ASSESSMENT REPORT

An Agency of City and County of Denver

Information Systems Cybersecurity Assessment

February 2018

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor

Timothy M. O'Brien, CPA
Auditor

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202
720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

February 15, 2018

AUDITOR'S REPORT

A third party has completed an Information Systems Cybersecurity Assessment. The assessment found some areas of strength, and some areas that need improvement, which have been communicated to the City's Technology Services department for further evaluation.

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

We extend appreciation to Technology Services and the personnel who assisted and cooperated with us during the assessment.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

The Auditor of the City and County of Denver is independently elected by the citizens 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 and providing 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 citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Manager

Audit Team

Shannon Kuhn, CISA, Audit Supervisor
Jared Miller, CISA, Audit Supervisor

Contractors

Cornerstone Partners
Bill Evert, Partner
Donald McLaughlin, Lead Consultant
Brian Cather, Lead Consultant

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) 913-5247

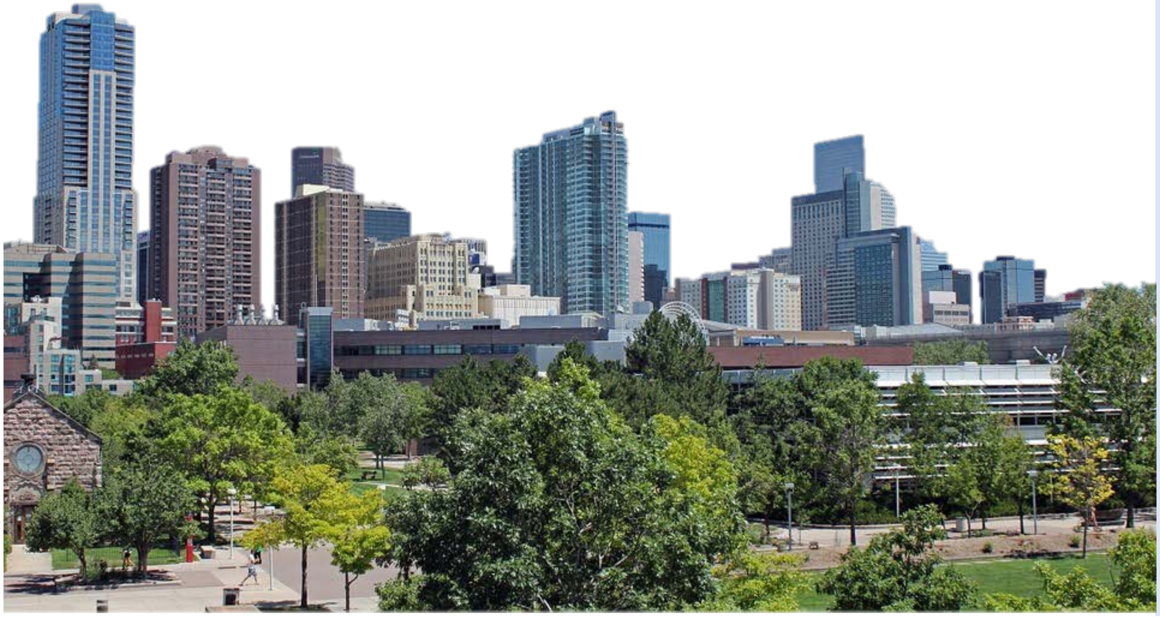
Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
Audit report year: **2018**

CORNERSTONE PARTNERS

www.cpcyber.com
303-928-4140

An Agency of City and County of Denver - Information Systems Cybersecurity Assessment

February 15, 2018



CORNERSTONE
PARTNERS

An Agency of City and County of Denver
Information Systems Cybersecurity Assessment

Background

Cornerstone Partners LLC (“Cornerstone”) was tasked by the Auditor to evaluate the Information Systems cybersecurity of an agency of the City and County of Denver (“City”) for the Agency, Technology Services and the Auditor's Office. As part of deliverables, Cornerstone will present a report to the Audit Committee and findings will be sent to the Agency and Technology Services. The results of the report will be limited to discussing any findings, vulnerabilities and risks found on an agency of the City and County of Denver.

A key to this improvement process is balancing the need for public access and transparency, while managing the implementation of both centralized and decentralized cybersecurity strategies. Currently, the City has a decentralized approach to information systems requirements, which affects how risk is approached and managed by the City.

When applying and evaluating the information systems cybersecurity for the agency of the City, one must weigh how the results of this assessment would influence the understanding of their overall risk levels and vulnerabilities. This understanding will help drive the allocation of valuable resources that are required for maintaining and actively improving its information system requirements and capabilities. The differing approaches to risk tolerance, levels of maturity between offices and departments, and the public facing requirement of the City affects the way they implement control measures and risk control processes.

Scope of Work

The scope of this engagement began with understanding the current posture of the agency of the City. The City's operating requirements of openness, transparency, and accessibility was crucial in understanding the scope of work. Cornerstone understands how the City must balance the public facing data requirements with the need to protect and ensure the confidentiality, integrity, and availability of data on its information systems.

This engagement focused on assessing the information systems cybersecurity of an agency of the City utilizing the National Institute of Science and Technology (NIST) Cybersecurity Framework (figure 1).

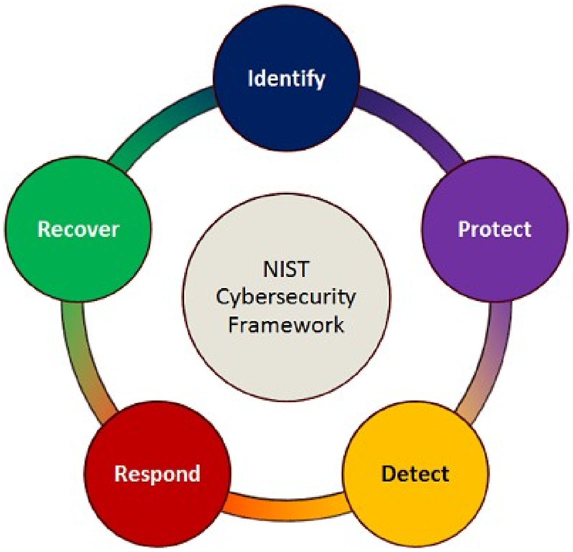


Figure 1

The Methodology

Cornerstone collected evidence and performed testing to enable an effective cybersecurity assessment of the agency of the City and County of Denver. The NIST methodology uses five key functional process areas of cybersecurity; however, the fourth and fifth key functional process areas, event response and event recovery, were not in scope during this engagement. The areas in scope included:

Risk Identification: Tools, strategies, and techniques for the identification and tracking of potential risks, and the organization's willingness to accept cybersecurity risk.

Event Protection and Prevention: Tools, strategies, and techniques used to safeguard and ensure delivery of critical information technology infrastructures and systems.

Event Detection: Tools, strategies, and techniques used to detect potential and actual occurrences of a cybersecurity event taking place, or an event that has taken place.

Social Engineering

Social engineering was in scope for this engagement and is defined asa non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices. When successful, many social engineering attacks enable attackers to gain legitimate, authorized access to confidential information.
Some common social engineering techniques include:

- **Baiting** – Attackers conduct baiting attacks when they leave a malware-infected device, such as a USB flash drive or CD, in a place where someone likely will find it. The success of a baiting attack hinges on the notion that the person who finds the device will load it into their computer and unknowingly install the malware. Once installed, the malware allows the attacker to advance into the victim's system.

- **Phishing** – Phishing occurs when an attacker makes fraudulent communications with a victim that are disguised as legitimate, often claiming or seeming to be from a trusted source. In a phishing attack the recipient is tricked into installing malware on their device or sharing personal, financial, or business information. Email is the most popular mode of communication for phishing attacks, but phishing may also utilize chat applications, social media, phone calls, or spoofed websites designed to look legitimate.

- **Spear phishing** – Spear phishing is a highly targeted type of phishing attack that focuses on a specific individual or organization. Spear phishing attacks use personal information that is specific to the recipient in order gain trust and appear more legitimate. Often this information is taken from victims' social media accounts or other online activity. By personalizing their phishing tactics, spear phishers have higher success rates for tricking victims into granting access or divulging sensitive information such as financial data or trade secrets.

- **Tailgating** – Tailgating is a physical social engineering technique that occurs when unauthorized individuals follow authorized individuals into an otherwise secure location. The goal of tailgating is to obtain valuable property or confidential information.

The Results

The assessment incorporated four parts: wireless, application, network, and social engineering. Wireless security would include any WiFi Access Points or the configuration of wireless networks at the agency's locations. The application security would include any configurations of applications that are critical to the agency's mission. The network security would include any device, connection, or asset the agency's employees could access. Social engineering utilizes the methods noted above.

Risk Identification

The risk identification function contains the basic ground work for understanding and managing cybersecurity risk to assets, data, and systems capabilities.

Event Protection and Prevention

The event protection and prevention function is focused on helping the organization develop and implement safeguards to reduce the impact of a potential cybersecurity event.

Event Detection

The event detection function is focused on assisting the organization on developing and implementing safeguards to detect the presence of a cybersecurity threat. By detecting cybersecurity events in a timely manner, the organization can reduce the potential impact the threat can have on the organization.

Conclusion

Cornerstone assessed the cybersecurity of an agency of the City and County of Denver for the Agency, Auditor and Technology Services. Cornerstone utilized the NIST Cybersecurity Framework and identified strengths and weaknesses using the three aforementioned key functional process areas of cybersecurity. A combined assessment of strengths and weaknesses in these three process areas was communicated to the Agency, Technology Services and the Auditor. Additionally, Cornerstone's assessment of the agency of the City, along with the associated findings, were reported to the Agency and Technology Services. The Agency has responded to these findings.