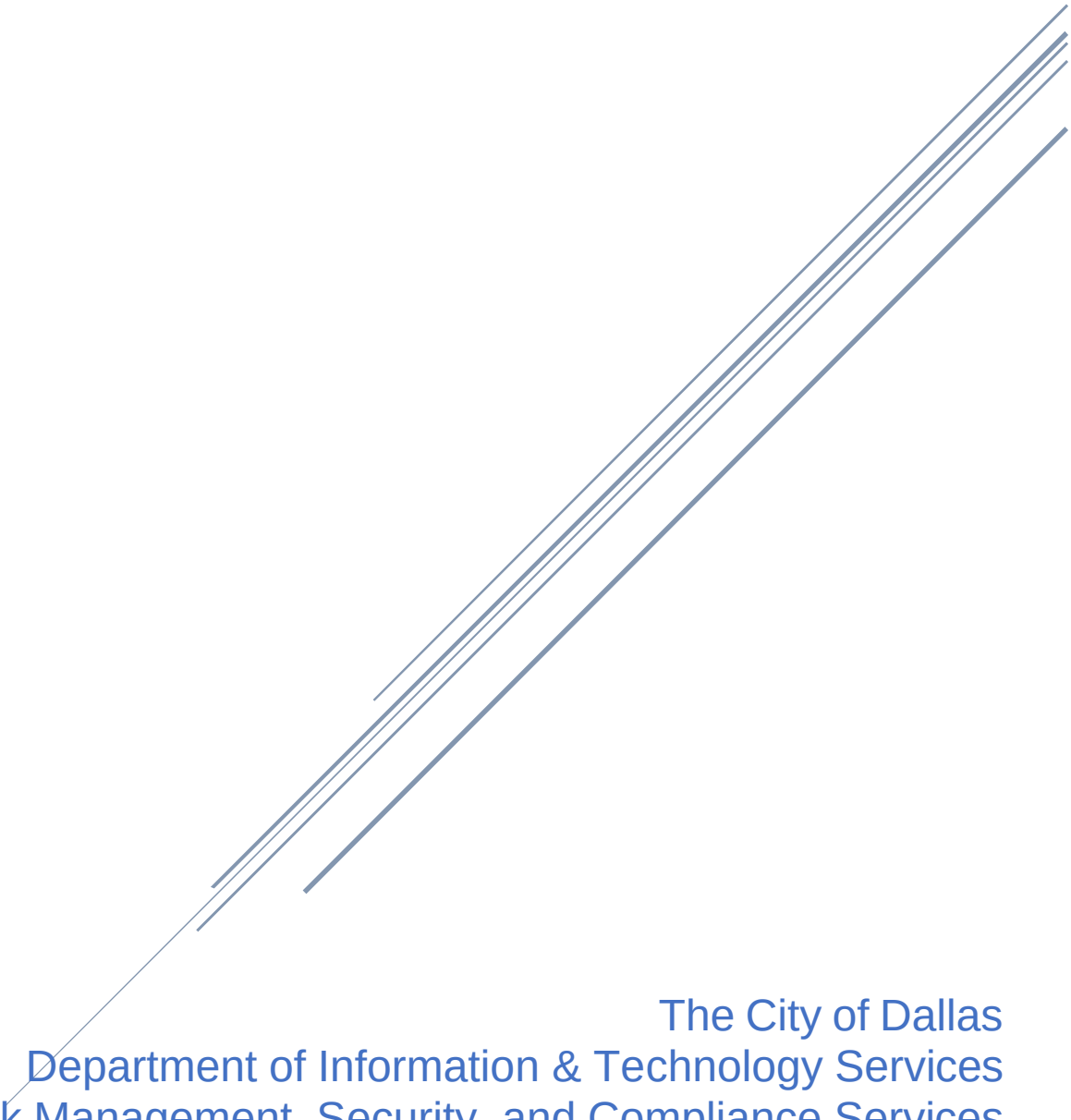
THE CITY OF DALLAS RANSOMWARE INCIDENT: MAY 2023

Incident Remediation Efforts and Resolution



The City of Dallas
Department of Information & Technology Services
ITS Risk Management, Security, and Compliance Services
September 20, 2023

Document Revision

Item	Change Description	Version	Date	Document State
1	Final Draft Document	1.0	08/30/2023	FINAL
2	Final Document	1.0	9/20/2023	FINAL

The City of Dallas Ransomware Incident: May 2023 Acknowledgements

The Chief Financial Officer of the City of Dallas and the Director of the Department of Information and Technology Services (ITS) acknowledge and thank the ITS Risk Management, Security, and Compliance Division for the efforts in capturing, analyzing, and reporting on information and events related to the City of Dallas 2023 Ransomware Incident: May 2023 – Incident Remediation Efforts and Resolution. Without their assistance, expertise, and background in information and cyber security matters, the City would not have as deep of an understanding as to the causes and effects related to this cyberattack upon City computing and communications resources.

General Source Information Acknowledgements

The City of Dallas acknowledges and thanks the many information sources that contributed to the construction of this document. Some source information was obtained through Gartner and Forrester research services. The City acknowledges and thanks those organizations for the guidance and assistance their individual contracted services provide the City. Some source information was also gathered from the elements of the United States Federal Government including but not limited to The National Institute of Standards and Technology (NIST), The Department of Homeland Security (DHS), The Department of Justice (DOJ), and others. The City acknowledges and thanks those organizations for the guidance and assistance for their services and standards provided to the City.

Since this document is not an academic paper, detailed citations are not used. This document will generally cite the sources of information used in the construction of this report using a bracketing artifice. The artifice used is square brackets with indication of the source within the square brackets. The following is an illustration of a citation used in this document: [Source], and [Source1, Source2].

Executive Summary

Purpose

This document provides an After-Action Report (AAR) to the Mayor, City Council, and City Executive Leadership pertaining to the ransomware incident initiated against the City of Dallas on the morning of Wednesday, May 03, 2023.

The purpose of an After-Action Report (AAR) is to analyze the management or response to an incident, exercise, or event by identifying strengths to be maintained and built upon, as well as identifying potential areas of improvement. [UH]

Context

The City of Dallas is a municipal corporation of the State of Texas. As the third largest Texas municipality, the hub of the fourth largest metropolitan area of the United States, and the ninth largest city within the United States, the City of Dallas is a logical choice for bad actors wishing to initiate and prosecute an Information Security (InfoSec) attack.

The City of Dallas is comprised of over 40 different departments, multiple offices, and several boards that support the many different missions assigned to it. Each department, office, and board effectively manages its own activities in support of the assigned missions. This diversity of approaches provides diversity in approach but also introduces a certain lack of organizational cohesion.

The City of Dallas operates over 860+ computer-based applications in support of approximately 100 technology and business services supporting City and City department missions. These applications and services are generally managed and operated by approximately 200 information technology (IT) professionals working within the City's Department of Information & Technology Services (ITS).

Royal Hacker Group and Initial Surveillance

Cyber criminals and hackers have found computer-based crime to be a viable and lucrative activity for financial and political gain. Over the past few decades, various hacker groups have banded and disbanded. In September 2022, a hacker group known as Royal came to the attention of law enforcement and cybersecurity officials.

Royal is identified as an amalgam of non-state actors believed to be composed of some very experienced cyber operators. Many Royal operators are believed to have previously belonged to other infamous cybercriminal groups including Conti Team One. [HHS]

In its short period of existence, Royal has successfully crippled – if not shut down – a shockingly large number of commercial, healthcare, and governmental entities. In the year 2022, ransomware victimized over 70 percent of organizations, marking a surge compared to the preceding five years and establishing the highest recorded proportion to date. This enduring

upward trajectory corresponds with the increasing profitability of ransomware for malicious actors. The incidence of ransomware exhibited a noteworthy annual growth rate of 13% during 2022, surpassing the cumulative increase of the preceding five years. Furthermore, the number of public ransomware victims escalated by 38% when compared to the initial quarter of 2023 and demonstrated an astounding 100% surge from the second quarter of 2022. This denotes a substantial 75 percent upswing in the mean count of monthly attacks in the United States between the initial and latter halves of the preceding 12-month period.

Royal began its cyber-attack surveillance and date exfiltration activities at the City of Dallas beginning in early April 2023. A review of system log data by both City and external cybersecurity experts identified the Royal group as having infiltrated the City and beginning its surveillance operations on April 7, 2023. Royal's initial access utilized the basic service domain service account, connecting to a server. Royal was then able to traverse the internal City infrastructure during the surveillance period using legitimate 3rd party remote management tools.

Using the City service account credentials, Royal performed reconnaissance activities in the City's IT infrastructure during the period of April 7, 2023, through May 4, 2023. During this time, Royal performed data exfiltration and ransomware delivery preparation activities. The data exfiltration activities performed during the surveillance period resulted in data leakages totaling an estimated 1.169 TB at a time prior to May 03, 2023.

During the surveillance period, Royal performed several actions to inject command and control software and established command-and-control beacons. The command-and-control beacons allowed Royal to prepare the City's network resources for the May 03, 2023, ransomware encryption attack.

Royal Ransomware Incident

Early on the morning of Wednesday, May 03, 2023, Royal began its ransomware attack on the City of Dallas. Using its previously deployed beacons, Royal began moving through the City's network and encrypting an apparently prioritized list of servers using legitimate Microsoft system administrative tools.

City attack mitigation efforts began immediately upon the detection of Royal's ransomware attack. To thwart Royal and slow its progress, City Server Support and Security teams began taking high-priority services and service supporting servers offline. As this was done, City service restoration identification activities began. Though service restoration could not begin until Royal was effectively removed from the City's network, service restoration teams needed to begin acquiring resources for service restoration efforts. For certain services such as Public Safety Computer-Aided Dispatch, those service restoration efforts began almost immediately.

Early in the attack, both internal and external cybersecurity, as well as external vendor support team professionals were called upon to assist the City in mitigating Royal and to recover its services. The Federal Law Enforcement was engaged and informed of the attack to provide guidance for future evidence needs. The external cybersecurity professionals provided expertise to identify, thwart, and remove Royal from the City's network while evidence was preserved and to Federal Law Enforcement of the Royal activities for possible future criminal prosecution efforts.

Notification of Information Disclosure

As obligated under State law, the City of Dallas provided notice to the State of Texas Office of the Attorney General (TxOAG). The City reported to the TxOAG that personal information of 26,212 Texas residents and a total of 30,253 individuals was potentially exposed due to the attack. The City reference to the City's notice was first published to the OAG's website on August 07, 2023. The OAG's website indicated that personal information such as names, addresses, social security information, health information, health insurance information, and other such information was exposed by Royal.

As required under federal law, and using different metrics for inclusion of individuals, the Department of Health and Human Services (HHS) was notified that the Sensitive Personal information (SPI) and Protected Health Information (PHI) of 30,253 individuals was potentially exposed by the activities of Royal. The breach submission date was recorded by HHS as of August 03, 2023.

Direct Costs of Ransomware Incident

To date, The Dallas City Council has approved a budget of $8.5 million in computer-based interdiction, mitigation, recovery, and restoration efforts directly tied to the Royal ransomware attack. This sum includes external cybersecurity professional services, identify theft and fraud protection services, and providers offering breach notification services to business partners and individuals that experienced data exposure due to the attack.

External cybersecurity professional services provided the City assistance that complemented the services provided by the City's external legal services team and that provided by federal, state, and local law enforcement agencies. The external cybersecurity professional services provided an alternative and experienced view to Royal, their activities, and relevant remediation approaches to reduce or remove damage caused by Royal. These efforts are largely complete, but an estimated final cost is to be provided by the end of 2023.

The breach notification service providers have provided data breach notifications to current, retired, and prior City personnel as well as their documented dependents when such information was exposed. The breach notification letters also offer complimentary two-year memberships in an identity protection program designed to deter individual identity theft or fraud. The cost for the first round of notifications will be provided by the end of 2023. Additional cost for this activity will be incurred as a second round of notifications is expected to occur in the fourth quarter of 2023 as additional individuals are identified. The second round of notifications is expected due to the City's detailed ongoing review of possible breached information.

To date, the City has dedicated a total of 39,590 hours towards the comprehensive remediation effort, of which ITS methodically documented 14,158 hours. Collaboratively, the City received support from external partners and contractors, who contributed an additional 1671 hours. These efforts encompassed various tasks such as the extraction of Mobile Dispatch Computer (MDC) and desktop units from fire and substations, the meticulous reconfiguration of compromised devices, the thorough reconstruction of technological infrastructure, and the ongoing vigilant

oversight of City technology environments as defined by the City's comprehensive security landscape.

As noted above, the City's current approved budget for the remediation of the Royal ransomware event is presently set to not exceed $8.5 million, The Dallas City Council was supportive and understanding in providing this initial budget amount as they understood that the attack response was ongoing and could extend significantly past the initial time and budget estimates.

City leadership is managing costs across both internal and external resources to ensure that Royal is removed from City computer and network resources. Presently, cost estimates are aligning with the initial budget approval from the Dallas City Council. The final cost analysis has not been completed at this time. The final forensic cost examination will be provided at a later date.

Section I – Royal Ransomware Incident – May 2023

This section of the document describes the ransomware incident on the City of Dallas initially identified on May 03, 2023. The incident on the City was claimed by the Royal Hacker Group and attributed by the United States Federal Bureau of Investigation (FBI) to that same group.

Royal Hacker Group

The threat actor group behind Royal ransomware first appeared in January 2022, pulling together actors previously associated with Roy/Zeon, Conti and TrickBot malware. Originally known as "Zeon" before renaming themselves "Royal" in September 2022, they are not considered a ransomware-as-a-service (RaaS) operation because their coding/infrastructure are private and not made available to outside actors [Kroll]. Backed by threat actors from Conti, Royal ransomware became one of the most prolific ransomware groups within three months of its founding. [TrendMicro]

Royal ransomware has been involved in high-profile attacks against critical infrastructure, especially healthcare since it was first observed in September 2022. Bucking the popular trend of hiring affiliates to promote their threat as a service, Royal ransomware operates as a private group made up of former members of Conti. [PA Unit42]

Since the start of 2023, Royal has escalated their attacks to focus on top tier corporations for larger ransoms. Their ransoms reportedly range from $250,000 to over $2 million. Although known for using the double extortion method of both encrypting and exfiltrating data, as of this writing the group does not have a data leak site where they publish the names of their victims. [Kroll]

Royal generally attempts to compromise victims through a BATLOADER infection, which threat actors usually spread through search engine optimization (SEO) poisoning. This infection involves dropping a Cobalt Strike Beacon as a precursor to the ransomware execution. [PA Unit42]

Royal ransomware made the rounds in researcher circles on social media in September 2022 after a cybersecurity news site published an article reporting how threat actors behind the ransomware group were targeting multiple corporations using targeted callback phishing techniques. [TrendMicro]

In its early campaigns, Royal deployed BlackCat's (another hacker group) encryptor, but later shifted to its own which dropped ransom notes like Conti's (a hacker group preceding the formation of Royal). After rebranding from Zeon to Royal, they began using the latter in its ransom notes generated by its own encryptor. [TrendMicro]

Malware

Malware, also known as malicious software or malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. [NIST 800-83r1]

End Point Response

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware. [CrowdStrike]

EDR security solutions record the activities and events taking place on endpoints and all workloads, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible. An EDR solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time. [CrowdStrike]

An EDR tool should offer advanced threat detection, investigation, and response capabilities — including incident data search and investigation alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment. [CrowdStrike]

Introduction

Early on the morning of Wednesday, May 03, 2023, the City of Dallas was directly challenged by unknown third-party aggressors which had infiltrated the City's production computing and communications environments. The aggressors, self-identified in a text file – and corroborated by the Federal Authorities– as Royal, used the organizational information it had gathered through its previous surveillance efforts to launch a ransomware attack against the City, its personnel, and various residents.

Between April 7, 2023, and May 3, 2023, Royal initiated cyber-attack operations against the City of Dallas. The initial entry point was established through the utilization of service account which connected to a server. Leveraging this initial access, the threat actor cleverly navigated the internal infrastructure of the City by exploiting legitimate third-party remote management utilities.

Prior to May 3rd Ransomware deployment the Royal group constructed what are typically known as "Beacons" using remote management utilities and legitimate pen-testing technologies to traverse the City's internal network. These actions provided staging for Royal to exfiltrate an estimated 1.169 TB of data through the initial impacted server. In addition to data exfiltration, the

Threat Actor's credential harvesting techniques. This provided a list of users, accounts, and devices.

At 2:04 AM CST on May 3, 2023, the Threat Actor deployed the ransomware onto the systems within the Dallas environment. This process of malware execution persisted until May 4, 2023, at 5:58 AM CST, marked by the final observed instance of the Royal ransomware file. Subsequent to this occurrence, no further indications of Threat Actor activities identified.

Incident Response Plan

At 8:30 AM May 3, 2023, ITS reviewed and enacted the Incident Response Plan (IRP) enabling the incident response processes for a Ransomware event. These processes included communication directives to the Mayor, City Council, and City Manager's office. The plan provides detailed steps for detecting, containing, eradicating, and recovering from the ransomware incidents. It encompasses some technical measures, while also addressing legal and regulatory considerations, public relations, and stakeholder notifications.

Intrusion and Incident Timeline

Intrusion(s) Timeline:

The following table provides further details pertaining to timelines and system recovery efforts:

Intrusion or Recovery Action/Activity	Approximate Date
Likely entry into network	April 07, 2023
Intrusion Surveillance Phase	April 07 – May 03, 2023
Account Credentials First Obtained	April 07 – May 03, 2023
Attack Beacons Installed	April 07 – May 03, 2023
Identification of Possible Attack	May 03, 2023, at 2:54 am
Security Team Begins Analysis	May 03, 2023, at 2:54 am
Likely Lateral Movement through Network Begins	May 03, 2023, at 2:54 am
Attack Mitigation Procedures Initiated	May 03, 2023, at 5:00 am
Bridge Call Opened	May 03, 2023, at 5:23 am
Sanitation Servers Identified as affected	May 03, 2023, at 5:32 am
Set of Servers Identified as Infected	May 03, 2023, at 6:00 am
Team expanded to include additional IT disciplines	May 03, 2023, at 7:00 am
Disaster Recovery Manager Notified of Ongoing Incident	May 03, 2023, at 7:46 am
Citywide Announcement of Widespread Service Outage Made to City Staff	May 03, 2023, at 8:05 am
IT Executive Leadership Notified of Ongoing Incident (CIO, CFO)	May 03, 2023, at 8:22 am
Incident Response Plan (IRP) Initiated	May 03, 2023, at 8:30 am
Communication to Federal Authorities	May 03, 2023, at 8:30 am
City's Office of the City Attorney (CAO) and Office of Emergency Management (OEM) Notified of Ongoing Incident	May 03, 2023, at 8:30 am

Intrusion or Recovery Action/Activity	Approximate Date
Preservation of Evidence Procedures Initiated	May 03, 2023, at 8:31 am
Notification to City Mayor and Council of Ongoing Incident	May 03, 2023, at 9:05 am
Preservation and Restoration of Public Safety CAD Services Set as a Priority	May 03, 2023, at 9:35 am
Infected Server Inventory Tracking Initiated	May 03, 2023, at 9:44 am
Content of Royal README.txt Message Shared with Incident Team	May 03, 2023, at 9:45 am
Critical Public Safety Servers Infected	May 03, 2023, at 11:10 am
Begin Disconnecting Servers	May 03, 2023, at 11:00 am
Rebuild of CAD Servers Begin	May 03, 2023, at 12:00 pm
News Outlets Announce the Attack to the Public	May 03, 2023, at 12:30 pm
New Servers Become Infected	May 03, 2023, at 1:22 pm
Infected Databases Identified	May 03, 2023, at 1:30 pm
Print Servers Are Disconnected	May 03, 2023, at 2:11 pm
Initial Analysis Determines 173 Servers Are Impacted	May 03, 2023, at 2:15 pm
Multiple Domains Impacted	May 03, 2023, at 2:15 pm
Assessment that Multiple Departments Impacted	May 03, 2023, at 2:15 pm
Server Reinfection Confirmed	May 03, 2023, at 5:00 pm
Additional Blocks by CrowdStrike	May 03, 2023, at 5:30 pm
Confirmation of a Development Services server infected	May 03, 2023, at 6:00 pm
Confirmed Database GIS Servers Infected	May 03, 2023, at 6:09 pm
Malware Execution Extinguished by the City	May 04, 2023, at 5:58 am
Incident Support Team (IST) Activation	May 08, 2023, at 9:00 am
Incident Support Team (IST) De-activation	June 09, 2023, at 5:00 pm

Recovery Efforts

The ITS Operational team initiated restorative actions promptly after the acknowledged occurrence of malware affecting the technological framework, crucial to the operational vitality of the City and essential for resident services. This encompassed pivotal constituents, such as technology infrastructure components and systems deemed mission critical, including Computer Aided Dispatch (CAD), 311 Services, GIS services, and City-facing communication websites, were evaluated in terms of the extent of their influence and ranked for the sequence of reinstatement. To assist in this effort, the Incident Support Team (IST) was activated to provide the responding teams with information pertinent to the recovery and restoration of specific services.

The ITS team expeditiously initiated 24/7-hour around the clock rotating scheduled with efforts for an immediate trajectory of recuperation and reconstruction, constrained within the parameters of virtualized infrastructure environments. However, these endeavors necessitated a temporary pause due to the incomplete neutralization of the malicious executable's through EDR and its ability to propagate throughout the network ecosystem. ITS instituted a temporary hold, redirecting their efforts toward eradicating the executable in question. This included implementing

security protocols aimed at eliminating remote management technologies and introducing security policies to prevent reinfection.

After confirming the efficacy of these measures through assessment against the existing IT security technologies and visibility, the restorative endeavors refocused on reinstating the mission-critical and essential infrastructural technologies necessary for application support. These restorative tasks were organized into distinct workstreams, each assigned to specialized teams dedicated to the recovery initiative. The 24/7 approach allowed for a targeted allocation of resources based on specific requirements. The teams were structured into segments comprising server/system recovery, asset retrieval, adherence to the DOD 5220.22 M standards for complete device purging to eliminate malware, and the subsequent reimagining of affected systems.

Through a collaborative and cooperative effort involving the City and external vendors, essential functionality was restored to critical systems. These systems included Computer Aided Dispatch (CAD), which regained basic functionality through a manual dispatch process, City Websites, and the Development Services Permitting System. This restoration was achieved by the conclusion of May 8, 2023. Following this initial phase of recovery, on May 11, 2023, the CAD dispatch system transitioned back to full automation for dispatch operations. Additionally, regular services such as water billing to residents, regional wants and warrants processing, and the utilization of services critical for City payment and financial processing resumed operations.

In the final analysis, it was ascertained that the event led to the impairment of 230 servers, necessitating comprehensive endeavors for their complete restoration and recovery through available backups. Among these affected servers, the City successfully retired more than 100 surplus servers hosting outdated applications, unsupported operating systems, or deemed non-essential for crucial municipal services. The cumulative count of 1,398 endpoint devices went through reconstruction directly due to the effects of the Royal ransomware infection.

Major Affected Services and Supporting Applications

The following is a table of known services and supporting applications that were affected by ransomware operations performed by the Royal Hacker Group against the City of Dallas:

Service/Application	Brief Service Description	Affected City Department
GIS	Enterprise Geographic Information System	DWU, Dallas Police, Dallas Fire-Rescue, Other
Fusion Center	Dallas Police multi-source intelligence fusion solution	Dallas Police
Computer-Aided Dispatch (CAD)	Emergency Services Computer-Aided Dispatch Service	Dallas Police, Dallas Fire-Rescue, Dallas EMS, Dallas Marshals
Report Management Service/Code Compliance Management System	DPD-Web Report Management System (RMS) and Code Compliance Management System (CCMS)	Dallas Police, Code Compliance Services

Service/Application	Brief Service Description	Affected City Departments
Public Safety File Shares	Remote data stores (server-based, cloud-based) for individual and group use	Dallas Police
Surveillance Cameras Management System	Street cameras used for Police surveillance of a venue (e.g., Fair Park) or of a location (e.g., Starlight program)	Dallas Police
Animal Management Services	Animal and animal support monitoring, system management solution	Dallas Animal Shelter
Building Permitting System	Building Inspection plan and permitting management solution	Development Services
Secure File Transfer Service	Secure file transfer protocol server physically present within the City Data Center	Information & Technology Services (ITS), all other City departments
Library Management Service	Dallas Library book, media, and artifact management solution	Dallas Library
Warrants Management Service	Court ordered warrant management solution	Dallas Police, Dallas Marshals, Dallas Municipal Courts, other local agencies interoperating with City warrant resources.
Remote Water Meter Reading Service	Remote water meter reading technology supporting Dallas Water Utilities billing and operations divisions	Dallas Water Utilities
Payment Card Acceptance Solution	Payment card acceptance services supporting Dallas Water Utilities Billing solution operations.	Dallas Water Utilities, other departments using ePay for payment acceptance.
Public Safety Mobile Data Computer Services	Mobile Data Computer (MDC) predominately used by polices, fire, Emergency Medical Services (EMS), and emergency services for remote digital communications between deployed assets and between deployed assets and City Computer-Aided Dispatch Services.	Dallas Police, Dallas Fire-Rescue, Dallas EMS, Dallas Emergency Services, and other City departments and agencies using Mobile Data Computer for the capture and presentation of service information.
Alerting Service	Fire Station Alerting solutions designed to reduce response times and improve first responders' quality of life.	Dallas Fire-Rescue
Secure Print Services	Citywide secure print services used to monitor and manage print of secure documents at designated print stations.	All departments.
Fax Services	These applications and systems securely transmit paperless, digital faxes. This digital faxing solution greatly reduces the faxing costs by connecting to onsite analog or	All departments.

Service/Application	Brief Service Description	Affected City Departments
	digital telephony, voice-over-IP or the cloud.	

Systems and Services Restoration May 09, 2023, through June 13, 2023

The following chart represents the systems and services restoration checklist that was leveraged during the recovery efforts. Green – indicates completed, tested, and returned to production, Yellow – indicates Completed and in testing, White – indicates staged and currently being built.

Date Restored	Restoration Phase	Color Status	Application/Service
5/5/2023	Phase 1	Green	Computer Aided Dispatch
5/8/2023			Incident Support Team Activated
5/9/2023	Phase 1	Green	Financial Server
5/9/2023	Phase 1	Green	City Website
5/9/2023	Phase 1	Green	Development Service System
5/10/2023	Phase 1	Green	Police/Fire Automated Dispatch
5/11/2023	Phase 2	Green	City Controller System
5/11/2023	Phase 1	Green	Payment Card Acceptance Solution
5/11/2023	Phase 2	Green	Warrants Management Service
5/11/2023	Phase 1	Green	Cyber Security Server
5/11/2023	Phase 1	Green	Remote Meter Reading Service
5/12/2023	Phase 1	Green	Records Management System
5/15/2023	Phase 2	Green	Dallas Police Crime System
5/15/2023	Phase 2	Green	Code Management Service
5/15/2023	Phase 1	Green	Field Base Reporting Service
5/15/2023	Phase 1	Green	Citizen Request Management Service
5/16/2023	Phase 3	Green	Dallas Police Crimes Server
5/16/2023	Phase 2	Green	Animal Management Service
5/16/2023	Phase 3	Green	Financial Management Service
5/16/2023	Phase 2	Green	Dallas Fire Rescue System
5/17/2023	Phase 4	Green	Application and Data Workflow Orchestration
5/17/2023	Phase 2	Green	City Secretary System
5/17/2023	Phase 2	Green	Sanitation System
5/19/2023	Phase 4	Yellow	Virtual Viewer
5/22/2023	Phase 5	Green	Dallas Police Narcotic System
5/22/2023	Phase 4	Green	Dallas Fire Rescue Incident System
5/22/2023	Phase 4	Green	City Attorney System
5/22/2023	Phase 5	Green	Evidence Management Service
5/22/2023	Phase 5	Green	Dallas Police Safety Servers
5/22/2023	Phase 2	Green	Dallas Fire Rescue Safety Servers

Date Restored	Restoration Phase	Color Status	Application/Service
5/22/2023	Phase 5	Green	Dallas Police System
5/22/2023	Phase 4	Green	Virtual Viewer Service
5/23/2023	Phase 4	Green	Print Server
5/24/2023	Phase 2	Green	Financial Service Reporting Service
5/24/2023	Phase 5	Green	Merchant Accounting Software
5/25/2023	Phase 4	Green	Life Event Certificate Management Service
5/25/2023	Phase 4	Green	GIS Water Server
5/26/2023	Phase 1	Green	Court Management System
5/26/2023	Phase 3	Green	Dallas Police Enhanced Neighborhood System
5/30/2023	Phase 5	Green	Payment Management System
5/30/2023	Phase 5	Green	Dallas Police Specialized Server
5/30/2023	Phase 3	Green	Dallas Police Impound System
5/30/2023	Phase 3	Green	Internal Workflow Management Service
5/31/2023	Phase 5	Green	Vital Statistics
6/2/2023	Phase 3	Green	Court Docket Management System
6/2/2023	Phase 5	Green	Dallas Fire Specialized Server
6/2/2023	Phase 4	Green	Dallas Police Warrants System
6/6/2023	Phase 6	Green	Employee Management System
6/6/2023	Phase 6	Green	Survey Management Service
6/8/2023	Phase 5	Green	Dallas Police Traffic Data System
6/8/2023	Phase 5	Green	Vehicle Management Safety Report System
6/13/2023	Phase 6	Green	Back-Up Site Servers
6/13/2023	Phase 6	Green	Dallas Water Billing Payment File Service
6/13/2023	Phase 6	Green	Street Maintenance and Repair Management Service
6/13/2023	Phase 6	White	Financial Services Management Service
6/13/2023	Phase 4	Yellow	File Share Resources
6/13/2023	Phase 6	Green	GED Testing Management Service
6/13/2023	Phase 3	Yellow	Dallas Fire Rescue Personnel Server
6/13/2023	Phase 3	White	Library System
6/13/2023	Phase 2	Yellow	Library Resource Reservation Service
6/13/2023	Phase 4	Yellow	Building Services Server
6/13/2023	Phase 6	Yellow	Library Resource Reservation Service
6/13/2023	Phase 2	Yellow	Library Resource Management Service
6/13/2023	Phase 5	Yellow	Dallas Fire Rescue Case Entry System
6/13/2023	Phase 5	White	Public Safety Back-up Site Server
6/13/2023	Phase 6	Yellow	Security Gate Server
6/13/2023	Phase 4	Yellow	Stormwater Management Service
6/13/2023	Phase 6	Yellow	Development Services System
6/13/2023	Phase 6	Green	Waste Management Server

Section II – Operational Risk Factors Conducive to the Incident

This section of the document details internal and external risk factors conducive to the Royal Ransomware incident upon The City of Dallas. The Royal Ransomware incident upon the City began early on the morning of Wednesday, May 03, 2023.

City Under Constant Cyber Attack

The City of Dallas rejects millions of questionable inbound Internet network connection requests monthly. These requests are for a variety of reasons; many having legitimate reasons with most generally considered to be malicious in nature. The City is a large municipality and may be considered a potential target by cybercriminals because most municipalities fail to adequately secure its network resources. Additionally, the City manages, operates, and maintains several critical infrastructure targets that are appealing to cybercriminals (e.g., potable water, storm water management, flood water management, airports, aviation management systems, first-responder communications networks, emergency management operations, street management systems [e.g., streetlights, traffic lights])

The City of Dallas attempts to manage access to its network resources (e.g., servers, routers, load balancers) using the latest-generation firewall technology. Physical firewall devices and appliances are deployed, managed, and operated at Dallas City Hall. The City uses core firewalls for enterprise network operation and for security purposes. Perimeter firewalls are managed and operated in support of public internet access. Despite the use of latest-generation technology, the City is subject to 24/7 intrusion attempts requiring the City to use a multitude of security technologies both hardware and software based to ensure that only authorized traffic may access and enter the City's network.

The City is a Conglomeration of Missions

The City of Dallas is comprised of over 40 different departments, multiple offices, and several boards that support the many different missions assigned to it. Each department, office, and board effectively manage its own activities in support of assigned missions. This diversity of approaches provides diversity in approach but also introduces a certain lack of organizational cohesion.

A recent City organization chart identified eight high level portfolios individually managed by Deputy City Managers and Assistant City Managers. These portfolios included Housing & Homeless Solution; Public Safety; Economic Development; Workforce, Education, & Equity; Transportation & Infrastructure; Quality of Life, Art & Culture; Environment & Sustainability; and Government Performance & Financial Management. The missions and mission objectives of each of these portfolios is as diverse as the next.

As stated previously, this creates a sizable attack surface for the data City departments utilize. Departments and residents rely daily use of Critical Infrastructure, Payment Cards, Health Care, and resident's personal information to maintain continuity.

Technical Debt

The need to maintain current systems technical debt represents the compromises and suboptimal solutions that can emerge during the development and maintenance of software systems, is normal and unavoidable. [Gartner] ITS has recognized the presence of technical debt in its Technology Accountability Report (TAR) and initiated the modernization process. There is a clear requirement for the City to persist in these endeavors. These compromises may pose challenges for securing the environment. While they may provide short-term benefits, they can lead to risk. In terms of cybersecurity, technical debt can potentially aid the success of cyber events by virtue of inadequate built-in security measures in newer systems and unremedied vulnerabilities.

Vulnerabilities

Correspondingly, for all organizations, vulnerabilities and remote technology management is key to reducing risk in the City. Vulnerabilities may emerge during the development processes, making them universal targets for hackers who continually search for such weaknesses to exploit them for their own purposes. Effective patch management, involving the routine application of software and system updates to address known vulnerabilities and enhance software security, is paramount in safeguarding against ransomware attacks. Protocols are susceptible due to their less modern architectures and security standards, which often lack modern encryption, authentication mechanisms, and defenses against evolving cyber threats. These protocols frequently persist with unresolved vulnerabilities, leaving them exposed to exploitation by malicious actors. [CISA]

All organizations need to reduce risk of entry points for attackers to infiltrate systems and spread ransomware throughout networks. The absence of contemporary security features, coupled with attackers' ability to exploit these vulnerabilities through specialized techniques, heightens the risk of successful cyber intrusions. [FBI] After threat actors successfully achieves code execution on a device or gains network access, they can proceed to deploy ransomware. It's worth noting that these infection methods have likely maintained their popularity due to the surge in remote work and schooling since 2020, [CISA]

Section III – Factors Directly Mitigating the Impact of the Incident

This section of the document details internal and external factors believed to have directly mitigated the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident upon the City has been identified as beginning early on the morning of Wednesday, May 03, 2023.

Introduction

This section of the After-Action Report (AAR) introduces and describes those factors that had directly impact upon ransomware incident mitigation.

Though interdiction, mitigation, and restoration of services was an “All Hands!” 24/7 effort, there were instances where the actions, activities, and ownership of just a few prevented the City Production computing and communications infrastructure from being dramatically damaged by Royal.

The City has developed and maintains a dynamic five-year strategic cyber security plan. The strategies identified in the plan rest upon a set of guiding principles, objectives, and priorities for cybersecurity that should benefit the City of Dallas’ over the coming three-to-five-year period. These principles, objectives, and priorities are selected from research and guidance from governmental authorities such as MITRE and the National Institute of Standards and Technology (NIST). It is believed that the use of this foundation will provide the City with the ability to appropriately select, deploy, manage, and operate cyber security technologies to effectively address, manage, and mitigate City IT vulnerabilities and threats.

The size and scope of the cybersecurity program has been increased to achieve the City’s strategic goals, including such efforts as improved public safety, critical infrastructure, and smarter cities. In addition to the important projects and security systems that will carry over from the last year’s improvements, new initiatives will be undertaken over the next three to five years to address emerging threats. This is to expand focus on identifying, protecting, detecting, responding, and recovering activities for the City of Dallas.

A threat environment can be managed and mitigated through identification, development, and use of appropriate cyber security initiatives. The City’s cyber security strategic plan identifies several sets of goals and addresses the City’s threat environment through use of appropriate cyber security initiatives supported by relevant investments in cyber security technology selected to protect the City’s information resources and assets.

The program roadmap, objectives, and intended outcomes have been identified and assessed by mature NIST functional families. This framework facilitates the monitoring and evaluation of the City’s efforts to implement cyber security controls and reduce risk.

Since 2019 the City of Dallas has evaluated the maturity of its Cybersecurity program. The evaluation utilizes NIST’s Common Security Framework (CSF) along with the application of the Capability Maturity Model Integration (CMMI) framework. This periodic evaluation provides the

City's Cybersecurity program with a direct view into essential areas of program operation and gives insight into five functional areas of cybersecurity (Identify, Protect, Detect, Respond, Recover) through inspection of City cyber security performance with 22 categories and 98 subcategories of management and control.

The City's Cybersecurity program is evaluated from Policy, Practice and/or Technology perspectives. These various perspectives assist City leadership in determining where investments should be made to continuously improve the City's ability to respond to and recover from any cyber security event.

Increased City InfoSec Investment

The City of Dallas has continuously augmented its commitment to Information Security (InfoSec) tools and solutions since the year 2019. These investments have bolstered and expanded the stratified strategy employed for cyber and information security. In 2019, the expenditure on IT security accounted for approximately 2.5% of the total IT budget. In contrast, as indicated by the projected budget for the 2023-24 fiscal period, a recommendation from the City Manager, coupled with the City Council's endorsement, is poised to elevate this allocation to nearly 10%. This substantial augmentation has enabled the City to curtail risk exposure and enhance the resilience of its technological infrastructure.

Despite the notable increase in overall expenditure, the maturation of the IT Operational program necessitated a comprehensive strategy and implementation methodology capable of accommodating the intricacies inherent to each supplemental IT security technology demand. The encumbrance of technological debt and the unwarranted intricacy inherent legacy networks introduce difficulties in adequately fortifying the network. Acknowledging the imperatives of the threat landscape becomes apparent that entities must empower all facets of a framework through meticulous planning, thereby safeguarding the infrastructure while simultaneously preparing for the expeditious execution of response and recovery measures.

Periodic Federal Agency Security Assessments

At intervals, the City of Dallas enters into arrangements with the United States Department of Homeland Security (DHS) to evaluate the security status of municipal information resources, including but not limited to its network and computer-based services. As recently as February 2023, the City finalized a fortnight-long collaboration with the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a Security Penetration Test, commonly denoted as a "Red Team exercise." This evaluation comprehensively examined the City's infrastructure from both external and internal vantage points. These collaborative undertakings have yielded substantial insights into the cybersecurity posture; pinpointing areas necessitating enhancement and remediation.

Zero Trust Technologies

The City's stratified strategy for cybersecurity and information security is synergistically reinforced by a Security Program that actively involves City personnel, facilitating secure autonomous work practices. Over the course of the previous five years, the City has implemented the subsequent security governance, cyber, and information security technologies in harmony with numerous cybersecurity directives at the Federal level. Concurrently, IT has introduced and administers zero-trust network technologies to enhance resource access and management within the network. A substantial proportion of these technologies harness Artificial Intelligence-driven systems to aid in detecting and mitigating conceivable threats.

1. System backups – following events in 2021 comprehensive and precisely coordinated data safeguarding structure, seamlessly integrating automated regular backups, encrypted storage spread across redundant locations, versioning functionalities, offline storage mechanisms, expedient recovery protocols, regular testing procedures, sustained historical data retention, lucid documentation, and strategic alignment with business continuity requisites. This all-encompassing methodology guarantees the conservation, integrity, and swift restoration of vital information and system recovery.

2. Identity and Access Management platforms – the City has deployed and operates a cloud-based identity and access management platform. Such platforms allow the City to centralize, manage, and secure user authentication into City applications/solutions to over 200 applications. The platform provides multifactor authentication to assist in only allowing authorized personnel to access and use City applications/systems.
3. Real-time Threat Detection – the City has deployed and operates real-time thread detection solutions. Using network detection and response technologies, the City can identify and respond to security incidents as they are happening. The technologies use "cloud-scale machine learning" (ML) algorithms and rule-based techniques to detect behaviors, anomalies, and software vulnerabilities to provide security recommendations to City staff.

4. Network Behavior Analysis - The City has deployed and operates technologies built upon machine learning technologies that allow the City to identify if malevolent traffic flow within City networks. If such behavior is identified, the technologies can rapidly slow or remove such traffic from City networks.

5. Security Information and Event Management (SIEM) – The City has deployed and operates security information and event management technologies that allows the City to have real-time visibility into network and server events. The City has also engaged a managed security service provider (MSSP) to assist it in the monitoring and management of the large volumes of data captured by its security information and event management solutions.

6. FAIR Risk Assessments – The Factor Analysis of Information Risk (FAIR) is a taxonomy of the factors that contribute to risk and how they affect each other. FAIR is primarily concerned with determining accurate probabilities for two risk components of data loss events: frequency and magnitude. FAIR complements other risk methodologies by providing a way to produce consistent, defensible belief statements about risk.

7. HIPAA Risk Assessment – HIPAA risk assessments are a method to identify areas where an organization's protected health information (PHI) could be at risk. Factors considered in a HIPAA breach risk assessment include the nature and extent of breached PHI, the types of identifiers and the likelihood of re-identification, the unauthorized person who accessed or used the breached PHI, whether PHI was actually acquired or viewed, and the extent to which the risk to PHI is present.

8. NIST 800-171 Data Confidentiality Assessments – The NIST 800-171 standard establishes the base level of security required of computing systems that use or store confidential unclassified information (CUI). All organizations that access U.S. government date must comply with NIST standards. As this is a given, an 800-171 risk assessment can identify if an organization adequately safeguards information in a compliant manner relative to the current version of NIST 800-171.

9. Recovery Planning – Recovery Planning aligns with the City's primary cybersecurity goals, to identify and become proactive toward potential recovery efforts. The City plans to improve the maturity of its risk management processes and procedures. These processes and procedures will include identification of any potential deficiencies within recovery planning. Continued efforts to include many tabletop exercises and technical testing of planned recovery effort will contribute to a more resilient recovery when needed.

10. Privacy Risk Management – Privacy Risk Management describes a method for managing the risks that the processing of personal data can generate to individuals. In data privacy risk management, the impacted asset would be personal data, and its classification level. Privacy risk assessment is a process for identifying and evaluating privacy risks, which organizations can use to build customer trust by developing more effective solutions to protecting individuals' privacy when designing or deploying systems, products, and services that process data. This process assists the City to bring privacy into parity with their broader portfolio of enterprise risks.

11. Governance, Risk, and Compliance (GRC) – Governance, Risk, and Compliance (GRC) is a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organization's governance and risk management with its technological innovation and adoption. Companies use GRC to achieve organizational goals reliably, remove uncertainty, and meet compliance requirements.

12. Security Operations Center (SOC) – The City's Security Operations Center is where security technologies are applied and used to identify remediation challenges to the security of City information resources. The City's SOC provides visibility into distinct security challenges and coordinates the remediation efforts to reduce or eliminate those security challenges.

13. Business Impact Analysis (BIA) – A Business Impact Analysis (BIA) attempts to predict the consequences of disruptions to business function processes due to loss of information

technology. The BIA attempts to gather information needed to develop recovery strategies. When developing a BIA, potential loss scenario should be identified using a risk assessment methodology.

14. Periodic Disaster Recovery Tabletop Exercises –Tabletop exercises are discussion-based group sessions where team members meet to discuss their assigned roles and responsibilities in the event an organizational disaster is declared. A facilitator guides participants through discussions of one or more potential scenarios so that participants can visualize how they would respond to the scenario. An additional discussion is held after the scenario has been resolved to identify lessons learned and to discuss the possibilities of better scenario responses. These exercises are held on a periodic basis.
15. Configuration Management Database (CMDB) – The City is in the middle of assessment and implementation to track and better identify assets and their current configurations. This deployment operates a cloud-based Configuration Management Database (CMDB) used to store deployment and usage information about software and hardware assets. Including both, software asset management solution that allows the City to identify, define, track, and manage the City's 860+ software assets and hardware asset management solution.
16. Vulnerability Management Solutions – The City has deployed and operates various vulnerability management technologies and solutions to identify and remediate both known and potential vulnerabilities associated with City hardware and software resources. The management of vulnerabilities allows the City to identify, define, prioritize, and remediate according to the City's perception of possible threats to its vulnerability pool.
17. Microsegmentation – The City has deployed a network management technology that allows the City to manage relatively small segments of its network separately than other segments of its network. This technology allows the City to attribute special network characteristics to unique portions of its network relative to other small segments and to the overall network as a whole.
18. Crisis Communications – The City has begun implementing ITS Crisis communication technologies to allow ITS to better report and communicate within the department and City staff. These technologies will be leveraged for both the internal response as well as recovery.

The City of Dallas plans to acquire, deploy, manage, and operate the following cybersecurity technologies over the coming five-year period:

1. Security Orchestration, Automation and Response (SOAR) – Security Orchestration, Automation and Response is a group of cybersecurity technologies that allow organizations to respond to some incidents automatically. It collects inputs monitored by a security operations team and helps define, prioritize, and drive standardized incident response activities.

2. Application Performance Management – The City has deployed and operates application performance management technologies that allows the City to monitor and manage the availability of software applications. The goal of such technology is to ensure appropriate levels of application services are provided to the City.

3. Network Performance Management – The City has deployed and operates network performance management technologies that allow the City to monitor and manage the service capacity of its various networks. The technologies allow the City to determine in advance if any service capacity challenges may present themselves to City staff during the performance of their duties.

4. Industrial Control Systems Cybersecurity – The City has deployed and operates intrusion detection and intrusion protection systems in support of City Industrial Control Systems (ICS). These systems assure the secure operation of industrial control network components and emerging Internet of Things (IoT) control points. This technology may be used to protect City operated critical infrastructure such as aviation environment assets, streets management technology (e.g., smart street lighting, traffic light systems).

The City's current IT security program played a pivotal role in effectively mitigating the threat of ransomware attacks by employing a multifaceted and proactive approach. First, the program emphasizes robust cybersecurity measures across various layers of the organization's infrastructure. It involves the implementation of advanced intrusion detection systems, firewalls, and network segmentation to isolate critical systems from potential threats.

Secondly, a focus on comprehensive user education and awareness. By consistently training employees and IT teams about the risks associated with ransomware, the program empowers them to recognize and respond to the event quickly and with purpose to remediation. This heightened awareness enhances the City's ability to prevent ransomware from gaining more paralyzing foothold for a lengthy timeframe. Moreover, employees are educated on the importance of regular data backups and secure data storage practices, ensuring that critical information can be restored in the event of an attack, thus reducing the likelihood of succumbing to ransomware extortion.

In essence, a diligent IT security program combines advanced technological safeguards limit the impact for ransomware and assist in expediting the recovery. This approach not only prevents initial infection but also facilitates swift detection and response, minimizing the potential impact and disruption caused by ransomware attacks.

Section IV – Findings

This section of the document describes findings pursuant to the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident has been identified as beginning early on the morning of Wednesday, May 03, 2023.

The following findings were the result of the City's engagement of the Royal Hacker Group beginning the morning of Wednesday, May 03, 2023.

Competent Incident Response Plans

The City of Dallas has managed and maintained Security Incident Response Plans for quite some time. Since 2019, the Department of Information and Technology Services (ITS) and its predecessor, the Department of Communications and Information Services (CIS) has engaged cybersecurity experts and federal agencies to assist in developing, managing, and maintaining current, relevant Incident Response Plans (IRP). The plans considered security incidents from a variety of sources and perspectives and identified approaches to remediating and resolving security incidents in a manner consistent with City goals and objectives for information resource management.

Security Incident Staff Periodically Exercised

The City of Dallas understands that plans without preparation are generally unproductive. To adequately prepare incident response staff for a variety of possible security incidents, the City periodically performs tabletop exercises, functional testing, and continuous updates to the Incident Response Plan. These exercises are performed to expose City staff to various attack vectors and possible attack interdiction techniques before they are needed to defend City information assets and resources. It is believed that the periodic tabletop exercises facilitated the prompt attention to the Royal ransomware attack and assisted staff coordinate during the actual threat to the City.

Identification

For 2023, the typical overall mean time to identify a data breach is 204 days [IBM]. This has been consistent over the past several years. Cybercriminals have become increasingly sophisticated in their methods of infiltrating systems and stealing sensitive information. This sophistication can contribute to the prolonged period it takes to detect these breaches, as attackers exploit vulnerabilities and use advanced techniques to avoid detection. The City's commitment to a cybersecurity program can directly attribute to the mean time of 27 days to identification, equating to a more "smash and grab approach".

Aggressive Incident Response

The City's response to Royal's ransomware incident of May 03, 2023, was considered both internally and externally as quite aggressive. Though there was an initial delay to identifying and

understanding that an attack against the City was underway, City leadership was able to turn a large number of resources toward the challenge in a very short period of time. As the timeline table displayed in Section II above indicates, Organizations typically require an average of 73 days to contain breaches in 2023, while requiring just 70 days on average in 2022 [IBM]. The City was effective at containing the issue in 1 day.

Vigorous measures were undertaken to ensure an uninterrupted round-the-clock commitment to the restoration of mission critical services for City critical infrastructure, public communications and essential services. The celerity of service restoration was of paramount importance. Both technology vendors and the cybersecurity experts contracted by the City expressed their commendation for the City's endeavors to prevent and eliminate unauthorized access by Royal to City information assets. Additionally, the City's protocols for service restoration also garnered appreciation.

Prompt Application and Service Restoration the recovery endeavor successfully attained a restoration rate exceeding 90 percent within an 18-day period. Through their concerted endeavors, methodical planning, and prompt execution, essential systems were successfully rehabilitated, thereby enabling the significant reinstatement of crucial services. It is important to note that this swift advancement was achieved despite the necessity to rebuild over 230 servers and 1,168 workstations. This rapid progress unarguably attests to the tenacity and resourcefulness of the recovery teams, underscoring their steadfast dedication to expeditiously surmount challenges and restore a state of normalcy.

Substantial Cybersecurity Investments Made in Advance of Incident

The City of Dallas understood that the information and cyber-security landscapes were quickly changing and began adopting and deploying risk-driven security technology in 2019. These investments correlated to the NIST Cybersecurity Framework (CSF) first published in 2014 and revised in 2018. The investments correlated to the five functional areas of the CSF: Identify, Protect, Detect, Respond, and Recover.

Relevant investments were made in technology areas such as Identity and Access Management (IAM), End-Point Detection and Response, Managed Detection and Response (EDR/MDR), Network-Centric Threat Detection and Response (NDR). The City’s financial dedication to cybersecurity growth from $3.4 million in 2019 to $7.8 million in 2023 with an additional $ 8.5 million for the event, is a direct contribution to protection of the resident’s data and assets. In addition, City staff dedicated to cybersecurity has grown from 18 full time resources in 2020 to 35 resources to manage security, compliance, and risk.

Section V –Recommendations

This section of the document describes recommendations to City management and operation teams in the context of the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident upon the City has been identified as beginning early on the morning of Wednesday, May 03, 2023.

Perform a Cybersecurity Program Review

The City of Dallas has an active Cybersecurity Program. This program involves various security initiatives and involves City personnel from various departments and personnel levels. The consultants recommended that the program review focus on the identification of current state program gaps. The recommended review should include an in-depth analysis of people, processes, and technologies to gain an understanding of breakdowns in capabilities against real-world techniques used by attackers. The recommendation that the output of the review be used to develop and implement a threat-centric and risk-based cybersecurity program.

Privacy/Security Risk Assessment (Long-Term)

ITS Risk Management and Privacy teams shall conduct departmental Privacy and Security Risk Assessments. This Assessment is imperative to systematically identify, evaluate, and mitigate potential risks associated with the collection, processing, and storage of personal and sensitive information. By assessing the department's data management practices, technical safeguards, and compliance with relevant regulations. The Assessment provides a robust foundation for implementing tailored security measures. The outcomes of this Assessment will enable the organization to proactively address vulnerabilities, educate City employees, protect against data breaches, and ensure compliance with legal and regulatory obligations. Furthermore, the Assessment's insights will facilitate informed decision-making, allocate resources judiciously, and establish a defensible position against potential legal liabilities stemming from data privacy and security breaches.

Improve Data Backup and Restoration Processes

Application, service backup, and restoration processes are not always emphasized as a component of information resource deployment into the City's production environments. This lack of emphasis causes applications and services to be introduced into City production environments without appropriately tailored backup, recovery, or restoration processes and procedures; instead relying upon generic approaches to these application and service activities. It is recommended that all applications and services be required to have appropriately tailored backup, recovery, or restoration processes and procedures defined before an application or service can be introduced into a City production environment.

Harden Network and Compute Assets

Information Technology asset resources (e.g., servers) are not consistently managed and operated in a hardened state. Resource hardening is a set of processes or procedures that attempts to protect IT resources against cyberattacks by reducing its attack surface.

Reduce, Eliminate and Manage Technical Debt

Many City applications and services are not operating the most current versions of the underlying software. Several significant applications and services are operating on software versions that are no longer supported by software manufacturers and vendors. This condition causes a mismatch between the City's ability to deliver technical services in support of City and individual department business missions and cybersecurity best practices to discourage or defeat potential Threat Actor intrusions. It is recommended that City leadership participate in ongoing prioritization of technical services so that technical debt is eliminated or focused to low priority City applications and services.

Update to the Incident Response Plan

The City's incident response plan shall continuously be reviewed because of this or any event and as technology evolves. The Plan serves as a pivotal framework guiding an organization's approach to identifying, assessing, and mitigating security incidents. However, after major incidents, lessons learned become important to understand what worked and what did not according to the plan. This allows ITS to incorporate current threat intelligence, advanced mitigation strategies, and industry best practices. The updates are imperative to ensure the Plan's continued relevance and effectiveness in addressing emerging cyber threats. By continuously maintaining the Plan the City is allowed to improve not only its ability to safeguard sensitive information but also demonstrates a proactive commitment to mitigating legal and financial risks associated with potential security breaches and recovery efforts.

Comprehensive Plan of Actions and Milestones (POAM)

These recommendations shall be consolidated into a comprehensive Plan of Actions and Milestones (POAM) to track remediation. This strategic document serves as a roadmap for implementing the identified security and privacy measures in a structured and organized manner. Each recommendation will be assigned a specific action to be undertaken, accompanied by a corresponding milestone, which outlines a target completion date or timeframe. The POAM will outline the responsible individuals or teams accountable for executing each action item and will delineate the required resources, budget, and dependencies for successful implementation. Additionally, the POAM will provide a mechanism for ongoing tracking, monitoring, and reporting of progress toward achieving the established milestones.

Section VI – Appendices

This section of the document provides appendices of information relevant to the Royal Ransomware incident upon the City of Dallas. The Royal Ransomware incident upon the City has been identified as beginning early on the morning of Wednesday, May 03, 2023.

Appendix A – Glossary

This section of the document provides a glossary of terms used within this document.

Term	Definition
AAR	After-Action Report
CIO	Chief Information Officer / Director of ITS
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CIS	Department of Communications and Information Technology (a forerunner to ITS)
CISA	Cybersecurity & Infrastructure Security Agency
ITS	Department of Information & Technology Services
MITRE	MITRE Corporation
NIST	National Institute of Standards and Technology
Targeted Risk Assessment (TRA)	An assessment of risk targeted to a specific activity dependent upon the vulnerabilities, threats, and impact caused by a successful impact of a threat through exploitation of identified vulnerabilities.
TxOAG	The State of Texas Office of the Attorney General

Appendix B – Information Sources

This section of the document provides a listing of informational sources used in the development of this document.

Identifier/Tag	Information Source
AWS	Amazon Web Services
CrowdStrike	CrowdStrike
Forrester	Forrester
Fortra	Fortra
Gartner	Gartner
HHS	US Department of Health and Human Services
IBM	IBM Corporation
ITIL2	Information Technology Infrastructure Library, Version 2, 2004
ITIL3	Information Technology Infrastructure Library, Version 3, 2007
ITIL4	Information Technology Infrastructure Library, Version 4, 2019
MITRE	MITRE Corporation
NIST	National Institute of Standards and Technology
OpenAI	The Open AI Foundation
PA Unit42	Palo Alto Unit 42
UH	University of Houston