ASSESSMENT REPORT
An Agency of the City & County of Denver
Cybersecurity Assessment
June 2018

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

Timothy M. O’Brien, CPA
Denver 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

Nicholas Jimroglou, CISA, Lead IT Auditor

Consultants

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
AUDITOR'S REPORT

Cornerstone Partners has completed a cybersecurity assessment of an agency within the City and County of Denver. The purpose of the assessment was to evaluate deficiencies and make recommendations to further improve the agency’s cybersecurity.

The assessment resulted in recommendations for improvements, which have been communicated to the City’s agency and Technology Services for further remediation.

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

Denver Auditor’s Office

[Signature]

Timothy M. O’Brien, CPA
Auditor
An Agency of City and County of Denver
- Information Systems Cybersecurity Assessment

June 21, 2018
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. This report describes only the work performed and does not include the results for security reasons. Cornerstone will also privately present findings to the Audit Committee and key technology individuals in the City.

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 the agency’s 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 an agency and Technology Services 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. 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 Standards and Technology (NIST) Cybersecurity Framework (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.
Phishing

Cornerstone believes that cybercriminals view phishing attacks as a successful (and easy) way of getting into an agency to launch more sophisticated attacks. Humans are, after all, increasingly seen as the weakest link and thus the most effective target for criminals looking to infiltrate an agency.

Phishing is a type of identity theft (usually through e-mail) where cybercriminals try to get users to hand over personal and sensitive information without them knowing it.

Some tips that might help an agency stay better protected against phishing attacks are:

- **Be sensible when it comes to phishing attacks** – Internet and email users can significantly reduce the chance of falling victim to phishing attacks by being sensible and smart while browsing online and checking emails. For example, never click on links, download files or open attachments in emails (or on social media) unless it is from a known, trusted source. Also, be wary of emails asking for confidential information – especially if it asks for personal details or banking information. Legitimate organizations, including and especially your bank, will never request sensitive information via email.

- **Review links** - Users should always place the mouse over a web link in an email to see if it is directed to the right website – that is, “the one that appears in the email text” is the same as “the one you see when you mouse-over”.

- **Suspicious e-mails** - Plenty of phishing emails are obvious. They will be punctuated with typos, excessive capitalization and exclamation marks. They may also have an impersonal greeting – think of those ‘Dear Customer’ or ‘Dear Sir/Madam’ salutations – or feature implausible and generally surprising content.

- **Browse securely with HTTPs** - Users should always, where possible, use a secure website (indicated by https:// and a security “lock” icon in the browser’s address bar) to browse, and especially when submitting sensitive information online.

Also, no one should use public, unsecured Wi-Fi for work, banking, shopping or entering personal information online. Convenience should never replace security.
The Results

The assessment incorporated three parts: wireless, application, and network. 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 and source code 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.

Risk Identification

The risk identification function contains the basic groundwork 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 in 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 of the threat on the organization.

Conclusion

Cornerstone assessed the cybersecurity of an agency of the City and County of Denver for the Auditor and Technology Services. Cornerstone utilized the NIST Cybersecurity Framework and identified strengths and weaknesses using the three-mentioned key functional process areas of cybersecurity. A combined assessment of strengths and weaknesses in these three process areas, along with the findings, was communicated to the agency, Technology Services, and the Auditor.