

TECH & AI CASE STUDY - LOCAL GOVERNMENT - 2025

Ransomware Recovery That Cut a City's Restore Time From 72 Hours to 4

Based on a delivery engagement with City of Marlow Bend

72h to 4h

RECOVERY TIME OBJECTIVE

24h to 15 min

RECOVERY POINT OBJECTIVE

0 to 4 per year

FULL-SERVICE RESTORE DRILLS

100% of Tier-1

IMMUTABLE BACKUP COVERAGE

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the City of Marlow Bend case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at City of Marlow Bend - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

The City of Marlow Bend is a mid-size municipality of 61,000 residents with 480 employees across police and fire administration, public works, utilities, finance, permitting and community services. Its technology estate is a mosaic typical of local government: a payroll and HR platform, a permitting system that citizens use online, a utilities billing system that collects water and refuse payments, email, and dozens of smaller applications maintained by individual departments. Services that residents experience as ordinary — a building permit issued on time, a water bill posted correctly, a paycheck arriving Friday — each depend on systems the city's small IT department keeps running.

Municipal government carries a distinctive security burden. The city cannot price risk the way a company can, because its services are not optional; a payroll outage does not just cost money, it damages trust in local government at the next council meeting. And the threat environment has made clear that municipalities are targets: ransomware crews have spent years extracting payments from cities precisely because residents cannot wait. Neighboring governments had been hit, council members were asking questions, and Marlow Bend's cyber insurer had begun demanding proof that the city could actually recover — not just that it owned backups.

02 Where Things Stood

The city's posture was tested by accident. During routine monitoring, staff discovered an attempted ransomware detonation that had been stopped by luck rather than by any control — a misconfiguration on the attacker's side, not a defense on the city's, and everyone who understood what had happened knew it. An honest assessment followed, and the findings were uncomfortable. Tape backups were tested once a year. The network was flat, connecting payroll, permitting and utilities billing in ways that meant one compromised credential could reach all of them. The continuity plan was paper, last revised in 2016, and it promised that services would return within 72 hours — a recovery objective nobody had ever validated against a real restore.

The financial exposure was quantified by the finance department rather than by IT: a two-week payroll outage would cost roughly \$1.1M in delayed disbursements and overtime, before counting the permitting and utilities revenue that would stall alongside it. IBM Security's 2024 research puts the average cost of a ransomware attack at \$4.91 million excluding any ransom payment, and the Verizon Data Breach Investigations Report finds ransomware or extortion present in a reported 32% of all analyzed breaches worldwide — figures that turned an abstract board concern into a budget line. The cyber insurance renewal now demanded documented recovery testing as a condition, which converted the city's untested backups from a technical detail into a procurement obstacle.

The endpoint picture completed the diagnosis: the intruder had entered through a server that EDR coverage had never reached, one of the machines that rarely connects to headquarters and therefore gets forgotten by every deployment project. One overlooked server had nearly become patient zero for the entire city.

03 The Challenge

The challenge was to rebuild the city's ability to withstand and recover from ransomware — not merely to buy better backups, but to prove recovery on a schedule and to a standard that satisfied three demanding audiences at once: council members accountable to residents, an insurer demanding documented testing, and department heads who needed their services back within hours, not days. CISA's joint ransomware guide recommends offline, encrypted, immutable backups with regular restore testing, noting that untested backups frequently fail when recovery matters most; Marlow Bend's annual tape test was exactly the pattern that guidance warns against. The deeper challenge was architectural honesty. Recovery time is not a property of a backup product; it is a property of an entire system — network paths, administrative access, restore tooling, staff practice and the order in which services return. A city that promises 72 hours must be able to demonstrate 72 hours, and Marlow Bend could not demonstrate anything, because it had never restored four critical services simultaneously under observation. The program therefore had to restructure the environment — backups, network, endpoints, access — and then rehearse recovery repeatedly until the city's own staff could execute it without outside help.

04 Discovery and Diagnosis

Emerson Technology began with a three-week assessment covering backup infrastructure, network topology, endpoint coverage, identity and the 2016 continuity plan. The backup audit inventoried every scheduled job, its media, its encryption state and its test history, and found that the city's recovery promise rested on tape media tested annually and located within reach of the same credentials that protected production. The network audit confirmed the flat topology and mapped the implicit trust paths between citizen-facing services, internal operations and the backup infrastructure itself — three functions that needed to become three zones.

The endpoint audit reconciled EDR deployment records against the actual machine inventory and produced the gap list that included the server the intruder had used; the discrepancy between "deployed" and "covered" was a governance finding as much as a technical one. Interviews with department heads established which services the city must restore first and in what order — payroll, permitting, utilities billing, email — and how long each department could operate on manual procedures before errors compounded. The diagnosis concluded with a recovery architecture proposal: a 3-2-1-1-0 backup discipline, segmented zones with brokered administrative access, EDR closure of the endpoint gaps, service-level runbooks and a quarterly rehearsal calendar, each element tied to the audience it would have to convince.

05 The Solution

The program rebuilt recovery as an engineered, rehearsed capability rather than a plan on paper.

Backups attackers cannot delete

Recovery was rebuilt around a 3-2-1-1-0 discipline: three copies of critical data, on two media, with one immutable object-storage copy that even domain admins cannot delete, and zero unverified backups. Tier-1 systems — payroll, permitting, utilities billing and email — replicate to immutable storage with 15-minute recovery points, so the worst realistic case is minutes of lost transactions rather than a day of city business. Backup repositories sit in a separate network zone with brokered administrative access: if domain admin credentials are compromised, backups remain outside an attacker's reach, which is the entire difference between a bad week and an unrecoverable event. Verification runs continuously, because a backup job that fails silently is a promise the city cannot keep.

Segmentation and endpoint closure

Network segmentation separated citizen-facing services, internal operations and backups into distinct zones, so a compromise in one cannot quietly spread to the others, and all administrative access is brokered and logged. EDR coverage was closed across every server and workstation, including the remote machines that rarely connect to headquarters — the exact class of endpoint the intruder had used. The deployment was verified against the machine inventory rather than the deployment tool's own report, closing the governance gap that had allowed one server to fall out of coverage entirely.

Runbooks, retainers and rehearsals

Recovery documentation was rewritten as service-level runbooks that restore business functions rather than raw servers: payroll comes back as a working payroll that department heads verify, not as a database that IT declares healthy. The city retained an incident response firm for surge capacity, because during a real event contracts take days you do not have and attackers count on that delay. The annual test was replaced with quarterly restore drills on a fixed schedule, each one timed and scored. Department heads rehearse manual fallbacks twice a year alongside the technical restores, so essential services stay alive on paper procedures while systems rebuild — and the drills surface gaps while they are still cheap to fix.

06 The First 90 Days

Weeks one through four executed the backup rebuild: immutable storage was stood up, Tier-1 replication configured at 15-minute recovery points, verification automation deployed, and the first supervised restore of a single system performed to baseline the tooling. Weeks five through eight delivered segmentation in staged form — policies monitored before enforcement — plus the brokered administration model and the EDR gap closure, verified machine by machine against the inventory. The incident response retainer was signed in the same window, with scope and activation steps documented so nobody negotiates a contract mid-incident. Weeks nine through twelve were the rehearsal phase, and they earned their budget immediately. The first full-service drill restored two Tier-1 services to clean-room infrastructure and uncovered three defects — a restore tool version mismatch, a DNS dependency nobody had documented and a permissions error on the backup repository — all fixed in production before they could become real incidents, which is precisely what drills are for. Runbooks were revised after each exercise with department head sign-off on what "restored" means for their function. By day 90 the city had a rehearsal calendar instead of an annual test, a recovery architecture that matched CISA's guidance point for point, and an evidence file — drill logs, timing data, immutable configuration reports — assembled for the insurer before it was requested.

07 The Results

In the concluding exercise, the city restored payroll, permitting, utilities billing and email in 4 hours from immutable storage — down from a 72-hour objective nobody had ever validated — with recovery points 15 minutes old and city staff executing the restores while IT supervised only exceptions. Quarterly drills are now standing calendar items, and the insurer accepted the program as evidence for renewal with no additional requirements. Department heads rehearse manual fallbacks twice a year alongside the technical restore, and the restore failures discovered in early drills were fixed in production before they could become real incidents.

METRIC	BEFORE	AFTER
Recovery time objective	72h	4h
Recovery point objective	24h	15 min
Full-service restore drills	0	4 per year

METRIC	BEFORE	AFTER
Immutable backup coverage	-	100% of Tier-1

The institutional changes outlast the technology. Council receives a recovery report grounded in timed, witnessed exercises rather than assurances, and the finance department's \$1.1M exposure estimate is now paired with a demonstrated four-hour recovery instead of an untested promise. The IT department's day-to-day confidence changed too: a failed verification alert is a work item, not a dread, and the question "would the backups actually restore" has an evidenced answer. The near-miss that started the program was luck; the current posture does not require any.

08

What Your Business Should Do

Marlow Bend's recovery program follows a discipline any organization can adopt, and it starts with the backups. Adopt 3-2-1-1-0 backup discipline — three copies, two media, one immutable or offline copy, zero unverified backups — because immutability is what stops attackers from deleting your escape route. Test restores quarterly, not annually, restoring real services to clean-room infrastructure on a fixed schedule and timing the result each run; untested backups fail at the worst possible moment, as CISA's ransomware guidance repeatedly warns. Write runbooks for business functions — recover payroll, permitting and billing as working services, not raw servers, so non-IT staff can verify each system before anyone declares recovery complete. Segment backups away from production in a separate network zone with brokered administrative access, because if domain admin credentials are compromised, backups must remain outside an attacker's reach. Close endpoint gaps with EDR coverage on every server and workstation, including the ones that rarely connect to headquarters — in Marlow Bend, one overlooked server nearly became patient zero. Retain incident response surge capacity before an incident, since contracts take days you do not have and attackers count on that delay. Rehearse manual fallbacks with operations, having department heads practice running essential functions on paper for a full day, which keeps services alive during restoration and surfaces procedural gaps early. Finally, tie your insurance renewal to test evidence: documented restore drills and immutable backup reports satisfy underwriters increasingly demanding proof of recovery testing, and clean evidence lowers premiums and friction. Walk through these eight steps with your leadership team using the action checklist in this practice book, and let the reflection questions open every drill debrief: when did you last restore a full production system from backup and how long did it take, if ransomware encrypted your backups tonight could the attackers delete them too, and who in your organization can delete backup jobs — is that list shorter than you would like?

REAL-WORLD PROOF & BENCHMARKS

IBM's 2024 Cost of a Data Breach report puts the average cost of a ransomware attack — excluding any ransom payment — at a reported \$4.91 million. - IBM Security, 2024

The Verizon Data Breach Investigations Report finds ransomware or extortion present in a reported 32% of all analyzed breaches worldwide, spanning every organization size. - Verizon DBIR, 2024

CISA's joint ransomware guide recommends offline, encrypted, immutable backups and regular restore testing, noting that untested backups frequently fail when recovery matters most. - CISA #StopRansomware Guide

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐**1. Adopt 3-2-1-1-0 backup discipline**

Keep three copies, on two media, with one immutable or offline copy, and verify zero backup errors. Immutability is what stops attackers from deleting your escape route.

OWNER

TARGET DATE

STATUS

--	--	--

☐**2. Test restores quarterly, not annually**

Restore real services to clean-room infrastructure on a fixed schedule and time the result each run. Untested backups fail at the worst possible moment, as CISA's ransomware guidance repeatedly warns.

OWNER

TARGET DATE

STATUS

--	--	--

☐**3. Write runbooks for business functions**

Recover payroll, permitting and billing as working services, not raw servers. Function-level runbooks let non-IT staff verify each system works before anyone declares recovery complete.

OWNER

TARGET DATE

STATUS

--	--	--

☐**4. Segment backups away from production**

Place backup repositories in a separate network zone with brokered administrative access. If domain admin credentials are compromised, backups must remain outside an attacker's reach.

OWNER

TARGET DATE

STATUS

--	--	--

☐**5. Close endpoint gaps with EDR coverage**

Deploy endpoint detection and response to every server and workstation, including the ones that rarely connect to headquarters. In this case, one overlooked server nearly became patient zero.

OWNER

TARGET DATE

STATUS

--	--	--

☐

6. Retain incident response surge capacity

Sign a retainer with an incident response firm before an incident. During a real event, contracts take days you do not have and attackers count on that delay.

OWNER

TARGET DATE

STATUS

--	--	--

☐

7. Rehearse manual fallbacks with operations

Have department heads practice running payroll or water-quality checks on paper for a full day. Manual fallback procedures keep essential services alive while systems restore, and they surface gaps early.

OWNER

TARGET DATE

STATUS

--	--	--

☐

8. Tie insurance renewal to test evidence

Use documented restore drills and immutable backup reports as underwriting evidence. Insurers increasingly demand proof of recovery testing, and clean evidence lowers premiums and friction.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. When did you last restore a full production system from backup — and how long did it actually take?

Q2. If ransomware encrypted your backups tonight, would the attackers be able to delete or encrypt them too?

Q3. Which three services must come back first for your organization to keep functioning, and does everyone agree?

Q4. How long could your finance operation run on manual fallback procedures before errors compound into real losses?

Q5. Does your cyber insurance renewal this year require documented recovery testing — and can you produce that evidence today?

Q6. Who in your organization can delete backup jobs, and is that list shorter than you would like?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Days 31-60 Focus: build and prove

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like City of Marlow Bend's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact