

RECEIVED

Public Notice

2022 FEB- 25 PM 3:28

220240

CITY SECRETARY
DALLAS, TEXAS

City of Dallas

1500 Marilla Street,
Council Chambers, 6th Floor
Dallas, Texas 75201

POSTED CITY SECRETARY
DALLAS, TX



Ad Hoc Committee on General Investigating and Ethics

March 1, 2022
2:00 PM

REVISED

2021 CITY COUNCIL APPOINTMENTS

COUNCIL COMMITTEE	
ECONOMIC DEVELOPMENT Atkins (C), Arnold (VC), McGough, Narvaez, Resendez, West, Willis	ENVIRONMENT AND SUSTAINABILITY Blackmon(C), Ridley (VC), Arnold, Bazaldua, Resendez, Schultz, West
GOVERNMENT PERFORMANCE AND FINANCIAL MANAGEMENT Mendelsohn (C), Willis (VC), Atkins, Bazaldua, McGough, Ridley, West	HOUSING AND HOMELESSNESS SOLUTIONS Thomas (C), Moreno (VC), Arnold, Blackmon, Mendelsohn, Ridley, Schultz
PUBLIC SAFETY McGough (C), Mendelsohn (VC), Atkins, Moreno, Resendez, Thomas, Willis	QUALITY OF LIFE, ARTS, AND CULTURE Bazaldua (C), West (VC), Arnold, Blackmon, Narvaez, Ridley, Thomas
TRANSPORTATION AND INFRASTRUCTURE Narvaez (C), Atkins (VC), Bazaldua, Mendelsohn, Moreno, Schultz, Willis	WORKFORCE, EDUCATION, AND EQUITY Schultz (C), Thomas (VC), Blackmon, McGough, Moreno, Narvaez, Resendez
AD HOC JUDICIAL NOMINATING COMMITTEE Resendez (C), Arnold, Bazaldua, Ridley, Thomas, West, Willis	AD HOC LEGISLATIVE AFFAIRS Atkins (C), McGough, Mendelsohn, Narvaez, Willis
AD HOC COMMITTEE ON COVID-19 RECOVERY AND ASSISTANCE Thomas (C), Atkins, Mendelsohn, Moreno, Ridley	AD HOC COMMITTEE ON GENERAL INVESTIGATING & ETHICS Mendelsohn (C), Atkins, Blackmon, McGough, Schultz

(C) – Chair, (VC) – Vice Chair

Handgun Prohibition Notice for Meetings of Governmental Entities

"Pursuant to Section [30.06](#), Penal Code (trespass by license holder with a concealed handgun), a person licensed under Subchapter H, Chapter 411, Government Code (handgun licensing law), may not enter this property with a concealed handgun."

"De acuerdo con la sección [30.06](#) del código penal (ingreso sin autorización de un titular de una licencia con una pistola oculta), una persona con licencia según el subcapítulo h, capítulo 411, código del gobierno (ley sobre licencias para portar pistolas), no puede ingresar a esta propiedad con una pistola oculta."

"Pursuant to Section [30.07](#), Penal Code (trespass by license holder with an openly carried handgun), a person licensed under Subchapter H, Chapter 411, Government Code (handgun licensing law), may not enter this property with a handgun that is carried openly."

"De acuerdo con la sección [30.07](#) del código penal (ingreso sin autorización de un titular de una licencia con una pistola a la vista), una persona con licencia según el subcapítulo h, capítulo 411, código del gobierno (ley sobre licencias para portar pistolas), no puede ingresar a esta propiedad con una pistola a la vista."

"Pursuant to Section [46.03](#), Penal Code (places weapons prohibited), a person may not carry a firearm or other weapon into any open meeting on this property."

"De conformidad con la Sección [46.03](#), Código Penal (coloca armas prohibidas), una persona no puede llevar un arma de fuego u otra arma a ninguna reunión abierta en esta propiedad."

Note: A quorum of the Dallas City Council may attend this Council Committee meeting.

The Ad Hoc Committee on General Investigating and Ethics meeting will be held by videoconference and in the Council Chambers, 6th Floor at City Hall.

The public is encouraged to attend the meeting virtually; however, City Hall is available for those wishing to attend the meeting in person following all current pandemic-related public health protocols.

The following videoconference link is available to the public to listen to the meeting and Public Affairs and Outreach will also stream the City Council Briefing on Spectrum Cable Channel 95 and bit.ly/cityofdallastv:

<https://dallascityhall.webex.com/dallascityhall/onstage/g.php?MTID=e2f5dd2b3e8a50c2652773a578e203741>

Call to Order

[22-608](#)

Discussion of the Report to the City of Dallas Regarding the City's March 2021 Data Loss Incident
[Erin Nealy Cox, Attorney, Partner at Kirkland & Ellis]

Attachments: [Report to the City of Dallas - March 2021 Data Loss Incident](#)

ADJOURNMENT

EXECUTIVE SESSION NOTICE

A closed executive session may be held if the discussion of any of the above agenda items concerns one of the following:

1. seeking the advice of its attorney about pending or contemplated litigation, settlement offers, or any matter in which the duty of the attorney to the City Council under the Texas Disciplinary Rules of Professional Conduct of the State Bar of Texas clearly conflicts with the Texas Open Meetings Act. [Tex. Govt. Code §551.071]
2. deliberating the purchase, exchange, lease, or value of real property if deliberation in an open meeting would have a detrimental effect on the position of the city in negotiations with a third person. [Tex. Govt. Code §551.072]
3. deliberating a negotiated contract for a prospective gift or donation to the city if deliberation in an open meeting would have a detrimental effect on the position of the city in negotiations with a third person. [Tex. Govt. Code §551.073]
4. deliberating the appointment, employment, evaluation, reassignment, duties, discipline, or dismissal of a public officer or employee; or to hear a complaint or charge against an officer or employee unless the officer or employee who is the subject of the deliberation or hearing requests a public hearing. [Tex. Govt. Code §551.074]
5. deliberating the deployment, or specific occasions for implementation, of security personnel or devices. [Tex. Govt. Code §551.076]
6. discussing or deliberating commercial or financial information that the city has received from a business prospect that the city seeks to have locate, stay or expand in or near the city and with which the city is conducting economic development negotiations; or deliberating the offer of a financial or other incentive to a business prospect. [Tex Govt. Code §551.087]
7. deliberating security assessments or deployments relating to information resources technology, network security information, or the deployment or specific occasions for implementations of security personnel, critical infrastructure, or security devices. [Tex Govt. Code §551.089]



City of Dallas

1500 Marilla Street
Council Chambers, 6th Floor
Dallas, Texas 75201

Agenda Information Sheet

File #: 22-608

Item #:

Discussion of the Report to the City of Dallas Regarding the City's March 2021 Data Loss Incident
[Erin Nealy Cox, Attorney, Partner at Kirkland & Ellis]

A photograph of the Dallas skyline, featuring the Reunion Tower on the left and a tall skyscraper in the center. The sky is a mix of orange and blue, suggesting a sunset or sunrise. A white diagonal line with a blue border runs from the top left towards the bottom right, separating the image from the white background.

KIRKLAND & ELLIS

**Report to the City of Dallas
March 2021 Data Loss Incident**

February 10, 2022

Report of Kirkland & Ellis LLP
to the City of Dallas regarding the March 2021 Data Loss Incident

February 10, 2022

I.	Executive Summary	4
A.	Kirkland’s Engagement	4
B.	Findings.....	4
C.	Evaluation and Recommendations.....	6
II.	Impetus for Independent Internal Investigation.....	7
A.	DA Inquiry and Resulting Press Release	7
B.	Discussion at City Council	8
III.	The Investigation.....	9
A.	Independence of Investigation	9
B.	Investigative Team.....	9
C.	Investigative Process.....	10
IV.	Background	11
A.	Dallas City Government and ITS.....	11
B.	The Dallas County District Attorney’s Office	11
C.	The Dallas Police Department	12
1.	Digital Evidence Storage Systems	12
2.	Limitations	13
V.	Technical Matters	14
A.	Archiving and Backup IT Services	14
B.	The Commvault Platform	15
1.	Overview.....	15
2.	Cloud Storage Locations.....	16

3.	Recalling an Archived File	16
VI.	Factual Findings.....	17
A.	Timeline of Key Events	17
B.	The 2020-2021 Data Migration	20
1.	Impetus and Planning.....	20
2.	Execution	21
3.	Analysis.....	21
C.	The Events of March and April 2021	23
1.	How the March Deletions Occurred	23
2.	Discovery of Issue within ITS	24
3.	Notification to DPD Leadership	25
4.	Role of Commvault Support	26
5.	Ongoing Deletions through August 2021	27
6.	Evidence of Motive.....	27
D.	August 2021 Discovery and Audit.....	27
1.	DA Cruzot’s Memo and Press Release	27
2.	The August Audit and Activation of Incident Response Plan	28
E.	Data Recovery Efforts.....	28
VII.	Root Cause Assessment	29
A.	Proximate Cause	29
B.	Systemic Contributors.....	30
C.	ITS Report Assessments	32
VIII.	Effects of the Data Loss Incident.....	32
A.	Effects on DPD	32
B.	Effects on the DA’s Office and the Criminal Justice System.....	33

IX.	Volume of Data Lost	34
X.	Previously Lost Data.....	34
XI.	Recommendations	34
	A. Data Safeguards and Redundancy	34
	B. Consult Vendor Experts as Needed	35
	C. DPD Resources and Staffing	35
	D. ITS Staffing and Training Needs	36
	E. Budgetary Issues and Allocation	36
	F. IT Management Protocols and Practices.....	37
	G. Departmental Protocols and Practices	37
	H. Inter-Departmental Communication and Coordination	37
	I. Departmental IT CIOs.....	38
	J. Citywide Assessment of Data Criticality	38
	K. Reformulating the Data Recovery Effort.....	39
XII.	Conclusion	39
XIII.	Appendices.....	40
	A. Appendix A – Chronology of Key Events Associated with Data Loss Incident	40
	B. Appendix B – Hard Client Deletions in Commvault Between April 2021 and August 2021	46
	C. Appendix C – Validation of Data Loss Volume.....	50
	1. Overall Validation Process	50
	2. Validation of K Drive Data Loss	51
	3. Validation of FUSION Data Loss.....	52
	4. Assessment of City Secretary and CAPERS	52

I. Executive Summary

This Report is organized into 12 sections, beginning with the scope and execution of our Investigation, and as follows:

- We describe the relevant policies governing the City of Dallas and the structure of relevant departments, as well as the technical background associated with the Data Loss Incident.
- We next provide a thorough account of the events that led to the Data Loss Incident based upon witness interviews and documents provided by the City of Dallas.
- We then provide a detailed summary of the actions and inactions of the ITS backup technician whose conduct caused the Data Loss Incident, and the response of ITS personnel and others to the event.
- We also discuss findings relating to the root cause of the event and other systemic factors that added to the potential impact of the Data Loss Incident.
- At the end of this Report, we offer our recommendations that relate both specifically to the findings of this Data Loss Incident and more broadly to larger systemic issues that we observed during this Investigation.

A. Kirkland’s Engagement

Kirkland & Ellis LLP (“Kirkland”) was engaged on November 1, 2021 (the “Engagement”) by the City of Dallas (the “City”), at the direction of the Dallas City Council (the “City Council”), to conduct a privileged, independent internal investigation (the “Investigation”) into the data loss incident that occurred at the City in and around the end of March 2021 (the “Data Loss Incident”). At the time, the City reported that approximately 22 terabytes of data had been lost, potentially irretrievably, with the bulk of the potentially affected data being associated with the Dallas Police Department (the “DPD”) and including data that constituted evidence in pending prosecutions in the Dallas County District Attorney’s Office (the “DA’s Office”).

Pursuant to our Engagement, we retained Stroz Friedberg LLC, an Aon company (“Stroz Friedberg”), to provide forensic services. Our Investigation involved, among other things: (i) a review of documents and data made available by relevant City departments, including DPD and the City’s Information Technology Services (“ITS”) department; (ii) interviews with 28 City and third-party witnesses, including multiple follow-up interviews; and (iii) consultation with Stroz Friedberg regarding relevant information technology (“IT”) and cybersecurity issues.

Our investigative steps are detailed below. A summary of our findings and recommendations follows.

B. Findings

- The immediate cause of the Data Loss Incident was a series of actions taken by an employee of the City, an ITS technician responsible for system backups and archiving (the “backup technician”), in late March 2021.

- In fall 2020 and spring 2021, ITS migrated the City’s servers from a cloud-based storage solution to on-premises servers located at City Hall. ITS initiated the server migration in response to escalating cloud data usage charges that exceeded budgetary requirements. The escalating charges were partially a result of increased charges associated with the City’s secondary cloud storage facility located at the time in Arizona.
- As part of the migration process, the backup technician made the following critical errors:
 - In migrating the DPD servers, the backup technician failed to properly copy data from the existing cloud-based storage systems to the newly implemented City Hall servers. The data at issue had been archived; thus, according to the vendor’s procedures, the backup technician should have restored the archived data, and then copied the restored data to the City Hall servers. Instead, he incorrectly copied the placeholder files that indicate data had been archived. Thinking that the servers had been properly migrated from the cloud to City Hall, the backup technician then deleted the archived data from the cloud-based servers. Thus, the archived data was no longer on the cloud-based servers. Because the data also was not properly copied to the City Hall servers, it was no longer recoverable.
 - In connection with the server migration, the backup technician also deleted settings in the City’s Commvault software that controlled archiving of DPD Family Violence and FUSION data. These deletions caused the loss of additional data, including approximately 13.17 terabytes of FUSION data.
- The backup technician’s actions that caused the Data Loss Incident appear to have been based on his flawed understanding of the City’s backup and archiving platform, Commvault, and of the steps necessary to properly migrate archived data from the City’s cloud-based storage to the City Hall servers.
 - During the course of our Investigation, we did not uncover any evidence that the backup technician had malicious intent or criminal purpose in deleting the data. Ultimately, any conclusion in this regard will be up to the appropriate law enforcement agency tasked with investigating this matter.
- The total volume of data lost in the Data Loss Incident was approximately 23.94 terabytes, of which approximately 3.26 terabytes were recovered from other sources. Consequently, the net loss of City data was approximately 20.68 terabytes. Based on the Investigation, these approximately 20.68 terabytes of data are permanently lost, and should be understood by all stakeholders to be unrecoverable in their original format.
- Thus far the effects (other than cost) of the Data Loss Incident appear to be relatively limited. DPD reported that, with one or two minor exceptions, every file it has identified as potentially lost in the Data Loss Incident has been found in another location (*e.g.*, emails or officers’ individual hard drives). The DA’s Office likewise reported that, as of January

2022, the Data Loss Incident has not had a substantial impact on prosecutions. It remains possible that there will be additional impacts in the future, although ITS, DPD, and the DA's Office are taking steps to minimize any future impact.

- The data implicated in the Data Loss Incident involved certain data archived in the cloud via Commvault. We found no evidence that the Data Loss Incident adversely impacted any other City data.

C. Evaluation and Recommendations

- ITS should have implemented safeguards to ensure the safety of critical City data during the server migration. Such safeguards could have included enabling the “soft delete” feature in the City’s cloud-based storage facility such that deleted data could be recovered. Additionally, ITS should have ensured that a secondary copy of the data was preserved until ITS confirmed that the migration project was successfully completed and verified.
- The backup technician’s understanding of and training on the Commvault platform were inadequate. Given his status as an IT professional and his responsibility for safeguarding critical City data, he should have taken the initiative to seek additional training from ITS and Commvault. Likewise, ITS leadership should have ensured he had a sufficient understanding of Commvault and/or brought in subject matter experts (including specialists from Commvault’s Professional Services team) to assist in a data migration that implicated critical City data.
- Given the potential effect on active criminal cases, the Data Loss Incident should have been identified as a critical incident at the time it occurred, and the City’s Incident Response Plan (“IRP”) should have been activated. This likely would have resulted in a more thorough assessment of the issue at the time it was discovered, as well as clearer communication between ITS and key stakeholders—including the DPD, the DA’s Office, the City Manager, and the City Council—regarding the scope of the data loss and steps being taken to mitigate its effects.
- ITS’ current data recovery effort is focused on identifying copies of potentially affected documents within other City systems using keyword searches for known information about affected cases, such as case numbers and officer names. It is not an effort to recover the original data, which ITS understands to be permanently lost. To date, ITS has completed searches for approximately 36% of the 17,484 affected cases.

It is unclear whether completing the planned recovery effort, which is not projected to wrap up until late 2022, will be worth the expense given, among other things, that the effort will not recover the lost data in its original format and that many affected files may never be needed in the future. ITS and other stakeholders should coordinate on developing a more efficient, targeted approach to recovering affected files on a prioritized basis going forward.

- The City should consider at least the following broader steps to mitigate the risk of a similar event occurring in the future:

- ITS needs to develop better processes and procedures for (i) understanding costs, benefits, and risks of potential data migration efforts, and (ii) mapping out all steps of proposed migrations and the potential risks that need to be mitigated with each step.
- The City needs to take steps to ensure that ITS and key stakeholder departments are coordinated so that ITS can adequately address all departmental IT needs, particularly for departments such as DPD that work with critical data day in and day out. For example, and as described more fully below, DPD and other such departments should establish a departmental Chief Information Officer positioned to fully understand the department's IT needs and advocate for the department in the planning and budgeting process.

A comprehensive assessment of root cause and our full recommendations are set forth in detail in sections VII and XI of this Report.

II. Impetus for Independent Internal Investigation

This section summarizes the events leading to the engagement of Kirkland by the City to conduct the Investigation of the Data Loss Incident.

A. DA Inquiry and Resulting Press Release

As described in more detail below, the chain of events that ultimately led to the Data Loss Incident began in fall 2020. ITS discovered the Data Loss Incident as a result of DPD user support requests and undertook initial remedial efforts in early April 2021.¹ Although ITS provided some information to DPD, ITS did not inform the DA's Office of the Data Loss Incident at that time.²

The DA's Office first became aware of a potential data loss incident on July 30, 2021. On that day, an Assistant Dallas County District Attorney ("ADA") discovered that certain DPD files related to a pending prosecution were inaccessible.³ The files in question had been stored on the "K" drive—a mapped DPD network share consisting of multiple underlying file servers where the evidence for the case at issue was stored.⁴ A DPD detective told the ADA that the K Drive had been corrupted, and that as a result, those files were no longer available.⁵ The ADA then informed the DA's Office's IT department of the issue.⁶

Throughout the next week, the DA's Office assessed the situation and informed their leadership, including the Dallas County Criminal District Attorney, John Creuzot (the "DA" or "DA Creuzot").⁷ On August 6, 2021, following inquiries from the DA's Office, ITS told the DA's Office that during a routine data migration, "multiple terabytes of DPD data had been deleted."⁸ On August 9, 2021, ITS provided additional detail, telling the DA's Office that between March 21, 2021 and April 5, 2021, approximately 22 terabytes of DPD data had been deleted.⁹ ITS also told the DA's Office that approximately 14 terabytes of data had been recovered, but the remaining eight terabytes were believed to be unrecoverable.¹⁰

On August 11, 2021, DA Creuzot published a press release titled "Disclosure Regarding Missing Data from Dallas Police Department's Network Drive."¹¹ In the press release, DA Creuzot stated that the City first became aware of the issue on April 5, 2021, but his office had only been

made aware on August 6, 2021.¹² DA Creuzot also directed all prosecutors to compare DPD's records to those maintained by the DA's Office to verify that all DPD evidence had been shared via the LEA portal (described below).¹³ The DA's Office then began making disclosures to defense attorneys and courts that evidence may have been deleted.¹⁴

B. Discussion at City Council

On August 12, 2021, Mayor Eric Johnson told the City Council that he had been "blindsided" the previous day by the news of the data loss, and requested that the council "call a joint special-called meeting of your committees to discuss the data deletion, the troubling lack of communication from city staff about what transpired, and the steps being taken to resolve the matter and prevent future consequences."¹⁵ In response, on August 18, 2021, the City Council was briefed on the data loss during a closed executive session.¹⁶

On September 10, 2021, the Ad Hoc Committee on General Investigating and Ethics (the "Ad Hoc Committee") considered agenda item #2 titled "Consider hiring a third-party consultant to complete an impartial comprehensive investigation of, and report about, the city's data loss."¹⁷ Chair Mendelsohn explained that the goals for any investigation would be "to understand exactly what happened and why; what was lost or restored; how the process can be improved and make sure those changes are implemented."¹⁸ The Ad Hoc Committee then instructed the City Attorney to issue a public request for submittals from law firms that could conduct an independent internal investigation.¹⁹ The request for submittals was open to any law firm that wished to submit a proposal.²⁰

The City received twelve proposals in response, which were reviewed by a panel of City attorneys consisting of Tammy Palomino (First Assistant City Attorney), Patricia DeLaGarza (Chief of Litigation), Ayeh Powers (Managing Attorney), and Stacey Rodriguez (Chief of General Litigation).²¹ The City Attorney's review panel then selected three law firms to present to the Ad Hoc Committee: Kirkland & Ellis LLP, Akin Gump Strauss Hauer & Feld LLP, and Polsinelli. Representatives of those firms, including Erin Nealy Cox, a partner in Kirkland's Dallas, Texas office, provided brief explanations of their submittals and answered questions from the members of the Ad Hoc Committee.²²

Following the law firms' presentations, the members of the Ad Hoc Committee individually announced the firm that they wished to conduct the independent internal investigation.²³ Chair Mendelsohn as well as Councilmembers McGough, Blackmon, and Schultz all selected Kirkland.^A

On November 1, 2021, Kirkland entered into a professional services contract with the City under which it committed to investigate the data loss, engage a forensic firm to analyze the lost electronic data, and provide a report: (1) detailing how and why the data was lost, (2) determining if the lost data was successfully recovered, (3) identifying any issues with the City's IT systems and protocols regarding maintaining and migrating electronic data, including, but not limited to,

^A Minutes of the Meeting of the Ad Hoc Committee on General Investigating and Ethics (Nov. 4, 2021). Councilmember Atkins was not present for all of the presentations and, therefore, chose not to participate in the selection process. *Id.*

monitoring and supervising actions of employees in ITS responsible for maintaining and migrating electronic data, (4) recommending changes to prevent such data losses from occurring in the future, including best practices, and (5) providing any other recommendations Kirkland deemed necessary based upon its experience conducting similar investigations.²⁴

III. The Investigation

A. Independence of Investigation

The City directed us to follow the facts wherever they led and permitted us to conduct this Investigation independent of interference or influence. While Kirkland's investigative mandate was defined by the City Council, Kirkland exercised its independent judgment in conducting the Investigation, including with respect to which documents it needed to review, which witnesses it needed to speak to, and which issues were relevant for further inquiry. The City Attorney and City Council were not kept apprised of the substance or process of Kirkland's investigation, and only given updates as to timing and overall progress. Even though the City Attorney hired us pursuant to the attorney-client privilege, we designed and executed the Investigation with no limits from them. In our sole discretion, we chose who to interview and what materials to review. We were given prompt access to documents, employees, and information, including contact information for current and former employees and third-party contractors.

The factual findings set forth in this report are solely advanced by Kirkland. The City exerted no influence over our reporting of the facts and findings.

Our investigation is not a response by us or by the City to any pending lawsuit or criminal investigation. Kirkland is not serving as counsel for the City in any civil litigation related to this Investigation. Kirkland has never previously provided legal representation to the City in any matter related to the Data Loss Incident, and while the City has paid Kirkland's legal fees incurred during the Investigation, payment is not contingent on any particular finding or outcome.

B. Investigative Team

The investigative team was led by Kirkland Partner Erin Nealy Cox, a former United States Attorney for the Northern District of Texas. Kirkland is a global law firm that serves a broad range of clients around the world and helps organizations solve their most complex problems. The Kirkland team that worked on the Investigation has significant experience conducting internal and government investigations, including extensive experience representing clients facing cybersecurity and data management challenges. In addition, Kirkland engaged Stroz Friedberg, a technical consulting firm, to provide forensic and technical assistance in the Investigation. Stroz Friedberg assisted in witness interviews, conducted a forensic review of all available data provided by the City and its vendors, conducted walkthroughs with ITS of certain processes associated with its current data recovery effort, and assisted in preparing this report. The members of the Stroz Friedberg team have a combined total of 55 years of experience in digital forensics and incident response work, in addition to backgrounds in law, military investigations, and corporate internal investigations.

C. Investigative Process

We began the Investigation immediately upon being engaged and started quickly coordinating with the City Attorney's Office, ITS, DPD, the DA's Office, and third-party services providers to schedule witness interviews and obtain documents. Over a three-month period, we interviewed 28 witnesses, including:

- The backup technician, who is no longer employed by the City.
- Members of the City's ITS team, including the executives, supervisors, and technicians involved in the City's response to the Data Loss Incident. We interviewed some members of the ITS team more than once.
- Several members of the City's Information Security team that serve in auditing and compliance roles.
- One contract employee working on the City's data recovery efforts.
- Numerous DPD officers at varying levels of leadership and command staff.
- Members of the DA's Office.
- Employees of Commvault who have personal knowledge related to the City's systems and the Data Loss Incident.

We requested and received documents and data files from ITS totaling approximately 211,000 pages and 3.41 gigabytes. We also received documents from the DA's Office, DPD, and Commvault. Of particular note, our review encompassed the following key documents and data sources:

- Memos, emails, and other documentation describing the Data Loss Incident and its potential effects.
- Commvault support tickets created as part of the City's response to the Data Loss Incident.
- Audit reports identifying relevant Commvault client and policy deletions.
- Commvault instructions and support materials, including those titled "Retiring a Client" and "Recovering Archived Data."
- A copy of the files and data from the backup technician's local machine.
- ITS' September 30, 2021 Initial Report on the Data Loss Incident (the "ITS Report").^B

^B Additional technical background on Commvault and the City's servers and cloud storage systems can be found in the ITS Report.

- An ITS plan for preventing future data loss incidents.

IV. Background

A. Dallas City Government and ITS

The City of Dallas provides a range of government services to its over 1.3 million residents. To provide these services, the City relies on ITS, which is responsible for managing the technology programs and operations of the City's various departments. According to ITS, it currently serves 46 customer departments, including DPD, Dallas Fire-Rescue, the City Attorney, the City Controller's Office, Dallas Water Utilities, the Department of Aviation, and the Department of Public Works.

The City's departments rely on ITS for IT programs and support, including the storage, backup, and archiving of data.²⁵ For example, DPD relies on ITS to maintain secure storage and archiving of evidence collected for criminal prosecutions.²⁶ ITS has staffed two individuals to assist its efforts to service DPD—a Business Relationship Manager to DPD and a Senior IT Manager for Public Safety, both of whom are responsible for liaising with DPD regarding its IT needs.²⁷ Reliance on ITS extends beyond the City's own departments, as DPD coordinates with the DA's Office in the prosecution of crimes committed in the City, and a loss of evidence stored by DPD could lead to an inability to maintain ongoing criminal prosecutions.²⁸

Historically, ITS has had five sub-groups: (i) Infrastructure; (ii) Servers and Networks; (iii) Radio Networking; (iv) Help Desk and Desktop Support; and (v) Managed-Service Contracts.²⁹ This report focuses on the Servers and Networks team, which during the relevant time period has been the group responsible for virtual, on-premises, cloud storage, and backup services, as well as server support and recovery services.^C

In June 2020, the City hired a new Chief Information Officer ("CIO").³⁰ The CIO has responsibility for and oversight of ITS.³¹ According to the CIO, when he first arrived in Dallas, he noticed a number of deficits in ITS.³² The role of these deficits in the Data Loss Incident is discussed in more detail below.

B. The Dallas County District Attorney's Office

The DA's Office is responsible for prosecuting misdemeanor and felony crimes that occur within Dallas County, including those that occur in the City.³³ As of 2020, there are approximately 2.7 million residents of Dallas County,³⁴ making it the ninth largest county in the United States.³⁵ Those residents are spread across over 30 incorporated cities that are patrolled by dozens of police departments and the Dallas County Sheriff's Department. The DA's Office receives reports, evidence, photographs, videos, audio recordings, and vast quantities of other data from these entities every day.³⁶ For the DA's Office's prosecutors to perform their duties properly, they must be able to receive and process digital evidence in an efficient and secure manner.

^C Interview of Witness on Nov. 5, 2021. Since this investigation began, backup recovery has reportedly been moved into its own separate team. Interview of Witness on Jan. 5, 2022.

C. The Dallas Police Department

DPD and its over 3,100 sworn officers and approximately 650 civilian employees require immense IT support to carry out their mission of making the City a safe place to live, work, and visit.³⁷ Officers build their cases with evidence such as 911 call recordings, photos, and videos.³⁸ DPD collects or generates approximately 800 terabytes of data per year.³⁹ That number will only increase over time as digital evidence including body cameras, video cameras, additional drone and helicopter footage, and other sources of data come online.⁴⁰ Naturally, DPD's IT needs include storing a massive amount of evidence in a secure location. And DPD must store this evidence for lengthy periods of time—starting at the time of collection, through the investigation, until the case goes to trial, and through any appeals.⁴¹ For certain types of cases, it is not unusual for this process to take years.

1. Digital Evidence Storage Systems

DPD currently relies on several systems to house its evidence. First, officers are able to upload all evidence to a division-specific location on the K Drive.⁴² Using a shared drive is important because, if a particular officer is out in the field, his or her colleagues or supervisors can still efficiently locate evidence files from the office.⁴³

Officers can also upload evidence to DPD's Records Management System ("RMS"), a case management system that can house certain kinds of digital evidence, as well as the City's account on Evidence.com.⁴⁴ After uploading evidence to RMS or Evidence.com, officers are then expected to transfer the casefile to the Lumen Law Enforcement Agency ("LEA") portal.⁴⁵ From there, the DA's Office is able to access any evidence in the LEA portal via the TechShare program.^D None of these platforms were affected by the Data Loss Incident. Finally, DPD has cellphone data stored on the FUSION server at City Hall.⁴⁶

^D See generally Interview of Witness on Dec. 7, 2021. TechShare is a county-owned technology platform that hosts software designed to help manage information throughout the life cycle of a case. For more information about the program, see <https://techsharetx.gov/>.

The following diagram summarizes at a high level the flow of DPD data through the City's systems:

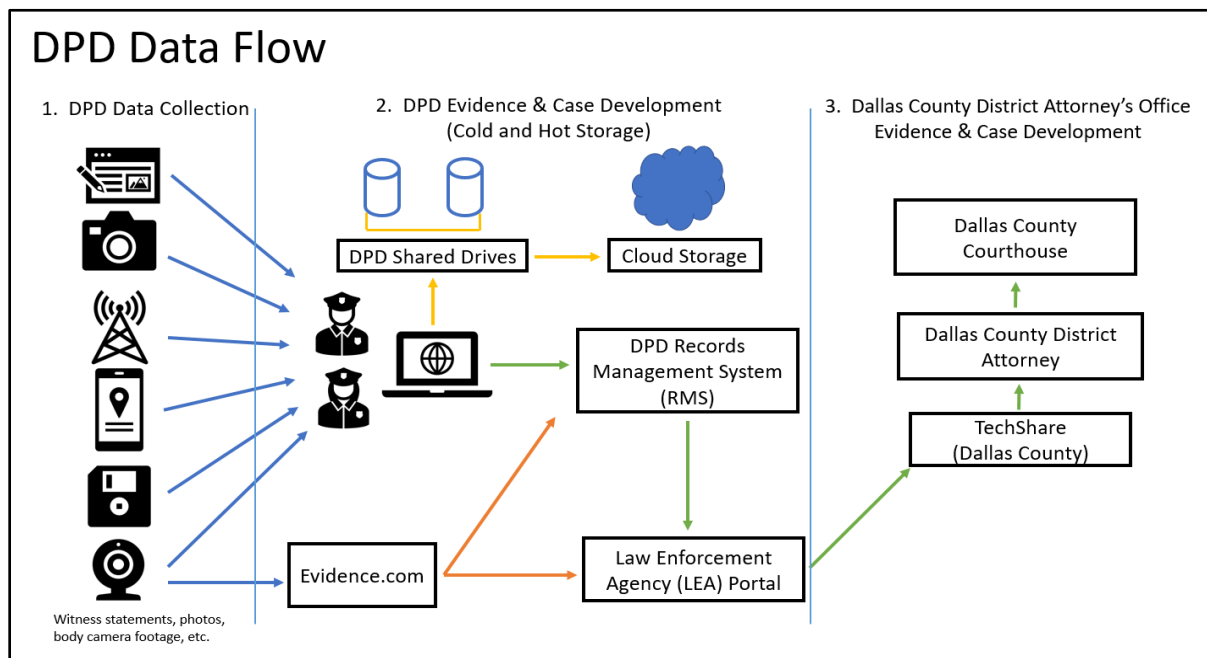


Fig. 1 – DPD Data Flow

2. Limitations

The K Drive, RMS, and LEA/TechShare platforms each have limitations. Within the K Drive, each DPD unit is only allocated a certain amount of data per month; it does not permit unlimited storage.⁴⁷ DPD units can request additional K Drive storage space from ITS, but the request can take several days to fulfill, and requests are often declined due to overall storage limitations or cost.⁴⁸ Reportedly, the process of uploading to the K Drive is also frequently slow, since upstream network bandwidth to the cloud is limited.⁴⁹ Officers report upload and download times in the range of hours, days, and weeks, not minutes.⁵⁰ As a result, some officers choose to skip the K Drive and instead upload evidence directly to RMS from their local drives.⁵¹ Other officers keep their data on a local laptop or thumb drives, and then wait to upload to RMS when a case is ready to present to the DA's Office.⁵²

While RMS does not have the same upload speed problems, it too has storage space constraints. Reportedly, files larger than 20 megabytes cannot be uploaded to RMS, and we understand certain large files (such as videos in general) cannot be placed on RMS because of space constraints. Instead this data is uploaded to Evidence.com or hand-delivered to the DA's office.⁵³ The LEA portal likewise has its limits. Officers have been told to only upload files less than five gigabytes in size, as the system becomes problematic for defense counsel when larger files are at issue.⁵⁴

Cell phone data presents another complication for DPD evidence storage. Cellebrite is one of the forensic tools DPD uses to collect data from cell phones.⁵⁵ In the past, cell phone data

collected from Cellebrite was stored on the server named FUSION.^E But in 2020, the FUSION server ran out of capacity, and DPD was not afforded additional storage options. As a result, DPD began using alternate storage devices.⁵⁶ DPD reports that since the Fusion center ran out of space, they have filled up approximately 15 two-terabyte hard drives with collected cell phone data.⁵⁷

As a result of the various issues presented by digital evidence, and given the need for redundancy, it appears individual DPD officers have developed their own strategies for storing and backing up collected evidence.⁵⁸ For example, DPD interviewees stated it is common for officers to keep duplicate copies of evidence on their local drives or Microsoft OneDrive.⁵⁹

V. Technical Matters

A. Archiving and Backup IT Services

As a general matter, backup and archiving serve two distinct functions. The purpose of creating backups of systems on a regular basis is to aid in recovering from an unexpected event, such as hardware failure or a natural disaster. In contrast, the purpose of archiving is to manage the costs associated with more expensive, high-availability data storage. Archiving is accomplished by moving files that have not been accessed for a period of time (as defined by the customer) to lower-cost storage locations (often referred to as cold storage).

Archiving is most suitable for data that is no longer actively in use but cannot yet be deleted due to operational or regulatory requirements.⁶⁰ In addition to cost efficiencies, some of the benefits of archiving include deduplication of data (identical data elements such as company logos are stored once rather than multiple times) and indexing of stored data for quick recall.

As noted, Commvault, a publicly traded enterprise software company, is the City's current provider for archiving and backup solutions. The City originally implemented Commvault in 2018 to replace its then-backup solution.⁶¹ Thereafter, the City expanded its use of Commvault to include archiving.⁶²

In general, we understand the archive periods set by ITS for data relevant to this Report were as follows:

Data Source	Archive Period
K Drive	18 months ⁶³
K Drive – Family Violence Data	9 months ⁶⁴
FUSION	10 months ⁶⁵

^E Interview of Witness on Nov. 9, 2021. The FUSION server contains a significant portion of all DPD-collected cell phone data. The Narcotics Unit and ICAC have the ability to conduct and store their own cell phone dumps. *Id.*

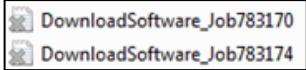
B. The Commvault Platform

1. Overview

Within the Commvault platform, customers can determine what systems are subject to archiving and/or backup processes, as well as the mechanics of such processes, including what data should be archived, when it should be archived, and where the archived data will be stored.⁶⁶

Commvault uses certain terms in describing the functionality on its platform, as summarized in the table below.

Term	Definition	Hypothetical Example
Client	In Commvault terminology, a “client” is a computer system containing data that is subject to being archived.	The City maintains certain servers on its premises to store digital files. Each of the servers are considered “clients.”
Client Policy	A “client policy” governs the criteria and mechanics of archiving data on a given client, as configured by the customer. ⁶⁷	The City sets a policy requiring that on particular servers, data older than one year will be archived every Friday night.
Storage Policy	A “storage policy” is a logical entity through which data from Commvault clients is archived. ⁶⁸ More concretely, a storage policy governs what data should be archived, where archived data should be stored, how long it should be kept, etc. ⁶⁹ A storage policy can encompass and govern data from multiple clients and/or client policies.	A storage policy could require that archived data should be kept for seven years before being deleted.

Term	Definition	Hypothetical Example
Stub	<p>Stubs are files retained on a client that point to archived data, functionally similar to a Windows shortcut.⁷⁰ These stubs act as a “pointer” to the archived file and appear the same as active files to the end-user except that they have an overlaid grey icon that indicates their archival status, as in the following example from Commvault’s support documentation:</p> 	<p>Using the above example, archived files would be retained for seven years by the system.</p> <p>When a file is archived, it is moved from the original storage location (<i>e.g.</i>, a file server) to the Commvault storage cloud and is replaced on the original system by a placeholder file known as a stub file.</p> <p>The placeholder file has a gray icon with an X logo indicating that the file has been archived.</p>
Rehydration	<p>The process of reversing the archiving process by pulling data back from the archive and replacing a stub with the full contents of the referenced file.⁷¹</p>	<p>A City technician can enter a command in the Commvault software that causes the software to re-download archived files to a file server, putting copies of them back on the server.</p>

2. Cloud Storage Locations

The City has two cloud-based storage facilities. The City’s primary cloud storage facility for Commvault is the Microsoft Azure Government Cloud.⁷² The City also had a secondary cloud storage facility that was located at an Azure data center in Arizona from approximately April 2019 through January 2021. Since approximately January 2021, the secondary cloud storage facility has been located in the same data center as the primary cloud storage facility.⁷³

3. Recalling an Archived File

The process of opening an archived file involves the following steps (see Fig. 2 below):

1. A user double-clicks on a stub for a file that has been archived (*e.g.*, File4.doc).
2. Commvault software checks the cloud for the storage location of the archived contents of the file.
3. Commvault software goes to that storage location and retrieves the archived contents of the file.
4. Commvault software replaces the stub file with the contents of the file and opens that file on the user’s system.

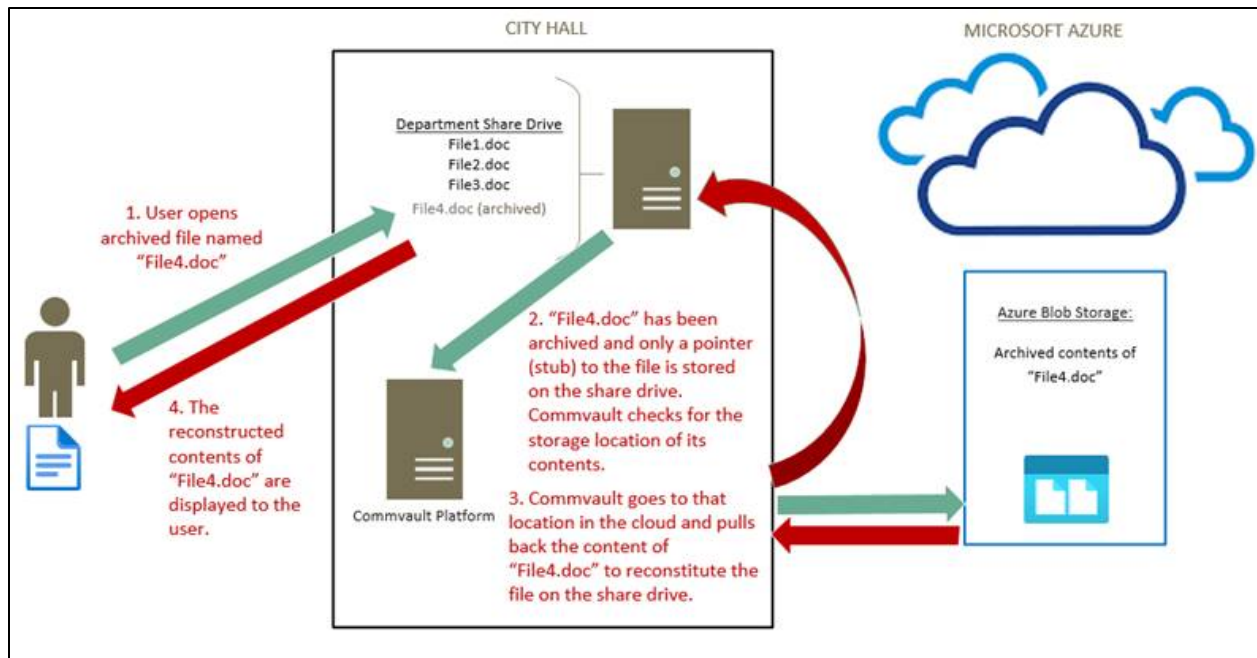


Fig. 2 – Depiction of the process to recall an archived file

VI. Factual Findings

A. Timeline of Key Events

The following timeline of key events identifies the most significant dates and events associated with the Data Loss Incident. A full chronology of relevant events is provided in **Appendix A**.

Date/Time*	Description of Event
2018	ITS implements Commvault as the City's backup solution, and subsequently expands its use of Commvault to include archiving. ⁷⁴
July 2020	Internal ITS discussions regarding the escalating data ingress and egress charges for the auxiliary Azure facility in Arizona which leads to the decision to redesign infrastructure. ⁷⁵
August 24, 2020	A change order governing the data migration planned for early 2021 from the cloud to on-premises storage at Dallas City Hall is submitted through ITS' change management system as a "Normal" change. ⁷⁶

* All times CDT.

Date/Time*	Description of Event
January 2021	The backup technician begins to execute the data migration plan by migrating four servers from the cloud to City Hall. ⁷⁷ While the backup technician attempts to rehydrate archived files on the servers before migration, errors in that process result in incomplete rehydration, meaning many files from the servers are not properly migrated. ⁷⁸
February 2021	The backup technician decommissions four of the improperly migrated in Azure. ⁷⁹ Three of the migrated servers were not decommissioned. ⁸⁰
March 30 - 31, 2021	The backup technician works to “clean up” the City’s Commvault system by executing 17 hard client deletions and five storage policy deletions. ⁸¹ As described herein, some of these deletions caused the loss of archived K Drive data.
April 5, 2021	ITS receives its first support-ticket from DPD regarding inaccessible K Drive files. ⁸²
April 5, 2021 11:00 AM	The backup technician shuts off all Commvault deletions, stopping the deletion process triggered by his “clean-up” actions. ⁸³
April 5, 2021 12:08 PM	The backup technician creates a support-ticket with Commvault with the description, “Archived and stubbed files not being recalled.” ⁸⁴
April 5, 2021 12:30 PM	The backup technician notifies his supervisor, the IT Manager for Servers and Networking, that he made a “mistake” during cleanup the week prior. ⁸⁵
April 5, 2021 6:22 PM	Commvault support identifies that “stub recalls were failing because the stubs were tied to deleted clients . . . that were deleted last week.” ⁸⁶
April 6, 2021 7:00 AM	The IT Manager for Servers and Networking informs the Infrastructure Assistant Director of the incident. ⁸⁷
April 6, 2021 9:27 AM	The Infrastructure Assistant Director informs the CIO. ⁸⁸
April 9, 2021	ITS works with Commvault support to confirm the scope of the data loss and identify potential next steps. ⁸⁹
April 10, 2021	The IT Manager for Servers and Networking informs the Senior IT Manager of Public Safety and the IT team supporting DPD that files for multiple divisions had been deleted and “might” be unrecoverable. ⁹⁰
April 12, 2021	The Senior IT Manager of Public Safety announces at the DPD Command Staff meeting at DPD headquarters that ITS is working on addressing an issue affecting the K Drive. ⁹¹

Date/Time*	Description of Event
April 13, 2021	The CIO notifies the Assistant City Manager via email “of potential mass data loss occurring because of an error during the performance of routine file transfers from Azure storage to the City Hall storage of the DPD file archives We are setting up a meeting with DPD leadership this afternoon.” ⁹²
April 19, 2021	The DPD Chief of Police releases an internal memo to all departmental personnel, stating: “IT Services have received reports of missing files or folders from network drives. All departmental personnel are asked to please check if any files or folders are missing from their network drives. If you are missing files or folders, please follow the steps in the attachment to restore the missing files or folders.” ⁹³
May-August 2021	The backup technician continues manual deletions of Commvault clients. ⁹⁴
July 30, 2021	An ADA is informed by officers that certain DPD files related to a pending prosecution are no longer available on the K Drive. ⁹⁵
Early to Mid-August 2021	DPD begins discovering issues with recalling FUSION data. ⁹⁶
August 6, 2021	ITS informs the DA’s Office of the deleted data. ⁹⁷
August 11, 2021	DA Creuzot issues a memo and press release regarding the data loss. ⁹⁸
August 12, 2021	The backup technician and the IT Manager meet for an “administrative leave interview.” ⁹⁹
Mid-August 2021	Commvault conducts an audit of deleted clients and policies and determines that the FUSION server has also been impacted due to a deleted storage policy. ¹⁰⁰
August 26, 2021 6:25 PM	The CISO activates the IRP to conduct an analysis of the data loss, elevating it to a severity level of P1. ¹⁰¹
August 27, 2021	Formal notice of possible data loss is sent to the City Manager’s Office, the Mayor’s Office, the City Council, and the DA’s Office. ¹⁰²
August 30, 2021	The backup technician is issued a notice of pre-termination hearing. ¹⁰³
October 22, 2021	The backup technician is terminated. ¹⁰⁴

B. The 2020-2021 Data Migration

1. Impetus and Planning

The advent of the City's Commvault system dates back to 2017. After receiving a large bill that year from the City's then-current backup provider, ITS decided to move to Commvault at some point during the following year.¹⁰⁵ The backup technician came to have primary responsibility at ITS for Commvault around this time.¹⁰⁶ Another senior system administrator served as an alternate for Commvault coverage, but was never meant to serve as a full backup resource, and received no training on Commvault until August 2021.¹⁰⁷ Commvault was engaged to advise ITS in the configuration or implementation of the City's platform, nor was Commvault's Professional Services team engaged by the City to provide guidance on implementation, migration strategies.¹⁰⁸

In 2020, and again due to escalating costs, ITS decided to implement another change and move away from cloud storage in favor of again hosting the City's data at City Hall.¹⁰⁹ In connection with this process, ITS chose to decommission the City's existing servers in the cloud.¹¹⁰ ITS' decision to migrate the City's servers from cloud storage back to on-premises was driven by cost: specifically, the escalating monthly costs associated with cloud data usage, primarily but not exclusively associated with the secondary cloud storage facility, which at the time was located at a data center in Arizona.^F

ITS submitted the change order that governed the data migration (the "Change Order") through its change management system on August 24, 2020, characterizing the change as a "Normal" change.¹¹¹ The Change Order listed the backup technician as responsible for the data migration, and provided the following description of the change:

Implement new Azure storage libraries to eliminate cross region egress charges. New libraries will only exist in the Texas region. The migration will be gradual in order to monitor.¹¹²

Pursuant to the Change Order, ITS planned to execute the migration (including consolidating certain servers) and then perform a cutover where the old servers would be taken offline and the new servers would be brought online in their place.¹¹³ After operating in that condition for thirty days without issue, the plan was to decommission the old cloud-based servers, including stopping backups of those systems, stopping monitoring and patching services, and deleting the servers.¹¹⁴ The Change Order was approved by the IT manager for Servers and Networking and the Infrastructure Assistant Director.¹¹⁵

One of the documents attached to the Change Order, "Implementation Plan for New Commvault Blob Storage Libraries," was authored by the backup technician and contains a list of steps that would need to be undertaken in connection with the server migration.¹¹⁶ The first item

^F Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 15, 2021; Interview of Witness on Jan. 5, 2022; Interview of Witness on Jan. 5, 2022. The move to the cloud was described as a "lift and shift" effort whereby everything from print and database servers to file servers were moved to the cloud with no redesign—their location was simply changed from the cloud to City Hall. Interview of Witness on Nov. 5, 2021.

in the list reads “delete Arizona library,” which meant that the data stored in the secondary cloud storage facility would be deleted as part of the migration process.¹¹⁷ The other steps in the document walk through certain Commvault data that would be migrated and deleted.¹¹⁸ The backup technician stated that although he received general input from Commvault on the migration process at various points, Commvault Technical Support did not review the Change Order or the attached list of steps.¹¹⁹

2. Execution

In January 2021, the backup technician began executing the “Implementation Plan.” Consistent with the order of steps in the “Implementation Plan,” the backup technician deleted the Commvault data in the secondary cloud storage facility in Arizona.^G The backup technician then attempted to migrate several servers with archived data from the City’s primary cloud storage location to the City’s new storage servers at City Hall, and later performed the cutover to activate the new servers.¹²⁰ Thirty days following completion of the migration, no errors or issues had been reported to ITS.¹²¹

At this point, the backup technician believed that all data on the City’s file servers that were previously located in the City’s cloud storage facility had been successfully relocated to the new servers in City Hall.¹²² The backup technician seemingly did not realize that the transferred files included millions of stubs, which represent archived files, and that the underlying archived data had not been properly migrated within Commvault through an appropriate rehydration process. The backup technician proceeded to delete four of the migrated server clients from Commvault¹²³ as well as a Commvault storage policy that governed the archiving of FUSION and Family Violence data.¹²⁴

3. Analysis

We identified several issues in the execution of the “Implementation Plan.” First, according to the backup technician, ITS relied on the relevant end users to verify they could still access

^G Witness accounts differ with respect to a few particulars related to the deletion of the secondary facility in Arizona. First, when asked about the fact that the list of steps in the “Implementation Plan” document is numbered, and the first step reads “delete Arizona library,” the backup technician stated that the document was simply intended to serve as a checklist of steps that would need to be taken at some point in the migration, not an ordered sequence of steps. Interview of Witness on Dec. 15, 2021. In contrast, the backup technician’s manager, who was involved in reviewing the Change Order and supporting documentation, stated that he understood the document to list the migration steps in the order they were to be executed, as identified by the backup technician. Interview of Witness on Jan. 5, 2022. Second, according to the backup technician, the Commvault Sales Engineer responsible for the City’s account recommended against deleting the secondary storage location in Arizona. Interview of Witness on Dec. 15, 2021. The backup technician also stated that he relayed this recommendation to his supervisors, and that despite his and Commvault’s objections, they directed him to go ahead and delete the servers stored in the Arizona facility. *Id.* In contrast, the Commvault Sales Engineer, when interviewed, stated he did not voice any objections. Interview of Witness on Jan. 5, 2021. He said that he always told the backup technician to keep archive data in the cheapest location and encouraged general redundancy of data, either in different regions or on different mediums. The Commvault Sales Engineer stated that his understanding was the City’s system met these requirements when moving from Azure to on-premises. *Id.* Notwithstanding these differing particulars, all witnesses agreed that the backup technician did in fact delete the secondary facility in Arizona before carrying out the rest of the migration. Interview of Witness on Dec. 15, 2021; Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022; Interview of Witness on Nov. 22, 2021.

everything they needed and submit a support ticket in the event of any issues.¹²⁵ Thus, when the backup technician did not hear reports of accessibility issues from DPD for 30 days after the cutover, he believed the migration project was adequately validated and did not take any additional validation steps.^H For example, the backup technician did not run a report to determine that the new stubs were referencing their intended locations in order to guarantee that all data had been properly migrated.¹²⁶ In addition, the backup technician failed to retain a copy of the data that he attempted to migrate in case something went wrong in the migration process. The lack of a duplicate copy created tragic consequences when mistakes were made. Because the Commvault archive data is stored in a special deduplicated storage container, it is not possible to reconstruct deleted files through forensic recovery, as frequently can be done on a typical desktop computer or other types of storage.^I When the backup technician’s “clean-up” activities destroyed the mapping between Commvault stubs and the corresponding files, this made it impossible to piece the deleted data back together. This caused the deletion of approximately 23.94 terabytes of City data.

The backup technician also failed to rehydrate files on user systems that had been archived. According to Commvault, one of the necessary steps for migrating a server with files archived by Commvault is to “rehydrate” the data that has been archived—that is, reverse the archiving process and replace the stubs with the underlying data.¹²⁷ In this case, however, the backup technician did not complete the rehydration process for all servers prior to migration, meaning that for some servers, only stubs were moved to the new on-premises location instead of the full file content.¹²⁸ Because those servers were incompletely migrated, the deletion of the relevant Commvault clients and storage policies resulted in the loss of their data.¹²⁹ We identified no evidence that anyone in ITS took any steps to validate that the migrated data was present and accessible, aside from waiting 30 days for users to self-report issues.¹³⁰ The IT manager stated he relied on the backup technician to validate the data migration, but he was not able to elaborate on the verification method used.¹³¹

^H Interview of Witness on Dec. 15, 2021. The backup technician also stated that he never had the time to take additional validation steps, due to time constraints imposed as a result of the constant project work required of the ITS department. *Id.*

^I In a Windows file system, each file is written to an available location on the relevant storage drive, and the file system tracks the location of each file on that drive in a table. When a file is deleted, the table entry that points to the file’s location on the drive is deleted and the location where the file contents reside becomes available for use. However, the file’s storage space itself is not ordinarily erased or overwritten, leaving the file contents intact on the drive, unless and until another file is written to the same storage space. As a result, it may be possible to later recover a deleted file, in part or in full, by examining the contents of unallocated space (space not associated with a file) on the drive. Examining unassigned space to attempt to recover deleted files is the typical first-line process employed in a forensic data recovery effort.

In contrast, Commvault stores data in what is known as a deduplicated format. When files are added, the file system checks for any whole or partial content matches among files that are already in the relevant storage container, and then simply maps those contents to the matching storage location. Given the amount of duplication often found in typical types of data such as emails and documents, this process of matching new files against existing data can result in significant reductions in the total volume of data stored. However, it can add certain risks: in particular, because the data is deduplicated, deleting a single file simply means deleting the relevant index entry for that file. There is no unique storage space from which the file could be recovered, and the index entry itself typically is not recoverable. As a result, once files are deleted from a deduplicated Commvault storage container, they cannot be recovered through traditional forensic techniques.

C. The Events of March and April 2021

1. How the March Deletions Occurred

By all accounts, the understanding within ITS was that as of March 30, 2021, the data migration was complete, and the Commvault software was now storing data to, and retrieving data from, the on-premises storage servers at City Hall.¹³² Thus, on Tuesday, March 30, 2021, the backup technician began the process of “cleaning up” Commvault clients and policies he believed to be no longer needed post-migration.¹³³

On March 30-31, 2021, the backup technician executed a series of deletions affecting 17 client policies and five storage policies.¹³⁴ Together, these policies primarily governed the archiving of data that DPD employees had saved to the DPD K Drive.¹³⁵ As a result of deleting these policies, any archives created under those policies were automatically deleted from the cloud by Commvault. Thus, the stubs that related to files stored on the DPD K Drive and that the backup technician had inadvertently transferred to the new storage servers at City Hall could no longer be rehydrated, because the archives had been deleted.

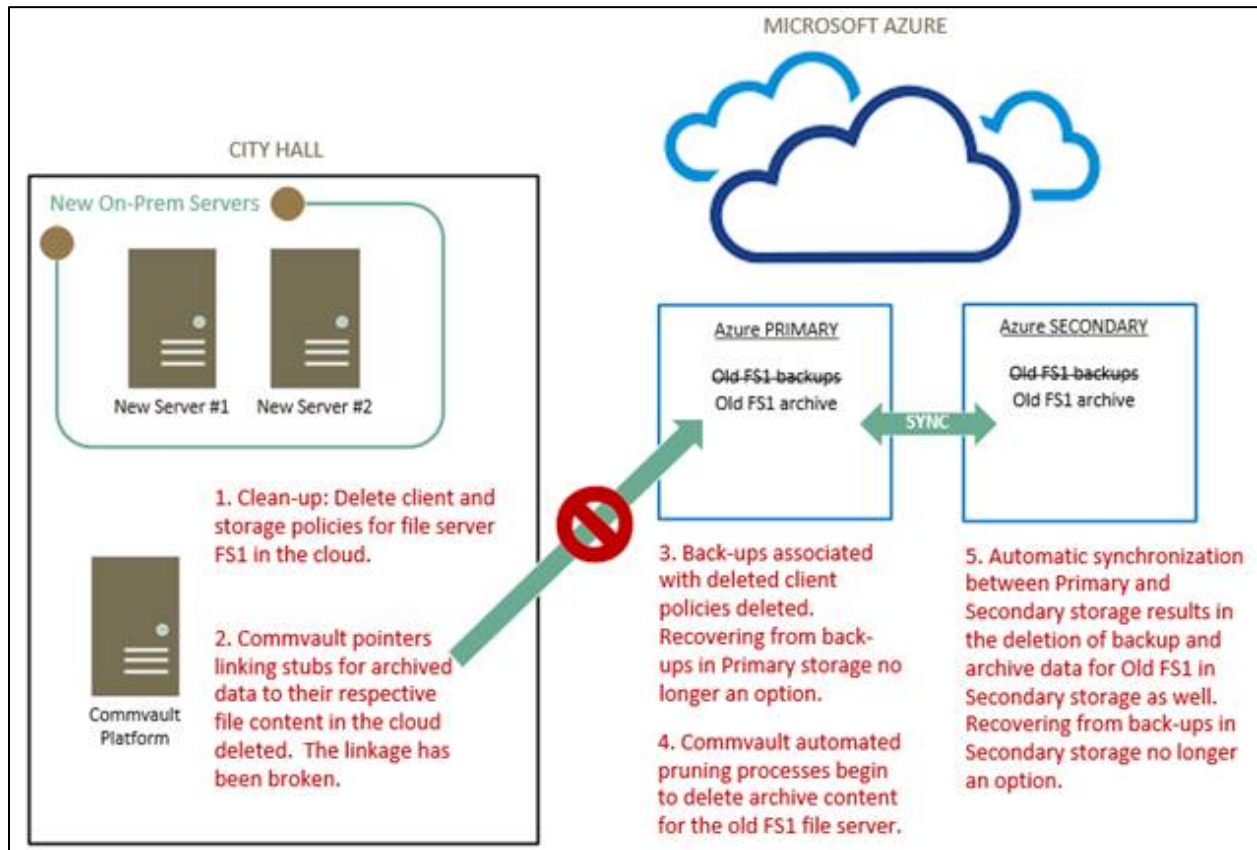


Fig. 3 – Depiction of deletion events

There are safeguards within the Commvault system to mitigate the risk of unintentional data deletion. For instance, to delete a storage policy, Commvault will prompt the end user regarding whether they want to proceed. If the user does wish to delete, they must manually type the phrase “erase and reuse media” as shown in the figure below.¹³⁶

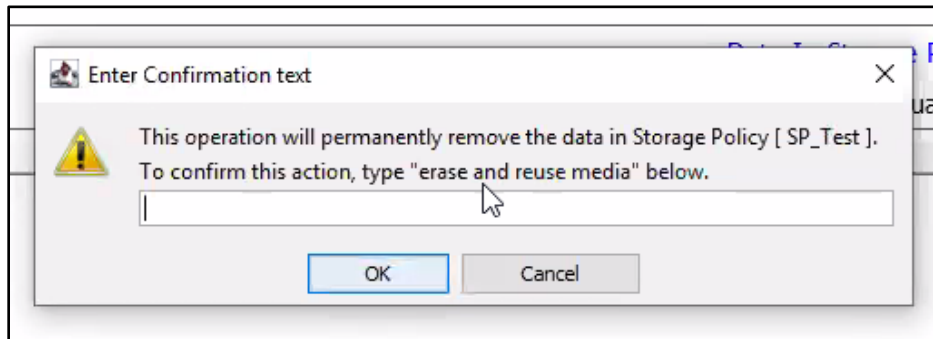


Fig. 4 – Commvault Policy Deletion Confirmation Message

Commvault provides similar warnings for deletion of a client.¹³⁷ In this case, the Commvault software notified the backup technician twice that proceeding with hard client deletions would result in the deletion of data.¹³⁸ Commvault support documentation states that such data becomes unrecoverable unless there is a backup containing information on the deleted entity (*i.e.*, storage policy or client).¹³⁹ The backup technician proceeded with the deletions, despite the warnings.

When interviewed, the backup technician confirmed he understood the secondary cloud storage facility in Arizona no longer existed at the time he proceeded with the above client and storage policy deletions because it had been migrated to the on-premises server. He also confirmed that he knew that executing the hard delete command could result in the deletion of archived data.¹⁴⁰ However, the backup technician stated that he paid no attention to these notifications because he thought the data had already been moved, and these alerts pertained only to the old archive which, in his belief, had already been migrated to its new location.¹⁴¹ Therefore, he believed it was safe to delete.¹⁴² He acknowledged that he did not understand at the time that the rehydration process had not been properly completed for the four decommissioned servers (resulting in the loss of the archived data from those servers).¹⁴³

2. Discovery of Issue within ITS

The first notification to ITS of any inaccessible archived data occurred on the morning of Monday, April 5, 2021, when ITS began receiving support tickets from DPD regarding inaccessible K Drive files.¹⁴⁴ Once the backup technician became aware of a potential issue, he immediately stopped the “clean-up” process that began on March 30, 2021.¹⁴⁵

That afternoon, the backup technician created a support ticket with Commvault that had the description: “Archived and stubbed files not being recalled.”¹⁴⁶ The backup technician then notified his supervisor, the IT Manager for Servers and Networking, that he had made a “mistake” the week prior.¹⁴⁷ Specifically, he informed his supervisor that he had deleted a number of clients tied to old servers which may have resulted in the deletion of a significant volume of files.¹⁴⁸ He

said that he informed his manager that DPD had been calling to report an inability to access data, which the backup technician now believed to be the result of his client deletions.¹⁴⁹

Throughout the following week, the backup technician and the ITS cloud administrator worked with Commvault and Microsoft, respectively, on potential avenues for remediation and/or recovery.¹⁵⁰ Among other things, the ITS cloud administrator contacted Microsoft to determine if the “soft delete” feature was enabled for the City’s storage accounts.^J Microsoft confirmed that the soft delete feature had not been available when the City initially switched to the Azure cloud and had never subsequently been added so it was not an option for recovery.¹⁵¹

On the morning of Tuesday, April 6, 2021, the IT Manager for Servers and Networking informed the Infrastructure Assistant Director of the incident and the extent of the known impact at that time.¹⁵² The Infrastructure Assistant Director reached out to the City’s Chief Information Officer on the evening of Tuesday, April 6, 2021.¹⁵³ At this time, the backup technician was actively working with Commvault to attempt to retrieve the lost data.¹⁵⁴

The Senior IT Manager of Public Safety was notified by the IT Manager for Servers and Networking on April 8, 2021 about the issue.¹⁵⁵ At this time, a DPD detective submitted a high-priority support ticket stating that he was not able to access certain files on the K Drive.¹⁵⁶ No one within ITS activated the City’s IRP at that time.

During a meeting on April 10, 2021, DPD was notified that files for multiple divisions had been deleted and might be unrecoverable.¹⁵⁷ The server team then provided a spreadsheet to begin narrowing the scope of what was lost.¹⁵⁸ The Senior IT Manager of Public Safety and the ITS Business Relationship Manager to DPD did not take further initial action beyond setting up a separate, prioritized queue for support tickets submitted by DPD related to the K Drive.¹⁵⁹

After consulting with both Commvault and Microsoft, the ITS server team provided a breakdown of events to the CIO.¹⁶⁰ Subsequently, on April 13, 2021, the CIO informed the Assistant City Manager via email of a “mass data loss occurring because of an error during the performance of routine file transfers from Azure storage to City Hall storage of the DPD file archives.”¹⁶¹

3. Notification to DPD Leadership

The Senior IT Manager of Public Safety attended a DPD Command Staff meeting on Monday, April 12, 2021 at DPD headquarters that included all the Chiefs, the majors for the substations and bureaus, and the IT team supporting DPD.¹⁶² The Senior IT Manager of Public Safety announced at the Command Staff meeting that ITS was working on an issue affecting the K Drive and directed DPD employees to submit a support ticket if a file believed to be inaccessible on the K Drive was needed for a court case.¹⁶³ The Senior IT Manager of Public Safety later

^J Interview of Witness on Nov. 5, 2021. Soft delete is a function available in Azure that protects files from accidental deletes or overwrites by maintaining the deleted data in the system for a specified retention period (between one and 365 days) selected by the customer. During the retention period, a soft-deleted object may be restored to its state at the time of deletion. After the retention period has expired, the object is permanently deleted. *See Soft Delete for Blobs*, Microsoft Azure (Jan. 27, 2022), <https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-blob-overview>.

provided DPD with a memorandum detailing a two-step process that involved (1) submission of a ticket to ITS regarding missing files and/or folders, and (2) providing a list of missing files and/or folders to be “restored.”¹⁶⁴ Eleven tickets were submitted by the end of that work week, and by the following Monday, there were 23 tickets in the queue.¹⁶⁵

On April 19, 2021, and due to the rising number of issues with accessing K Drive files, the DPD Chief of Police released an internal memo to all departmental personnel stating:

IT Services have received reports of missing files or folders from network drives. All departmental personnel are asked to please check if any files or folders are missing from their network drives. If you are missing files or folders, please follow the steps in the attachment to restore the missing files or folders.¹⁶⁶

Included with the Chief’s memo was the above-referenced memorandum written by the Senior IT Manager of Public Safety outlining the steps officers could take to “have [their] missing files or folders restored.”¹⁶⁷ It is clear from all of our conversations with DPD and from the wording used in the notification to employees from the Senior IT Manager, such as “restore,” that DPD did not understand at the time that the data was unrecoverable.¹⁶⁸

4. Role of Commvault Support

As described above, the backup technician opened a Commvault support ticket on the afternoon of April 5, 2021. Within a few hours, the assigned Commvault Support Engineer had identified the cause of the problem: that “stub recalls were failing because the stubs were tied to deleted clients that were deleted last week.”¹⁶⁹ The Commvault Support Engineer further explained that the data loss appeared to have been caused by a failure to properly “rehydrate” relevant data:

From discussion, the stubs from the clients in question were migrated to new hardware, however, not all of the data was re-hydrated which is required in order to re-stub the data to associate with the new client. As a result some of the old stubs were still associated to the previous client, and deleting the clients removed the metadata from the Commserve database and also triggered pruning from cloud storage . . . the data required to rebuild the index has been pruned from the Azure cloud library, so that data is physically inaccessible at the moment.¹⁷⁰

In other words, Commvault explained that the backup technician had copied the placeholder stubs instead of the file contents, and that this resulted in automatic deletion of the archived data after the backup technician deleted the relevant clients and storage policies in Commvault.

Commvault support worked with the backup technician over the next few weeks to provide a clearer picture of the impact of the deletion. On April 15, 2021, the Commvault Support Engineer confirmed that 4.1 million stub files had been affected—these stub files were “located on the destination file servers that were tied to the deleted source clients, which were deleted on March 31.”¹⁷¹ On Tuesday, April 20, 2021, the Commvault Support Engineer further confirmed that “the jobs tied to the deleted clients pre-dating the point when the incident occurred [on March 31] have all still failed [data] verification thus far, meaning none of the data from affected jobs is recoverable.”¹⁷²

In the support-ticket regarding the Data Loss Incident, Commvault subsequently memorialized the following “Incident Resolution”:

Customer unknowingly migrated stubs without rehydrating the data and then deleted the original clients so data was pruned and unrecoverable. Worked with development to provide [a] list of affected stubs and proper steps/documentation for requested stub migration scenarios to prevent [the] issue going forward.¹⁷³

Additionally, Commvault Support concluded that the underlying cause for the incident was “Commvault (Configuration and Product),” while the secondary cause was “General Knowledge/Training.”¹⁷⁴

5. Ongoing Deletions through August 2021

Despite the issues resulting from the deletion of client and storage policies, the backup technician continued hard deletion of clients from Friday, May 7, 2021 through Thursday, August 5, 2021.¹⁷⁵ A full listing of these deletions is provided in **Appendix B**. These deletions indicate that the backup technician failed to appreciate the magnitude of the incident and that his deletion of client and storage policies was not consistent with Commvault guidance. Ultimately, however, the data subject to these deletions was either backed up elsewhere, or had not been archived by Commvault, so no data was actually lost.

6. Evidence of Motive

While examining the backup technician’s motives is not a core purpose of this Investigation, it may be worth noting that we did not uncover any evidence suggesting that the backup technician had malicious intent or criminal purpose in deleting City data. Multiple witnesses volunteered their opinion that there was no malice in the backup technician’s actions, and no documentary or testamentary evidence suggested the backup technician had any ulterior motive for his actions. Ultimately, however, investigative conclusions as to the backup technician’s intent will be the purview of the law enforcement agencies investigating the Data Loss Incident, who have may access to additional sources of evidence and investigative tools.

D. August 2021 Discovery and Audit

1. DA Creuzot’s Memo and Press Release

On Tuesday, August 3, 2021, the Division Chief of the Grand Jury and Intake Division at the DA’s Office contacted a DPD Chief because some prosecutors had heard about a possible data loss.¹⁷⁶ On Friday, August 6, 2021, ITS told the DA’s Office that the City had discovered that multiple terabytes of DPD data had been deleted during a data migration in March.¹⁷⁷

In attendance at that virtual meeting were the City’s CIO, the Infrastructure Assistant Director, several DPD Chiefs, and DA Creuzot, along with other members of the DA’s staff.¹⁷⁸ DA Creuzot requested precise information regarding the deletion, and in the late afternoon of Wednesday, August 9, 2021, DPD relayed the following information from ITS: that approximately 22 terabytes of DPD data had been deleted, approximately 14 terabytes were recovered, and approximately eight terabytes remained missing and were believed to be unrecoverable.¹⁷⁹ Shortly

after, DA Creuzot released an internal memorandum to his staff and a letter to judges disclosing the missing data from DPD's network drive.¹⁸⁰

2. The August Audit and Activation of Incident Response Plan

After the meeting with the DA's Office and DPD's discovery of inaccessible FUSION files, the City's CIO determined that a broader assessment was necessary.¹⁸¹ This included a review of the migration, backups, archives, and anything else in which the backup technician may have been involved.¹⁸² This broader assessment also included a larger team, including the City Chief Information Security Officer's ("CISO's") team and individuals beyond ITS, such as outside consultants and Commvault support. In mid-August 2021, Commvault conducted a broad review of the City's servers.¹⁸³ During this review, Commvault found that the City's FUSION server had also been impacted, not from the data migration or the March deletion, but from a separate storage policy the backup technician had deleted in January 2021.¹⁸⁴

Because Commvault discovered there had been additional data loss beyond the initial discovery, on August 26, 2021 the CISO activated the City's IRP in order to conduct a more thorough analysis of the data loss.¹⁸⁵ Once the IRP was activated, the IR manager worked with DPD and ITS to assess the incident using the risk matrix outlined in the IRP.¹⁸⁶ The IR manager later engaged Commvault, the ITS security team, and DPD.¹⁸⁷

E. Data Recovery Efforts

The CIO identified two different sets of recovery efforts: one occurring prior to Friday, August 6, 2021, and the other occurring after August 6, 2021.¹⁸⁸ In the initial phase of recovery, the backup technician and the cloud administrator worked with Commvault and Microsoft during the first few weeks to assess and determine options, methods, and approaches to recover data.¹⁸⁹ Commvault identified 8.5-8.7 million relevant stubs through its investigation, and ITS, in coordination with DPD, determined that they mapped to 17,484 DPD cases and 966,018 case-related files.¹⁹⁰ Many stubs related to files that were not tied to a case, such as memos or other administrative documents.¹⁹¹ The recovery team worked with DPD to correlate the 17,484 cases to officers.¹⁹²

After August 6, 2021, ITS took a different approach to recovery.¹⁹³ The CISO was put in charge of weekly Friday meetings with DPD and the DA's Office beginning August 20, 2021,¹⁹⁴ where he provided updates on the recovery effort and what data was found.¹⁹⁵ The CISO also requested that his Senior Manager for Compliance, Risk, and eDiscovery assemble a team (the "Recovery Team") to begin the process of determining what data was lost and recovering it.¹⁹⁶ DPD and the DA's Office provided the CISO with two lists of priority cases to review—an initial list containing approximately 600 prioritized cases and a second list containing approximately 1,100 prioritized cases.¹⁹⁷ The recovery effort focused not on recovering the files that were deleted, but on searching for potential duplicates of the data in other locations, such as Office 365, OneDrive, SharePoint, Teams, or any other secondary location.¹⁹⁸ The Recovery Team searched the City's Microsoft Office 365 Compliance Center¹⁹⁹ for key terms potentially relevant to each case, such as the name of the defendant, date of offense, address, name of the victim, type of case, case number, or name of the officer.²⁰⁰ If a match was found within the contents of a file, the file was copied to a separate repository that was created specifically for the recovery effort.²⁰¹

To date, the Recovery Team continues to track and report metrics on the document search effort to DPD, and then shares the metrics with the DA’s Office. The Recovery Team currently has conducted searches for approximately 36% of the 17,484 cases.²⁰² The Recovery Team completes approximately 100-200 searches a week, at which rate the CISO estimates the project will be complete by late 2022.²⁰³ To date, the Recovery Team has identified 4,137,272 files that potentially match one of the 966,018 lost case-related files.²⁰⁴

The following table summarizes the current status of the Recovery Team’s search process:²⁰⁵

Category	Total Volume	Volume Completed to Date	Percent Completed to Date
DA Priority Cases	1,081	1,081	100%
All Cases	17,494	6,253	35.7%

VII. Root Cause Assessment

A. Proximate Cause

As detailed in this Report, the Investigation confirmed that the most immediate cause of the data loss was the Commvault deletion commands that the backup technician executed in the course of data migration. The backup technician stated he took these actions in an effort to “clean up” data after migrating City servers from Azure to the on-premises data center at Dallas City Hall.²⁰⁶ When he was interviewed, the backup technician acknowledged that he made a mistake by deleting relevant clients without verifying their data was duplicated elsewhere, and that he did not fully understand the implications of his actions.²⁰⁷ We uncovered no indication that the backup technician intended to cause data loss or other harm to the City’s systems; rather, he appears to have been attempting to carry out the data migration consistent with his sincerely-held understanding, although flawed, of the Commvault software. The consequences of his actions were dire. The backup technician acknowledged, and all other relevant interviewees agreed, that the backup technician’s actions resulted in the deletion of at least 22 terabytes of archived data.^K Further, both the IT manager and the Infrastructure Assistant Director indicated that during their investigation of the Data Loss Incident, they came to understand that the backup technician’s “clean up” process was not done in accordance with appropriate Commvault process, nor was it called for by the approved Change Order for the migration project.²⁰⁸

Despite bearing primary responsibility within ITS for Commvault, evidence suggests that the backup technician did not have enough expertise with the platform to understand its complexities and nuances. The backup technician completed a five-day, entry-level training course

^K Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 22, 2021; Interview of Witness on Dec. 15, 2021; Interview of Witness on Jan. 5, 2022. Based on our validation work, the total initial data loss was approximately 23.94 terabytes, and the total net data loss was approximately 20.68 terabytes after recovery of 3.26 terabytes. See Section IX. Twenty-two terabytes represents the approximate volume of data loss that ITS and DPD had identified as of early August 2021. Interview of Witness on Nov. 22, 2021.

in 2018 when the City transitioned to Commvault. This training covered topics such as deployment, storage configuration, storage policies, monitoring, security, and data management.²⁰⁹ However, the backup technician did not receive additional Commvault training until almost three years later, in 2021.²¹⁰ The Infrastructure Assistant Director instructed the IT manager to send the backup technician to Commvault training due to an incident that had occurred in 2019 in which Commvault backups had stopped running after a firewall configuration change.²¹¹ Even though this incident occurred in 2019, the backup technician did not receive the additional training until January 2021. Out of the three supplemental training courses that he attended, two were repeats of entry-level courses taken back in 2018.²¹² In short, the backup technician’s knowledge and understanding of Commvault were inadequate for his role and responsibilities at ITS. Going forward, leadership in ITS needs to ensure that employees’ knowledge and skills are commensurate with their roles in the department.

In addition, a two-person authentication process should have been in place for key steps in the data migration, such as policy and client deletions. This could have led to questions concerning the deletions by a second trained individual. More broadly, a second individual at ITS could have been designated as a subject matter expert on Commvault to provide vetting and input on all data migration steps, including the Change Order and the process for implementing it. More expertise in Commvault was needed within ITS at both the line and leadership levels. While there is no guarantee these steps, if in place, would have prevented the data loss, they would have almost certainly reduced the risk.

B. Systemic Contributors

While the backup technician’s actions were the most immediate cause of the data loss, other risk factors were present.

First, ITS had not implemented any data redundancy plan prior to the Data Loss Incident, which might have allowed for recovery of the lost data. For example, had a “soft delete” function been in place, any deleted data would have remained available and recoverable after deletion. Likewise, if a secondary data repository had been in use, most, if not all, of the data likely would have been recoverable.^L Interviewees differed in their accounts of exactly why the data stored in the secondary cloud was deleted prior to the backup technician’s deletion activities in Commvault.^M But the broader and more significant point is that none of the responsible parties at ITS—including the backup technician and his supervisors—took steps to ensure that *any* form of data redundancy was in place before executing commands in Commvault that posed potential adverse consequences for multiple terabytes of critical City data.

Beyond the need for data redundancy, the Investigation identified inadequacies in ITS procedures for reviewing and approving change orders and other changes to the City’s systems. The City has a change management process in place to review proposed changes²¹³ that includes a Change Advisory Board (“CAB”) composed of representatives from the business and ITS²¹⁴ and a technical review board that issues final approvals.²¹⁵ However, the individuals we interviewed

^L This recoverability would depend on precisely how the secondary repository was configured—which would again have been subject to determination at ITS to maximize redundancy and recoverability in the event of any incident.

^M See footnote G.

who reviewed the Change Order acknowledged that they did not have much understanding of the complexity of Commvault, and essentially were relying on the backup technician to identify and execute the appropriate steps.²¹⁶ It also appears that little attention was given to identifying potential risks—such as a lack of data redundancy—prior to executing the Change Order. Going forward, ITS needs to more carefully and systematically evaluate the need for significant changes and how they should be implemented. The execution of the 2020-2021 data migration appears to have been symptomatic of a larger lack of strategy and planning around how the City intended to use the cloud to meet its information technology needs.

Deficiencies in inter-departmental communication and coordination appear to have contributed to the Citywide impact of the data loss. For example, the archiving of data from the FUSION server came as a surprise to the DPD personnel managing that system, and was only discovered when DPD needed to access cell phone evidence.^N We also heard from multiple stakeholders within DPD that there is a lack of sufficient consultation with DPD relating to the appropriateness and criteria for archiving data for the department.²¹⁷ Most interviewees were not aware that archiving had been in place, and those that were stated they had not been able to provide meaningful input into the determination of archiving criteria.²¹⁸ Moreover, a broader question exists around the wisdom of archiving DPD case data on the current timetables given that, unlike typical internal files that grow stale after a period of time, this data is collected in the course of active police investigations that may take months or years to go to trial. These examples point to a significant lack of coordination, collaboration, and information sharing taking place between ITS and the internal customers it needs to support.

Further, as set forth in detail above, ITS became aware of the possibility of a large-scale data loss no later than April 5, 2021. The backup technician was aware as early as April 9, 2021 that the data deleted from the cloud storage facilities as a result of his client and storage policy deletions was unrecoverable.²¹⁹ By all accounts, ITS, DPD, the CIO, and the Assistant City Manager were then briefed at some level regarding the suspected data loss in the following weeks. However, it is not clear that parties outside ITS fully understood the potential scope or implications of the data loss. For several months, the loss of evidence was addressed on essentially a piecemeal basis outside ITS, with individual DPD officers submitting support tickets for help locating individual inaccessible files. Messaging to DPD regarding the recoverability of the impacted data remained ambiguous in the weeks following the discovery of the data loss even though ITS was told by Commvault as early as April 9, 2021, that the relevant data was unrecoverable in its original format (*i.e.*, from cloud storage). Discussions between ITS and Commvault in the early April timeframe indicate a shift in focus to obtaining a granular understanding of impacted K Drive data.^O In contrast, until ITS shared the full impact of the data loss in early August, multiple DPD witnesses believed that the data was not permanently lost, but merely temporarily inaccessible, and possibly recoverable in the future.²²⁰

^N Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 8, 2021. Fortunately, because the cell phone device at issue was still in police custody, the detectives were able to request a new search warrant and reacquire the forensic image. Interview of Witness on Nov. 9, 2021.

^O Commvault's Director of Customer Support confirmed they worked with the City for a period of time to determine the impact of deletion, and they determined that data was effectively gone. Interview of Witness on Dec. 20, 2021.

Finally, notwithstanding ITS' early understanding of the scope of the data loss, the City did not activate its IRP in April 2021 in response to the Data Loss Incident.²²¹ The City's IRP was not invoked until August, approximately four and a half months after the data loss occurred. There is broad agreement within ITS that this should have been done in April 2021.²²² It is unclear precisely and to what extent invoking the IRP would have impacted the City's ability to potentially recover data, but at minimum, doing so would have helped clarify the scope of the data loss. In addition to helping clarify the scope of the data loss, invoking the IRP in April 2021 could have enabled better inter-departmental communication regarding next steps.

C. ITS Report Assessments

In connection with this Investigation, we reviewed the ITS Report in depth and conducted detailed interviews with its authors. The majority of the ITS Report's recommendations relate holistically to the maturity of ITS' systems and processes, rather than specifically to the Data Loss Incident.²²³ The ITS Report's specific recommendations related to the Data Loss Incident—such as enabling the “soft delete” feature going forward—are generally consistent with those in this Report.

While ITS' broader and more holistic challenges are not the core focus of this Investigation, information we reviewed validates the need to continue building organizational maturity within ITS, consistent with recognized industry standards and best practices. In October 2020, the CIO hired Forrester—a research and advisory company—to conduct an enterprise IT maturity assessment for the City after he saw certain deficits in its functioning.²²⁴ Forrester found, in part, that “major challenges exist in the organization culture, communications, and collaboration. A complex landscape, lack of mature operational processes, and mounting technical debt pose major risks which create impediments to realize the value of increasing technology investment.”²²⁵

ITS' lack of organizational maturity is the landscape on which the specific processes and actions that led to the Data Loss Incident played out. Addressing these holistic issues does not have the same immediate urgency as do the specific root causes of the Data Loss Incident. That said, the City would be well-served by ITS' continued development in this area.

VIII. Effects of the Data Loss Incident

A. Effects on DPD

As discussed above, interviewees indicated that because of network latency and storage capacity issues, DPD historically did not have a consistent process across all divisions to save digital evidence.²²⁶ Ironically, this lack of a consistent file-saving practice likely prevented the Data Loss Incident from having far more significant DPD-wide consequences.²²⁷ The City is fortunate that DPD's data was saved in other locations such as officers' desktops, email, and external DPD hard drives and thumb drives.²²⁸

Unfortunately, DPD's Family Violence Unit appears to be unusual in that it was the only unit in which officers consistently followed a specific protocol for saving digital evidence to the K Drive.²²⁹ The intent behind this is logical and reasonable. The Family Violence Unit has thousands of cases per year (more than any other unit that investigates crimes against people)²³⁰ and numerous officers that transfer in and out of the Unit.²³¹ As a result, there was significant

benefit to maintaining a strict adherence to a consistent electronic evidence protocol. Unexpectedly (and tragically), because the Family Violence Unit followed a strict protocol to save evidence to the K Drive, the Family Violence Unit was disproportionately affected by the Data Loss Incident's K Drive deletions.²³² This loss was exacerbated by the Family Violence Unit's transition to a paperless filing system in 2019.²³³

Notably though, DPD personnel expressed skepticism that the data loss would have a significant effect on prosecuting criminal cases that fall within the jurisdiction of the Family Violence Unit.²³⁴ This belief is based on the fact that family violence cases are rarely suspended because decisions about whether a case will be presented to the DA's Office are made relatively quickly as compared to other types of cases.²³⁵ A member of the Family Violence Unit explained that "[w]e pretty much always know who the suspect is and can make our cases a lot faster [than other divisions]. Unlike robbery where they might never know [the perpetrator]. 99.9% of the time, we have a suspect."²³⁶ As the data loss was restricted solely to archived data—which would not include data from active (and therefore recent) family violence cases—many at DPD believe that any lost data was not likely going to be needed in any active court case.²³⁷ That said, while it may be unlikely that any archived data would be needed for an active case, this does not mean that the lost data did not hold potential current or future evidentiary value. Since family violence offenders have a high recidivism rate and often commit crimes of violence, the lost archived evidence may be useful in future cases or be needed to maintain a conviction in the appeal of a case.²³⁸

B. Effects on the DA's Office and the Criminal Justice System

As noted above, the DA's Office was unaware of the data loss until July 30, 2021.²³⁹ At first, the DA's Office was highly concerned about which cases might have been impacted by the Data Loss Incident.²⁴⁰ There was also concern about the DA's Office complying with its obligations under the Michael Morton Act.²⁴¹ This Act requires the State to turn over exculpatory evidence and make a record of the evidence that has been disclosed to the defense.

Fortunately, those concerns have not materialized. Uncertainty about what data was actually lost may, in some limited cases, be slowing the pace of prosecution due to motions from defense counsel.²⁴² One ADA also identified a murder case in which the prosecution could not get quick verification from DPD that no data was missing. As a result, the DA's Office had to announce it was not ready to go to trial and the suspect was released on a personal bond.²⁴³ In general, however, DA's Office interviewees confirmed the data loss has not had a substantial impact to date on the DA's Office's ability to prosecute active cases.^P Both DPD and the DA's Office felt that the lost data will not substantially affect the DA's Office's ability to carry out its mission "to enhance public safety and community well-being by supporting victims, holding people who commit crimes accountable, and engaging the community to prevent harm."²⁴⁴

^P Interview of Witness on Dec. 7, 2021; Interview of Witness on Dec. 7, 2021; Interview of Witnesses on Jan. 25, 2022; Interview of Witness on Jan. 25, 2022. While the data loss has not stopped prosecutors from bringing cases, in some instances criminal defense attorneys have cited the data loss event in filing motions requesting an independent party to review the case file for completeness. Interview of Witness on Dec. 7, 2021; Interview of Witness on Jan. 25, 2022. Thus far, most, if not all, such motions have been denied. Interview of Witness on Dec. 7, 2021; Interview of Witness on Jan. 25, 2022.

IX. Volume of Data Lost

The Investigation validated the volume of data lost in the Data Loss Incident. The details of this work are set forth in **Appendix C**, but at a high level, our validation process included discussions with ITS, and a review of relevant documentation and data—including Commvault logs and reporting from the City’s Azure dashboard. We validated that the City lost a net total of approximately 20.68 terabytes of archived data in its original format, after recovering approximately 3.26 terabytes that were initially believed lost. The lost data all came from the City’s K Drive (including Family Violence) and FUSION servers.

The following table summarizes the approximate gross and net data lost from each category of server:

Servers	Initial Data Loss	Volume Recovered	Net Data Loss
K Drive	10.77 TB ²⁴⁵	3.26 TB ²⁴⁶	7.51 TB ²⁴⁷
FUSION	13.17 TB ²⁴⁸	0 TB ²⁴⁹	13.17 TB
<u>Total:</u>	23.94 TB	3.26 TB	20.68 TB

As noted, further details are given in **Appendix C**.

X. Previously Lost Data

We reviewed documents and questioned witnesses regarding the City’s historical policies and procedures for the storage, backup, and archiving of its data.²⁵⁰ The Investigation did not identify any notable data loss incidents other than the Data Loss Incident at issue here.

XI. Recommendations

Based on this Investigation, the City should consider at least the following next steps to mitigate the risk of similar data loss events occurring in the future.

A. Data Safeguards and Redundancy

Proper redundancy controls need to be established, particularly as relates to archived data. Opportunities for improvement include the following:

- Design and implement a testing and verification process for data migration. This should include a process to test and verify the data migration process prior to any migration or deletion of data. The verification process should include a testing environment with test data that can be used to minimize risk to the production environment.
- Require two-person authorization for any process that can have a major impact to the environment if not performed appropriately or in accordance with policy (such as the client and storage policy deletions).

- Implement the “soft delete” feature in Azure. We understand this has been done and recommend that ITS keep the “soft delete” functionality in place. ITS should also ensure that any analogous protective features are enabled on any future backup and archive systems the City may establish.

B. Consult Vendor Experts as Needed

ITS should plan (and budget for) consultation with outside experts when undertaking critical projects, such as data migration and implementing enterprise-wide technology solutions.

- Regardless of what backup and archiving system is used, ITS should involve subject matter experts during data migration planning and, if possible, during any critical data migration. The consultation should include validating relevant or impactful changes or specific modifications proposed to the clients and policies attached to migrated server data.
- ITS should involve other vendor experts, such as subject matter experts, when needed in connection with future projects.

C. DPD Resources and Staffing

As described above, a lack of adequate IT resources at DPD constituted a contributing factor in the Data Loss Incident. Going forward, the City should take time to carefully evaluate DPD’s budgetary, resource, and staffing needs with the goal of remedying the issues identified in this Report. In particular:

- As described more generally below, the City should consider establishing a Departmental CIO at DPD.
- DPD should be allocated adequate budget to build out its IT infrastructure, including adding additional on-premises and/or cloud storage, Evidence.com capacity, and network throughput/bandwidth as needed.
- In addition to budget allocation, the procurement process for critical infrastructure purchases should reflect input from individuals who understand DPD’s unique data and storage needs. It should also reflect the results of any IT infrastructure assessment (discussed below) and/or strategic plan that DPD may establish for its future long-term IT development.
- The City should consider conducting a full IT infrastructure assessment for DPD in order to fully identify all resource needs (including ones that may be beyond the scope of this Report). This could establish specific projects and milestones to implement any recommendations arising from the assessment.

D. ITS Staffing and Training Needs

ITS should consider expanding and refining training for its employees to ensure that employees acquire and maintain adequate subject matter expertise with respect to critical systems.^Q In particular, the City should:

- Ensure that ITS staff designated as technical subject matters experts have proper training with the technology being used.
- Solicit input from key vendors (such as Commvault and Microsoft) on what skills and training would be needed to have one or more fully qualified subject-matter experts on staff at ITS.
- Cross-train employees sufficiently to ensure that there is not a single point of failure for key systems if a particular ITS resource is unavailable.

E. Budgetary Issues and Allocation

ITS indicated that it currently has adequate budget for current needs.²⁵¹ However, the input of important stakeholders, such as DPD and the DA's Office, does not seem to be fully taken into consideration. Reportedly, requests for needed items are routinely declined due to lack of budget. While the City's overall procurement and budgeting process is beyond the scope of this Report, preliminary recommendations for the future include:

- The City should ensure a smoother and more streamlined procurement process that works well for different stakeholders by allowing them to efficiently take advantage of available IT spend.
- To the extent that budget constraints are an issue, added budgetary needs relevant to data backup/migration should be appropriately evaluated and given proper weight considering the events described in this Report.
- Budgetary control and planning should include input from ITS data governance stakeholders. For example, this Investigation revealed that the person that owns the budget line item for the migration to cloud was not part of the decision-making around the migration, and thus could not provide valuable input.²⁵² Such stakeholders should be involved in budget-setting conversations to ensure that the City's data needs are appropriately met.

^Q These recommendations do not address backfilling the backup technician's position at ITS, as it is our understanding that the department has hired two new resources since the Data Loss Incident to be subject-matter experts and lead ITS' efforts with respect to Commvault.

F. IT Management Protocols and Practices

Based on our interviews, it appears the operating model within ITS has traditionally been reactive in nature and largely siloed from customer departments. ITS should aim to shift to a more strategic and proactive operating model. In particular:

- The City should develop a cohesive vision of where it wants to be in the near, mid, and long-term (planning out at least 3-5 years). In connection with that process, ITS should work with the various stakeholders to understand what they need in terms of technology and personnel. Among other things, this will help inform decisions around spend and prioritization to resolve resource conflicts.
- The City should implement a clearly defined and carefully thought-out plan based on a strategic approach to building a backup architecture that works for the current state and planned growth. This plan would need to systematically take into account all relevant considerations. For example, the Investigation uncovered a pattern of decision-making within ITS that appears to have been based solely on cost. Going forward, ITS should find ways to evaluate needs with an eye toward strategic growth, with input around business needs from appropriate stakeholders in affected departments, and with consideration of potential first- and second-order implications of alternative courses of action.
- As part of planning for strategic growth, additional focus should be given to identifying and pursuing more scalable storage solutions. The volume of the City's data has grown at a breakneck pace and will continue to do so. ITS should investigate data storage options that are easily scalable to meet the evolving needs of the City, particularly DPD and other public safety departments that have a need to manage large volumes of critical data.

G. Departmental Protocols and Practices

The City should conduct a review of departmental policies and procedures related to data storage and backup. In particular:

- This should include ensuring that departments consistently save data to properly backed-up repositories.
- In connection with a review of data storage practices, a review of infrastructure and bandwidth for high priority departments (such as DPD) is needed. As discussed, multiple interviewees from DPD complained of inordinately slow speeds for upload and download, which discouraged adherence to existing storage guidelines. Attention cannot be focused only on creating more consistent policies and procedures around data storage if the underlying infrastructure does not allow critical departments to implement those policies efficiently.

H. Inter-Departmental Communication and Coordination

Based on this Investigation, both particularized and systemic communication difficulties between ITS and its customer departments (primarily DPD) impacted the Data Loss Incident and

subsequent remediation efforts. For example, departments outside ITS seemingly were not aware of how the Commvault archive system worked and what data would be archived. Consequently, these departments were not in a position to understand the potential scope or implications of the Data Loss Incident at the time it occurred. In particular, despite the availability of ITS liaisons, there appears to be a substantial disconnect between ITS and DPD. Numerous interviewees, not limited to just DPD interviewees, complained that ITS lacks a customer service mentality and does not understand the technological tools that DPD needs to successfully function.²⁵³ Therefore, going forward:

- Data stakeholders should provide the business requirements/data retention requirements and ITS should make recommendations to meet those needs. For example, the majority of DPD data is electronic evidence in support of criminal investigations, which is very different from typical business files and needs to be treated with the utmost care in close collaboration with DPD. Also, as noted, it appears DPD did not consistently follow protocols for digital evidence storage because of bandwidth and network latency issues. Any such problems should be raised and comprehensively addressed as part of the inter-departmental coordination process.
- The City should develop generalized processes to improve inter-departmental communication/coordination and visibility for all stakeholders. For example, when ITS eliminated the secondary cloud storage facility in Arizona, the disaster recovery leader and other application owners were not aware of these decisions, making the City vulnerable from a data recovery perspective.

I. Departmental IT CIOs

As referenced above, the City should consider establishing specific Chief Information Officer (“CIO”) roles within departments (such as DPD) that host critical data for the City. These individuals would report to the heads of departments, such as DPD’s Chief of Police. While ITS currently has liaisons who are responsible for communicating with customer departments, they are employed by ITS and do not appear to have in-depth familiarity with departments’ IT infrastructure, processes, or specific use cases for their data. Establishing formalized CIO roles at key departments such as DPD could serve as a significant step in mitigating the risk of a similar data loss event occurring in the future. Departmental CIOs could also be tasked with advocating for their departments in connection with IT budgeting discussions and educating ITS leaders on department-specific needs.

J. Citywide Assessment of Data Criticality

The City should conduct a Citywide assessment of data classification and criticality, consistent with the recommendations in the ITS Report and work already being done by the CISO’s team to develop the City’s IT maturity.

- The assessment should involve ITS, representatives from other relevant departments, and any other key stakeholders. Departmental representatives should be individuals who have adequate technical understanding of the City’s IT systems and are well-versed in their departments’ IT needs, as well as strategic growth goals.

- Such an assessment can be strategically scoped, but should focus on helping determine, among other things, the types of data each department is storing, the relevant systems and data custodians, whether the data is being backed up and how long it needs to be backed up, the impact if the data is lost, and acceptable disaster recovery limits for Recovery Time Objective (“RTO”) and Recovery Point Objective (“RPO”) for critical systems such as those used by Public Safety Departments. This information can be used to inform the budgeting and planning process for City IT system development going forward.

K. Reformulating the Data Recovery Effort

The City has currently spent a considerable amount of time and resources, both in employees and in total dollar, on its e-discovery search effort, and the CISO estimates it will spend \$750,000 from end-to-end.²⁵⁴ While the search effort is admirable for its thoroughness, the benefit of continued case-by-case e-discovery searches through late 2022 is potentially questionable given the relative cost. We recommend that the City give further consideration to potential approaches to prioritizing the cases being targeted in the e-discovery effort, identifying and storing potential case-related data in a less labor-intensive fashion, and giving serious consideration to stopping the effort at some point short of identifying files for all 17,484 identified cases.

XII. Conclusion

It is critical that DPD and its officers are able to collect and maintain evidence in a secure way that protects the integrity of each investigation.²⁵⁵ It is equally critical that the integrity of the digital evidence the DA’s Office relies on for its prosecutions be maintained and protected. Digital evidence is a key factor in many, if not the vast majority, of today’s cases, and lack of reliable data management could imperil successful law enforcement within the Dallas community.²⁵⁶ The DA’s Office must be capable of receiving large quantities of data from the law enforcement entities it serves, storing that data securely and properly, and then converting that data into evidence that can be introduced in a court of law subject to strict evidentiary standards. When digital evidence is deleted, misplaced, or mishandled, it can lead to the dismissal of criminal charges or prevent a jury from seeing valuable evidence that it needs in order to make its determination of guilt or innocence.

Unfortunately, the Data Loss Incident both directly imperiled the City’s law enforcement mission and is a symptom of much broader challenges that have the potential to pose significant challenges down the road. The City is fortunate that the impact of the Data Loss Incident has not been more significant.

Our report has identified both specific root causes and contributing systemic factors that led to the Data Loss Incident, as well as recommendations for remedial measures and opportunities for continued development of the City’s IT functions and processes. Our assessment in this regard is based on our expertise and independent judgment as applied to the statements of the witnesses we interviewed, and the voluminous record made available to us by the City.

While this Report may help confirm the circumstances and root cause of the Data Loss Incident, much work remains to address the issues that made the Data Loss Incident possible. We hope this Report is helpful to the City as it continues to evaluate next steps in remediation efforts as well as long term strategy concerning data pertaining to DPD.

XIII. Appendices

A. Appendix A – Chronology of Key Events Associated with Data Loss Incident

Date/Time*	Description of Event
2018	ITS implements Commvault as its backup solution, and eventually expands its use of Commvault to include archiving. ²⁵⁷
April 2019	ITS creates its Arizona-based Microsoft Azure storage account. ²⁵⁸
June 2020	The City hires a new Chief Information Officer (“CIO”). ²⁵⁹
July 23 - 28, 2020	The IT Manager for Servers and Networking emails a Microsoft representative requesting assistance in understanding the City’s storage setup and data centers, particularly in relation to large bandwidth charges. ²⁶⁰
August 21, 2020	The IT Manager for Servers and Networking emails the Infrastructure Assistant Director regarding the cost of Azure cloud storage and potential alternatives. ²⁶¹
August 24, 2020	A change order governing the data migration planned for early 2021 from the Azure cloud to on-premises storage at Dallas City Hall is submitted as a “Normal” change. ²⁶²
October 2020	The newly hired CIO hires research and advisory firm Forrester to perform an IT Maturity Assessment of ITS. ²⁶³
September 2020	ITS makes certain technical adjustments to its Arizona-based Microsoft Azure storage accounts to reduce egress charges. ²⁶⁴
December 16, 2020	Forrester shares the results of its IT Maturity Assessment with ITS leadership. The assessment lists out strengths, key opportunities, challenges, and recommendations for ITS, including recommendations related to disaster recovery and IT maturity. ²⁶⁵
January 10, 2021	The IT Manager for Servers and Networking emails the Infrastructure Assistant Director and notes that the Arizona-based storage will be deleted by the end of the week. ²⁶⁶
January 23, 2021	ITS turns off the archive in anticipation of data migration. ²⁶⁷
January 2021	The backup technician executes the data migration plan moving all server data in the Azure cloud to an on-premises location at Dallas City Hall. ²⁶⁸

* All times CDT.

Date/Time*	Description of Event
February 2021	The backup technician decommissions four of the migrated servers in Azure, which result in no reported errors or issues at that time. ²⁶⁹
March 4, 2021	The backup technician emails the ITS Cloud Administrator stating that he has put old DPD cloud storage offline as of the preceding day, and that he would monitor and confirm when the old storage could be deleted. He writes that it would probably be a good idea to wait at least one or two weeks to make sure no users were trying to access the files (seemingly to ensure all files were still accessible). ²⁷⁰
March 30 - 31, 2021	The backup technician begins the process of “cleaning up” data he believes is no longer needed post-migration by executing a series of client and storage policy deletions. Over the course of two days, the backup technician conducts a total of 17 hard client deletions and five storage policy deletions. ²⁷¹
April 5, 2021	ITS begins receiving support tickets from DPD regarding inaccessible K Drive files. ²⁷²
April 5, 2021 11:00 AM	The backup technician shuts off all Commvault data deletions, stopping the “clean-up” process. ²⁷³
April 5, 2021 12:08 PM	The backup technician creates a support ticket with Commvault with the description, “Archived and stubbed files not being recalled.” ²⁷⁴
April 5, 2021 12:30 PM	The backup technician notifies his supervisor, the IT Manager for Servers and Networking, that he made a mistake during clean-up the week prior. ²⁷⁵
April 5, 2021 5:22 PM	Commvault support identifies that “stub recalls were failing because the stubs were tied to deleted clients that were deleted last week.” ²⁷⁶
April 6, 2021 7:00 AM	The IT Manager for Servers and Networking informs the Infrastructure Assistant Director of the incident. ²⁷⁷
April 6, 2021 6:08 PM	A Commvault Support Engineer ran a search for broken stubs on the City’s servers. The Commvault Support Engineer also advises the backup technician to “not delete any clients as that’s where the backup data sits.” ²⁷⁸
April 6, 2021 9:27 AM	The Infrastructure Assistant Director informs the CIO of the situation. ²⁷⁹
April 7, 2021 (morning)	The Infrastructure Assistant Director and the CIO discuss via phone the data migration and potential impacts. ²⁸⁰

Date/Time*	Description of Event
April 9, 2021 4:58 PM	The Commvault Support Engineer tells the backup technician that the ticket will be escalated to the Commvault Development team so “they can assist with providing the next steps for compiling a list of unrecoverable stubs.” ²⁸¹
April 9, 2021 5:14 PM	Commvault Support confirms that “much of the data appears to be unrecoverable as ‘Soft Delete’ was disabled on the Azure storage account, and now customer is looking report [sic] of all impacted files.” ²⁸²
April 10, 2021	The IT Manager for Servers and Networking informs the Senior IT Manager of Public Safety and the IT team supporting DPD that, due to a missed step in the data migration, files for multiple divisions had been deleted and might be unrecoverable. The ITS team develops a spreadsheet to begin narrowing the scope of what was lost. ²⁸³
April 12, 2021	The Senior IT Manager of Public Safety announces at the DPD Command Staff meeting at DPD headquarters that ITS is working on addressing an issue affecting the K Drive. ²⁸⁴
April 13, 2021 2:53 PM	The CIO notifies the Assistant City Manager via email of a “mass data loss occurring because of an error during the performance of routine file transfers from Azure storage to the City Hall storage of the DPD file archives We are setting up a meeting with DPD leadership this afternoon.” ²⁸⁵
April 13, 2021	The CIO arranges a meeting with DPD leadership to work on the process for reporting any issues related to this data loss. ²⁸⁶
April 15, 2021 11:43 AM	The Commvault Support Engineer confirms that 4.1 million stub files have been affected. ²⁸⁷
April 19, 2021	The DPD Chief of Police releases an internal memo to all departmental personnel, asking all personnel to check for any missing files or folders and follow the identified steps to “restore” those files or folders. ²⁸⁸
April 20, 2021 1:14 PM	The Commvault Support Engineer confirms that “the jobs tied to the deleted clients pre-dating the point when the incident occurred [on March 31] have all still failed [data] verification thus far, meaning none of the data from affected jobs is recoverable.” ²⁸⁹
April 22, 2021	The CIO requests assistance from DPD to investigate the data loss. ²⁹⁰
April 27, 2021 3:28 PM	The backup technician writes a document entitled “City of Dallas_Data Migration Scenarios,” outlining the process he followed when moving archived data. The backup technician provides the document to Commvault support. ²⁹¹

Date/Time*	Description of Event
April 28 - May 7, 2021	The Commvault Support Engineer reviews the “City of Dallas_ Data Migration Scenarios” document with members of the Commvault Support, Development, and Professional Services teams. The Commvault Support Engineer notes that the document contains “incorrect steps.” Commvault support refines the steps for file archive migration and returns an edited copy of the document to the backup technician. ²⁹²
May 7, 2021	The backup technician executes a hard client deletion. ²⁹³
May 14, 2021	The backup technician reaches out to Commvault and requests a demonstration with Professional Services of the exact procedures and steps for data migration. ²⁹⁴
May 18, 2021	The backup technician follows up with Commvault, again asking to schedule a demonstration with Professional Services. ²⁹⁵
May 19, 2021	The backup technician executes a hard client deletion. ²⁹⁶
June 7, 2021	The backup technician executes a hard client deletion. ²⁹⁷
Around June 17, 2021	The migration scenarios demonstration with Professional Services occurs. ²⁹⁸
June 21, 2021	The backup technician executes nine hard client deletions. ²⁹⁹
June 23, 2021	The backup technician executes 19 hard client deletions. ³⁰⁰
June 24, 2021	The backup technician executes four hard client deletions. ³⁰¹
June 25, 2021	The backup technician executes one hard client deletion. ³⁰²
June 23, 2021	The backup technician executes 19 hard client deletions. ³⁰³
June 29, 2021	The backup technician executes two hard client deletions. ³⁰⁴
July 30, 2021	An Assistant Dallas County District Attorney is informed by officers that certain DPD files related to a pending prosecution were no longer available on the K Drive. ³⁰⁵
Early to Mid-August 2021	DPD reports to ITS that it cannot access files from FUSION. ³⁰⁶
August 3, 2021 3:56 PM	A Division Chief of the DA’s Office reaches out to a DPD Executive Assistant Chief for more information on the data loss. ³⁰⁷

Date/Time*	Description of Event
August 4, 2021	DPD forwards a request from the DA's Office for more information on the data loss to ITS. The ITS Business Relations Manager forwards the email to the ITS Executive Team. ³⁰⁸
August 5, 2021	The backup technician executes 11 hard client deletions. ³⁰⁹
August 6, 2021	DPD and ITS inform the DA's Office that, back in April 2021, the City discovered that multiple terabytes of DPD data had been deleted during a data migration of a DPD network drive. ³¹⁰
August 9, 2021	ITS informs DPD, who then informs the DA's Office, that between March 21, 2021 and April 5, 2021, approximately 22 terabytes of DPD data were deleted over the course of a few days, and approximately eight terabytes remain missing and are believed to be unrecoverable. ³¹¹
August 11, 2021	Dallas County Criminal District Attorney John Creuzot issues a memo regarding the data loss. ³¹²
August 11, 2021	The data loss issue begins receiving media attention.
August 12, 2021	Mayor Eric Johnson sends a memo to City Councilmembers B. Adam McGough and Cara Mendelsohn, stating he was "blindsided" by the news of the data loss and requested that the council members "call a joint special-called meeting of your committees to discuss the data deletion, the troubling lack of communication from city staff about what transpired, and the steps being taken to resolve the matter and prevent future consequences." ³¹³
August 12, 2021	The backup technician and IT Manager meet for an "administrative leave interview." ³¹⁴
August 13, 2021	A number of news outlets, including ABC News, Fox News, the <i>Dallas Morning News</i> , and the <i>New York Post</i> report that Jonathan Pitts, a murder suspect who was scheduled to go on trial that same week, was released on a personal recognizance bond from Dallas County jail after it was determined the evidence against him might have been lost. ³¹⁵
August 18, 2021	The Dallas City Council is briefed on the data loss during a closed, executive session. ³¹⁶
Mid-August 2021	Commvault conducts an audit of deleted clients and policies, which involves investigating other servers. Commvault determines that the FUSION server has also been impacted due to a storage policy deleted in January 2021. ³¹⁷
August 20, 2021	CISO begins hosting regular weekly meetings with DPD and the DA's Office, providing updates on the data recovery effort. ³¹⁸

Date/Time*	Description of Event
August 26, 2021 6:25 PM	The CISO activates the Incident Response Plan to conduct an analysis of the data loss, elevating it to the highest severity level under the Plan. ³¹⁹
August 26, 2021 6:30 PM	The Incident Response Manager begins triaging with DPD and ITS and assesses the Data Loss Incident using the risk matrix outlined in the IRP. ³²⁰
August 26, 2021	The Senior IT Manager of Public Safety emails DPD Chiefs a breakdown of on-premises servers and actions taken by ITS in support of those servers. ³²¹
August 26, 2021	Lynn Richardson, the Chief Public Defender for Dallas County, calls for an independent audit into 18 distinct murder cases.
August 27, 2021	Formal notice of possible data loss is sent to the City Manager’s Office, the Mayor’s Office, the City Council, and the DA’s Office. ³²²
August 30, 2021	The backup technician is issued a notice of pre-termination hearing. ³²³
August 31, 2021	The CIO sends an email containing responses to questions posed by the DA’s Office regarding the data loss incident. ³²⁴
September 1, 2021	Outside vendor Birch Cline is hired to develop a remediation protocol to attempt to locate and retrieve lost data. ³²⁵
September 10, 2021	The Ad Hoc Committee on General Investigating and Ethics considered agenda Item #2 regarding potentially hiring a third-party consultant to complete an independent investigation of the Data Loss Incident. The Committee then instructs the City Attorney to issue a request for submittals for law firms that could conduct an independent internal investigation. ³²⁶
October 14, 2021	Pursuant to Agenda Item “A 21-1991,” the Ad Hoc Committee on General Investigating and Ethics interviews the top three proposed law firms to conduct an independent investigation on behalf of the City. The Committee selects Kirkland & Ellis LLP. ³²⁷
October 22, 2021	The backup technician is issued a notice of termination. ³²⁸
October 27, 2021	Pursuant to Agenda Item 47, the City Council authorizes entering into a professional services contract with Kirkland & Ellis LLP to conduct an investigation of the data loss incident. ³²⁹
November 1, 2021	Kirkland & Ellis LLP enters into a professional services contract with the City of Dallas under which it committed to investigate the data loss, engage a forensic firm to analyze the lost electronic data, and provide a report. ³³⁰

B. Appendix B – Hard Client Deletions in Commvault Between April 2021 and August 2021

The following table summarizes all client deletion commands the backup technician executed in the City’s Commvault software between April 2021 and August 2021. The deletions that caused the Data Loss Incident are designated with gray rows.

Date/Time	Description
03/30/2021 21:34:55 UTC (16:34:55 CDT)	Hard client deletion
03/30/2021 21:44:36 UTC (16:44:36 CDT)	Hard client deletion
03/30/2021 21:47:47 UTC (16:47:47 CDT)	Hard client deletion
03/30/2021 21:49:51 UTC (16:49:51 CDT)	Hard client deletion
03/30/2021 21:50:28 UTC (16:50:28 CDT)	Hard client deletion
03/31/2021 15:14:50 UTC (10:14:50 CDT)	Hard client deletion
03/31/2021 15:28:49 UTC (10:28:49 CDT)	Hard client deletion
03/31/2021 22:03:57 UTC (17:03:57 CDT)	Hard client deletion
03/31/2021 22:14:10 UTC (17:14:10 CDT)	Hard client deletion
03/31/2021 22:27:19 UTC (17:27:19 CDT)	Hard client deletion
03/31/2021 22:29:05 UTC (17:29:05 CDT)	Hard client deletion
03/31/2021 22:29:36 UTC (17:29:36 CDT)	Hard client deletion
03/31/2021 22:30:08 UTC (17:30:08 CDT)	Hard client deletion
03/31/2021 22:30:37 UTC (17:30:37 CDT)	Hard client deletion
03/31/2021 22:31:06 UTC (17:31:06 CDT)	Hard client deletion
03/31/2021 22:31:38 UTC (17:31:38 CDT)	Hard client deletion
03/31/2021 22:37:15 UTC (17:37:15 CDT)	Hard client deletion
05/07/2021 16:31:39 UTC (11:31:39 CDT)	Hard client deletion
05/19/2021 16:42:50 UTC (11:42:50 CDT)	Hard client deletion
06/07/2021 14:27:14 UTC (09:27:14 CDT)	Hard client deletion

Date/Time	Description
06/21/2021 15:44:42 UTC (10:44:42 CDT)	Hard client deletion
06/21/2021 15:46:55 UTC (10:46:55 CDT)	Hard client deletion
06/21/2021 15:47:16 UTC (10:47:16 CDT)	Hard client deletion
06/21/2021 15:47:35 UTC (10:47:35 CDT)	Hard client deletion
06/21/2021 15:47:57 UTC (10:47:57 CDT)	Hard client deletion
06/21/2021 15:48:15 UTC (10:48:15 CDT)	Hard client deletion
06/21/2021 15:48:15 UTC (10:48:34 CDT)	Hard client deletion
06/21/2021 15:49:11 UTC (10:49:11 CDT)	Hard client deletion
06/21/2021 15:49:36 UTC (10:49:36 CDT)	Hard client deletion
06/23/2021 14:48:49 UTC (09:48:49 CDT)	Hard client deletion
06/23/2021 15:16:26 UTC (10:16:26 CDT)	Hard client deletion
06/23/2021 15:18:22 UTC (10:18:22 CDT)	Hard client deletion
06/23/2021 15:18:39 UTC (10:18:39 CDT)	Hard client deletion
06/23/2021 15:18:56 UTC (10:18:56 CDT)	Hard client deletion
06/23/2021 15:19:15 UTC (10:19:15 CDT)	Hard client deletion
06/23/2021 15:19:30 UTC (10:19:30 CDT)	Hard client deletion
06/23/2021 15:19:48 UTC (10:19:48 CDT)	Hard client deletion
06/23/2021 15:20:04 UTC (10:20:04 CDT)	Hard client deletion
06/23/2021 16:28:13 UTC (11:28:13 CDT)	Hard client deletion
06/23/2021 20:18:43 UTC (15:18:43 CDT)	Hard client deletion
06/23/2021 20:21:02 UTC (15:21:02 CDT)	Hard client deletion
06/23/2021 20:22:15 UTC (15:22:15 CDT)	Hard client deletion
06/23/2021 20:22:23 UTC (15:22:33 CDT)	Hard client deletion

Date/Time	Description
06/23/2021 20:22:52 UTC (15:22:52 CDT)	Hard client deletion
06/23/2021 20:25:35 UTC (15:25:35 CDT)	Hard client deletion
06/23/2021 20:32:50 UTC (15:32:50 CDT)	Hard client deletion
06/23/2021 21:41:46 UTC (16:41:36 CDT)	Hard client deletion
06/23/2021 21:41:56 UTC (16:41:56 CDT)	Hard client deletion
06/24/2021 14:04:42 UTC (09:04:42 CDT)	Hard client deletion
06/24/2021 14:05:07 UTC (09:05:07 CDT)	Hard client deletion
06/24/2021 14:29:49 UTC (09:29:49 CDT)	Hard client deletion
06/24/2021 14:30:07 UTC (09:30:07 CDT)	Hard client deletion
06/25/2021 17:17:35 UTC (12:17:35 CDT)	Hard client deletion
07/26/2021 17:24:39 UTC (12:24:39 CDT)	Hard client deletion
07/26/2021 17:25:13 UTC (12:25:13 CDT)	Hard client deletion
07/26/2021 17:26:04 UTC (12:26:04 CDT)	Hard client deletion
07/26/2021 17:26:36 UTC (12:26:36 CDT)	Hard client deletion
07/26/2021 17:27:56 UTC (12:27:56 CDT)	Hard client deletion
07/26/2021 17:28:55 UTC (12:28:55 CDT)	Hard client deletion
07/26/2021 17:29:18 UTC (12:29:18 CDT)	Hard client deletion
07/26/2021 17:29:40 UTC (12:29:40 CDT)	Hard client deletion
07/26/2021 17:30:17 UTC (12:30:17 CDT)	Hard client deletion
07/26/2021 17:30:52 UTC (12:30:52 CDT)	Hard client deletion
07/26/2021 17:31:55 UTC (12:31:55 CDT)	Hard client deletion
07/26/2021 17:32:21 UTC (12:32:21 CDT)	Hard client deletion
07/29/2021 14:42:03 UTC (09:42:03 CDT)	Hard client deletion

Date/Time	Description
07/29/2021 16:42:34 UTC (11:42:34 CDT)	Hard client deletion
08/05/2021 17:07:25 UTC (12:07:25 CDT)	Hard client deletion
08/05/2021 17:07:47 UTC (12:07:47 CDT)	Hard client deletion
08/05/2021 17:08:04 UTC (12:08:04 CDT)	Hard client deletion
08/05/2021 17:08:33 UTC (12:08:33 CDT)	Hard client deletion
08/05/2021 17:08:49 UTC (12:08:49 CDT)	Hard client deletion
08/05/2021 17:09:05 UTC (12:09:05 CDT)	Hard client deletion
08/05/2021 17:09:20 UTC (12:09:20 CDT)	Hard client deletion
08/05/2021 17:09:36 UTC (12:09:36 CDT)	Hard client deletion
08/05/2021 17:09:52 UTC (12:09:52 CDT)	Hard client deletion
08/05/2021 17:10:13 UTC (12:10:13 CDT)	Hard client deletion
08/05/2021 17:10:32 UTC (12:10:32 CDT)	Hard client deletion

C. Appendix C – Validation of Data Loss Volume

1. Overall Validation Process

As part of this Investigation, we used several methods to validate the volume of data loss reported by ITS.³³¹ Based on available data sources, the volume of data loss suffered by the City as a result of the March 2021 deletions is as follows:

- Approximately 13 terabytes of FUSION data.
- 11 TB of K Drive data were initially lost, and 3.5 terabytes of data were recovered from three servers that the backup technician had not decommissioned. A total of 7.51 terabytes of data were deemed unrecoverable.

In the course of the August audit, CAPERS and City Secretary servers were believed to potentially be implicated as well, but it was subsequently confirmed that duplicate copies of their data had been maintained. Therefore, the net data loss was as follows:

Location	Volume Loss	Number of Files
K Drive	7.51 TB	4.1 million files
FUSION Server	13.167 TB	4.6 million files
CAPERS Server	N/A	No data loss
City Secretary	N/A	No data loss

Based on its audit of deleted clients and policies conducted in August 2021, Commvault concluded there were only four servers impacted with data loss:³³²

Affected Server*	Categorization in Report	Cause of Data Loss
DPD FUSION	FUSION	Deleted storage policy
Family Violence	K Drive	Deleted storage policy
DPD File Server 1	K Drive	Deleted client
DPD File Server 2	K Drive	Deleted client

* Server names anonymized.

2. Validation of K Drive Data Loss

As discussed above, the K Drive is a mapped network share where DPD officers, detectives, and other staff from various divisions store case files (*i.e.*, evidence) and administrative data. Prior to the move to the Azure cloud, the K Drive consisted of 6-8 on-premises file servers at City Hall and DPD headquarters.³³³ Thereafter, in 2021 and because of cost overruns caused by the number of servers, active use of archived data in cold storage, and increasing egress charges, ITS decided to migrate the file servers back to City Hall, as detailed above.

Based on interviews, the total volume of data initially believed to be lost from the March 31, 2021 deletion varied from 8 terabytes to 11 terabytes to 14 terabytes.³³⁴ The amount of 22 terabytes was reported in August after further assessment.³³⁵ The net volume of K Drive data loss of approximately 7.51 terabytes was validated by reviewing the output from the City's Azure dashboard. The following graphic shows the initial data loss on April 1 of 10.77 terabytes (65.47 terabytes minus 54.7 terabytes) and subsequent recovery of 3.26 terabytes (increase from 54.7 terabytes on April 1 to 57.96 terabytes on April 12), resulting in a net data loss of 7.51 terabytes (65.47 terabytes minus 57.96 terabytes):

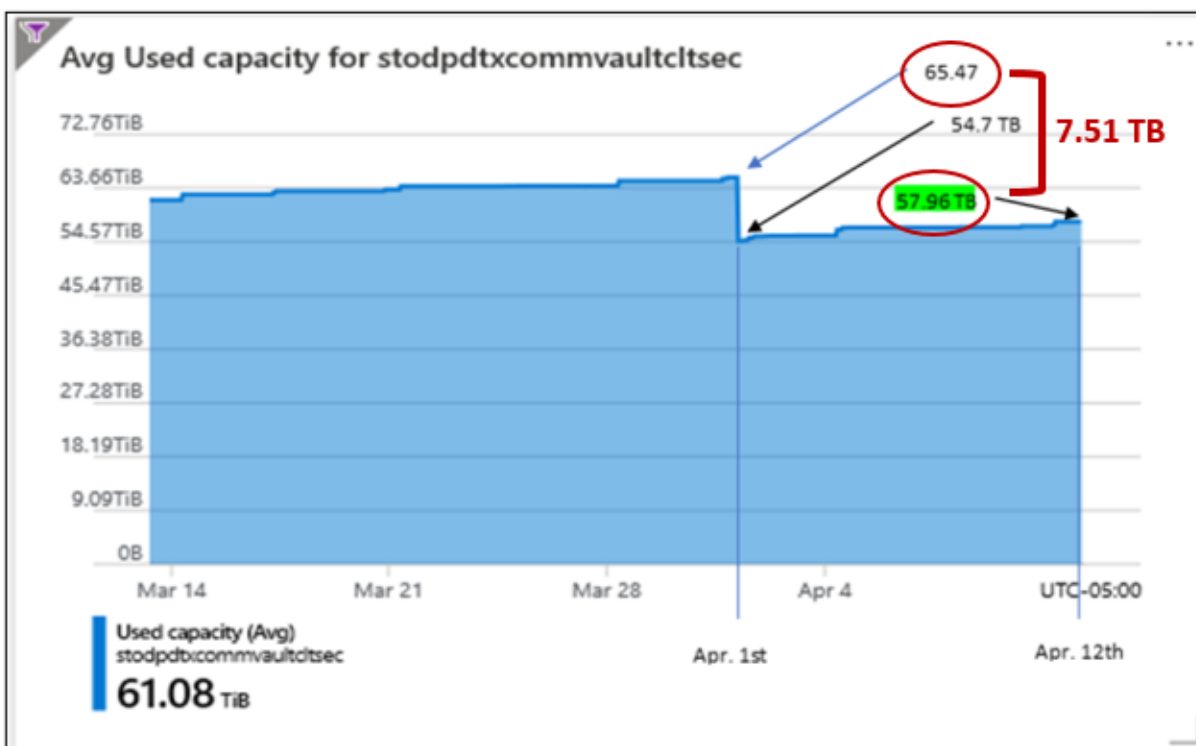


Fig. 5 – Screenshot of Microsoft Azure Dashboard Showing Data Loss Volume

To date, there are parts of the K Drive and DPD file servers still in Azure, specifically: 15 drives storing about 10 terabytes each.³³⁶ Following the conclusion of the investigation, ITS plans to complete a mass rehydration and move these remaining systems to City Hall.³³⁷

3. Validation of FUSION Data Loss

The FUSION server is an on-premises 14-terabyte server that primarily stores mobile device images collected by the DPD FUSION Center.³³⁸ The server had approximately 10 terabytes in use (*i.e.*, storage area where files already reside) and 4 terabytes of free space (*i.e.*, storage area where new files may be stored).³³⁹ Because of the size of the cellphone images and how quickly they filled the FUSION server, ITS enabled Commvault archiving on the server.³⁴⁰

We confirmed that the entire 14 terabyte server was impacted in the Data Loss Incident, as new files had not been saved to the FUSION server since approximately September 2020—meaning most of the data on FUSION had already been archived when the relevant Commvault storage policy was deleted in January 2021.³⁴¹ The server has a total capacity of 14.6 terabytes and 14.5 terabytes of that storage were in use, as shown in the figure below.³⁴² Because all of the data was over 18 months old, all of the data was archived. Therefore, when the archive was deleted, all data on FUSION was deleted.

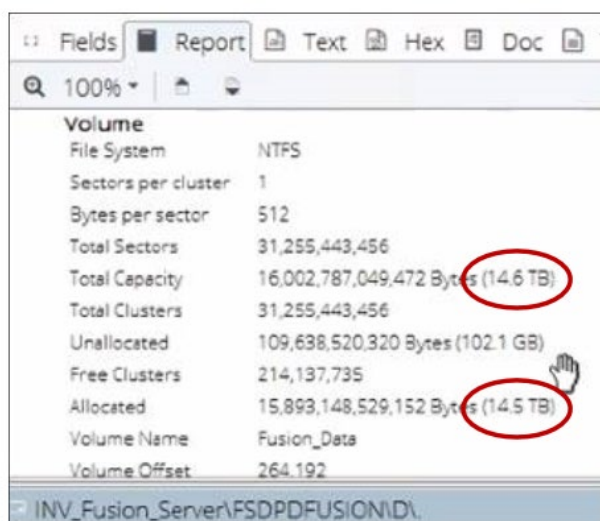


Fig. 6 – Screenshot Showing Size of Forensic Image of the FUSION Server

4. Assessment of City Secretary and CAPERS

The City, with the help of Commvault, determined that the backup technician deleted multiple policies for CAPERS and the City Secretary’s office. However, the archives from the City Secretary and CAPERS were saved elsewhere in the network. As a result of this redundancy, these servers suffered no ultimate data loss.³⁴³

-
- ¹ *E.g.*, Interview of Witness on Nov. 5, 2021.
- ² Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022; Memorandum, John Creuzot, Dallas County Criminal District Attorney, Disclosure Regarding Missing Data from Dallas Police Department’s Network Drive (Aug. 11, 2021) [Creuzot Memo], <https://www.dallascounty.org/Assets/uploads/docs/district-attorney/policies/Memo%20re%20DPD%20Data%20Loss.pdf>.
- ³ Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022.
- ⁴ Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022; Interview of Witness on Nov. 22, 2021.
- ⁵ Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022.
- ⁶ Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022.
- ⁷ Interview of Witness on Dec. 7, 2021; Creuzot Memo (Aug. 11, 2021).
- ⁸ Creuzot Memo (Aug. 11, 2021).
- ⁹ *Id.*
- ¹⁰ *Id.*
- ¹¹ *Id.*
- ¹² *Id.*
- ¹³ *Id.*
- ¹⁴ *Id.*
- ¹⁵ Letter from Eric Johnson, Dallas Mayor, to Adam McGough and Cara Mendelsohn, Dallas City Councilmembers (Aug. 12, 2021).
- ¹⁶ Minutes of the Meeting of the Dallas City Council (Aug. 18, 2021).
- ¹⁷ Minutes of the Meeting of the Ad Hoc Committee on General Investigating and Ethics (Sept. 10, 2021).
- ¹⁸ Minutes of the Meeting of the Ad Hoc Committee on General Investigating and Ethics (Oct. 14, 2021).
- ¹⁹ *Id.*
- ²⁰ *Id.*
- ²¹ *Id.*
- ²² Minutes of the Meeting of the Ad Hoc Committee on General Investigating and Ethics (Nov. 4, 2021).
- ²³ *Id.*
- ²⁴ Request for Submittals, City of Dallas (Sept. 17, 2021).
- ²⁵ *Information & Technology Services: About Us*, City of Dallas, <https://dallascityhall.com/departments/ciservices/Pages/About-Us.aspx>.
- ²⁶ *See generally* Interview of Witness on Dec. 9, 2021; Interview of Witness on Nov. 5, 2021.
- ²⁷ Interview of Witness on Nov. 5, 2021.
- ²⁸ Interview of Witness on Dec. 7, 2021.
- ²⁹ Interview of Witness on Nov. 22, 2021.
- ³⁰ Interview of Witness on Nov. 5, 2021.
- ³¹ *Information & Technology Services: About Us*, City of Dallas, <https://dallascityhall.com/departments/ciservices/Pages/About-Us.aspx>.
- ³² Interview of Witness on Nov. 5, 2021.
- ³³ *Our Mission*, Dallas County Criminal District Attorney, <https://www.dallascounty.org/government/district-attorney/mission.php>.
- ³⁴ *Quick Facts: Dallas County, Texas*, U.S. Census Bureau, <https://www.census.gov/quickfacts/fact/table/dallascountytexas/POP010220>.

35 *US County Populations 2021*, World Population Review, <https://worldpopulationreview.com/us-counties>.

36 Interview of Witness on Dec. 7, 2021.

37 *History*, Dallas Police Department, <https://dallaspolice.net/abouts/dpdhistory>.

38 Interview of Witness on Dec. 2, 2021.

39 Interview of Witness on Dec. 2, 2021.

40 *Id.*

41 *See* Interview of Witness on Dec. 2, 2021.

42 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 21, 2021; Interview of Witness on Dec. 21, 2021.

43 Interview of Witness on Dec. 21, 2021; Interview of Witness on Dec. 21, 2021.

44 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 21, 2021.

45 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 2, 2021.

46 *E.g.*, Interview of Witness on Dec. 2, 2021.

47 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 21, 2021.

48 Interview of Witness on Dec. 2, 2021.

49 *See* Interview of Witness on Dec. 2, 2021.

50 *See id.*

51 *Id.*

52 *Id.*; Interview of Witness on Dec. 21, 2021.

53 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 21, 2021.

54 Interview of Witness on Dec. 7, 2021; Interview of Witness on Dec. 7, 2021.

55 Interview of Witness on Nov. 9, 2021.

56 Interview of Witness on Nov. 9, 2021.

57 Interview of Witness on Nov. 9, 2021.

58 *See* Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 21, 2021; Interview of Witness on Dec. 21, 2021; Interview of Witness on Dec. 2, 2021.

59 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 21, 2021; Interview of Witness on Dec. 21, 2021.

60 *See, e.g., 6 Dos and Don'ts: For Data Archiving*, Iron Mountain, <https://www.ironmountain.com/resources/whitepapers/d/6-dos-and-donts-for-data-archiving>.

61 Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022; Interview of Witness on Dec. 3, 2021.

62 Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 3, 2021.

63 Interview of Witness on Nov. 5, 2021.

64 Interview of Witness on Dec. 2, 2021.

65 Interview of Witness on Nov. 9, 2021.

66 *See Creating an Archive Plan*, Commvault (Oct. 21, 2021), https://documentation.commvault.com/11.26/essential/127324_creating_archive_plan.html.

67 Interview of Witness on Jan. 5, 2021; *see Glossary: Subclient Policy*, Commvault, https://documentation.commvault.com/11.24/essential/50021_glossary.html.

68 *Glossary: Storage Policy*, Commvault, https://documentation.commvault.com/11.24/essential/50021_glossary.html.

69 Interview of Witness on Dec. 20, 2021.

70 *Glossary: Stubs*, Commvault, https://documentation.commvault.com/11.24/essential/50021_glossary.html.

71 Interview of Witness on Jan. 5, 2021; Interview of Witness on Dec. 20, 2021.

72 Interview of Witness on Jan. 5, 2022; Interview of Witness on Jan. 5, 2021; Interview of Witness on Dec. 15, 2021; Interview of Witness on Nov. 22, 2021.

73 Interview of Witness on Jan. 5, 2022; Interview of Witness on Nov. 8, 2021; Interview of Witness on Dec. 15, 2021; Interview of Witness on Nov. 22, 2021.

74 Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022; Interview of Witness on Dec. 3, 2021.

75 ITS email chain dated July 23, 2020 - July 28, 2020.

76 *Change Order Detail: 116670*, ITS (opened Aug. 24, 2020).

77 Interview of Witness on Nov. 5, 2021.

78 *See* Interview of Witness on Dec. 15, 2021.

79 Interview of Witness on Nov. 5, 2021.

80 *Id.*

81 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021); *Audit Trail Report: Delete Storage Policy*, Commvault (generated Aug. 26, 2021).

82 Creuzot Memo (Aug. 11, 2021); ITS and DPD email chain date Aug. 9, 2021.

83 ITS Data Loss Initial Report, at 10.

84 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

85 Interview of Witness on Nov. 5, 2021.

86 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

87 Interview of Witness on Nov. 22, 2021.

88 ITS Data Loss Initial Report, at 11.

89 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

90 Interview of Witness on Dec. 2, 2021.

91 *Id.*

92 Email from ITS email chain dated April 13, 2021.

93 *Chief's Update: Document 21-2015*, Dallas Police Department (April 19, 2021).

94 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021).

95 Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022.

96 Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 2, 2021; Interview of Witness on Nov. 5, 2021.

97 Creuzot Memo (Aug. 11, 2021).

98 *Id.*

99 Letter from legal representative to ITS dated Nov. 1, 2021.

100 Interview of Witness on Dec. 22, 2021; Interview of Witness on Dec. 20, 2021.

101 ITS Data Loss Initial Report, at 11; Interview of Witness on Dec. 9, 2021.

102 ITS Data Loss Initial Report, at 11; Interview of Witness on Dec. 9, 2021.

103 *Notice of Pre-Termination Hearing to Backup Technician*, City of Dallas (Aug. 30, 2021).

104 *Notice of Termination to Backup Technician*, City of Dallas (Oct. 22, 2021).

105 Interview of Witness on Nov. 5, 2021.

106 Interview of Witness on Dec. 15, 2021.

107 *See* Interview of Witness on Jan. 5, 2022.

108 Interview of Witness on Jan. 5, 2021.

109 Interview of Witness on Nov. 5, 2021.

110 *Id.*

111 *Change Order Detail: 116670*, ITS (opened Aug. 24, 2020).

112 *Id.*

113 Interview of Witness on Nov. 5, 2021.

114 *Id.*

115 *Change Order Detail: 116670*, ITS (opened Aug. 24, 2020).

116 Interview of Witness on Dec. 15, 2021.

117 *See* Implementation Plan for New Commvault Blob Storage Libraries (attached to Aug. 24, 2020 change order).

118 *See id.*

119 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021); Interview of Witness on Dec. 15, 2021.

120 Interview of Witness on Nov. 5, 2021.

121 *Id.*

122 *Id.*

123 *Id.*

124 Interview of Witness on Dec. 9, 2021.

125 Interview of Witness on Dec. 15, 2021.

126 *Id.*

127 Interview of Witness on Jan. 5, 2021; Interview of Witness on Dec. 20, 2021.

128 Interview of Witness on Jan. 5, 2022; Interview of Witness on Dec. 20, 2021.

129 Interview of Witness on Jan. 5, 2022.

130 Interview of Witness on Dec. 15, 2021.

131 Interview of Witness on Jan. 5, 2022.

132 Interview of Witness on Nov. 5, 2021.

133 Interview of Witness on Dec. 15, 2021; ITS and DPD email chain dated Aug. 9, 2021.

134 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021); *Audit Trail Report: Delete Storage Policy*, Commvault (generated Aug. 26, 2021).

135 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021); *Audit Trail Report: Delete Storage Policy*, Commvault (generated Aug. 26, 2021).

136 Interview of Witness on Dec. 20, 2021.

137 January 24, 2022 Commvault Walkthrough.

138 Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 20, 2021.

139 *Recovering Data Associated with Deleted Clients and Storage Policies*, Commvault (Oct. 28, 2021), https://documentation.commvault.com/11.21/essential/43719_recovering_data_associated_with_deleted_clients_and_storage_policies.html.

140 Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 22, 2021.

141 Interview of Witness on Dec. 15, 2021.

142 *Id.*

143 *Id.*

144 Creuzot Memo (Aug. 11, 2021); ITS and DPD email chain dated Aug. 9, 2021; Interview of Witness on Nov. 5, 2021.

145 ITS Data Loss Initial Report, at 10.

146 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

147 Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 15, 2021.

148 Interview of Witness on Nov. 5, 2021.

149 *See* Interview of Witness on Dec. 15, 2021.

150 Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 15, 2021.

151 Interview of Witness on Nov. 5, 2021.
152 Interview of Witness on Nov. 22, 2021.
153 Interview of Witness on Nov. 5, 2021.
154 *Id.*
155 Interview of Witness on Dec. 9, 2021.
156 *Id.*
157 Interview of Witness on Dec. 2, 2021.
158 Interview of Witness on Nov. 5, 2021.
159 *Id.*; Interview of Witness on Dec. 2, 2021.
160 Interview of Witness on Nov. 5, 2021.
161 *See* ITS email chain dated April 13, 2021.
162 Interview of Witness on Dec. 2, 2021; Interview of Witness on Nov. 5, 2021.
163 Interview of Witness on Dec. 2, 2021.
164 *See Public Safety Memo re Missing Files and Folders*, City of Dallas.
165 Interview of Witness on Dec. 2, 2021.
166 *See Chief's Update: Document 21-2015*, Dallas Police Department (April 19, 2021).
167 *See Public Safety Memo re Missing Files and Folders*, City of Dallas.
168 Interview of Witness on Dec. 2, 2021; Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 9, 2021.
169 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).
170 *Id.*
171 *Id.*
172 *Id.*
173 *Id.*
174 *Id.*
175 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021).
176 Interview of Witness on Dec. 7, 2021.
177 Creuzot Memo (Aug. 11, 2021).
178 Interview of Witness on Nov. 5, 2021.
179 Creuzot Memo (Aug. 11, 2021).
180 *Id.*
181 Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 2, 2021.
182 Interview of Witness on Nov. 5, 2021.
183 Interview of Witness on Dec. 20, 2021.
184 *Id.*
185 Interview of Witness on Dec. 9, 2021.
186 Interview of Witness on Dec. 3, 2021.
187 *Id.*
188 Interview of Witness on Jan. 5, 2022.
189 Interview of Witness on Nov. 8, 2021.
190 Interview of Witness on Dec. 9, 2021; Interview of Witness on Dec. 3, 2021; Update from Witness on February 9, 2022.
191 *See* Interview of Witness on Dec. 9, 2021; Interview of Witness on Nov. 8, 2021.
192 Interview of Witness on Dec. 9, 2021.
193 Interview of Witness on Jan. 5, 2022.

194 Interview of Witness on Nov. 9, 2021.

195 Interview of Witness on Dec. 9, 2021.

196 Interview of Witness on Dec. 3, 2021.

197 Interview of Witness on Dec. 9, 2021; Interview of Witness on Dec. 22, 2021.

198 Interview of Witness on Jan. 5, 2022; Interview of Witness on Dec. 9, 2021; Interview of Witness on Dec. 22, 2021; Interview of Witness on Dec. 7, 2021.

199 Interview of Witness on Dec. 22, 2021; Interview of Witness on Dec. 3, 2021.

200 Interview of Witness on Dec. 22, 2021; Interview of Witness on Dec. 3, 2021.

201 Interview of Witness on Dec. 3, 2021.

202 Interview of Witness on Dec. 22, 2021.

203 Interview of Witness on Dec. 9, 2021.

204 Numbers provided by Witness and current as of February 9, 2022.

205 Numbers provided by Witness and current as of February 9, 2022.

206 Interview of Witness on Dec. 15, 2021.

207 *Id.*

208 Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022.

209 *Commvault Professional Foundations Instructor-led*, Commvault, <https://ea.commvault.com/CourseGroup/Index/68/39>; *Commvault Professional Advanced Instructor-led*, Commvault, <https://ea.commvault.com/CourseGroup/Index/70/39>; Interview of Witness on Dec. 20, 2021.

210 Interview of Witness on Jan. 5, 2022; Interview of Witness on Nov. 22, 2021.

211 Interview of Witness on Jan. 5, 2022; Interview of Witness on Nov. 22, 2021.

212 Interview of Witness on Dec. 15, 2021.

213 Interview of Witness on Dec. 3, 2021.

214 ITS Data Loss Initial Report, at 60.

215 Interview of Witness on Dec. 3, 2021.

216 *See* Interview of Witness on Jan. 5, 2022; Interview of Witness on Jan. 5, 2022; Interview of Witness on Nov. 22, 2021.

217 Interview of Witness on Dec. 21, 2021; Interview of Witness on Dec. 8, 2021; Interview of Witness on Dec. 2, 2021.

218 Interview of Witness on Dec. 2, 2021.

219 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

220 Interview of Witness on Dec. 2, 2021; Interview of Witness on Dec. 2, 2021.

221 Interview of Witness on Jan. 5, 2022.

222 Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022.

223 Interview of Witness on Dec. 9, 2021.

224 Interview of Witness on Nov. 5, 2021.

225 *City of Dallas — IT Maturity Assessment*, Forrester (Dec. 14, 2020).

226 Interview of Witness on Dec. 2, 2021.

227 Interview of Witness on Dec. 2, 2021.

228 *Id.*

229 *Id.*

230 Interview of Witness on Dec. 21, 2021.

231 *Id.*

232 Interview of Witness on Dec. 2, 2021.

233 *Id.*; Interview of Witness on Dec. 21, 2021.

234 Interview of Witness on Dec. 2, 2021.

235 Interview of Witness on Dec. 21, 2021.

236 *Id.*

237 Interview of Witness on Dec. 2, 2021.

238 Interview of Witness and Witness on Jan. 25, 2022. *See also* Interview of Witness on Dec. 2, 2021.

239 Interview of Witness on Dec. 7, 2021.

240 Interview of Witness and Witness on Jan. 25, 2022.

241 Interview of Witness on Jan. 25, 2022; Interview of Witness on Dec. 7, 2021. *See* Tex. Code Crim. Proc. art. 39.14.

242 Interview of Witness on Dec. 7, 2021; Interview of Witness on Jan. 25, 2022.

243 Interview of Witness on Dec. 7, 2021.

244 *Our Mission*, Dallas County Criminal District Attorney, <https://www.dallascounty.org/government/district-attorney/mission.php>.

245 Azure dashboard graphic showing change in volume from 65.47 TB to 54.7 TB (10.77 TB less) as of April 1.

246 Azure dashboard graphic showing change in volume from 54.7 TB to 57.96 TB (3.26 TB recovered between April 1 and April 12).

247 Azure dashboard graphic showing change from 65.47 TB (on April 1) to 57.96 TB (on April 12).

248 Data Loss Assessment Update – 8/27/2021.

249 Interview of Witness on Nov. 9, 2021; Interview of Witness on Jan. 5, 2022; Stroz Friedberg EnCase analysis.

250 Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022; Interview of Witness on Nov. 22, 2021; Interview of Witness on Dec. 15, 2021.

251 Interview of Witness on Jan. 5, 2022.

252 Interview of Witness on Nov. 5, 2021.

253 Interview of Witness on Dec. 7, 2021.

254 Interview of Witness on Dec. 9, 2021.

255 Interview of Witness on Dec. 7, 2021; Interview of Witness on Nov. 9, 2021.

256 *See* Interview of Witness on Nov. 9, 2021; Interview of Witness on Dec. 7, 2021; Interview of Witness on Nov. 9, 2021.

257 Interview of Witness on Nov. 5, 2021; Interview of Witness on Jan. 5, 2022; Interview of Witness on Dec. 3, 2021.

258 ITS email chain dated Jan. 24, 2022.

259 Interview of Witness on Nov. 5, 2021.

260 Emails among ITS email chain dated July 23, 2020 - July 28, 2020.

261 ITS email chain dated Aug. 20, 2020 - Aug. 24, 2020.

262 *Change Order Detail: 116670*, ITS (opened Aug. 24, 2020).

263 City of Dallas — IT Maturity Assessment, Forrester (Dec. 14, 2020).

264 ITS email chain dated Jan. 24, 2022.

265 City of Dallas — IT Maturity Assessment, Forrester (Dec. 14, 2020).

266 ITS email chain dated Jan. 11, 2021.

267 Interview of Witness on Nov. 5, 2021.

268 Interview of Witness on Nov. 5, 2021.

269 Interview of Witness on Nov. 5, 2021.

270 ITS email chain dated March 4, 2021.

271 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021); *Audit Trail Report: Delete Storage Policy*, Commvault (generated Aug. 26, 2021).

272 Creuzot Memo (Aug. 11, 2021); ITS and DPD email chain dated Aug. 9, 2021.

273 ITS Data Loss Initial Report, at 10; Interview of Witness on Dec. 9, 2021.

274 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

275 Interview of Witness on Nov. 5, 2021.

276 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

277 ITS Data Loss Initial Report, at 10.

278 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

279 ITS Data Loss Analysis Report, at 11; Interview of Witness on Dec. 9, 2021.

280 ITS Data Loss Analysis Report, at 11; Interview of Witness on Dec. 9, 2021.

281 ITS Data Loss Analysis Report, at 11; Interview of Witness on Dec. 9, 2021.

282 ITS Data Loss Analysis Report, at 11; Interview of Witness on Dec. 9, 2021.

283 Interview of Witness on Dec. 2, 2021.

284 *Id.*

285 ITS email chain dated April 13, 2021.

286 *Id.*

287 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

288 *Chief's Update: Document 21-2015*, Dallas Police Department (April 19, 2021).

289 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

290 ITS and DPD email chain dated April 22, 2021.

291 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

292 *Id.*

293 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021).

294 *Incident Details: TR_210405_307*, Commvault Support (created April 5, 2021).

295 *Id.*

296 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021).

297 *Id.*

298 *Id.*

299 *Id.*

300 *Id.*

301 *Id.*

302 *Id.*

303 *Id.*

304 *Id.*

305 Interview of Witness on Dec. 7, 2021; Interview of Witness and Witness on Jan. 25, 2022.

306 Interview of Witness on Nov. 5, 2021; Interview of Witness on Dec. 2, 2021; Interview of Witness on Nov. 5, 2021.

307 ITS and DPD email chain dated Aug. 9, 2021.

308 ITS and DPD email chain dated Aug. 4, 2021.

309 *Audit Trail Report: Hard Delete Client*, Commvault (generated Aug. 26, 2021).

310 Creuzot Memo (Aug. 11, 2021).

311 *Id.*; ITS and DPD email chain Aug. 9, 2021.

312 Creuzot Memo (Aug. 11, 2021).

313 Johnson Letter (Aug. 12, 2021).

314 Letter from legal representative to ITS dated Nov. 1, 2021.

315 "Texas murder suspect granted bond after police data loss," ABC News (Aug. 13, 2021), <https://abcnews.go.com/US/wireStory/texas-murder-suspect-granted-bond-police-data-loss-79449121>; "Texas

murder suspect granted bond after police data loss,” Fox News (Aug. 14, 2021), <https://www.foxnews.com/us/texas-murder-suspect-bond-data-loss>; Krista Torravla, “Dallas murder suspect to be released from jail while city determines if it lost evidence,” Dallas Morning News (Aug. 13, 2021), <https://www.dallasnews.com/news/courts/2021/08/13/dallas-murder-suspect-to-be-released-from-jail-while-city-determines-if-it-lost-evidence/>; Isabel Vincent, “Texas murder suspect released on bond after police data loss,” New York Post (Aug. 14, 2021), <https://nypost.com/2021/08/14/texas-murder-suspect-released-on-bond-after-police-data-loss/>.

- 316 Minutes of the Meeting of the Dallas City Council (Aug. 18, 2021).
- 317 Interview of Witness on Dec. 22, 2021; Interview of Witness on Dec. 20, 2021.
- 318 Interview of Witness on Nov. 9, 2021.
- 319 ITS Data Loss Analysis Report, at 11; Interview of Witness on Dec. 9, 2021.
- 320 Interview of Witness on Dec. 3, 2021.
- 321 ITS and DPD email chain dated Aug. 26, 2021.
- 322 ITS Data Loss Analysis Report, at 11.
- 323 *Notice of Pre-Termination Hearing to Backup Technician*, City of Dallas (Aug. 30, 2021).
- 324 ITS, DPD and DA’s Office email chain dated Aug. 31, 2021.
- 325 Interview of Witness on Dec. 22, 2021.
- 326 Minutes of the Meeting of the Ad Hoc Committee on General Investigating and Ethics (Sept. 10, 2021).
- 327 Minutes of the Meeting of the Ad Hoc Committee on General Investigating and Ethics (Oct. 14, 2021).
- 328 *Notice of Termination to Backup Technician*, City of Dallas (Oct. 22, 2021).
- 329 Minutes of the Meeting of the Dallas City Council (Oct. 27, 2021).
- 330 Professional Legal Services Contract between the City of Dallas and Kirkland & Ellis, LLP (Nov. 1, 2021); Request for Submittals, City of Dallas (Sept. 17, 2021).
- 331 ITS Data Loss Analysis Report, at iii-iv.
- 332 Interview of Witness on Dec. 22, 2021.
- 333 Interview of Witness on Dec. 2, 2021.
- 334 Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 9, 2021; Interview of Witness on Nov. 22, 2021; Interview of Witness on Dec. 7, 2021; Interview of Witness on Dec. 7, 2021.
- 335 Interview of Witness on Nov. 9, 2021.
- 336 Interview of Witness on Nov. 5, 2021.
- 337 *Id.*
- 338 *See* Interview of Witness on Dec. 2, 2021; Interview of Witness on Nov. 8, 2021; Interview of Witness on Nov. 5, 2021.
- 339 Interview of Witness on Nov. 8, 2021.
- 340 Interview of Witness on Dec. 2, 2021.
- 341 Interview of Witness on Nov. 9, 2021.
- 342 *See Screenshot from EnCase Virtual Walkthrough* (Jan. 9, 2022).
- 343 Interview of Witness on Nov. 5, 2021; Interview of Witness on Nov. 5, 2021.