RAYTON CORP

Issue No. 1 · July 2026

THE TECHNOLOGY BRIEF

The Maturity Gap
What downtime and breaches actually cost - with the verified numbers.

The AI Question
Why AI readiness is an operations problem - with the 2025 numbers.

The Boardroom Scorecard
Ten questions, twenty points - a self-assessment for executives.

info@raytoncorp.com
www.raytoncorp.com
21 North St, Illovo, Johannesburg, 2196

+27 10 026 3646
+1 682 297 7347
+1 873 738 4411

Inside this issue

Most businesses inherit their technology environment rather than design it - and the gaps usually become visible only during an outage or a breach. This issue is about seeing them early.

OUR EDITORIAL STANDARD

Every statistic in this issue is drawn from a named, dated, publicly identifiable source - the study and year appear beside each figure, and full references are on page 14. Numbers you can defend in an exco meeting are the only numbers worth printing.

FROM THE PUBLISHER

Welcome to the first edition of the Rayton Technology Brief.

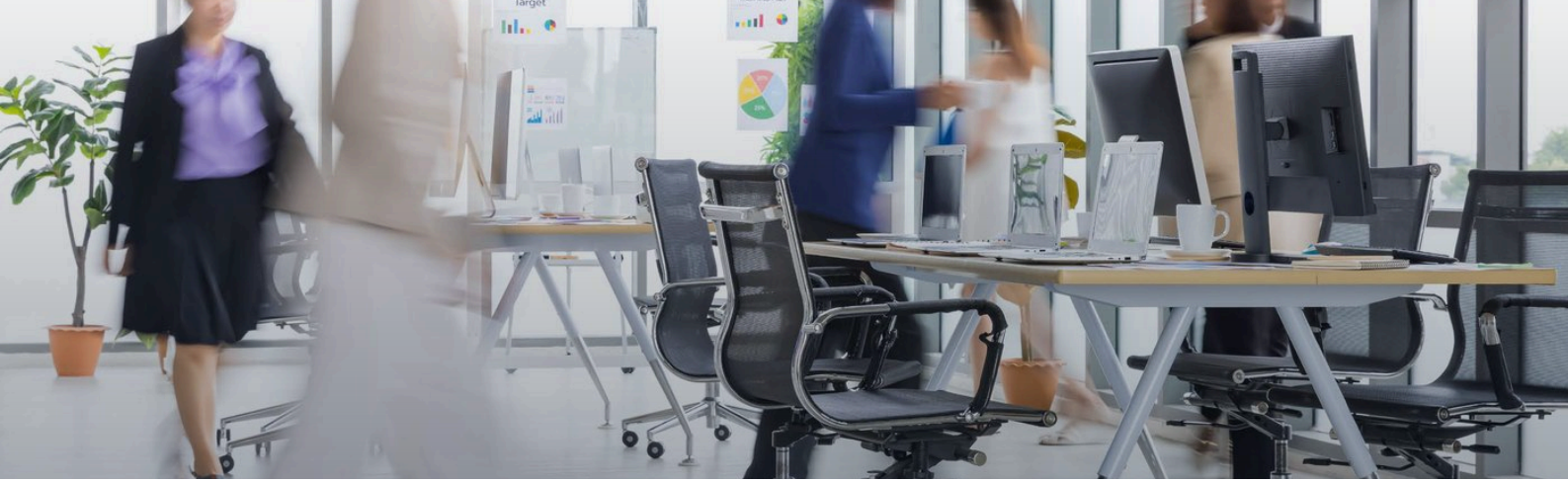
Technology plays a critical role in every modern organisation - yet few leadership teams get the chance to step back and ask how mature, resilient, and aligned their environment really is. Day-to-day operations, understandably, take priority.

The purpose of this publication is simple: to share practical, evidence-based insight that helps business leaders think clearly about technology, operational risk, cybersecurity, and long-term resilience. It is written to be used - discussed at exco, handed to a colleague, kept on a desk.

In this first edition we define what technology maturity looks like, examine what the best independent research says fragility actually costs, and give you two tools you can apply immediately: a five-stage maturity model and a ten-question boardroom scorecard. We also take an honest, numbers-first look at the AI question every board is now being asked.

My hope is that this issue sparks a meaningful conversation inside your organisation - and helps you see where your own environment can be made stronger. Thank you for reading.

Christo Boshoff
CHIEF EXECUTIVE OFFICER, RAYTONCORP



FEATURE · THE STATE OF THE ENVIRONMENT

The maturity gap

Technology maturity is **not defined by having internet, IT support, or security tools in place.** A mature environment is proactive, visible, resilient, and operationally aligned - and the distance between that and "it mostly works" is where risk lives.

Most environments grow reactively: a vendor added here, a system bolted on there, ownership split across teams and suppliers. Each decision was reasonable on its own. Together they produce fragmentation across infrastructure, cybersecurity, communications, support, and operational ownership - and with it, slower response, duplicated cost, and limited visibility into the true health of the environment.

The gap stays invisible because nothing is obviously broken. It surfaces the way independent research says it does: as an outage priced by the hour, a breach priced by the incident, and a recovery measured in days. The figures on this page are what "finding out the hard way" costs - each from a named study you can verify on page 14.

Read them less as a warning than as a budget case: prevention is cheap against these baselines - and the rest of this issue is about how to buy it deliberately.

DOWNTIME

90%+

of mid-size and large enterprises say a single hour of downtime now costs **more than $300,000** - and 41% put it at **$1 million to $5 million-plus**.

SOURCE · ITIC, 2024 HOURLY COST OF DOWNTIME SURVEY

54%

of significant outages cost over **$100,000**; roughly **one in five** exceeds $1 million.

SOURCE · UPTIME INSTITUTE, ANNUAL OUTAGE ANALYSIS 2024

$4.44m

global average cost of a data breach in 2025. For South African organisations the average is **R44.1 million**, with financial services highest at R70.2m.

SOURCE · IBM & PONEMON INSTITUTE, COST OF A DATA BREACH REPORT 2025

DIAGNOSIS

Common signs of operational immaturity

None of these is an emergency on its own. Three or more, and the environment is running on luck and individual heroics rather than on systems. Tick honestly:

- **Multiple vendors operating independently** across the environment, with no single view of the whole.
- **Cybersecurity, infrastructure, and support managed separately** - three contracts, three dashboards, three versions of the truth.
- **Limited visibility** into operational risks, vulnerabilities, and the real state of assets.
- **Reactive support** that only engages after disruption has already reached users.
- **Slow incident response** caused by unclear ownership and undefined escalation paths.
- **Backup, continuity, and recovery processes that are rarely reviewed or tested** - a backup that has never been restored is a hope, not a control.
- **Heavy reliance on individuals** instead of documented systems and governance - resilience that resigns when they do.

The business impact

Operational immaturity creates more than technical debt - it creates business risk. When environments fragment, organisations consistently experience:

→ **Increased downtime** and operational disruption

→ **Greater exposure** to security and continuity failures

→ **Reduced visibility** into infrastructure and risk

→ **Difficulty scaling** operations efficiently

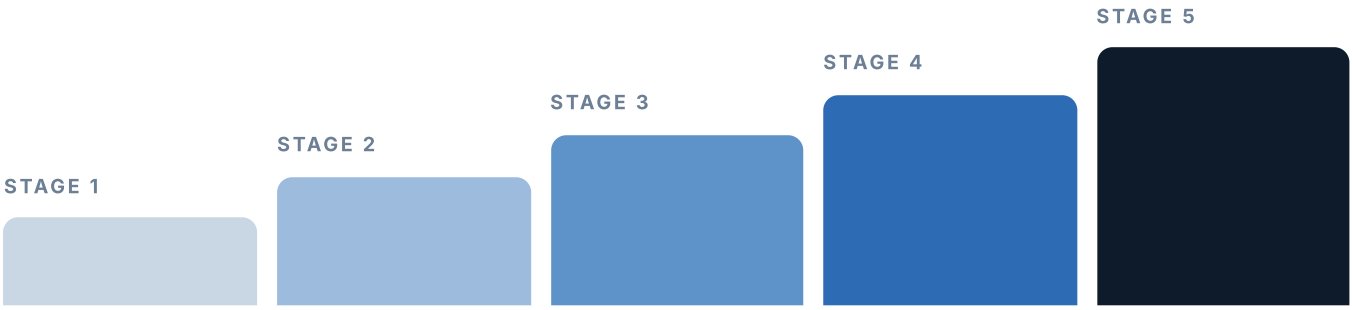
→ **Slower resolution** and poor provider coordination

→ **Leadership uncertainty** about true maturity

FRAMEWORK · KEEP THIS PAGE

The five stages of technology maturity

Maturity is not a purchase; it is an operating condition. Use the model below to place your organisation honestly - most sit between **Stage 1 and Stage 2** and believe they are at Stage 3. The scorecard on page 11 will test that belief with numbers.



Reactive

How it feels: Firefighting. Issues are discovered by users; fixes depend on whoever is available.

What breaks: Anything, unpredictably. Downtime is priced at the moment it happens.

Stabilising

How it feels: Basics exist - backups, antivirus, a helpdesk - but they are unverified and unowned.

What breaks: Recovery. Controls that were never tested fail exactly when they are needed.

Proactive

How it feels: Monitored. Issues are found before users report them; patching and access follow a cadence.

What breaks: The seams - handoffs between vendors and teams during complex incidents.

Managed

How it feels: Accountable. One operating framework, clear ownership, SLAs measured and reported to leadership.

What breaks: Little - and when it does, the path to resolution is already defined.

Optimised

How it feels: Strategic. Technology risk is governed like financial risk; continuity is rehearsed, not assumed.

What breaks: Nothing by accident. Planned exercises deliberately stress-test the environment, so weaknesses surface before attackers or outages find them.

How to move one stage - not five

Maturity fails as a transformation project and succeeds as a sequence. Each stage is earned by making the previous one boring: verified backups before monitoring, monitoring before governance. Page 12 turns this into a 90-day plan.

Why the middle is dangerous

Stage 2 is where most losses happen: enough tooling to feel safe, not enough verification to be safe. Confidence rises faster than capability - the gap between the two is precisely what the figures on page 03 price.

PRACTICE

What mature organisations do differently

Mature organisations treat technology as an **operational ecosystem**, not a collection of isolated services. Rather than reacting after disruption, they design for **visibility, accountability, resilience, and continuity** - so that infrastructure, security, connectivity, support, and workplace technology operate inside one framework. Six habits recur in every environment we would call mature:

HABIT 1

Centralised operational visibility

Leadership can see infrastructure performance, security posture, open risks, and support health in one place. No single view means every decision is made on partial truth.

HABIT 2

Proactive monitoring & support

Issues are identified and resolved early through continuous monitoring and structured support - measured by problems prevented, not tickets closed.

HABIT 3

Stable, scalable infrastructure

Cloud and on-premise environments are designed for continuity and growth: documented, standardised, and capable of absorbing change without drama.

HABIT 4

Secure modern work

Collaboration, mobility, and productivity are enabled without multiplying risk - identity-first access, managed devices, and data protection built into daily work.

HABIT 5

Security as an operation

Cybersecurity is embedded in daily operations - monitoring, vulnerability management, incident readiness, and governance - not a product bought once a year. Page 07 shows why the 2025 data makes this non-negotiable.

HABIT 6

Tested continuity

Backups are restored on a schedule, failover is rehearsed, and recovery time is a known number. Continuity is treated as a capability to demonstrate, not a document to file.

The shift under way

Leading organisations are moving away from fragmented technology structures and toward integrated ecosystems built around accountability and long-term resilience. The result is measurable: greater visibility, stronger continuity, faster coordination - and environments that support the business instead of surprising it.

Identity is the new perimeter

The most reliable threat research of the past year tells a consistent story: attackers are not breaking in - **they are logging in.**

Microsoft's telemetry shows **97% of identity attacks are password attacks** - spray and brute force against weak, reused credentials - with identity attacks up 32% in the first half of 2025 alone. Verizon's analysis of 12,195 confirmed breaches finds stolen credentials the top initial access vector (22%), followed by exploited vulnerabilities (20%), with the **human element present in 60% of breaches**.

Ransomware, once the attacker's weapon of last resort, now appears in **44% of all breaches** - up from 32% a year earlier - and it discriminates by size: **88% of breaches at small and mid-sized organisations** involve ransomware, against 39% at large enterprises. Smaller firms are not flying under the radar - they are the target.

The supply chain compounds it. Third-party involvement in breaches **doubled in a single year, from 15% to 30%** - your exposure now includes every provider with a password to your environment.

The encouraging news sits in the same reports: victims are recovering better (64% now refuse to pay ransoms, up from 50% two years ago; the median payment fell to $115,000), and the highest-impact defences are neither exotic nor expensive. They are operational habits - listed on the right.

>99%

of identity-based attacks are blocked by **phishing-resistant MFA** - even when the attacker already holds a valid username and password.

SOURCE · MICROSOFT DIGITAL DEFENSE REPORT 2025

44%

of breaches involved ransomware in 2025 - and **88%** of breaches at SMBs, versus 39% at large enterprises.

SOURCE · VERIZON 2025 DATA BREACH INVESTIGATIONS REPORT

15→30%

third-party involvement in breaches **doubled** year over year - vendor risk is now breach risk.

SOURCE · VERIZON 2025 DATA BREACH INVESTIGATIONS REPORT

Five controls that do the heavy lifting

1 · Phishing-resistant MFA on every account - admins first, no exceptions for executives.

2 · Patch cadence with SLAs, prioritising edge devices, VPNs, and internet-facing systems.

3 · 24/7 detection endpoint detection plus someone actually watching - alerts nobody reads protect nobody.

4 · Tested, isolated backups restored on a schedule, with copies ransomware cannot reach.

5 · Least privilege access reviewed quarterly; vendor and service accounts held to the same standard as staff.

AI-ready is operations-ready

Every leadership team is being asked for an AI plan. The 2025 breach research carries an uncomfortable message for most of them: **AI amplifies the operational state it lands on.** Mature environments compound their advantage; immature ones compound their risk.

Adoption is outrunning oversight. Among breached organisations studied by IBM, **63% had no AI governance policy at all**, and 97% of AI-related security incidents happened where AI access controls were missing. Unsanctioned "shadow AI" - staff quietly using unapproved tools - added an average of **$670,000** to breach costs where usage was high.

Attackers moved first. AI-generated phishing now achieves more than four times the click-through of traditional campaigns, and one in six breaches already involves AI-driven attack techniques. The defensive dividend is just as real - organisations using security AI and automation extensively saved **$1.9 million per breach** and shortened response by 68 days - but that dividend is only collected by teams whose identity, logging, and monitoring foundations already work.

The practical conclusion for boards: an AI initiative inherits your identity model, your data hygiene, your monitoring coverage, and your governance discipline on day one. It does not skip the staircase on page 05 - it steepens it.

63%

of breached organisations had **no AI governance policy** to manage AI or prevent shadow AI.

SOURCE · IBM & PONEMON, COST OF A DATA BREACH REPORT 2025

$670k

average added to breach costs where **shadow AI** use was high - unapproved tools leadership cannot see.

SOURCE · IBM & PONEMON, COST OF A DATA BREACH REPORT 2025

4x+

AI-generated phishing achieves over four times the click-through of traditional campaigns.

SOURCE · MICROSOFT DIGITAL DEFENSE REPORT 2025

Five questions before your first AI project

1 · Ownership
Who owns AI risk - a name, not a committee?

2 · Data reach
Which data could an AI tool touch, and is that data classified?

3 · Shadow use
How would you detect unapproved AI use across the business today?

4 · Non-human identity
Are agents, integrations, and service accounts governed like people?

5 · Visibility
Does monitoring extend to the new surface AI creates?

The arithmetic of always-on

Attacks and outages do not keep office hours. Before 24/7 coverage is a strategy question, it is an arithmetic one - and the arithmetic surprises most executives.

One seat, always watched: a week is 168 hours and a full-time analyst covers 40. That is **4.2 people for a single around-the-clock seat** before leave, training, sickness, and turnover - realistically five to six. Add an escalation layer and senior cover, and a credible in-house 24/7 capability starts at **eight to ten specialists**, before tooling, management, and the recruitment cycle.

The market compounds it. ISC2 measured a record global shortfall of **4.8 million cybersecurity professionals** in 2024 - and by 2025 the constraint had shifted from headcount to skills, with 95% of teams reporting at least one skills gap. IBM's research puts a price on the shortfall: organisations with significant security-staffing gaps recorded breach costs roughly **$1.76 million higher**. Even well-funded internal teams struggle to hold depth across every specialism a modern environment demands: detection, identity, patching, backup, network, cloud.

Three honest models follow. **Build** - right when scale, regulation, or data sensitivity justify permanent shift teams, typically at large-enterprise size. **Partner** - 24/7 monitoring, response, and specialist depth as a service, with the economics shared across many environments. **Co-managed** - a partner carries nights, weekends, and specialist depth while the internal team keeps business context and control; increasingly the default for mid-sized organisations. There is no single right answer. There is a wrong one: assuming daytime staffing provides night-time protection.

4.2

people needed to keep **one seat watched around the clock** - before leave, training, and turnover.

SOURCE · STAFFING ARITHMETIC: 168-HOUR WEEK / 40-HOUR ROLE

4.8m

record global shortfall of cybersecurity professionals measured in 2024.

SOURCE · ISC2 CYBERSECURITY WORKFORCE STUDY 2024

59%

of security teams call their **skills gaps critical or significant** - up from 44% a year earlier.

SOURCE · ISC2 CYBERSECURITY WORKFORCE STUDY 2025

Questions that reveal real coverage

1 · The 02:13 test
Who acknowledges an alert at 02:13 - a name, not a team?

2 · The clock
What is the measured time-to-acknowledge, and time-to-engage?

3 · The surprise
What happened to the last alert nobody expected?

4 · The authority
Does night cover include authority to act, or only to notify?

GOVERNANCE

The vendor sprawl problem

Every additional provider adds capability - and a seam. Incidents live in the seams.

When connectivity, infrastructure, security, and support each belong to a different vendor, no single party owns the outcome. Diagnosis becomes negotiation: each provider proves their component works while the business stays down. Accountability gaps do not appear in any contract - they appear at 2 a.m. during an incident.

The market has noticed. In Gartner's survey of security and risk leaders, **75% of organisations were pursuing security vendor consolidation - up from 29% just two years earlier** - citing dissatisfaction with the operational inefficiency of fragmented stacks. Tellingly, the top expected benefit was not cost: **65% expected an improved risk posture.** Fewer, deeper relationships are easier to see, govern, and hold to account.

Verizon's finding on page 07 is the sharp end of the same trend: with third-party involvement in breaches doubling to 30%, every vendor relationship is now part of your attack surface. Consolidation is not about buying less - it is about ensuring that everything you buy answers to one operating framework, one escalation path, and one accountable owner.

Whether you consolidate to one partner or govern several, the questions on the right separate providers who own outcomes from providers who own components. Ask them annually. Write down the answers.

75%

of organisations were pursuing **security vendor consolidation**, up from 29% in 2020 - driven by operational inefficiency, not cost.

SOURCE · GARTNER SURVEY OF 418 ORGANISATIONS, SEPT 2022

Six questions for every provider

1. Who is accountable when the fault sits between you and another vendor?

2. What do you monitor proactively - and what would you have caught last quarter?

3. When was our recovery last tested end-to-end, and what was the measured time?

4. Which of your staff can access our environment, and how is that access secured and reviewed?

5. What is your own security posture - certifications, audits, incident history?

6. Can you show us the live state of our environment - patching, backups, open risks - on one view, today?

Consolidation, done right

Consolidate accountability, not just invoices. One bill from a provider who still subcontracts blindly changes nothing. The test is a single owner with authority across the whole stack - and a named escalation path.

Insist on evidence, not assurances. A mature partner reports in numbers leadership can read - patch compliance, backup test results, incidents detected and resolved - every month, without being asked.

Contract for outcomes. SLAs on response and recovery time, measured and reported on a cadence leadership actually sees - the numbers that prove the partnership is working.

TOOL · PHOTOCOPY FREELY

The boardroom scorecard

Ten questions, answered honestly by the executive team - not the IT team alone. Score each: **2 = yes, verified in the last 12 months · 1 = partly, or unverified · 0 = no, or unknown.** "Unknown" scores zero on purpose: not knowing is the finding.

Nº	QUESTION	SCORE 0-2
01	Can leadership see the current health of infrastructure, security, and support in **one view**?	
02	Is there a **single accountable owner** for technology outcomes - internal or external - with authority across vendors?	
03	Has a **full restore from backup** been performed and timed in the last 12 months?	
04	Is **phishing-resistant MFA enforced on every account**, including executives, admins, and vendor accounts?	
05	Are critical patches applied within a **defined, measured SLA** - especially on internet-facing systems?	
06	Is the environment **monitored 24/7 by people who act**, not just tools that alert?	
07	Does a **written, rehearsed incident response plan** exist, with names, roles, and an out-of-band contact path?	
08	Do you know your **maximum tolerable downtime** for core systems - and has recovery been proven inside it?	
09	Is **third-party access** inventoried, least-privileged, and reviewed at least quarterly?	
10	Would the environment **run unchanged if one key person resigned** tomorrow - documentation, credentials, and all?	

0-7

Reactive. The environment runs on luck. Start with visibility and one verified restore - this week, not this quarter.

8-13

Stabilising. Foundations exist but are unproven. Verify controls before adding new ones.

14-17

Proactive. Strong operations; the risk now sits in seams between providers. Fix accountability.

18-20

Managed → Optimised. Maintain the cadence and pressure-test assumptions with exercises.

Re-score every six months. The trend matters more than the number - a 12 moving up beats a 16 standing still.

TOTAL _____ / 20 · DATE _____

PLAYBOOK

The first 90 days

Moving one maturity stage is a quarter's work, done in the right order. Each phase ends with **proof** - something you can show the board, not something you can only describe.

DAYS 1-30 · SEE

Establish the truth

Inventory every asset, account, vendor, and access path. Switch on centralised logging and alerting. Run one full restore from backup and time it. Score the environment on page 11 - honestly.

Proof: A one-page environment map, a timed restore result, a baseline score.

DAYS 31-60 · STABILISE

Close the biggest gaps first

Enforce phishing-resistant MFA on every account. Set and start measuring patch SLAs, edge devices first. Define one incident path - who is called, in what order, on what number - and remove standing access nobody can justify.

Proof: MFA coverage at 100%, first patch-SLA report, a printed call tree that survived a test call.

DAYS 61-90 · SYSTEMATISE

Make it governance, not heroics

Set the operating cadence: monthly service and risk review, quarterly access review, six-monthly restore test and scorecard re-run. Walk the executive team through one tabletop continuity exercise. Assign a single accountable owner for the whole environment.

Proof: A review calendar with names on it, one exercise report, a re-scored card that moved.

A note on budget. Almost everything above is configuration, process, and discipline rather than procurement. The spend conversation comes after Day 90 - and it will be a better conversation, because it will be about closing measured gaps instead of buying reassurance.

ABOUT THE PUBLISHER

How mature is your environment, really?

Many organisations only discover operational weaknesses after a major outage, a security incident, or an audit. The scorecard on page 11 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

REFERENCES

Sources & further reading

Every figure in this issue traces to one of the studies below. All are publicly identifiable; most are free to download. We encourage you to read the originals - and to hold this publication, and every provider you work with, to the same standard.

ITIC - 2024 Hourly Cost of Downtime Survey

Independent survey of 1,000+ firms worldwide (Nov 2023 - Mar 2024). Cited for: 90%+ of mid-size and large enterprises reporting hourly downtime above $300,000; 41% from $1m to over $5m. *itic-corp.com*

Uptime Institute - Annual Outage Analysis 2024

Global analysis of significant outages. Cited for: 54% of major outages costing over $100,000; nearly one in five exceeding $1 million. *uptimeinstitute.com*

IBM & Ponemon Institute - Cost of a Data Breach Report 2025

Study of 600 breached organisations, March 2024 - February 2025. Cited for: $4.44m global average breach cost; R44.1m South African average; R70.2m in local financial services; 63% of breached organisations lacking AI governance; a $670,000 shadow-AI cost premium; $1.9m saved with extensive security AI. The 2024 edition priced significant security-staffing shortages at roughly $1.76m in added breach cost. *ibm.com/reports/data-breach*

Verizon - 2025 Data Breach Investigations Report

Analysis of 22,000+ incidents and 12,195 confirmed breaches. Cited for: ransomware in 44% of breaches (88% at SMBs vs 39% at large enterprises); third-party involvement doubling from 15% to 30%; human element in 60%; credentials 22% and vulnerabilities 20% of initial access; median ransom $115,000; 64% of victims refusing to pay. *verizon.com/dbir*

Microsoft - Digital Defense Report 2025

Microsoft Threat Intelligence, drawing on trillions of daily signals. Cited for: 97% of identity attacks being password attacks; identity attacks up 32% in H1 2025; phishing-resistant MFA blocking over 99% of identity-based attacks even with valid credentials; AI-generated phishing achieving over four times the click-through of traditional campaigns. *microsoft.com/mddr*

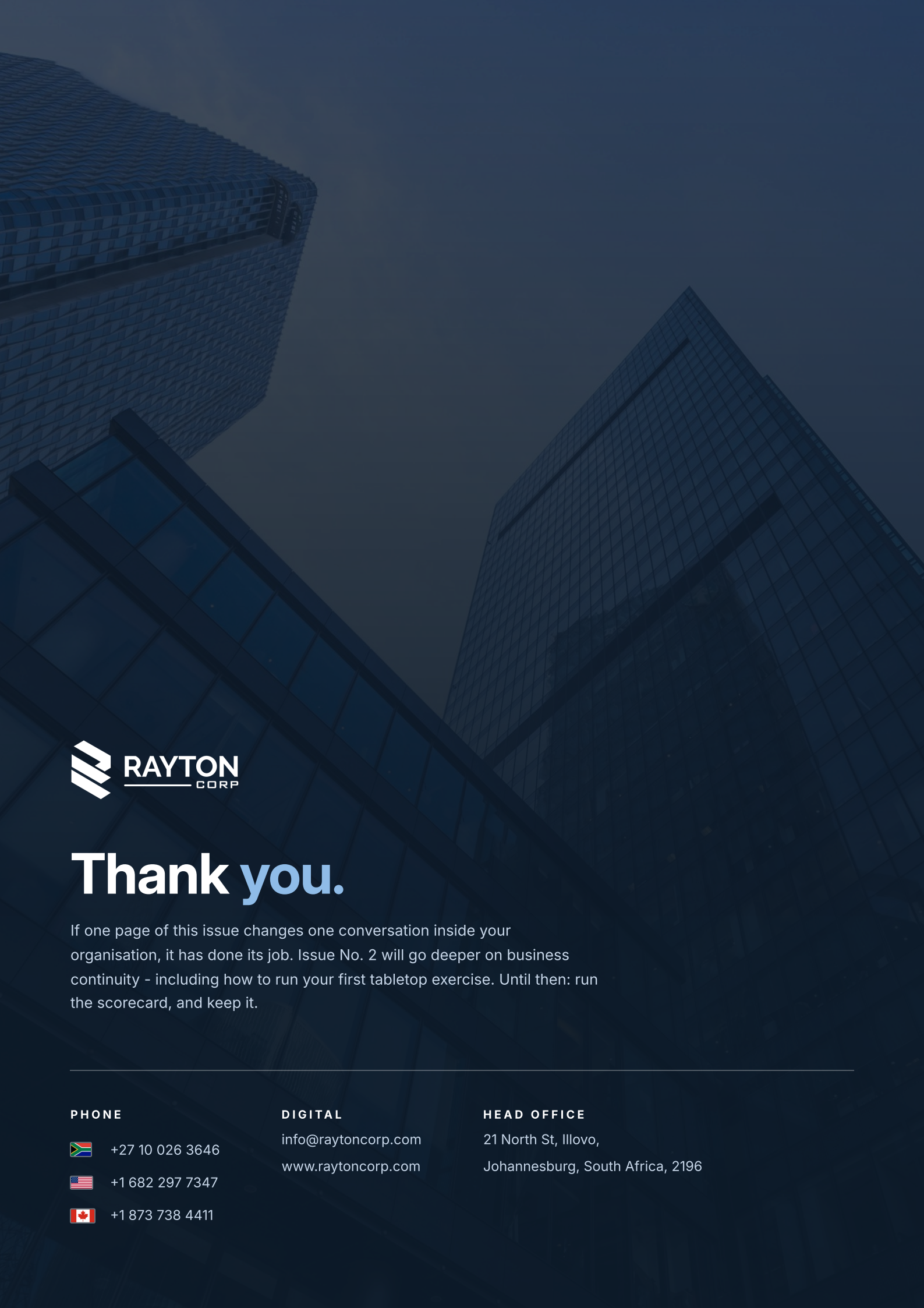
Gartner - Security Vendor Consolidation Survey, Sept 2022

Survey of 418 organisations across North America, APAC, and EMEA. Cited for: 75% pursuing security vendor consolidation, up from 29% in 2020; 65% expecting improved risk posture as the primary benefit. *gartner.com*

ISC2 - Cybersecurity Workforce Study 2024 & 2025

Annual survey of 16,000+ security professionals worldwide. Cited for: the record 4.8 million global workforce gap (2024); 95% of teams reporting at least one skills gap and 59% rating theirs critical or significant (2025). *isc2.org/research*

How to read these numbers. Survey figures are global or regional averages and reflect each study's sample and method; your exposure depends on your industry, size, and dependence on technology. Use them as directional benchmarks for risk conversations - and pair them with your own measured data wherever possible. Statistics were verified against the original publishers in 2026; where a study is older (Gartner, 2022), the date is shown so you can weigh it accordingly.



RAYTON CORP

Thank you.

If one page of this issue changes one conversation inside your organisation, it has done its job. Issue No. 2 will go deeper on business continuity - including how to run your first tabletop exercise. Until then: run the scorecard, and keep it.

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