CITY AUDITOR'S OFFICE

Ransomware Readiness Assessment

June 15, 2023 AUDIT NO. 2303

June 15, 2023

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for the *Ransomware Readiness Assessment*, which was included on the Council-approved FY 2022/23 Audit Plan as a contracted information technology (IT) audit. This audit was conducted to evaluate the effectiveness of controls for preventing, identifying, responding to, and recovering from a ransomware event.

We contracted with an independent IT audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of the work included an assessment of relevant cybersecurity controls and facilitating table-top exercises to test the City's readiness to detect and respond to a ransomware event.

The assessment identified several areas that can be matured to help improve the City's ability to respond to a ransomware event. We provided a separate confidential report of the results and related recommendations to the IT department. This information is not detailed in the public report due to its sensitive nature.

If you need additional information or have any questions, please contact me at (480) 312-7851.

Sincerely,

Lai Cluff, CIA
Acting City Auditor

Audit Team:
Travis Attkisson, Sr. Auditor

TABLE OF CONTENTS

AUDIT HIGHLIGHTS

Ransomware Readiness Assessment

June 15, 2023 Audit No. 2303

WHY WE DID THIS AUDIT

This Ransomware Readiness Assessment audit was included in the Council-approved fiscal year 2022/23 Audit Plan. The objective of this audit was to evaluate the effectiveness of controls for preventing, identifying, responding to, and recovering from a ransomware event.

BACKGROUND

We contracted with an independent IT audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of the work included an assessment of relevant cybersecurity controls and facilitating table-top exercises to test the City's readiness to detect and respond to a ransomware event.

Ransomware is a continuously evolving form of malware that can encrypt the City's data, preventing organizations from accessing computer files and systems, and requiring a ransom to be paid to recover the data.

The National Institute of Standards and Technology (NIST) established standards to better manage and reduce cybersecurity risk. The NIST Cybersecurity Framework (CSF) is organized by five key functions – Identify, Protect, Detect, Respond, and Recover. BerryDunn assessed approximately 70 NIST CSF control subcategories relevant to ransomware and incident response preparedness.

City Auditor's Office

City Auditor 480 312-7851
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

Several areas can be matured to help improve the City's overall ability to respond to a ransomware event.

Overall, BerryDunn found that the City has foundational pieces in place to effectively detect and respond to a ransomware or cyber related event.

BerryDunn assessed 68 NIST CSF security control subcategories relevant to ransomware and incident response preparedness. The assessment identified 23 areas with low to moderate risk ratings where improvements were recommended.

In general, areas for improvement included developing and enhancing:

- Response plans and security policies to reflect the operating environment, minimize potential impacts of an event, and to take into consideration the business needs of City departments.
- Communication paths and personnel responsibilities during an event.

WHAT WE RECOMMEND

We recommend the IT department implement the recommendations identified in the BerryDunn detailed report.

MANAGEMENT RESPONSE

The department agreed with the recommendations and plans to implement changes by December 2024.

BACKGROUND

This *Ransomware Readiness Assessment* audit was included in the Council-approved fiscal year 2022/23 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The objective of this audit was to evaluate the effectiveness of controls for preventing, identifying, responding to, and recovering from a ransomware event. We contracted with an independent IT audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of the work included an assessment of relevant cybersecurity controls and facilitating table-top exercises to test the City's readiness to detect and respond to a ransomware event.

Ransomware and Cybersecurity

Ransomware is a continuously evolving form of malware that can encrypt the City's data, preventing organizations from accessing computer files and systems, and requiring a ransom to be paid to recover the data. Cyber criminals may also threaten to release sensitive or personal data to the public. Ransomware attacks in local government are increasingly being reported, with significant impact to critical services. In a 2020 survey conducted by the ICMA, local governments responded that phishing emails were the most common attack vectors, observing an increase in "spear" phishing, where individuals and departments are more specifically targeted. In 2022, the FBI and several other security agencies issued a Joint Cybersecurity Advisory, reporting that 2021 trends showed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally.[1]

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a framework for organizations to better manage and reduce cybersecurity risk. It is the framework that has been adopted by the City's IT Department. NIST CSF is organized into five key functions – Identify, Protect, Detect, Respond, and Recover, as presented in Figure 1.

Figure 1. NIST Cybersecurity Framework

Identify: Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.
Protect: Develop and implement the appropriate safeguards to ensure delivery of services.
Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

SOURCE: NIST Special Publication 1271 – Quick Start Guide, August 2021.

(continued on next page)

[1] February 9, 2022 Joint Cybersecurity Advisory: "2021 Trends Show Increased Globalized Threat of Ransomware", jointly issued by Federal Bureau of Investigations (FBI), Cybersecurity & Infrastructure Security Agency (CISA), National Security Agency, Australian Cyber Security Centre, United Kingdom's National Cyber Security Centre.

There are 108 NIST CSF security control subcategories, which are outcome-driven statements that provide considerations for creating or improving a cybersecurity program. BerryDunn assessed approximately 70 of these subcategories that have an influence on ransomware readiness. While these security controls are also relevant for other potential malware or cybersecurity threats, this assessment more specifically addresses ransomware due to its increased prevalence and potential risk to the City. As part of the assessment, the audit team also designed and conducted table-top exercises to test the City's preparedness and responsiveness to potential ransomware events.

OBJECTIVES, SCOPE, AND METHODOLOGY

A *Ransomware Readiness Assessment* audit was included in the Council-approved fiscal year 2022/23 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The objective of this audit was to evaluate the effectiveness of controls for preventing, identifying, responding to, and recovering from a ransomware event.

We contracted with an independent IT audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. As required by Government Auditing Standards, we evaluated the qualifications and independence of these specialists and documented the nature and scope of the specialist's work, including the objectives and scope of work, intended use of the work to support the audit objectives, the specialist's assumptions and methods used, and the specialist's procedures and findings.

For this assessment, BerryDunn followed guidance from the following standards:

- National Institute of Standards and Technology (NIST), Cybersecurity Framework V1.1, April 2018.
- NIST, Interagency/Internal Report (IR) 8374, Ransomware Risk Management: A Cybersecurity Framework Profile, February 2022.
- Cybersecurity and Infrastructure Security Agency (CISA) Ransomware Guide, September 2020.

BerryDunn assessed 68 NIST CSF security control subcategories, across the 5 core functions (*Identify, Protect, Detect, Respond, and Recover),* that have an influence on ransomware readiness. To facilitate the analysis of the NIST CSF core functions, BerryDunn developed a survey that was distributed to 11 City departments with technology staff. Additionally, they reviewed policies, procedures, and relevant documentation and conducted personnel interviews. The audit team interviewed technology staff from the IT department, Water Services, Police Department, and Traffic Management.

To test the City's ransomware preparedness and responsiveness, BerryDunn also designed and conducted two table-top exercises to test the City's capabilities and identify opportunities in an effort to enhance current ransomware response practices.

Overall, BerryDunn found that the City has foundational pieces in place to effectively detect and respond to a ransomware or cyber related event. The assessment identified several areas that can be matured to help improve the City's ability to respond to a ransomware event. Recommendations were made to improve the City's ransomware readiness.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Audit work took place from January to April 2023.

FINDINGS AND ANALYSIS

1. Several areas can be matured to help improve the City's overall ability to respond to a ransomware event.

Overall, the City has foundational pieces in place to effectively detect and respond to a ransomware or cyber related event. The assessment identified several areas that can be matured to help improve the City's overall ability to respond to a ransomware event. Of the 68 NIST Cybersecurity Framework control subcategories evaluated, the assessment identified 23 areas for improvement, as shown in Table 1. These areas were all classified as Low or Moderate risk.

Table 1: Summary of controls assessed and recommendations by CSF function.

NIST CSF Function	Controls assessed	Areas for Improvement
Identify (ID)	19	6
Protect (PR)	18	10
Detect (DE)	12	2
Respond (RS)	13	3
Recover (RC)	6	2
Total	**68**	**23**

SOURCE: Summarized from BerryDunn Ransomware Readiness Assessment report.

In general, the areas for improvement included further developing and enhancing:

- Response plans and security policies to reflect the current operating environment, mature the City's response capabilities, and minimize the potential impacts of an event. Plans and policies should take into consideration the business needs of City departments and be applied consistently across the enterprise.
- Communication paths and personnel responsibilities during an event.

Detailed findings and recommendations were provided to the IT department and are not detailed in this public report due to the sensitive nature of the information.

Recommendations:

The IT Department should implement the recommendations identified in the BerryDunn detailed report.

MANAGEMENT ACTION PLAN

1. Several areas can be matured to help improve the City's overall ability to respond to a ransomware event.

Recommendations:

The IT Department should implement the recommendations identified in the BerryDunn detailed report.

MANAGEMENT RESPONSE: The Management acknowledges and fully agrees with the recommendations highlighted in the BerryDunn detailed report. Recognizing the importance of proactive measures, we are committed to implementing these recommendations to enhance the City's cybersecurity posture and respond effectively to ransomware events.

PROPOSED RESOLUTION: The BerryDunn detailed report has provided valuable insights into areas that require maturation to strengthen the City's overall response capabilities against ransomware attacks. Recognizing that implementing all recommendations simultaneously may be overwhelming or resource-intensive, a phased approach will be adopted to prioritize and systematically address each area of improvement. We will adopt a strategic plan to complete all necessary enhancements by December 2024 while ensuring minimal disruption to daily operations.

RESPONSIBLE PARTY: Information Technology and All Impacted Departments

COMPLETED BY: DECEMBER 2024

City Auditor's Office
7447 E. Indian School Rd., Suite 205
Scottsdale, Arizona 85251

OFFICE (480) 312-7756
INTEGRITY LINE (480) 312-8348

www.ScottsdaleAZ.gov/auditor

CITY OF SCOTTSDALE

The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability and integrity.