

Issue No. 2 · August 2026

THE TECHNOLOGY BRIEF

The Cost of an Hour

What downtime really invoices - and why 90% of enterprises now put it above \$300,000.

Eight Single Points of Failure

The person, the password, the pipe: a field guide to what actually stops you.

Your First Tabletop

The 60-minute drill we promised you in Issue No. 1. It is on page 12.

Inside this issue

In July we argued that maturity is an operating condition. This issue makes it physical: what stops when technology stops, how long you can bear it, and the drill that turns a binder into a capability. Everything here is designed to be practised, not filed.

A letter from our CEO	02
The promise we made you in July - kept, on schedule.	
The cost of an hour	03
The verified numbers behind downtime - and the one statistic about recovery nobody frames.	
Eight single points of failure	04
The person, the password, the power, the pipe - a field guide.	
How long can you be down?	05
RTO, RPO and maximum tolerable downtime, in plain English, with a table to fill in.	
Backups that actually restore	06
3-2-1-1-0, immutability, and why a backup is a hope but a restore is a fact.	
The failover myth	07
Five comfortable claims, and the one-line test that checks each of them.	
People are systems too	08
Key-person risk, runbooks, and the leaver protocol.	
When the screens go dark, talk	09
The first-hour communications kit: channels, shells, and the single-voice rule.	
The continuity pack	10
Five documents that must exist on paper - with owners and review dates.	
The restore stopwatch	11
One email to whoever runs your backups - and the one-line reply to expect back.	
Your first tabletop	12
The 60-minute executive drill. No slides, no blame, one log.	
How mature is your environment, really?	13
About the publisher - the Executive Environment Maturity Review.	
Sources & further reading	14
Every number, traced to the original study.	

OUR EDITORIAL STANDARD

Every figure in this issue comes from a named, dated study or the public record - and where a number is a survey result rather than a measurement, we say so. Full references on page 14. One more standard: the tools in these pages are checklists, not silver bullets. They only work when they are practised.



The drill we promised you in July.

Last month, on the back cover of our first issue, we made a promise: that Issue No. 2 would go deeper on business continuity, including how to run your first tabletop exercise. This is that issue, and the drill is on page 12, exactly where we said it would be. A publication that writes about reliability should start by being reliable.

Continuity has a reputation as the dull corner of technology: binders, acronyms, appendices. We think the opposite. Continuity is the most commercial question in this magazine - what stops when the screens stop, how long can you bear it, and who decides at two in the morning. Every other investment protects value; this one protects the ability to trade at all.

So this issue is deliberately physical. It is written to be printed, marked up, argued with and practised. You will find tables with blank rows, checklists with owners, and a stopwatch page that asks you for exactly one email, nothing more.

Run the drill. Keep the log of what nobody could answer. That list - not this magazine - is the real deliverable. Thank you for reading.

Christo Boshoff

CHIEF EXECUTIVE OFFICER, RAYTONCORP



The cost of an hour

Downtime is usually priced after the fact - by the invoice, the overtime, the apology. The organisations that handle it well price it in advance, **and then design backwards from the number.**

The advance numbers are not small. In ITIC's 2024 global survey, more than 90% of mid-size and large enterprises put the cost of a single hour of downtime above \$300,000, and for a substantial minority the figure exceeds \$1 million. The Uptime Institute's analysis points the same direction: over half of significant outages now cost more than \$100,000, and the expensive ones are getting more expensive.

But the statistic that should reorganise your calendar is about recovery, not outage. In Veeam's 2025 study of 1,300 organisations - 900 of which had suffered a ransomware attack in the previous year - only one in ten of those attacked recovered more than 90% of their data. A majority got back less than half. The gap between "we have backups" and "we got our business back" is where continuity actually lives.

This issue walks that gap end to end: what stops, for how long, on whose decision, from which copy of the data, announced in which words. None of it requires new spending to begin. It requires an afternoon, a printer, and the willingness to write down numbers you can be held to.

\$300_k+

the hourly cost of downtime for more than 90% of mid-size and large enterprises surveyed.

SOURCE · ITIC HOURLY COST OF DOWNTIME, 2024

1 in 10

attacked organisations that recovered more than 90% of their data. A majority recovered less than half.

SOURCE · VEEAM 2025 RANSOMWARE TRENDS (N=1,300)

89%

of attacked organisations found that the attackers had targeted their backups too.

SOURCE · VEEAM 2025 RANSOMWARE TRENDS

Continuity is a verb

A plan that has never been executed is a document. The pages that follow are built for execution: every one ends in something you can do, measure, or put a name against. The binder is the by-product. The capability is the point.

Eight single points of failure

A single point of failure is anything that stops the business when it stops - and most of them are not servers. Walk this list with your leadership team and mark each one green, amber or red. Honesty here is worth more than spend.

The person

SPOF 01

One administrator holds the passwords, the history and the habits. Their holiday is your outage; their resignation is your incident.

FIRST MOVE · Document their ten most critical tasks this month. Then have someone else perform each one, supervised.

The password

SPOF 02

Break-glass credentials that nobody can find at 02:00 - or that everybody can find, taped to a monitor.

FIRST MOVE · Sealed envelope or vault entry, two named holders, an access log, and a test-open twice a year.

The power

SPOF 03

The UPS that has never been load-tested; the generator with last year's fuel.

FIRST MOVE · Schedule a controlled failover test out of hours. If the answer is 'we cannot risk it', that is the finding.

The pipe

SPOF 04

One internet line, one provider, one street cabinet. Connectivity is the utility everything else assumes.

FIRST MOVE · Price a second path on different infrastructure - even a modest LTE failover changes the shape of a bad day.

The platform

SPOF 05

One server, one cluster, one cloud tenant that everything touches. Concentration feels efficient until it fails all at once.

FIRST MOVE · List what shares its fate. If the answer is 'everything', segmentation belongs on the next budget.

The payment run

SPOF 06

Payroll and supplier payments have dates that do not move for incidents.

FIRST MOVE · Write the manual procedure for running the next payment cycle with core systems down - bank tokens, approvals, paper trail.

The paper

SPOF 07

The process that exists only in someone's head. Undocumented is unrecoverable.

FIRST MOVE · Pick your three most revenue-critical processes and write the one-page 'how we do this by hand' version.

The partner

SPOF 08

A supplier whose outage stops you - logistics, software, materials. Dependency is fine; unpriced dependency is not.

FIRST MOVE · Map your top five, and put continuity obligations in the contracts, in both directions.

How long can you be down?

RTO

Recovery time objective - how long until it works again. The clock starts at failure and stops when the process runs, not when a server boots. It is a promise, so it must be a number someone signed.

RPO

Recovery point objective - how much work you can afford to lose. If backups run nightly, your honest RPO is 24 hours: a full day of orders, entries and email, gone. Say the number out loud before you accept it.

Maximum tolerable downtime (MTD) is the business version of the question: past this point, the damage stops being an inconvenience and starts being structural - lost customers, breached contracts, a payroll missed. Every core process has one, whether or not it is written down. Write it down. In pencil is fine; unsigned is not.

PROCESS	MTD	OWNER	LAST TESTED
Taking customer orders	___ hours	_____	___ / ___
Invoicing & payments out	___ hours	_____	___ / ___
Payroll	___ days	_____	___ / ___
Email & calendars	___ hours	_____	___ / ___
Your production system: _____	___ hours	_____	___ / ___

The pairing rule. Every MTD must be paired with a recovery capability that beats it - and the proof is a measured restore time, not an architecture diagram. Page 11 gives you the stopwatch; page 12 gives you the rehearsal. If the measured number is bigger than the tolerable one, you have found this quarter's priority for free.

Backups that actually restore

Attackers read the same manuals defenders do. In Veeam's 2025 research, **89% of attacked organisations found their backups had been targeted too** - because destroying the copy is what turns an incident into a ransom.

The counter is a rule you can say in one breath: 3-2-1-1-0. Three copies of your data, on two different types of storage, one of them off-site, one of them immutable or offline - a copy that no administrator credential, including a stolen one, can alter or delete - and zero errors when the backup is verified. Immutability is the clause that matters most and the one least adopted: in the same study, only 32% of organisations used immutable storage.

Then comes the discipline that separates hope from fact: restoring. A backup is a hope; a restore is a fact. The only evidence that your recovery works is a clock that was running while it happened - a full restore of a real system, to working state, timed, witnessed, and written down. Do it quarterly, rotate which system you test, and file the number next to the MTD it must beat.

One more habit worth stealing from the organisations that recover well: verify cleanliness before you restore. Recovering an infected copy replays the incident. Verification, isolation and a known-good sequence are what make the restore an ending rather than a repeat.

The rule, unpacked

- 3** Copies of the data - production plus two.
- 2** Different media or platforms - not one basket.
- 1** Copy off-site - distance is a control.
- 1** Copy immutable or offline - beyond any stolen credential.
- 0** Errors on verification - tested, not assumed.

32%

of organisations use immutable backup storage - the single clause attackers cannot argue with.

SOURCE · VEEAM 2025 RANSOMWARE TRENDS

Evidence beats assurance. Whoever runs your backups - an internal team, a partner, or both - the artefacts to ask for are the same: the verification report, the immutability setting, and the last timed restore. Any mature operator, ours included, should produce all three without notice.

The failover myth

Every organisation has sentences it says about resilience. Each one below is fine as an answer - and dangerous as an assumption. The right-hand column is the one-line test that turns the sentence into evidence.

THE COMFORTABLE CLAIM	THE ONE-LINE TEST
"We're in the cloud, so we're resilient."	Which region or zone do you fail over to, who presses the button, and when did anyone last press it? Cloud moves the failure domain; it does not delete it.
"We replicate every night."	Then your recovery point is 24 hours. Read yesterday's order count aloud and ask the room whether losing it is acceptable. If not, the schedule is a decision waiting to be made.
"Our provider handles it."	Ask for the evidence pack: the last verification report, the immutability setting, and the most recent timed restore. Any provider worth keeping - including us - should hand these over without notice.
"We have a generator."	When was it last run under real load, and how old is the fuel? A generator that has never carried the building is a theory with a fuel tank.
"We have a DR plan."	Date of the last full exercise, and the measured time to working state. If the answer is a year and an estimate, the plan is a document, not a capability.

Island mode: the grown-up version

The hardest continuity question of 2025 was asked in a car factory: can the part of the business that makes money keep running while the part that reads email is contained? One British manufacturer's answer was no - and the restart took five weeks. We dissect that story fully in October. The lesson is available now: separate what earns from what browses, and rehearse running degraded.

Score yourself

- ☐ All five tests answered with dates
- ☐ Three or four - gaps named, owners assigned
- ☐ Two or fewer - start with page 11's stopwatch

People are systems too

Ask what your riskiest system is and you will hear a server name. It is more often a person: **the one brain that holds the passwords, the history and the habits.**

The one-brain problem. If a single individual is the only route to any critical system, your continuity plan has a pulse and takes annual leave. The fix is not distrust; it is documentation and duplication. Nobody should be irreplaceable by accident.

Runbooks, not folklore. A runbook is one page per task: purpose, steps, credentials location, escalation, last review date. The test of a good one is brutal and cheap - a competent colleague performs the task using only the page, while the expert stays silent.

The leaver protocol. The day someone with privileged access resigns, a clock starts: access inventory within a day, transfer of duties within a week, credentials rotated on exit, break-glass envelopes re-sealed. Run it with warmth and without exception - it protects the leaver as much as the business.

The cross-training grid

List critical tasks down the side, people across the top. Every task needs two ticks. Blanks are findings.

TASK	A	B	C
Restore a server from backup	✓	✓	·
Fail over the internet link	✓	·	·
Run payroll manually	·	✓	·
Reach every staff member off-system	✓	·	✓

The co-managed advantage

Depth of cover is the quiet argument for pairing an internal team with a partner: your people keep the context, the partnership supplies the second and third pair of hands at 02:00, on leave days, and during resignations. Continuity of knowledge is a staffing design, not a document.

This month's exercise. Choose the three tasks whose absence would hurt most. Write the runbook for each. Then watch someone else perform them. Budget: three hours, zero rand.

When the screens go dark, talk

In a serious incident the systems you would use to communicate are often the systems that are down. **The communications plan therefore starts with a channel that does not depend on you.**

The out-of-band rule. A pre-agreed group on an independent platform, a printed phone tree in three drawers, and personal-mobile numbers for the leadership team. Establish it now, test it quarterly with a two-line drill message, and never let it live only inside the network it is meant to survive.

One voice. Appoint the spokesperson before the incident and route everything through them. Two well-meaning updates that disagree cost more trust than an hour of silence.

Say three things. What you know, what you are doing, and when you will update next - then keep that appointment even if the update is "no change". Never speculate about cause, scope or blame; early guesses become quotes. And note for September: where personal information is involved, notification stops being a courtesy and becomes a legal duty with its own clock. Next month's issue walks that path end to end.

SHELL · TO STAFF, HOUR ONE

"We are managing a technology incident affecting [systems]. Please do not attempt logins or workarounds. Updates at [time] via [channel]. Direct any external questions to [name]."

SHELL · TO CUSTOMERS

"We are experiencing a technology issue affecting [service]. Your [orders/data] status: [known facts only]. We will update by [time]. Thank you for your patience."

SHELL · TO KEY PARTNERS

"We have an incident in progress and are working to restore [dependency]. Expected impact on you: [honest estimate]. Single contact: [name, personal mobile]."

Print these shells tonight. Fill the brackets in an incident, not the sentences. The discipline of pre-written words is that they are written by the calm version of you.

Five documents that must exist on paper

If your continuity plan lives only on the systems it is meant to survive, it is a hostage, not a plan. These five pages belong in a physical folder in two places - and each carries an owner and a review date, because an unowned document decays into fiction.

1 • The contact tree

ON PAPER

Every staff member reachable off-system; leadership personal mobiles; the out-of-band channel; key customers and suppliers with named humans, not switchboards.

OWNER _____ · LIVES FRONT OFFICE + OFFSITE ·
REVIEWED ____ / ____

2 • The restart sequence

ON PAPER

The order in which the business comes back - dependencies first, revenue next, convenience last - with the owner and target time for each step. This is the page the JLR story is about.

OWNER _____ · LIVES SERVER ROOM + OFFSITE ·
REVIEWED ____ / ____

3 • The MTD table

ON PAPER

Page 5 of this issue, completed and signed: each core process, its maximum tolerable downtime, and the measured restore time that must beat it.

OWNER _____ · LIVES THIS FOLDER · REVIEWED ____
/ ____

4 • The critical vendor list

ON PAPER

Top suppliers and platforms, emergency contacts, contract numbers, and the continuity clauses you hold in both directions. Include your technology partner's escalation path.

OWNER _____ · LIVES FINANCE + OFFSITE ·
REVIEWED ____ / ____

5 • The words

ON PAPER

Page 9's three statement shells plus a blank decision log: time, decision, decider, reason. In an incident the log is your memory and, later, your evidence.

OWNER _____ · LIVES WITH THE CONTACT TREE ·
REVIEWED ____ / ____

The two-drawer test

Could a capable colleague, with the building empty and the network down, open one drawer and begin? If yes, you have a continuity pack. If no, you have intentions. Assemble it once; page 12's drill will tell you what it is missing.

The restore stopwatch

You do not run restore tests - whoever runs your backups does: your IT team, your technology partner, or both. Your part is one email that commissions the fact, and knowing what a good answer looks like when it comes back. Ten minutes, once, done.

THE EMAIL · COPY IT AS WRITTEN

To: Whoever runs your backups - internal IT, your technology partner, or both

Subject: Timed restore test - one line back, please

"Please schedule a restore test of our most critical system this month: restore it to a working state in a safe environment, time it from start until a real task works, and send me a single line back - the system, the date, the measured time-to-working, and who verified it. No report needed, just the line. If anything makes this difficult, that is worth a conversation."

THE REPLY TO EXPECT

"Invoicing system · restored 14 August · 3 h 40 m to working · verified by T. Naidoo"

That single line back is the fact. File it in the continuity pack (page 10), beside the tolerance you wrote on page 5.

Send it to anyone - including us. A mature operation will welcome this request and answer it without drama. Hesitation, or a report where a line would do, is itself an answer.

If the number beats your page 5 tolerance

Good - now make it routine with one more sentence in the same thread: "Same again each quarter, please, rotating systems." They keep the stopwatch and the log; you keep the one-line replies.

If it misses - or nobody can say

You have just found the quarter's priority for the price of an email. Put both numbers - the measured time and the tolerance - on the agenda of your next review meeting, and ask what closing the gap costs.

Email sent ☐ ____ / ____ · Reply received ☐ ____ / ____ · Beats the page 5 tolerance: yes ☐ no **Your part is finished.**

Why one email works

Evidence beats assurance, and this is the cheapest evidence in this magazine. Four one-line replies, a year from now, will be the most persuasive exhibit in any budget, audit or insurance conversation you have - and you will not have lifted anything heavier than a send button.

Your first tabletop

The 60-minute drill we promised in Issue No. 1. One scenario, four phases, no slides. Cast: CEO, CFO or risk owner, operations lead, IT lead or technology partner, and whoever would speak for the company. The scenario, read aloud: **"It is 06:00 on an ordinary Tuesday. Every screen in the business is dark, and nobody yet knows why."**

Phase 1 · Detect

15 MIN

1. How do we find out - who notices first, and who do they call at 06:00?
2. What is our out-of-band channel, and does everyone in this room know it without looking?
3. Within one hour, what do we actually know versus assume?

GOOD SOUNDS LIKE · A named first-caller, a channel that works with the network down, and comfort saying 'we do not know yet'.

Phase 2 · Decide

15 MIN

1. Who has authority to shut systems down or keep them down - alone, at dawn, without a meeting?
2. Which processes stop immediately, and what is the MTD for each (page 5)?
3. At what point do we activate the continuity pack (page 10) - and where is it?

GOOD SOUNDS LIKE · One name with pre-agreed authority, MTDs quoted from memory or paper, and a folder someone can walk to.

Phase 3 · Communicate

15 MIN

1. Who speaks - and what do staff hear in hour one, in what words?
2. Which three customers or partners must hear from a human, and who calls them?
3. What do we refuse to say, however hard we are pressed?

GOOD SOUNDS LIKE · The page 9 shells read aloud with the brackets filled, one voice appointed, speculation banned out loud.

Phase 4 · Begin the restart

15 MIN

1. What comes back first, second, third - and who owns each step of the sequence?
2. Which restore have we actually timed, and does that number beat the MTD it serves?
3. What would we be doing right now if the outage were malicious rather than mechanical?

GOOD SOUNDS LIKE · A restart order recited without debate, a measured restore time on the record - or page 11's email already sent - and the honest answer that malice changes the sequence.

The output

Log every question that met silence - with a name and a date against each. That list is your continuity programme for the quarter, written by your own team. Re-run the drill in ninety days and watch the list shrink; the shrinking is the metric.

Ground rules

Hard stop per phase. No blame - the drill tests the system, not the people. Phones down, one scribe. And invite your technology partner into the room: a mature provider should want to be tested.

How mature is your environment, really?

Many organisations only discover operational weaknesses after a major outage, a security incident, or an audit. The first continuity drill on page 12 gives you the honest first reading; for organisations that want an independent one, RaytonCorp conducts an **Executive Environment Maturity Review** - a structured assessment of:

- Infrastructure stability and operational visibility
- Cybersecurity maturity and exposure
- Vendor fragmentation and accountability gaps
- Connectivity resilience across sites and environments
- Business continuity readiness
- Alignment between technology and business objectives

The output is a plain-language report your board can read: where you sit on the five-stage model, which gaps carry real risk, and a sequenced plan to close them - whether or not RaytonCorp is the partner that executes it.

Book a review: info@raytoncorp.com · +27 10 026 3646 · www.raytoncorp.com

RaytonCorp at a glance

97.6%

Average technical support SLA compliance, 2024-2025

24/7

Network Operations Centre - continuous monitoring

24/7

IT Service Desk and SOC / SIEM monitoring

RSA & USA

International delivery across two continents

Microsoft Solutions Partner



Security

Recognised capability across secure operations and modern security practice



Infrastructure (Azure)

Expertise across modern infrastructure, cloud, and operational scalability



Modern Work

Capability across Microsoft 365, collaboration, and secure workplace operations

Sources & further reading

Every figure in this issue traces to the records below. Survey findings are labelled as such; where we reference a 2025 incident ahead of our October dissection, the underlying sources are listed here too.

Veeam - 2025 Ransomware Trends & Proactive Strategies

Survey of 1,300 organisations, 900 of which suffered at least one ransomware attack in the prior year. Key findings used in this issue: only 10% of attacked organisations recovered more than 90% of their data, with 57% recovering less than half; 89% found their backups targeted; 32% used immutable backup storage.

ITIC - Hourly Cost of Downtime Survey, 2024

Annual global survey of mid-size and large enterprises. More than 90% of respondents put the cost of a single hour of downtime above \$300,000, with a substantial share reporting figures beyond \$1 million per hour.

Uptime Institute - Annual Outage Analysis, 2023

Industry analysis of significant reported outages: over half of respondents said their most recent significant outage cost more than \$100,000, with the share of very expensive outages rising year on year.

Jaguar Land Rover statements & Cyber Monitoring Centre, 2025

Referenced on page 7: JLR's proactive September 2025 shutdown and phased five-week restart, per company statements; UK-wide impact independently modelled at £1.9bn by the Cyber Monitoring Centre. Our October issue dissects this case in full.

How to read this issue. The statistics above describe populations; your numbers will differ, which is exactly why the blank tables exist. Fill them with measurements, not estimates - and hold every claim in these pages, and every provider you work with, to the standard of evidence on request.



Thank you.

A continuity plan is a love letter to your future self on the worst morning of the year. If this issue leaves you with one signed MTD table, one timed restore, and one drill on the calendar, it has done its job. Issue No. 3 puts on the regulator's glasses: POPIA, the notification clock, and what "reasonable measures" must now prove. Until then: run your first drill on page 12, and keep the silence log.

PHONE



+27 10 026 3646



+1 682 297 7347



+1 873 738 4411

DIGITAL

info@raytoncorp.com

www.raytoncorp.com

HEAD OFFICE

21 North St, Illovo,

Johannesburg, South Africa, 2196