organization. Information technology assets can take many forms — from traditional computer workstations to servers, where each asset has a name and an IP address.

Many cybersecurity-related risks can be traced back to poor asset management. Unknown devices on a network will not receive updates or patches — leaving the devices vulnerable to unwanted exposure to malware or hacking attacks.

Information technology administrators cannot expect to securely maintain their assets if they do not have proper asset management. For this reason, many leading practices list asset management as the first step in a cybersecurity strategy.

The most common framework is the National Institute of Standards and Technology's Cybersecurity Framework, as shown in Figure 1.

FIGURE 1. National Institute of Standards and Technology's Cybersecurity Framework



Source: *Graphic design by Auditor's Office staff based on federal framework.*

The first of five core functions in that framework is to "identify" — that is, to "develop an organizational understanding to manage [the] cybersecurity risk to systems, people, assets, data, and capabilities."[1]

The institute further explains:

> "The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy."[2]

Asset management is complex. An organization's asset management system should include all devices: traditional workstations and servers, networking devices, cloud-based systems, cloud-based applications, vendor-managed systems, employees' personal devices used for work purposes, and physical security devices such as badge readers and cameras.[3] For large or complex organizations, assets may number in the thousands.

To add to the complexity of asset management, organizations can track their assets on a system level or by application, which may require multiple servers per system. These systems may also be hosted by cloud services. When a system is cloud-hosted, risk and responsibility for the system is shared between the organization and a third-party vendor. As such, assets managed by vendors should also be tracked by the organization's asset management system.

Making Asset Management Easier

These complexities can be made easier with processes and technologies that support an organization's asset management efforts.

PROCESSES – A defined "system development life cycle" ensures new systems are added to the asset management system and retired systems are removed. When this process is defined in a policy, it ensures the organization's information technology department will talk with business system owners before a system is connected to or removed from the network.

[1] National Institute of Standards and Technology, Cybersecurity Framework (Version 1.1), "Framework for Improving Critical Infrastructure Cybersecurity" (2018), accessed May 12, 2021, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. The National Institute of Standards and Technology is a laboratory and nonregulatory federal agency within the U.S. Department of Commerce.

[2] National Institute of Standards and Technology.

[3] Different cloud computing service models include Iaas, or "infrastructure as a service"; PaaS, or "platform as a service"; and SaaS, or "software as a service."

TECHNOLOGY – Organizations use a variety of technologies to manage their assets and keep their asset management systems updated. For example, automated resource discovery tools can be set up to scan all networks in an organization's environment. Then, any new IP addresses are added to the asset management system and a system owner is defined and documented. Organizations can also leverage security endpoints, which can be set up to scan and install on all devices on a network.

Even organizations with minimal asset management can use a list from their system's Active Directory or their chosen remote monitoring and management tools to provide a starting point for building an asset management database.

Good Asset Management

The benefits of good asset management are numerous. Information technology personnel can better answer questions related to operating systems, manufacturer support, software licensing, vulnerabilities, and business system owners. With an accurate inventory, administrators can ensure equipment is patched in a timely manner and they can plan other security measures as needed.

Additionally, this information enables faster responses to security alerts and allows the organization to focus on the assets that present the greatest risk. It also makes the audit process easier on the organization and makes it easier to determine compliance with software licenses.

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.