Government CIO

Expert Exchange

Q2 Executive summary
May 16, 2024

kyndryl

Overview

In this Expert Exchange session, several CIOs met virtually to take two “deep dives” into topics critical to their work: 1) A member success story of data governance models amid large-scale transformations and migrations and 2) How one county responded to a catastrophic cyber-attack last January. The agenda was based on advanced interviews with participants.

Hosts

Anita Mikus - Kyndryl – Vice President, Government

Rajesh Jaluka – Kyndryl – Chief Technology Officer, Healthcare and Government

Table of Contents

Data Governance Deep Dive

The group took a deep dive into one state's experience developing a robust data governance program as it made its large-scale digital transformation. The state's department significantly improved its permit systems statewide through the technological upgrade. Due to data being housed in myriad disparate legacy systems and certain organizational cultural factors operating under the surface, the permit system was plagued by gridlock and delays.

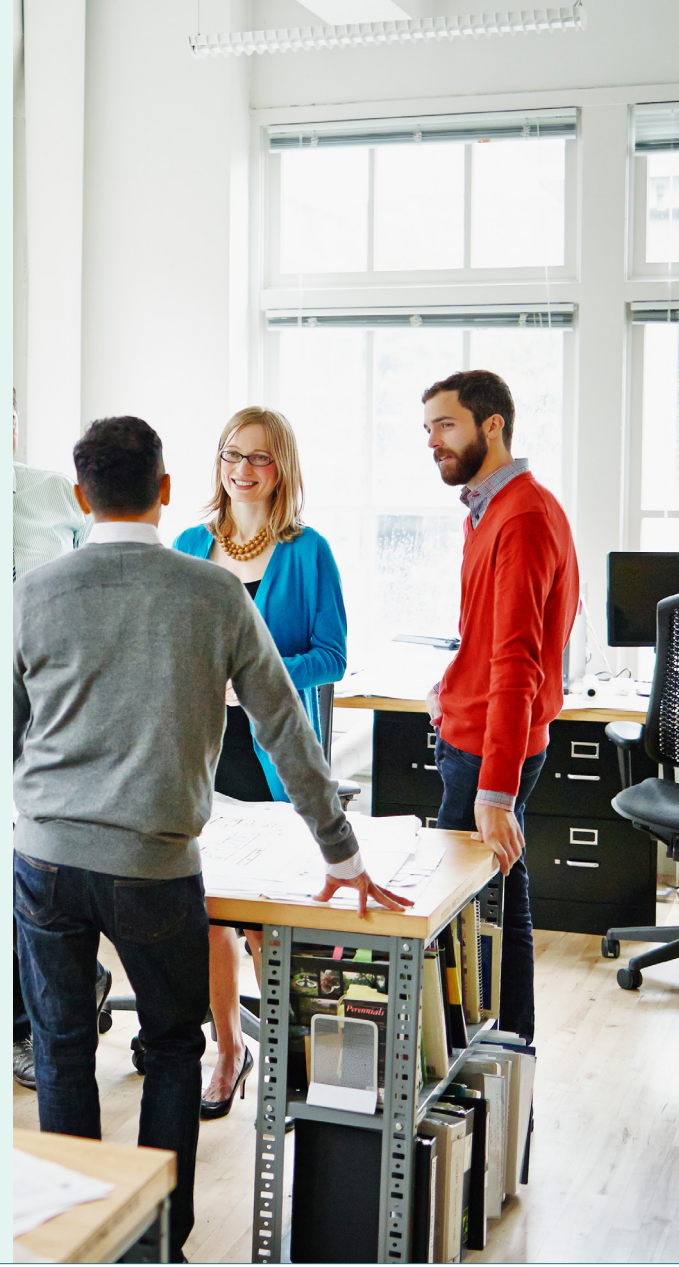
The executive shared their journey of overcoming resistance from facilities managers and building a standard data model. These efforts were supported by generous funding, which facilitated hiring a data scientist, a secretary for the initiative, and eventually a chief data officer for the department.

"The business did not want to continue to pursue it. But I could not continue to build the system without the data model. So, we just went reverse shadow IT and went shadow business. And we started building our data model as far as possible while still trying to get the businesses on board."

— CIO Government Expert Exchange member

Kyndryl Data and AI services: Realize business value with data and AI transformation

Learn more →



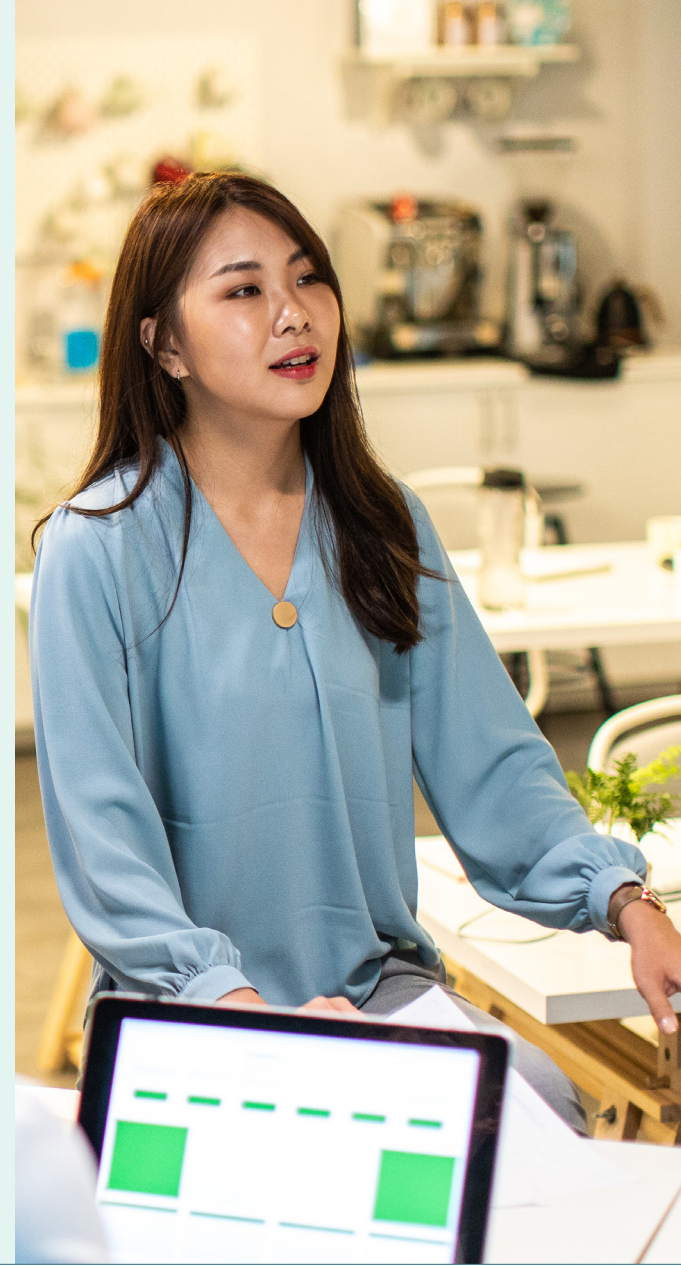
Securing Funding for the Data Governance Initiative

Many leaders were interested in how the executive department secured funding for this large-scale transformation. The member explained that they had a very well-thought-out and articulated plan, dating back to 2018, but the success in getting it resourced also had to do with several other factors, including COVID. After the pandemic, the state legislature had a surplus of money, and, the leader explained, straightening out the permits process "scratched their itch" to spend the money.

In addition, because the previous process was so fraught with problems, it was easy to show how the investment decreased the delays in the permitting process. The leader gave the example that before, as a permit case moved through the process, it would get put in different-colored paper folders. The person responsible for the green folder step in the process retired, and the open cases piled up on their desks for six months.

"We could tell from the complaints that came in that if a person said, 'Where's my permit?' it would take a couple of days to find out where it was... And the Secretary was like, 'If Domino's can track a pizza, we can track a permit.'"

— CIO Government Expert Exchange member



Cybersecurity Preparedness and Response

The group was also interested to hear how one organization dealt with a near-catastrophic cyber-attack in early 2024. The leader described the attack as “equivalent to 9/11, when all the planes stopped flying” and shared how they managed the crisis step by step. Due to learnings from a previous breach in a major city, the team had secured good cyber insurance and reasonable attorneys in place.

On January 28, 2024, the team realized their system was compromised. After a brief meeting, the team decided to bring the whole system down. The executive “did it the old-fashioned way,” putting everything on a disk and flying it from their on-prem data site to a vendor with a cloud instance in Arizona.

As the recovery process got underway, the first thing they did was rebuild the payroll so that they could deploy staff round-the-clock to reconstitute the rest of the system. Under the emergency authorization, every employee, right up to the CIO, would get paid to work overtime if necessary. Afterward, they went step by step, system by system, to bring things back online and securely move them to the cloud.

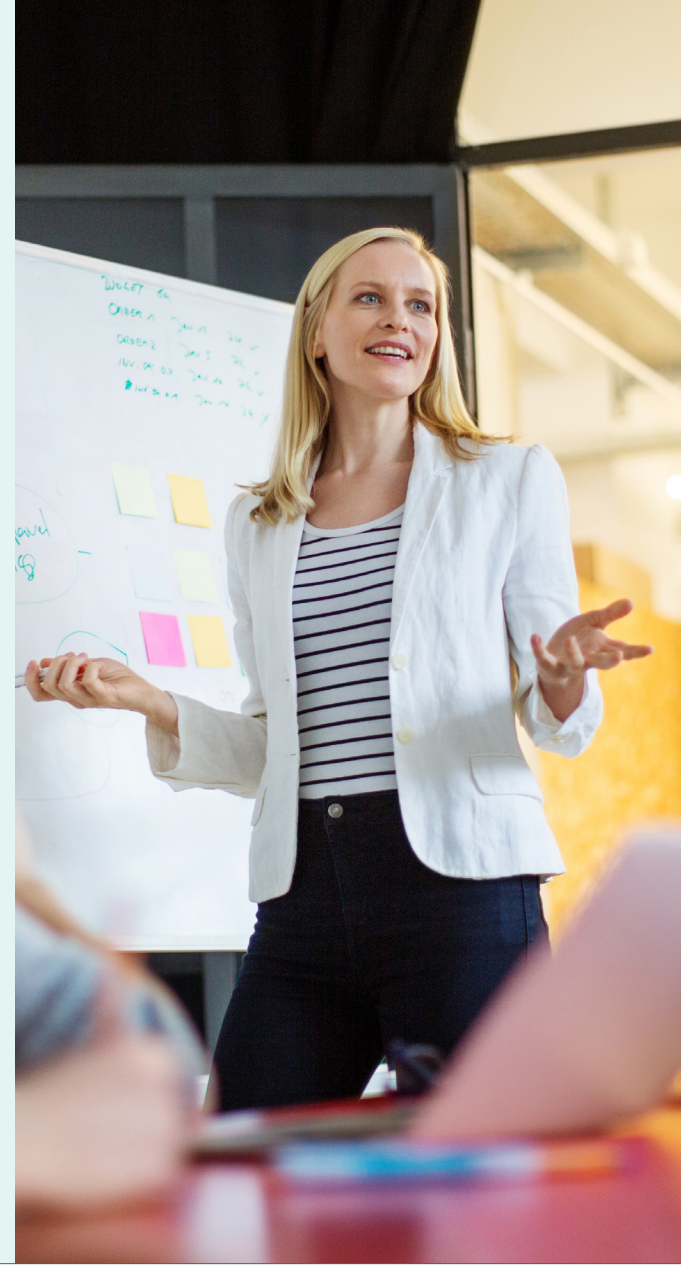
The executive emphasized the importance of communication when responding to a cyber-attack. They had “internal press conferences” with all levels to ensure everyone was on the same page and that the next steps were planned.

“I think we were successful because we had the right companies in place, and our communication was paramount. It was very key... So, everything was planned out methodically to a fault.”

— CIO Government Expert Exchange member

Incident response and incident recovery: simply better together

Learn more →



kyndryl

The Expert Exchange is hosted by **Kyndryl**, Inc. Please contact **Anita Mikus** or **Rajesh Jaluka** with any questions about Kyndryl or this Exchange.