August 24, 2026
gocorptech.com

CORPORATE TECHNOLOGIES LLC

SMB Technology & Cyber Resilience Index

Q2 2026 Edition

Published by Corporate Technologies, Eden Prairie, MN

Table of Contents

Executive summary

The first edition of this index documented a gap between what small and mid-sized businesses believe about their IT resilience and what their operational data shows. One edition later, the gap has not closed. What has changed is how precisely it can be measured.

Veeam's 2026 Data Trust and Resilience Report found that 90% of security leaders are confident they can recover from an attack, yet only 28% of organizations hit by ransomware actually restore their data in full. Hiscox's 2026 Cyber Readiness Report found that 56% of U.S. small businesses experienced at least one cyberattack in the past twelve months, averaging 2.38 attempts each. And the Verizon 2026 Data Breach Investigations Report, published in May, found that where organization size was known, 96% of ransomware victims were small and mid-sized businesses.

This edition also marks a change in how the index itself is measured. The Q1 edition drew on operational roll-ups from the managed client base. For Q2, the underlying figures come directly from quarter-scoped instrumentation: the ConnectWise RMM patching platform, the Huntress managed detection platform, application control logs, and a full export of the quarter's service tickets. Where the new instrumentation measures something different from the legacy roll-ups, this report says so explicitly rather than forcing a false trendline; several metrics are therefore not directly comparable to Q1. A recurring theme of the quarter is that better instruments change the readings before they change the reality.

Operational stability held. Outage frequency, duration, and recovery time were essentially unchanged from the prior reading, even as the client base absorbed 9.19 billion analyzed security events over the quarter. The index's largest gap, meanwhile, did not move. Documented recovery objectives and tested restores remain at 5% of clients, while the industry data on what happens to untested backups during an incident grew worse.

> "Most SMBs don't lack awareness, but measurement," said Jim Griffith, CEO of Corporate Technologies, in the Q1 2026 edition. "This index exists to replace assumptions with operational evidence, and to give business owners a benchmark they can actually act on."

Executive summary

> "SMB adoption of AI still trails the enterprise, but criminal adoption hasn't waited," said Jim Griffith, CEO of Corporate Technologies. "Phishing, smishing, and social engineering have become materially harder for individuals to detect, which means a company's resilience can no longer depend on any single layer. The network, the employees, and the core applications all have to hold."

Q2 2026 at a glance

9.19 billion security events analyzed across the client base	**0** ransomware detonations detected all quarter	**~2.6 hrs/yr** typical client downtime, against a 14-hour industry average
93.3% support tickets resolved remotely	**8.5 hrs** average resolution for critical (P1) issues	**5%** of clients have a tested restore, the index's widest gap

Figures are Q2 2026 (April to June) from Corporate Technologies operational instrumentation. Full detail in the pillar analysis.

The five pillars of this index and their Q2 findings:

1. Availability & Downtime

The managed client base recorded 499 unplanned outages across roughly 1,700 client organizations, an average of 0.29 per client for the quarter and effectively identical to the prior reading of 0.294. Average outage duration and mean time to recovery both held at 132 minutes, putting a typical client's annual downtime around 2.6 hours against the 14-hour industry average (ITIC, 2024). Every recorded outage occurred during business hours, consistent with hardware and software failure patterns rather than cyber-initiated incidents.

2. Backup & Disaster Recovery Readiness

Backup automation (71%) and offsite or cloud replication (60%) remain well above industry averages. Documented RPO/RTO targets and 90-day tested restores remain at 5% each, unchanged from the prior edition and still the widest gap in the index. The external context deteriorated. Veeam's 2026 research finds only 28% of ransomware victims fully restore their data, and Semperis' 2025 study found just 23% of victims recover within a day, down from 39% a year earlier.

3. Cyber Resilience

This quarter the index moved from a single blocked-threat count to a full detection funnel, drawn from the Huntress platform's quarter-scoped reporting. Over the quarter it analyzed 9.19 billion events across 47,482 monitored entities, filtered to 127,016 signals, 892 human investigations, and 215 confirmed incidents, 134 of them critical. No ransomware detonation was detected across the client base during the quarter; the 278,476 ransomware canary files deployed on 13,379 endpoints, none of which triggered, provide the highest-confidence slice of that evidence. 126 of the 215 incidents (59%) originated in identity systems rather than on endpoints, a pattern directionally consistent with Sophos' 2026 finding that 79% of ransomware attacks now begin with compromised identities. MFA adoption held at 63% of managed users, still roughly 1.7 times the published SMB benchmarks, and still leaving 37% of users exposed.

4. Operational Maturity

The help desk metrics promised in the Q1 edition arrive in this one, with 99,545 tickets logged in the calendar quarter, 93.3% resolved remotely, and Priority 1 issues resolved in an average of 8.5 hours. This edition also adopts stricter patch-compliance instrumentation. Measured as the percentage of devices fully current on every applicable patch, desktop compliance is 65.3% and server compliance 86.3% (90% and 95% respectively against policy thresholds). These figures are lower than the legacy roll-up reported in Q1 because they measure a harder standard, not because patching deteriorated; the distinction, and the reason this index prefers the harder number, is discussed in the pillar analysis.

5. Financial Impact

Modeled downtime cost for the managed client base held at approximately $32,500 per year for a 50-employee firm at the base scenario of $12,500 per hour, roughly 80% below the modeled cost of industry-average downtime. The external economics shifted in an unexpected direction this quarter. Median ransom payments fell to $769,000 (Sophos, 2026) while average recovery costs rose 11% to $1.7 million, and cyber insurance rates declined for a twelfth consecutive quarter.

Pillar	Internal Benchmark (Q2 2026)	Industry Benchmark	Delta
Availability & Downtime	~2.6 downtime hrs/yr, 132-min MTTR	~14 unplanned downtime hrs/yr (ITIC, 2024)	Well below industry norm; stable
Backup & DR	71% automated / 5% tested restores	28% of ransomware victims fully restore (Veeam 2026)	Strong automation, unmoved testing gap
Cyber Resilience	215 verified incidents; 0 ransomware detonations; MFA 63%	56% of SMBs attacked annually (Hiscox 2026); MFA 34–40%	MFA well above benchmark; no detonations against a high-targeting backdrop
Operational Maturity	Blended resolution 39.0 hrs (P1: 8.5 hrs); 93.3% remote; strict patch compliance 65.3–86.3%	21.96-hr avg resolution (Freshservice 2025); 59% patch within 6 days (Adaptiva 2026)	Mixed: fast on critical work; patching now measured strictly
Financial Impact	~$32.5k/yr modeled downtime cost	~$175k/yr at industry-average downtime (2024 baseline)	~80% lower modeled cost

2. Methodology & Data Sources

2a. Data Period & Scope

Internal operational data covers Q2 2026 (April–June 2026) and is drawn from the full active SMB client base of approximately 1,700 managed client organizations. All data is aggregated and anonymized, with metrics expressed as averages, percentages, or ranges across the entire managed portfolio. No client identifiers appear in this report, and source exports containing client-level detail are deliberately reduced to aggregates before inclusion.

The prior edition reported on Q4 2025 data. This edition moves the index onto a same-quarter cadence: the reporting period is the calendar quarter immediately preceding publication. Comparisons with the prior edition in this report therefore span two calendar quarters (Q4 2025 to Q2 2026), which readers should keep in mind when interpreting trend statements.

External industry benchmarks are sourced from primarily U.S.-focused research published between 2024 and 2026, supplemented by global studies where noted. Several sources cited in the Q1 edition have newer editions, including the Verizon 2026 Data Breach Investigations Report, Sophos' State of Ransomware 2026, Veeam's 2026 Data Trust and Resilience Report, the Hiscox Cyber Readiness Report 2026, and Adaptiva's State of Patch Management 2026. This edition cites the updated figures, alongside benchmarks newly consulted for this edition such as the Freshservice 2025 Service Management Benchmark. Where a newer edition does not restate a previously cited statistic, this report either labels the figure with its original year or retires it. A full source list appears in the Appendix.

2b. A Note on Measurement Changes in This Edition

This edition replaces several legacy roll-up figures with quarter-scoped platform instrumentation. Three changes matter for anyone comparing this report against Q1:

Security incidents.
Q1 reported 379 security escalations from operational roll-ups. Q2 reports 215 verified incidents from the Huntress platform's Q2-scoped detection funnel, a count produced by a documented pipeline (signal → human investigation → confirmed incident) covering exactly April 1 through June 30. The two figures come from different pipelines with different definitions and should not be read as a 43% decline.

Threat volume.
Q1 reported 12,977 blocked ransomware attempts as a single count. The Q2 instrumentation does not produce an equivalent single number; it produces a funnel (Section 4c), which is both more informative and more honest about what automated defenses actually do. The single count is retired.

Patch compliance.
Q1 reported 94% endpoint and 99% server compliance from a legacy measure. Q2 reports from the RMM platform's device-level assessment, under two defined standards: a strict standard (device is current on every applicable patch) and a policy standard (device is within the patching policy's compliance threshold). The strict numbers are substantially lower than the legacy figures. This index adopts the stricter instrumentation going forward, for the same reason it prefers operational data over surveys. The stricter number describes the standard an attacker actually tests.

All internal operational metrics in this report were compiled from platform exports reviewed by the operations organization under Ben Silver, Chief Operating Officer, whose team is responsible for service delivery across the managed client base.

2c. Why Operational Data Is More Reliable Than Surveys

The majority of SMB technology benchmarks rely on self-reported survey data, which systematically inflates security posture, a measurement problem known as social desirability bias. The pattern repeats across the current research cycle. Devolutions found 71% of SMBs confident in their ability to handle a major incident while only 22% report a security posture advanced enough to justify it, and Veeam's 2026 report set 90% recovery confidence against a 28% full-restore reality.

Operational data removes the self-reporting layer where that distortion lives. A patch is either applied or it isn't, and a backup job either succeeded or it failed. This edition extends that principle to the index's own history. Where Q2 instrumentation produced a harder number than the Q1 roll-up, the harder number is reported.

> "The uncomfortable part of instrumenting everything is that the numbers get worse before they get better," said Ben Silver, Chief Operating Officer. "A device-level patch assessment will always read lower than a policy roll-up. We publish the stricter number because that's the one an attacker interacts with."

2d. Limitations & Assumptions

Internal data reflects a managed client base, which skews toward organizations that have already invested in structured IT support. Results should not be generalized to all U.S. SMBs without this caveat. External benchmarks vary in methodology, sample size, and geography, and several widely circulated SMB statistics could not be traced to primary sources during this edition's verification pass; those figures have been retired or re-attributed rather than repeated (see Appendix 8c).

Service-level agreement (SLA) compliance remains the one help desk metric not yet reportable: the current ticketing exports preserve a live SLA status but not the original per-ticket SLA target alongside actual close time, so a true met/breached rate cannot yet be computed. The reporting capability is being built and SLA compliance is planned for the Q3 edition. Consistent with this index's practice, the gap is stated rather than estimated around.

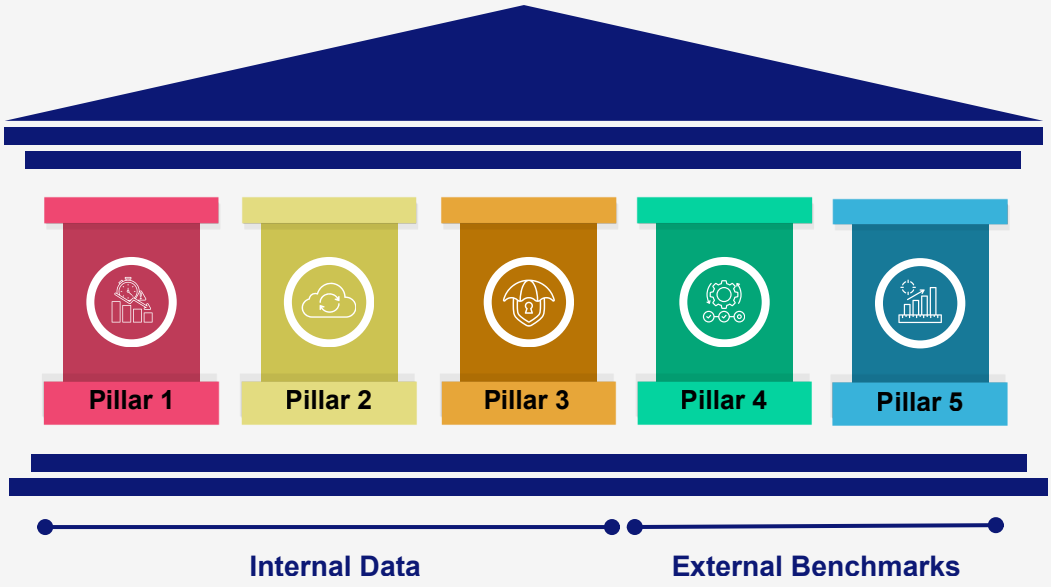
3. Index Overview: How the Scoring Framework Works

The index is structured around five fixed pillars, each measuring a distinct dimension of SMB technology and cyber resilience. The pillars do not change between editions; the instrumentation behind them improves.

- **Pillar 1: Availability & Downtime** measures the frequency, duration, and recovery speed of unplanned IT outages.
- **Pillar 2: Backup & Disaster Recovery Readiness** assesses backup automation, offsite and immutable coverage, restore testing frequency, and the presence of documented recovery objectives.
- **Pillar 3: Cyber Resilience** evaluates multi-factor authentication adoption, endpoint protection coverage, verified incident volume, and patch management compliance.
- **Pillar 4: Operational Maturity** examines patching enforcement, help desk responsiveness, automation, and IT service standardization. Beginning this edition, it includes full service-desk metrics.
- **Pillar 5: Financial Impact** models the cost of downtime and cyber risk exposure based on internal operational metrics and published industry cost benchmarks.

Pillar Framework

How the Index Measures SMB Resilience



Pillar 1

Availability & Downtime

- Outage frequency
- Outage duration
- MTTR

Pillar 2

Backup & Disaster Recovery Readiness

- Backup automation
- Offsite replication
- Restore testing
- RPO/RTO documentation

Pillar 3

Cyber Resilience

- MFA adoption
- EDR/MDR coverage
- Patch compliance
- Threat blocking

Pillar 4

Operational Maturity

- Patch enforcement
- Automation
- IT standardization
- Help desk (future metric)

Pillar 5

Financial Impact

- Downtime cost modeling
- Risk exposure
- Cost reduction vs industry

4. Pillar-by-Pillar Analysis

4a. Availability & Downtime

Industry Benchmark

Infrastructure is getting more reliable while the outages that remain grow more expensive. The Uptime Institute's 2026 Annual Outage Analysis, published in May, found per-site outage rates declining for a fifth consecutive year, yet 57% of organizations in the same study reported that their most recent major outage cost over $100,000, and one in five put the figure above $1 million for the second straight year.

Expectations continue to climb faster than delivery. ITIC's 2025 Global Server Hardware and Server OS Reliability Report (published February 2026) found 96% of midsized and large enterprises now require at least 99.99% uptime, no more than 52 minutes of downtime a year. Yet ITIC's 2024 downtime research found 60% of businesses cannot accurately calculate their own hourly downtime cost. Most of the market holds IT to a standard it has never priced.

Semperis' 2025 ransomware study found only 23% of victims recovered within a day, down from 39% the year before, with the share needing a week to a month rising from 11% to 18%.

Internal Benchmark

Across the managed client base in Q2 2026, 499 unplanned outages were recorded across approximately 1,700 client organizations, an average of 0.29 outages per client per quarter, or roughly 1.17 per year. Average outage duration was 132 minutes. Mean time to recovery (MTTR) was also 132 minutes. All recorded outages occurred during business hours.

The Q1 edition reported this rate only as a portfolio average; the underlying counts are published from this edition forward.

The Delta

The outage rate is effectively unchanged from the prior reading of 0.294. One reading at a low outage rate can be luck; two consecutive readings at the same level, across roughly 1,700 organizations, make luck a less plausible explanation and a stable operating process a more plausible one.

The business-hours concentration repeated as well. All outages occurred during working hours, the pattern of hardware and software failing under active load rather than of cyber incidents, which disproportionately strike outside staffed hours. Semperis' holiday-risk research found 52% of ransomware attacks land on weekends or holidays, precisely when 78% of organizations cut security staffing by half or more. The absence of after-hours outages is consistent with failure-driven rather than cyber-initiated downtime; the detection workload that ran around the clock over the same period appears in Pillar 3.

Comparison with Prior Edition

Metric	Q4 2025 reading	Q2 2026 reading	Trend
Outages per client per quarter	0.294	0.29 (499 / ~1,700)	Stable
Average outage duration	132 minutes	132 minutes	Stable
MTTR	132 minutes	132 minutes	Stable
Outages during business hours	100%	100%	Stable

Quick Fact

The fastest quartile of intrusions reached data exfiltration in 72 minutes in 2025, down from nearly five hours a year earlier. The average SMB's recovery clock still runs in hours and days. (Palo Alto Networks Unit 42, 2026)

4b. Backup & Disaster Recovery Readiness

Industry Benchmark

Confidence in recovery is common; proven recovery is rare. Veeam's 2026 Data Trust and Resilience Report, the successor to its long-running Data Protection Trends series, found that 90% of security leaders believe they can recover quickly from an attack, yet only 69% say their recovery time objectives align with their business continuity goals, and only 28% of organizations hit by ransomware fully restored their data. Victims recovered an average of 72% of affected data; 44% recovered less than three-quarters of it.

Kaseya's most recent State of Backup and Recovery research found more than 60% of organizations believe they can recover from downtime within hours while only 35% actually can, and Backblaze's most recent survey (2024) found only 42% of organizations that performed a restore got all of their data back.

Attackers have organized around this weakness. Veeam's Ransomware Trends research found backup repositories targeted in 96% of ransomware attacks in its 2024 edition, with those attacks at least partially successful 76% of the time; its 2025 edition put targeting at 89% of attacks, with roughly a third of affected repositories modified or deleted. Despite this, the same 2025 research found only 32% of organizations use immutable backup repositories, the one architecture ransomware cannot encrypt, alter, or delete.

MSP360's 2025 survey of managed service providers adds a stark continuity dimension: nearly 88% of MSP client organizations could stay operational for less than a week after a major disruption, and half could last only a single day.

Internal Benchmark

Within the managed client base, 71% of clients have automated backups, 60% have offsite or cloud replication, and 11% have immutable backups. Five percent have documented RPO and RTO targets, and 5% have conducted a tested restore within the last 90 days. Every one of these figures is unchanged from the prior edition.

> "Backup remains the pillar where SMB confidence and operational reality diverge most sharply," said Katie Kelly, Director of Integration Services. "Within our managed client base, 71% of clients have automated backups and 60% replicate offsite or to cloud, yet only 5% have documented RPO/RTO targets and just 5% have tested a restore in the last

> 90 days, a gap that mirrors the broader industry data, where nine in ten security leaders say they can recover and barely more than a quarter of ransomware victims actually restore in full. The risk profile is intensifying: with the overwhelming majority of ransomware attacks now targeting backup repositories, and roughly a third of targeted repositories altered or deleted, unverified backups are no longer a passive gap. They are the primary attack surface. This is why centralized backup monitoring has moved from a nice-to-have to a core resilience control. A scheduled job that reports 'success' is not the same as a recoverable backup; without continuous, independent monitoring (the direction Corporate Technologies is moving with its Backup Monitoring solution, to centralize visibility and accountability across the client base), silent failures, broken chains, and tampered repositories remain invisible until the moment of recovery, when it is too late. Monitoring transforms backup from a logged activity into a measured, verifiable outcome, closing the RPO gap this index identified last quarter as the place where the real risk hides."

The Delta

Automation and replication remain well above industry norms. The 71% automated backup coverage is more than double the ~30% full-automation rate industry surveys have reported (as cited in the Q1 edition), and 60% offsite coverage leads published SMB adoption figures. The strong half of this pillar held.

So did the weak half, and that is the more important result. The Q1 edition identified 5% RPO/RTO documentation and 5% tested restores as the single widest gap in the index; six months on, both figures are identical. Nothing about stable operations naturally produces recovery documentation. No outage forces a client to write down how much data loss is acceptable, and no successful backup job prompts anyone to test a restore. The gap does not close passively, in a managed environment or anywhere else; it closes when testing and documentation become a scheduled, monitored obligation.

Between the 2024 and 2026 research cycles, full-restore rates after ransomware fell to 28%, same-day recovery nearly halved, and repository-targeting became standard attacker practice, while immutable backup adoption industry-wide sits at 32%, and at 11% within this client base. The gap has not widened on paper, but the cost of falling into it has.

Comparison with Prior Edition

Metric	Q4 2025 reading	Q2 2026 reading	Trend
Automated backups	71%	71%	Stable
Offsite/cloud replication	60%	60%	Stable
Immutable backups	11%	11%	Stable
Documented RPO/RTO	5%	5%	Unchanged; widest gap in the index
Tested restores (last 90 days)	5%	5%	Unchanged; widest gap in the index

Quick Fact

Only 28% of organizations hit by ransomware fully restored their data, even though 90% of security leaders were confident they could recover. Organizations that increased their cyber budgets achieved full recovery 40% of the time versus 16% for those that didn't. (Veeam, 2026)

4c. Cyber Resilience

Industry Benchmark

The way into an SMB is now a login, not a payload. Sophos' State of Ransomware 2026, published in July, found that 79% of ransomware attacks originate from compromised identities. The Verizon 2026 Data Breach Investigations Report found 73% of ransomware victims had suffered a prior credential compromise, half of them within 95 days of the ransomware event: a window in which detection could have prevented the attack. And in a finding that should end the "too small to be targeted" argument permanently, the 2026 DBIR reports that where victim size was known, 96% of ransomware victims were small and mid-sized businesses. Ransomware itself rose to 48% of all breaches, from 44% the year before.

The size penalty now shows up at the response stage as well. Sophos found only 34% of small organizations (100–250 employees) stopped ransomware attacks before encryption or extortion, against 46% of organizations with several thousand employees, and encryption success rates industry-wide climbed to 56%, from 50%.

Published SMB multi-factor authentication adoption remains in the 34–40% range (JumpCloud puts it at 34% for firms of 26–100 employees), while Microsoft's guidance continues to note that more than 99.9% of compromised accounts lacked MFA. Yet Sophos' 2026 research found 97% of victim organizations with compromised credentials had MFA enabled in some form; the compromised account simply sat outside it, on an uncovered VPN, admin console, or legacy application. Adoption is necessary; coverage is what protects. On the patching side, the 2026 DBIR found exploitation of unpatched vulnerabilities is now the single most common way breaches begin, at 31% of all breaches. That is a different population from Sophos' ransomware-specific figure, but the same picture. Attackers enter through exposed identities and unpatched edges rather than malware alone.

Internal Benchmark

This edition reports the security workload from quarter-scoped platform instrumentation for the first time, as a detection funnel rather than a single count:

Detection funnel, Q2 2026 (Apr 1 – Jun 30)	Volume
Events analyzed (all modules)	9.19 billion, across 47,482 monitored entities
Signals detected	127,016
Manually investigated	892
Verified incidents	215 (134 critical, 28 high, 53 low)
Incidents resolved by quarter end	210 of 215
Ransomware detonations	0 detected (278,476 canary files across 13,379 endpoints; none triggered)

Of the 215 verified incidents, 126 (59%) originated in identity systems (Microsoft 365 identity detection and response) versus 89 on endpoints, the client base's own data echoing the industry's identity-first shift, though the populations differ: this figure covers all verified incidents, while Sophos' 79% describes the initial access vector of ransomware attacks specifically. Automated antivirus additionally blocked 5,298 malware files, and 77,464 persistence-mechanism signals were screened during the quarter.

MFA adoption across the managed client base stands at 63%. Endpoint protection coverage, measured by the security platform as agents deployed and reporting across managed endpoints, is 98.6% (31,874 of 32,313 endpoints; 439 unprotected). Patch compliance under the new strict standard appears in Pillar 4; firewall (99%) and M365/SaaS (100%) compliance are unchanged.

The Delta

In ninety days, the attack surface of roughly 1,700 small and mid-sized businesses absorbed 9.19 billion analyzed events and 127,016 threat signals; the "too small to be targeted" misconception does not survive those numbers. Nearly all of it was handled automatically; 215 incidents were real enough to verify, 134 of them critical, and none became a ransomware event. Set against a backdrop where 96% of identified ransomware victims are SMBs, a zero-detonation quarter is not the absence of targeting. It is targeting, absorbed.

Fifty-nine percent of verified incidents began in the identity layer, not on devices, the same pattern Sophos found industry-wide. The managed client base's 63% MFA adoption is roughly 1.7 times the published SMB rate, and this quarter's incident distribution shows the exposure that remains. The 37% of users without MFA, and the covered users whose VPNs and legacy applications sit outside it, are the surface the identity-led incident pattern points at. MFA coverage, not MFA adoption, is becoming the metric that matters, and it is a natural candidate for future instrumentation in this index.

As set out in Section 2b, the 215 verified incidents replace the prior edition's 379 escalations without implying a 43% improvement. And endpoint protection was previously reported at 53% under a narrower definition (EDR/MDR product coverage); the platform's deployment measure (98.6% of managed endpoints protected and reporting) is the figure this index will carry forward, and the remaining 439 unprotected endpoints are an identified, finite remediation list rather than an unknown.

Comparison with Prior Edition

Metric	Q4 2025 reading	Q2 2026 reading	Trend
MFA adoption	63%	63%	Stable; 37% residual exposure
Verified security incidents	379 (legacy escalation count)	215 (Huntress-verified)	Not comparable; measurement changed
Ransomware outcome	12,977 blocked attempts (legacy count)	Full funnel; 0 detonations	Measurement changed; outcome unambiguous
Endpoint protection	53% (EDR/MDR product definition)	98.6% (platform deployment measure)	Not comparable; definition changed
Firewall / M365 patch compliance	99% / 100%	99% / 100%	Stable

Quick Fact

79% of ransomware attacks now originate from compromised identities, and 59% of this quarter's verified incidents across the managed client base began in the identity layer, not on endpoints. (Sophos State of Ransomware 2026 / internal data)

4d. Operational Maturity

Industry Benchmark

The Freshservice 2025 Service Management Benchmark, drawn from 187 million tickets across 10,551 organizations, reports an average resolution time of 21.96 hours, first-contact resolution of 74.14%, and resolution SLA adherence of 96.16%. It is also the first benchmark cycle in which AI assistance shows up as a measured operational variable rather than a promise. Organizations using AI copilots resolved tickets 76.6% faster, and AI agents deflected 65.7% of tickets outright.

Adaptiva's State of Patch Management 2026 found 59% of organizations now deploy patches within six days, up from just 15% in 2023: a fourfold improvement that retires the long-standing "77% take more than a week" statistic this index cited last quarter. The improvement is real but shallow. Over 60% of organizations still rely on manual processes somewhere in the patch lifecycle, only 8% have fully autonomous patching, and only 49% include third-party applications in patching workflows even though 74% experience third-party vulnerabilities. Deployment speed improved; coverage discipline did not.

The structural constraints tightened, too, with U.S. cybersecurity job openings rising roughly 57,000 year-over-year to 514,359 (CyberSeek, June 2025), and commonly cited benchmarks still put the small-business IT staffing ratio around 1:18. Process maturity remains uneven, with 52% of SMBs managing privileged access manually via spreadsheets or shared vaults (Devolutions), roughly a third maintaining a formal incident response plan, and only 47% of businesses under 50 employees reporting any security plan at all (CrowdStrike). In Guardz's research, 80% of SMBs with a formal incident response plan avoided major damage from attacks.

Internal Benchmark

The Q1 edition committed to delivering help desk metrics in Q2. They follow.

Ticket volume and delivery. 99,545 tickets were logged in the calendar quarter (April 1 – June 30), spanning all ticket types: end-user requests alongside automated monitoring, network, and security alerts. 99,455 of these carry priority classifications and form the basis of the resolution-time analysis below; the remaining 90 were child tickets that inherit their parent ticket's priority rather than carrying one of their own. 93.3% were resolved remotely; 6.7% required onsite support.

Resolution time. Mean time to resolution was 39.0 hours; the median was 25 minutes. The gap between those figures reflects what a managed service desk actually processes. Roughly two-thirds of tickets are machine-generated monitoring and security alerts that auto-resolve quickly and pull the median down to minutes, while a smaller population of complex, project-adjacent, and onsite issues runs for days and pulls the mean up. By priority:

Priority	Tickets	Avg resolution (hours)	Avg resolution (days)
P1 (critical)	11,228	8.5	0.35
P2	61,261	11.4	0.48
P3	26,868	114.3	4.76
P4	98	141.1	5.88
Total (priority-classified) / weighted avg	99,455	39	1.63

Application control responsiveness. The quarter's application-control logs (ThreatLocker) record approximately 3,831 software-approval requests actioned across 369 client organizations, with a median turnaround of 11 minutes, a useful independent check on responsiveness, measured by a different system than the ticketing platform.

Patch enforcement. Under the strict device-level standard adopted this edition (every applicable patch current), desktop compliance is 65.3% and server compliance 86.3%; against policy thresholds, 90% and 95% respectively. Firewall compliance is 99% and M365/SaaS 100%. The strict desktop figure, in particular, is the kind of number a legacy roll-up hides and honest instrumentation exposes, largely reflecting the constant arrival of new patches against week-scale deployment windows.

SLA compliance cannot yet be computed from the available exports, which preserve live SLA status but not the original per-ticket target. It is planned for Q3 (see Section 2d).

The Delta

Against the Freshservice benchmark's 21.96-hour cross-industry average, the like-for-like figure is the blended 39.0-hour mean, and on that comparison the managed desk reads slower. The composition explains why. The internal figure spans every automated monitoring and security alert alongside human-initiated requests, including a long tail of scheduled, multi-visit, and after-hours work. The priority breakdown is the more informative read (critical issues resolved in an average of 8.5 hours, P2 issues in 11.4), and the 11-minute median on application-control approvals points the same direction. When something is urgent, the response is fast. Both readings are reported; neither is curated away.

Q1 reported 94% endpoint compliance and called patch enforcement the strongest operational metric in the index. Under this edition's stricter device-level standard, desktop compliance reads 65.3%, a less flattering number and a more useful one, because it measures the standard an attacker actually tests. The available industry comparators measure different things (Adaptiva's figures track organization-level deployment speed, not device-level full compliance), so no direct delta is claimed. What the new measure provides is a baseline that cannot flatter, and from Q3, a trendline.

> *(Sales leadership field observations, Q2)* Discovery conversations with prospective clients this quarter repeatedly surfaced the operational absences this index measures: missing documentation, unknown system inventories, and no regular reporting from incumbent providers. The clearest shift in buyer priorities is that cybersecurity has moved from a want to a need, driven substantially by insurance carriers requiring specific controls and backup practices as conditions of coverage.

Comparison with Prior Edition

Metric	Q4 2025 reading	Q2 2026 reading	Trend
Patch enforcement (endpoints)	94% (legacy measure)	65.3% strict / 90% policy	Not comparable; stricter standard adopted
Patch enforcement (servers)	99% (legacy measure)	86.3% strict / 95% policy	Not comparable; stricter standard adopted
Firewalls / M365	99% / 100%	99% / 100%	Stable
Help desk metrics	Not yet available	Full quarter reported	Delivered as committed
SLA compliance	Not yet available	Not yet available; tooling in progress	Q3 commitment

Quick Fact

Organizations using AI copilots on their service desks resolved tickets 76.6% faster, and AI agents deflected 65.7% of tickets before they reached a human. The first benchmark cycle where AI shows up in the operational data, not the marketing. (Freshservice Service Management Benchmark, 2025)

4e. Financial Impact

Industry Benchmark

The ransom got cheaper this cycle and everything else got more expensive. Sophos' 2026 research puts the median ransom demand at $698,000, down roughly 65% over two years, and the median payment at $769,000, down from $1 million. (The payment median is computed only among organizations that paid, a different and typically larger-incident population than all demand recipients, which is why it can sit above the demand median.) Average recovery cost moved the other direction, rising 11% to $1.7 million per incident. The transaction is shrinking; the disruption is not. NetDiligence's most recent claims study (10,402 claims analyzed) reinforces the divergence from the insurance side. Average SME incident cost rose almost 30% year-over-year to $264,000, even as large-company average costs fell 19%, and insurance covered 69% of SME incident costs versus 27% for large firms.

The Calyptix/ITIC 2025 SMB survey (715 SMB respondents) found the most common hourly downtime cost band for small businesses is $1,000–$5,000, with 8% exceeding $25,000 per hour. That distribution argues for modeling downtime as a range anchored to a firm's own revenue and payroll, exactly as this index's methodology does, rather than quoting headline averages drawn from enterprise samples.

The insurance market turned decisively in buyers' favor. Marsh's global index recorded a twelfth consecutive quarterly decline in cyber insurance rates (down 4% globally in Q2 2026), and NAIC data shows U.S. cyber premium volume fell for the first time on record in 2024, while small-business premiums average roughly $1,552 per year (Insureon, April 2026). Carriers are competing on price but underwriting on controls. MFA, backup verification, and endpoint protection are increasingly the price of admission rather than premium discounts.

Bluevine's most recent survey found 39% of U.S. SMBs hold less than one month of operating expenses in cash reserves, and Mastercard's global survey found nearly one in five SMBs that suffered a cyberattack subsequently filed for bankruptcy or closed. Set a $264,000 average incident against a reserve base measured in weeks, and the arithmetic explains the closures without needing embellishment.

Internal Benchmark (Modeled)

Applying the unchanged base scenario of $12,500 per hour to Q2 operational data, at 0.29 outages per quarter with an average duration of 132 minutes, a 50-employee client faces approximately 2.6 hours of downtime per year, or roughly $32,500 in modeled annual downtime cost at the base scenario, with a sensitivity range of approximately $19,500 (at $7,500/hour) to $52,000 (at $20,000/hour). An SMB experiencing the industry-average 14 hours of annual downtime (ITIC, 2024, the most recent edition to publish this figure) faces approximately $175,000 at the same base scenario.

Given the Calyptix/ITIC 2025 distribution, the $12,500 base scenario sits toward the upper end of measured SMB hourly costs; it reflects a 50-employee, $20 million-revenue firm with fully loaded compensation, and readers at smaller scale should apply the sensitivity floor rather than the base. The model's structure, assumptions, and guardrails are unchanged from Q1 and restated in Appendix 8b.

> "As Q2 closes, the financial takeaway is straightforward: many SMBs still underestimate the cost and operational risk of IT outages and cyber incidents," said Sam Mahn, Chief Financial Officer. "Too many owners still assume downtime will last only a few hours and create limited disruption. In reality, incidents can stretch into days, interrupt revenue, strain customer relationships, and create six-figure recovery costs."

The Delta

The modeled downtime-cost advantage held at roughly 80% against the industry-average scenario, a differential of approximately $142,500 per year, which continues to exceed the typical cost of managed IT coverage for a firm of this size.

The median ransom fell 65% over two years while recovery costs rose 11%; the dominant cost of an incident is now the disruption, not the payment. That is a cost curve resilience investment bends and a ransom negotiation does not. The insurance market's soft pricing points the same direction. Coverage is historically cheap for SMBs that can document their controls, and unreliable for those that cannot.

> "Heading into Q3, the message for SMB owners is simple: cyber resilience should be treated as a core operating discipline, not a discretionary technology project," Mahn said. "Quantify the true cost of downtime, test backup and recovery plans, and make sure resilience funding is built into the operating budget."

Comparison with Prior Edition

Metric	Q4 2025 reading	Q2 2026 reading	Trend
Modeled annual downtime cost (50-employee base)	~$32,500	~$32,500	Stable; tracks stable outage data
Industry comparison scenario	~$175,000	~$175,000 (2024 baseline, labeled)	Stable
Median ransom payment (industry)	~$1M (2025 research)	$769,000 (Sophos 2026)	Falling
Average recovery cost (industry)	$1.53M (2025 research)	$1.7M (Sophos 2026)	Rising; up 11%
Cyber insurance rates (US)	Declining	Twelfth consecutive quarterly decline	Buyer's market, controls-gated

Quick Fact

39% of U.S. small businesses hold less than one month of operating expenses in reserve. The average SME cyber incident now costs $264,000. The gap between those two numbers is the quiet driver behind one in five attacked SMBs closing or filing for bankruptcy. (Bluevine 2025 / NetDiligence 2025 / Mastercard 2025)

5. Key Findings & Trends

Five cross-cutting patterns emerge from the second edition of this index

1. Better measurement changed the numbers more than the threat did.

The most instructive deltas in this edition are definitional. A device-level patch assessment reads 65.3% where a legacy roll-up read 94%. A quarter-scoped detection pipeline verifies 215 incidents where an escalation count logged 379. There is no evidence the environment changed that much in six months; the instruments demonstrably did. The practical lesson for SMB leaders is to ask, of every reassuring metric an IT provider reports, what standard it is measured against.

> "We publish this index because the SMB market runs on confident claims and thin evidence," said Ugur Gulaydin, VP of Marketing at Corporate Technologies. "Our job isn't to market past that noise. It's to put real operational data in front of business owners, including the numbers that don't flatter us, and give them a benchmark they can trust and act on."

2. Identity has replaced the endpoint as the front door.

Sophos found 79% of ransomware attacks now originate from compromised identities; Verizon found 73% of ransomware victims had a prior credential compromise, half within a 95-day window where detection was possible. The internal data points the same direction, with 59% of this quarter's verified incidents beginning in the identity layer. Coverage, not adoption, is becoming the MFA metric that matters; most breach victims had MFA somewhere, just not everywhere.

3. The recovery gap is structural, and it does not close on its own.

Two consecutive editions show RPO/RTO documentation and tested restores at 5%, unmoved through six months of otherwise stable operations. Nothing in day-to-day IT operations naturally generates recovery discipline; no successful backup job prompts a restore test. Meanwhile full recovery after ransomware fell to 28% industry-wide, and same-day recovery nearly halved.

4. The economics of an incident inverted.

Median ransom demands fell 65% in two years while average recovery costs rose 11% to $1.7 million, and SME claim costs rose 30% while large-company costs fell. At the same time, cyber insurance entered its twelfth consecutive quarter of rate declines, making coverage historically affordable for SMBs that can document their controls. The rational response is the one this edition's CFO commentary prescribes: fund resilience as an operating discipline and insure the tail.

5. Stability is an outcome, not an accident.

The client base's outage rate held at 0.29 per client per quarter across two editions, roughly a fifth of the industry-average annual downtime, while absorbing 9.19 billion analyzed security events and ending the quarter with no detected ransomware detonations. In the same period, industry research recorded declining per-site outages globally but sharply slower ransomware recovery and faster attacker timelines. The pattern across the pillars is consistent. Where a discipline is instrumented, enforced, and monitored (backup automation, threat detection, response speed), outcomes hold; where it depends on episodic human attention (recovery documentation, restore testing, MFA completion), it stalls.

> "The reliance on technology for SMB success is only going to increase, and consumer expectations have already gone 24/7," said Jim Griffith, CEO of Corporate Technologies. "A service issue that could wait until tomorrow morning a decade ago now costs you the customer tonight. Choosing an IT partner with the scale, redundancy, and operational discipline to deliver around the clock is becoming a differentiator, not a luxury."

6. What “Good” Looks Like for SMBs

Resilience is not binary. There is no single threshold that separates a protected business from an exposed one, and the appropriate target depends on industry, regulatory environment, and risk tolerance. A 15-person marketing agency and a 120-person medical device manufacturer face different threat profiles and operate under different compliance obligations.

The three-tier maturity framework introduced in the first edition is unchanged, deliberately, because a stable yardstick is what makes quarter-over-quarter movement measurable. What has changed is the evidence behind it, with each tier's defining practices now mapping to a quarter of internal operational data and a fresh research cycle.

Tier 1: Baseline (Survive an Incident)

At a minimum, an SMB should be able to absorb a disruption without losing critical data or facing an open-ended recovery timeline. That starts with automated backups on a defined schedule with offsite replication, not a manual process that depends on someone remembering to run it. MFA should be enabled on all business-critical systems and email; the 63% adoption across the managed client base leads the industry average but remains short of full coverage. Patching should be deployed within 30 days of release for operating systems and core applications, a standard most of the industry now clears, with 59% of organizations deploying within six days (Adaptiva, 2026).

A basic incident response plan should exist in writing, with contact information and initial response steps defined; 80% of SMBs with a formal plan avoided major damage from attacks. And a cyber insurance policy should be in place with coverage validated against the organization's actual security posture, at a moment when a soft market makes coverage historically affordable and carriers underwrite on documented controls.

This tier makes an organization recoverable, not yet resilient.

Tier 2: Structured (Recover Predictably)

The difference between Tier 1 and Tier 2 is the difference between having tools and having a process. At this level, RPO and RTO targets are formally documented for all business-critical systems, and restore procedures are tested at least quarterly, not assumed to work because a backup job reported success. The distinction matters more than ever. With backup repositories targeted in roughly nine of ten ransomware attacks, an untested backup is an assumption dressed as a control.

EDR or MDR runs across all endpoints with 24/7 monitoring, defined escalation paths, and response SLAs that are tracked and reported. Help desk performance is measured against concrete metrics: ticket resolution time by priority, remote-versus-onsite split, and (as instrumentation matures) SLA compliance. Privileged access is managed through a centralized system rather than the spreadsheets and shared vaults that 52% of SMBs still rely on.

Organizations at Tier 2 can predict their recovery timeline with reasonable accuracy. When an incident occurs, they know what they are recovering, how long it will take, and who is responsible for each step.

Tier 3: Resilient (Withstand and Adapt)

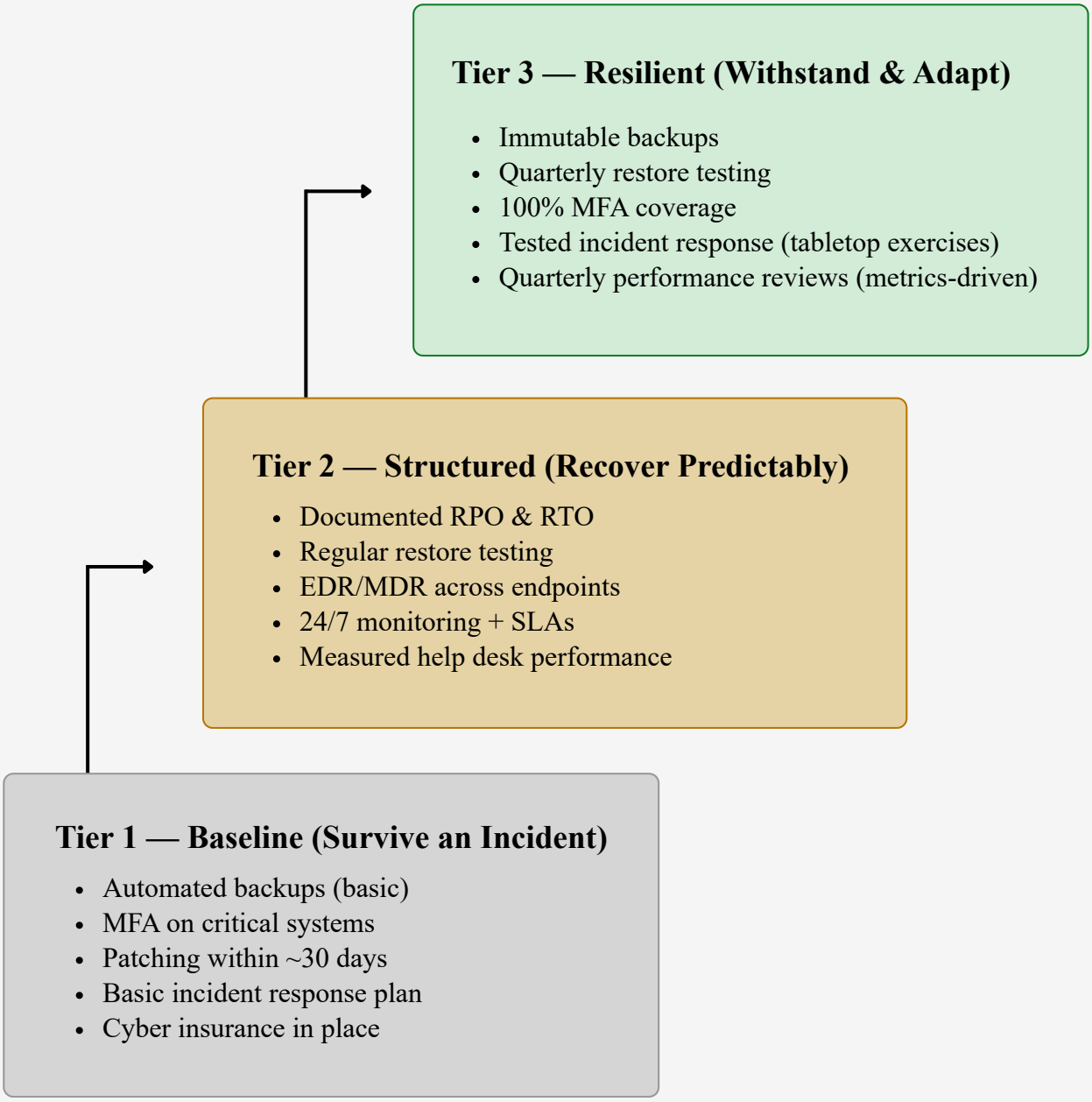
Tier 3 organizations treat resilience as an operational discipline, not a project. Backups are immutable, meaning ransomware cannot encrypt, alter, or delete them, and restore testing is conducted quarterly with results documented. Industry-wide, only 32% of organizations have immutable repositories; within this index's client base the figure is 11%. This is the control with the largest gap between its importance and its adoption, everywhere.

MFA coverage reaches 100% of users and systems, including the VPNs, admin consoles, and legacy applications where the 2026 research shows partially-covered organizations get breached. The incident response plan is tested annually through tabletop exercises simulating realistic scenarios: ransomware, data exfiltration, extended outages, and, given that half of ransomware attacks now land on weekends and holidays, off-hours response. Cyber insurance compliance is actively maintained, with MFA, encryption, and backup documentation verified against insurer requirements.

At this level, IT performance is reviewed quarterly with the managed service provider using index-level metrics and trend data, and written security policies are reviewed annually against NIST CSF or an equivalent framework. The organization measures its own defenses and improves them systematically.

Most SMBs in this index operate between Tier 1 and Tier 2. The internal data shows strong performance on automation, detection, and response speed, but persistent gaps in recovery documentation, immutable backup coverage, and universal MFA deployment. Closing those gaps is the path from Tier 1 to Tier 3, and with two editions of trend data now in hand it is measurable quarter over quarter.

SMB Maturity Model
From Survival to Resilience



7. Practical Recommendations by Maturity Level

The data in this index continues to point to a consistent pattern. The largest gaps in SMB resilience aren't exotic or expensive to close; they're foundational: documented recovery objectives, tested restores, MFA on every system, and monthly reporting from IT providers. The 90-day action plan below is unchanged in structure from the first edition, because the gaps it addresses did not move. The emphasis within it has been updated to reflect this quarter's data.

Days 0–30: Close the Critical Gaps

The first 30 days are about visibility. Most SMBs do not have an accurate picture of what's actually protected, what's actually patched, and what would actually happen if a critical system went offline tomorrow.

Start with MFA, audited as a coverage problem, not a yes/no question. List every system that touches sensitive data, email, financial applications, and remote access, and identify which sit outside MFA enforcement. VPNs, admin consoles, and legacy applications are where the 2026 breach research says the gaps live. The target is 100% of users and 100% of systems.

Move to backups. Verify that automated backups are running on a defined schedule and confirm that offsite or cloud replication is active. Don't assume; check. Then document recovery objectives, with RPO and RTO targets in writing for every business-critical system. Two editions of this index have now found documented recovery objectives at 5%; even rough initial targets ("we can tolerate four hours of data loss," "billing needs to be back within six hours") are materially better than the undocumented assumptions that 95% of even this managed client base is running on.

> "Even rough initial targets are better than undocumented assumptions," said Katie Kelly in the Q1 2026 edition. "The act of defining what's acceptable, how much data you can afford to lose and how quickly systems need to come back, forces a conversation most SMBs have never had."

Key actions:

- Audit MFA coverage across all systems, including VPN, admin, and legacy applications; target 100%.
- Verify automated backup status and offsite replication.
- Document RPO and RTO targets for all business-critical systems, even as rough estimates.
- Request a monthly operational report from the IT provider showing actual patch, backup, and monitoring activity, and ask what compliance standard the patch numbers are measured against.

Days 31–60: Build the Structure

With visibility established, the second phase tests assumptions. The industry data is unambiguous about why. More than 60% of organizations believe they can recover from downtime within hours; 35% actually can. Only 28% of ransomware victims fully restore their data. The only way to know which category an organization falls into is to test.

Execute a full restore from backup, not a file recovery but a system-level restore simulating an actual outage or ransomware scenario. Document time to recovery, data completeness, what failed, and what worked. Given that backup repositories are targeted in roughly nine of ten ransomware attacks, this is also the moment to evaluate whether current backups would survive an attack at all. That is the immutability question, and only about a third of organizations industry-wide can answer yes to it.

Draft or update a formal incident response plan with defined roles, escalation paths, communication procedures, and specific steps for the first hour, first four hours, and first 24 hours. The payoff is now quantified; 80% of SMBs with formal plans avoided major attack damage. A plan that exists only as a vague intention to "call IT" is not a plan.

Then review cyber insurance against actual security posture. The market is the softest it has been in three years, with rates down for twelve consecutive quarters, but carriers underwrite on documented controls. Verify that MFA documentation, backup verification records, and access-control evidence meet the insurer's specific requirements for claim eligibility, before an incident makes the question urgent.

Key actions:

- ✔ Execute a full system-level restore test and document results.
- ✔ Evaluate whether backups would survive a repository-targeting attack; price immutable storage.
- ✔ Draft or update a formal incident response plan with hour-by-hour procedures.
- ✔ Review cyber insurance coverage against documented controls while the market favors buyers.

Days 61–90: Verify and Sustain

The final phase shifts from building to sustaining. The most common failure mode in SMB resilience isn't the absence of a plan but the decay of one. Procedures go stale as staff turn over, and backup operations drift. The recurring measurement cadence is what prevents that decay; this quarter's data shows cadence-driven disciplines holding while episodic ones sat still.

Conduct a tabletop exercise simulating a ransomware incident, and schedule it for the scenario the attackers actually choose. Half of ransomware attacks land on weekends and holidays, when most organizations cut security coverage by half or more. Walk through who makes the isolation call at 2 a.m. on a Saturday, who contacts the insurance carrier, who communicates with clients, and how long the business can operate without its primary systems.

Establish a quarterly cadence for restore testing with documented results. A single successful test is a data point; a quarterly cadence is a trend, and documented test results double as the evidence insurers increasingly require.

For organizations working with a managed service provider, this is the moment to evaluate whether the provider has the scale and structure to deliver the outcomes documented in this index. The market includes providers of widely varying scale and operating models. The questions that separate scaled providers from undersized ones are straightforward: How many employees does the MSP have? Is there actual staffing across all 168 hours per week? Are there dedicated teams for help desk, monitoring, project work, and technology roadmap services? What operational metrics does it report monthly, and measured against what standard?

Key actions:

- Conduct a tabletop exercise including an off-hours scenario.
- Establish quarterly restore testing with documented results.
- Benchmark the current environment against this index's pillar metrics.
- Evaluate MSP capability: headcount, real 24/7 staffing, dedicated functional teams, and measured reporting.

Self-Assessment: Can You Say Yes to All of the Following?

The following eight statements correspond to the foundational controls and processes measured across the five pillars of this index. They represent the minimum operational baseline that separates organizations with measurable resilience from those operating on assumptions.

- MFA is enabled on all systems accessing sensitive or financial data, including VPN, administrative, and legacy applications.
- Automated backups are running with offsite or cloud replication.
- RPO and RTO are documented for all business-critical systems.
- Backups have been tested with a full restore within the last 90 days.
- All endpoints, servers, and firewalls are patched within 30 days of release.
- A formal incident response plan exists and has been reviewed within the last 12 months.
- Cyber insurance is in place with coverage validated against current security controls.
- The IT provider delivers monthly reports showing what was patched, backed up, monitored, and resolved.

If fewer than six of these statements are true, the organization is carrying materially more operational and financial risk than its leadership likely recognizes. The data in this index continues to suggest that for most small businesses, the distance between "we think we're covered" and "we actually are" is measured in hundreds of thousands of dollars.

> "Small and midsize businesses are operating in an environment where technology is no longer just an enabler; it is fundamental to business resilience and long-term growth," said Justin Stansbury, VP of Sales. "As threats become more sophisticated and IT environments grow more complex, operational resilience must become a leadership priority rather than solely an IT responsibility. Organizations that invest in proactive cybersecurity, business continuity planning, and strategic technology management are significantly better positioned to minimize disruption, maintain customer trust, and adapt to changing demands. The most successful SMBs will be those that treat technology not as a cost center, but as a strategic asset."

8. Appendix

8a. Definitions

RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time. An RPO of 4 hours means the organization can tolerate losing up to 4 hours of data.

RTO (Recovery Time Objective): The maximum acceptable time to restore a system or application after a failure. An RTO of 2 hours means the system must be back online within 2 hours.

MTTR (Mean Time to Recovery): The average time required to restore normal operations after an unplanned outage.

MFA (Multi-Factor Authentication): A security method requiring two or more verification factors to access a system, such as a password plus a mobile authenticator code.

EDR (Endpoint Detection and Response): Security software installed on individual devices that continuously monitors for and responds to cyber threats.

MDR (Managed Detection and Response): A service that combines EDR technology with human security analysts who monitor, investigate, and respond to threats on behalf of the organization.

ITDR (Identity Threat Detection and Response): Monitoring and response tooling focused on identity systems (login activity, account configuration, and privilege changes) rather than devices. The source of 59% of this quarter's verified incidents.

Ransomware canary file: A decoy file planted on protected endpoints and monitored continuously; encryption or modification of a canary file provides early, high-confidence detection that ransomware is executing.

Immutable Backup: A backup that cannot be altered, encrypted, or deleted by anyone for a defined retention period.

8. Appendix

8a. Definitions

Strict patch compliance: The percentage of devices current on every applicable patch at the time of assessment. **Policy patch compliance:** The percentage of devices within the thresholds defined by patching policy (e.g., inside the allowed deployment window). This edition reports both.

MSP (Managed Service Provider): A third-party company that remotely manages a client's IT infrastructure and end-user systems on a proactive, subscription basis.

SOC (Security Operations Center): A centralized team or facility responsible for monitoring and responding to cybersecurity threats around the clock.

8b. Financial Modeling Assumptions

Pillar 5 cost estimates use the following methodology, unchanged from the Q1 2026 edition:

- Direct hourly downtime cost is calculated as: (annual revenue ÷ 2,080 working hours) + (average hourly compensation × number of employees).

Average hourly compensation is modeled at $60 per hour (within a modeled $45–$95 range), inclusive of wages, benefits, and overhead. For a 50-employee firm at $20 million in annual revenue, this yields a base scenario of approximately $12,500 per hour. Sensitivity analysis is applied at $7,500 per hour (lower bound) and $20,000 per hour (upper bound).

Annual downtime cost is the product of hourly cost, average outage duration, and annual outage frequency. SMB breach cost exposure is modeled in bands ($250,000–$1.5 million for minor to moderate incidents, $1.5 million–$5 million for major incidents), recognizing industry variation. Industry benchmarks for ransomware recovery, cyber insurance claims, and cash reserves are sourced from Sophos, NetDiligence, Bluevine, and Insureon as cited in the text.

The financial model's base scenario parameters, sensitivity ranges, and guardrails were validated by Sam Mahn, Chief Financial Officer, for the Q1 2026 edition; the model is applied unchanged in this edition. All downtime and breach cost figures are expressed as ranges with stated assumptions and shouldn't be interpreted as outcome guarantees.

8c. External Sources

Sources new to or updated in this edition are drawn from 2025–2026 publications; figures retained from earlier editions are labeled with their original year in the text. The list includes sources consulted during this edition's verification pass as well as those cited directly

- Verizon 2026 Data Breach Investigations Report
- Sophos State of Ransomware 2026
- Veeam Data Trust and Resilience Report 2026
- Veeam Ransomware Trends Report 2025 (and 2024 edition, where labeled)
- IBM Cost of a Data Breach Report 2025
- Semperis 2025 Ransomware Risk Report
- Semperis 2025 Ransomware Holiday Risk Report (coverage)
- Uptime Institute Annual Outage Analysis 2026
- ITIC 2025 Global Server Hardware and Server OS Reliability Report (published February 2026)
- Calyptix/ITIC 2025 SMB Security and Hourly Cost of Downtime Survey
- ITIC 2024 Hourly Cost of Downtime Survey (retained figures labeled 2024)
- Palo Alto Networks Unit 42 2026 Global Incident Response Report
- EMA Network Management Megatrends 2026
- Kaseya/Unitrends State of Backup and Recovery Report 2025
- Backblaze 2024 State of the Backup (with The Harris Poll)
- MSP360 State of Backup Report for MSPs 2025
- Keepit Annual Data Report 2026
- Infrascale RPO/RTO Statistics (U.S. technology-leader survey, 2025)
- Hiscox Cyber Readiness Report 2026
- CrowdStrike 2025 State of SMB Cybersecurity
- Devolutions State of IT Security in SMBs 2024–25
- Guardz 2025 SMB Cybersecurity Report
- JumpCloud MFA Statistics (2024 survey)
- Cyber Readiness Institute MFA research
- Microsoft Partner Center security documentation (MFA and account compromise)
- Adaptiva/Demand Metric State of Patch Management 2026
- Freshservice (Freshworks) Service Management Benchmark Report 2025
- SQM Group First Call Resolution Benchmarks (2022 study)
- CompTIA/Lightcast CyberSeek (June 2025 update)

8c. External Sources

- Mastercard 2025 Global SMB Cybersecurity Survey
- NetDiligence 2025 Cyber Claims Study
- NAIC 2025 Cyber Insurance Report
- Marsh Global Insurance Market Index / Cyber Insurance Market Update, Q2 2026
- Insureon Cyber Liability Insurance Cost Data (April 2026)
- Bluevine SMB Cash Flow Survey (2025)
- Gartner Market Guide for Managed Detection and Response (2023 and 2025 editions, as labeled; summary coverage)
- Industry MSP pricing surveys (2026)

Sources cited in the Q1 2026 edition and retired in this edition following verification review: the National Cyber Security Alliance's "60% of small companies close within six months" statistic (formally disavowed by the NCSA itself); the Dun & Bradstreet outage-frequency attribution; the "40% of cyber insurance claims denied / 82% of denials involve missing MFA documentation" claim cluster (no traceable primary source); and the "57% of SMBs report $100,000+/hour downtime costs" figure (not reproducible in ITIC's published materials; superseded by the Calyptix/ITIC 2025 SMB survey distribution).

8d. Disclaimers

Internal data reflects a managed client base and should not be generalized to all U.S. SMBs without acknowledging this selection effect.

Several metrics in this edition are reported from new, quarter-scoped instrumentation under definitions that differ from the prior edition's legacy roll-ups. Where a definition changed, this report identifies the change explicitly, and quarter-over-quarter comparisons for those metrics are marked "not comparable." Readers should not construct trendlines across a definitional break.

Financial impact estimates are modeled based on published industry benchmarks and internal operational data; they should not replace professional financial or actuarial analysis.

External benchmarks vary in methodology, sample composition, and geographic scope. Financial exposure estimates, including insurance claim averages and ransomware recovery costs, are jurisdiction-dependent and subject to individual policy terms. They are provided as modeled scenarios for planning purposes and shouldn't be interpreted as outcome guarantees.

Risk mitigation approaches referenced in this index align with NIST Cybersecurity Framework principles.

About Corporate Technologies

Corporate Technologies is a managed IT, cybersecurity, and cloud services provider supporting small and mid-sized businesses across the United States since 1981. Find your local team across our markets and locations.