Memorandum

CITY OF DALLAS

DATE September 1, 2023

TO Honorable Mayor and Members of the City Council

SUBJECT **After Action Review Report (AAR) of May 3rd Ransomware Incident**

On May 3, 2023, the City of Dallas experienced a ransomware incident against its computing and telecommunications environment, disrupting operations, damaging equipment and software, and necessitating the activation of the City's Incident Response Plan (IRP). In the subsequent weeks, the City's Information & Technology Services (ITS) Department worked with internal and external partners to contain the threat, review and cleanse the environment, and safely restore impacted services. As of the date of this memorandum, services have been restored and IT operations normalized.

As a key component of the City's IRP, an After-Action Review (AAR) has been conducted and a report completed by ITS which provides:

1. Background information on the threat actor,
2. A detailed timeline of events prior to, during, and following the initial incident,
3. An assessment of factors which served to mitigate the impact of the ransomware,
4. Key findings, and,
5. Recommendations for ongoing improvements to the security of the City's technology environment.

On September 6, 2023, a briefing will be provided to the Mayor and City Council members during the day's scheduled Council meeting. An overview of the AAR will be briefed and the City's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) will be available to answer questions.

As there is still an active Federal criminal investigation into the threat actor, some information is limited in distribution. As such a closed session will be scheduled (pursuant to Sec. 551.076 and Sec. 551.089 T.O.M. A.) to provide the Mayor and Council Members with further information regarding the security assessment related to this security incident relating to the City's information resources technology.

The AAR briefing presentation is attached and presented for your review and consideration. A publicly available AAR will be issued following the briefings to the Mayor and City Council.

DATE September 1, 2023

SUBJECT **After Action Review Report (AAR) of May 3rd Ransomware Incident**

If you have any questions, please contact William (Bill) Zielinski, Chief Information Officer and Director of Information & Technology Services.

Jack Ireland
Chief Financial Officer

[Attachment]

c: T.C. Broadnax, City Manager
Tammy Palomino, Interim City Attorney
Mark Swann, City Auditor
Bilierae Johnson, City Secretary
Preston Robinson, Administrative Judge
Kimberly Bizor Tolbert, Deputy City Manager
Jon Fortune, Deputy City Manager
Majed A. Al-Ghafry, Assistant City Manager
M. Elizabeth (Liz) Cedillo-Pereira, Assistant City Manager
Robert Perez, Assistant City Manager
Carl Simpson, Assistant City Manager
Genesis D. Gavino, Chief of Staff to the City Manager
Directors and Assistant Directors

City of Dallas

The City of Dallas Ransomware Incident: May 2023

Dallas City Council
September 06, 2023

Dr. Brian Gardner
Chief Technology & Information Security Officer
Department of Information and Technology Services
City of Dallas

Presentation Overview

- Background/History
- May 3, 2023
- City Operational Impact
- Impact Mitigation
- Recovery
- Acknowledgements
- Findings
- Recommendations
- City Investments

Background/History

April 7-May 3, 2023

- Royal Group performed
  - Reconnaissance &
  - Staging
- Less than 1 month
- Leakage of 1.169 TB of the 3.8 PB data the City has

Background/History

Reconnaissance

- Exfiltration of Data
- Command-and-Control Beacons
- Preparation to Deliver Encryption to Files
- Review of Users (Who is Who)

Background/History

- 70% of Organizations suffer Ransomware
- 100% surge from the second quarter of 2022
- Mean time to identify a data breach is 204 days
  - City identified in 27 days
- Mean time is 73 days to contain breaches
  - City contained in 1 day

May 3, 2023

- Use of Service Account
- Threat Actor Begins Encrypting Files
- Ransom Request Files Found On 996 Hosts
- Incident Response Plan (IRP) Activated
- Multiple Incident Response Teams Activated
  - Internal Teams
  - Vendors
  - Cybersecurity Professionals
- Mitigation Efforts Initiated & Paused

City Operational Impact

- Interruption to All City Operations
  - All City Departments
  - Impact
    - Public Safety
    - Public Facing Services
    - Technology Infrastructure

Impact Mitigation

- Increased in Information Security Budget
- Periodic Reviews by Federal and Outside Organizations
- Addition of Zero Trust Technologies

Recovery

- May 3, 2023
  - Focus on Eradication
- May 4, 2023
  - Last known Infection
- Full Recovery Work Began
- Priorities set Based on Previous IRP
- Communication to State & Federal Authorities

Recovery

- Information provided to Law Enforcement
- Incident Support Team (IST)
- Multiple Remediation Team working in Coordination
- City currently has 14,000 assets
  - 230 Server
  - 1,168 Workstations
    - Less than10% of assets infected

Recovery

- Over 90% restoration by June 9, 2023
- Currently 99.9% restoration
  - Small portion of
    - Test
    - Development
    - Unsupported systems needing upgraded
- Removed 100 servers of technical debt

Acknowledgements

- Dallas Fire Rescue
- Dallas Police Department
- Office of Emergency Management
- GTS
- State & Federal Agencies
- Outside Vendors

Findings

- Incident Response Plan Revisions
- Security Incident Staff Periodically Exercised
- Identification/Detection of Threat
- Aggressive Incident Response
- Substantial Cybersecurity Investments Made in Advance of Attack

Recommendations

Plan of Action & Milestones

- Cybersecurity Program Review
- Privacy and Security Risk Assessments
- Backup and Recovery Processes
- Network Hardening
- Actively Manage Infrastructure and Software
- Update to the Incident Response Plan

City Investments

Cybersecurity Spend

- 2019 2.5% of the total ITS budget
- 2023 ~10% of the total ITS budget
- Innovative Technologies
- Strategic Plan
- $8.5 million in computer-based interdiction, mitigation, recovery, and restoration efforts

City of Dallas

The City of Dallas Ransomware Incident: May 2023

Dallas City Council
September 06, 2023

Dr. Brian Gardner
Chief Technology & Information Security Officer
Department of Information and Technology Services
City of Dallas