April 07
gocorptech.com

CORPORATE TECHNOLOGIES

SMB Technology & Cyber Resilience Index

Q1 2026 Edition

Published by Corporate Technologies, Eden Prairie, MN

Table of Contents

Executive summary

Most small and mid-sized businesses believe they are resilient. Operational data tells a different story.

Industry research consistently shows a wide gap between perceived and actual IT readiness among U.S. SMBs. According to Devolutions' 2025 State of IT Security report, 71% of SMBs express confidence in their ability to handle a cyber incident, yet only 22% have a security posture advanced enough to withstand one. CrowdStrike's 2025 survey found that incident rates are nearly identical for SMBs with security plans (25%) and those without (24%), confirming that plans without execution offer no real protection.

This index is designed to close that gap in measurement, combining anonymized, aggregated operational data from a managed SMB client base with external industry benchmarks from more than 40 sources. Our quarterly benchmark measures what's actually happening inside SMB IT environments, not what business owners believe is happening.

> "Most SMBs don't lack awareness, but measurement," said Jim Griffith, CEO of Corporate Technologies. "This index exists to replace assumptions with ope_ rational evidence, and to give business owners a benchmark they can actually act on."
>
> Most SMB reports rely on self-reported surveys or tool-generated compliance stats," said Ugur Gulaydin, VP of Marketing, who commissioned the index. "They lack real-world performance context, such as actual downtime, actual restore success rates, and actual incident volumes. This index is designed to fill that gap with operational data that measures outcomes over intentions."

The five pillars of this index and their top-line findings:

1. Availability & Downtime

The managed client base experienced 0.294 outages per client per quarter (roughly 1.18 per year) compared to an industry average of approximately 5 per year. Average outage duration was 132 minutes, within the upper range of routine incidents but well below the 8-24 hour range typical of cyber-related outages. All recorded outages occurred during business hours, consistent with hardware and software failure patterns rather than cyber-initiated incidents.

2. Backup & Disaster Recovery Readiness

71% of clients have automated backups and 60% have offsite or cloud replication, both above industry averages. However, only 5% have documented recovery points and recovery time objectives, and only 5% have tested restores within the last 90 days. Industry benchmarks place RPO/RTO documentation at 25-35% and restore testing at 54% (ever tested). This is the single widest gap in the index.

3. Cyber Resilience

Multi-factor authentication adoption stands at 63%, nearly double the industry rate of 34-40% for SMBs. Endpoint detection and response coverage is 53%, above the estimated 25-40% industry range. Patch compliance rates of 94-100% across endpoints, servers, firewalls, and M365 stand in contrast to an industry where 60% of breaches trace to unpatched known vulnerabilities. In Q4 2025, 12,977 ransomware attempts were blocked across the client base.

4. Operational Maturity

Patch enforcement reached 100% across all categories. In an industry where 77% of organizations need more than a week to deploy patches, this level of enforcement reflects structured operational discipline. Help desk responsiveness metrics will be incorporated in future editions as internal measurement matures.

5. Financial Impact

Modeled downtime costs for the managed client base are approximately $32,500 per year for a 50-employee firm at the base scenario of $12,500 per hour, compared to $175,000 per year for SMBs experiencing the industry-average 14 hours of unplanned downtime (sensitivity range: $105,000-$280,000). The managed model reduces modeled downtime cost by approximately 80% at the base scenario.

Pillar	Internal Benchmark	Industry Benchmark	Delta
Availability & Downtime	~1.18 outages/year	~5 outages/year	~4x better
Backup & DR	71% automated backups / 5% tested restores	~30% / 54%	Mixed performance (strong automation, weak testing)
Cyber Resilience	MFA 63% / patching 94–100%	MFA 34–40% / patching ~60%	Above industry benchmark
Operational Maturity	100% patch enforcement	77% take >1 week	Significantly above industry benchmark
Financial Impact	~$32.5k/year downtime cost	~$175k/year	~80% lower cost

This is the first edition of a quarterly series. The value of the index compounds over time as quarter-over-quarter trend data accumulates, enabling SMB leadership teams to measure progress, identify emerging risks, and make investment decisions grounded in operational evidence rather than assumptions.

2. Methodology & Data Sources

2a. Data Period & Scope

Internal operational data covers Q4 2025 (October–December 2025) and is drawn from the full active SMB client base. All data is aggregated and anonymized, with metrics expressed as averages, percentages, or ranges across the entire managed portfolio.

External industry benchmarks are sourced from U.S.-focused research published between 2024 and 2026. Primary sources include:

- Verizon Data Breach Investigations Report,
- IBM Cost of a Data Breach Report,
- Sophos State of Ransomware,
- Kaseya/Unitrends State of Backup and Recovery,
- ITIC Hourly Cost of Downtime Survey,
- ConnectWise SMB Threat Report,
- Devolutions State of IT Security in SMBs,
- CrowdStrike State of SMB Cybersecurity,
- Semperis Ransomware Study,
- JumpCloud and the Cyber Readiness Institute MFA surveys,
- and others.

A full source list appears in the Appendix.

All internal operational metrics referenced in this report were reviewed and validated by Ben Silver, Chief Operating Officer, whose team is responsible for service delivery across the managed client base.

2b. How Internal and External Data Are Used

Internal data serves as the primary operational benchmark: what is actually happening inside managed SMB environments. External data provides industry context and comparison: what the broader SMB market reports or experiences.

Where internal data outperforms industry benchmarks, the gap reflects the measurable impact of structured managed services. Where it underperforms or matches, it reveals systemic gaps that persist even in well-supported environments. This index reports both without distinction.

2c. Why Operational Data Is More Reliable Than Surveys

The majority of existing SMB technology benchmarks rely on self-reported survey data. This creates a well-documented measurement problem known as social desirability bias: the tendency for respondents to overstate positive behaviors and understate vulnerabilities.

This bias systematically inflates reported security posture. SolarWinds, for example, found that 87% of businesses rate their cyber defenses as “average or better,” yet 71% had suffered at least one breach in the prior year. Sophos reported that 69% of ransomware victims believed they were well-prepared before being attacked.

> "No amount of tools matters if you don't measure real outcomes," said Jim Griffith, CEO. "SMBs are spending more on cybersecurity than ever, but spending and readiness are not the same thing. The only way to know whether your environment is actually protected is to look at what the systems are telling you.”

Operational data eliminates this distortion. Patch compliance is measured by automated timestamp, not self-assessment. Backup success or failure is logged, not recalled from memory. Uptime is tracked continuously, not estimated in a survey response. A patch is either applied or it isn’t. A backup either succeeded or it failed.

2d. Limitations & Assumptions

Internal data reflects a managed client base, which skews toward orga_ nizations 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.

Where possible, U.S.-specific data has been prioritized, such as financial impact figures in Pillar 5, which are modeled using published industry cost benchmarks applied to internal operational metrics. The modeling methodology is explained in that section. Help desk responsiveness metrics (average ticket resolution time, first-call resolution rate, SLA compliance) are not yet available for this edition and will be incorporated in Q2 2026 as internal measurement processes mature.

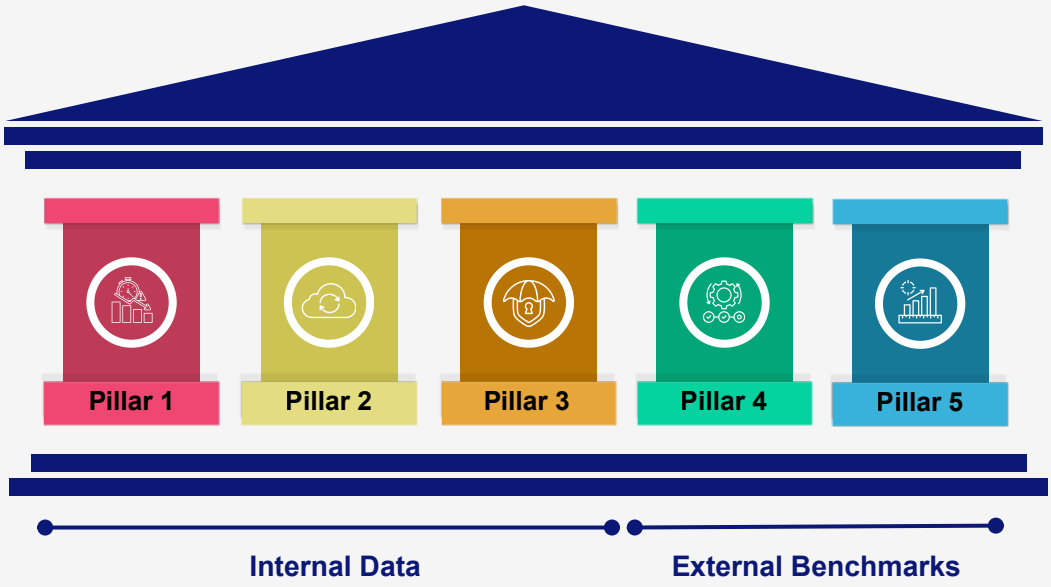
3. Index Overview: How the Scoring Framework Works

The index is structured around five fixed pillars, each measuring a distinct dimension of SMB technology and cyber resilience. Together, they provide a comprehensive view of operational readiness.

- **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, threat blocking activity, and patch management compliance.
- **Pillar 4: Operational Maturity** examines patching enforcement, help desk responsiveness, automation, and IT service standardization.
- **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

Unplanned IT downtime is one of the most consistent and least visible drains on SMB productivity and revenue. Dun & Bradstreet's long-running benchmark estimates that the average business experiences approximately 5 network outage events per year.

The ITIC 2024 Hourly Cost of Downtime Survey found that 90% of organizations now require a minimum of 99.99% uptime — meaning no more than 52 minutes of downtime per year — yet the average SMB delivers roughly 99.84%, or approximately 14 hours of unplanned downtime annually. The gap between expectation and reality is roughly tenfold.

Routine outages stemming from hardware failures, software glitches, and network issues typically last 30 minutes to 2 hours (EMA Research, 2024). Cyber-related incidents are far more severe: Semperis' 2025 study found that over half of ransomware-affected organizations remain offline for 8-24 hours, and 76% need more than a full day to return to normal operations.

Meanwhile, IBM reports that full operational recovery from a major cyber incident exceeds 100 days for 76% of organizations. Perhaps most revealing, ITIC found that 60% of businesses cannot accurately calculate their own hourly downtime cost, suggesting that the majority of SMBs lack even basic visibility into one of their most consequential financial exposures.

Internal Benchmark

Across the managed client base in Q4 2025, the average outage rate was 0.294 per client per quarter, or approximately 1.18 per year. The average outage duration was 132 minutes. Mean time to recovery (MTTR) was also 132 minutes. All recorded outages occurred during business hours.

> "The concentration of outages during business hours is consistent with what we see operationally," said Ben Silver, Chief Operating Officer. "Hardware and software failures tend to surface under active load. The fact that we're not seeing after-hours incidents is a direct reflection of 24/7 monitoring catching threats before they trigger outages."

The Delta

Outage frequency in the managed environment is roughly four times lower than the industry average. Duration falls within the upper range of routine incidents but well below the 8-24 hour range associated with cyber-related outages, suggesting that proactive monitoring and structured escalation are catching problems before they become catastrophic.

All recorded outages occurred during business hours, a pattern that's consistent with hardware and software failures surfacing under active system load. The threat blocking data in Pillar 3 (4c. Cyber Resilience), where 12,977 ransomware attempts were intercepted in Q4 2025 alone, addresses the attack landscape separately.

Metric	Internal Benchmark	Industry Benchmark
Outages per year	~1.18	~5.0
Average outage duration	132 minutes	30 min–2 hrs (routine); 8–24 hrs (cyber)
MTTR	132 minutes	Hours to days (Palo Alto Networks)
Outages during business hours	100%	~48% routine; 52% ransomware on weekends/holidays

Quick Fact

90% of organizations now require 99.99% uptime — under 52 minutes of downtime per year. The average SMB delivers roughly 14 hours. (ITIC, 2024)

4b. Backup & Disaster Recovery Readiness

Industry Benchmark

Backup and disaster recovery readiness among U.S. SMBs remains critically underdeveloped despite being the last line of defense against ransomware and data loss. Approximately 75% of small businesses operate without any documented disaster recovery plan. Among those with plans, Kaseya's 2025 report found that 60% of organizations believe they can recover from downtime within hours, but only 35% actually can.

Testing is widely neglected. Industry data indicates that 46% of small businesses have never tested their backup and disaster recovery plan. Only 15% test backups daily, and 25% test disaster recovery once per year or less (Kaseya/Unitrends, 2025). Backup job success rates average approximately 57%, and only 42% of organizations that experienced data loss were able to restore all their data (Backblaze, 2024).

Unfortunately, documentation of formal recovery objectives remains uncommon. Industry estimates place RPO/RTO documentation at 25-35% of SMBs, with one in six SMB executives unable to state their own recovery time objective (Infrascale).

Veeam's 2024 Data Protection Trends Report found that 76% of organizations have a gap between their backup frequency and their acceptable data loss threshold. Attackers have adapted accordingly, with ransomware now targeting backup repositories in 93-96% of incidents (Veeam, 2024), and only 10% of ransomware victims recover more than 90% of their data.

Internal Benchmark

Within the managed client base, 71% of clients have automated backups — well above the approximately 30% rate of full automation reported industry-wide, while 60% have offsite or cloud backup replication. 11% have immutable backups, and 5% have both documented RPO and RTO targets and conducted tested restores within the last 90 days.

> "The RPO gap is where the real risk hides," said Katie Kelly, Director of Integration Services. "Because only 5% of clients have a defined recovery point objective and many rely on daily or infrequent backups, organizations face a significant risk of losing a full day or more of business data when an incident occurs. Most don't discover that gap until they're in the middle of a crisis."

The Delta

There's an obvious split here because backup automation and off-site replication are strong relative to the industry. The 71% automation rate more than doubles the industry benchmark, and 60% offsite coverage exceeds the purpose-built cloud backup adoption rate of approximately 22-30% among self-managed SMBs.

However, the RPO/RTO documentation rate of 5% and the tested restore rate of 5% are the most significant gaps in the entire index. Both fall below the already-low industry benchmarks of 25-35% and 54%, respectively. This means that the vast majority of clients have backups running but lack documented targets for how quickly systems must be restored and how much data loss is acceptable. Without those targets, and without regular testing, a backup is an assumption, not a guarantee.

Kelly also identifies four false assumptions that consistently surface during onboarding and audits.

> "SMBs assume their backups cover all data, but they often don't. They assume all backups are equal, when immutable and mutable backups have fundamentally different survival rates against ransomware. They assume off-site replication is unnecessary. And they treat backup as synonymous with business continuity, which it is not without tested recovery procedures and documented objectives."

Metric	Internal Benchmark	Industry Benchmark
Automated backups	71%	~30% fully automated
Offsite/cloud backups	60%	22-30% (purpose-built)
Immutable backups	11%	35-45% (self-managed); 62% (MSP-managed)
Documented RPO/RTO	5%	25-35%
Tested restores (last 90 days)	5%	54% (ever tested)

Quick Fact

93–96% of ransomware attacks now target backup repositories. If backups are not immutable and regularly tested, they may not survive the incident they are designed to protect against. (Veeam, 2024)

4c. Cyber Resilience

Industry Benchmark

Cyber resilience among U.S. SMBs presents a structural paradox: attack volu_ mes continue to increase while adoption of foundational defenses remains low.

The Verizon 2025 Data Breach Investigations Report found that ransomware features in 88% of all SMB-related data breaches, compared to 39% for large enterprises. 47% of small businesses under $10 million in revenue were hit by ransomware in the past year (Sophos/ConnectWise, 2024), and over 66% of all ransomware attacks in 2024-2025 targeted businesses with fewer than 500 employees.

Multi-factor authentication (MFA) — the single most impactful foundational security control — has been adopted by only 34% of SMBs with 10-200 employees (JumpCloud, 2024; Cyber Readiness Institute, 2024). Microsoft's data is unambiguous, too, finding that 99.9% of compromised accounts did not have MFA enabled.

Endpoint detection and response (EDR) and managed detection and response (MDR) adoption are accelerating but remain limited. Gartner previously projected that 60% of organizations would use MDR services by the end of 2025, but CrowdStrike's survey indicates that SMBs still rely primarily on firewalls (91%) and traditional antivirus (70%). Estimated EDR/MDR penetration among U.S. SMBs in the 10-200 employee range is approximately 25-40%.

Patch management also remains a persistent vulnerability. Automox reports that 60% of breached organizations cite an unpatched known vulnerability as the root cause. 77% of organizations need more than a week to deploy patches (Adaptiva/Demand Metric, 2024), and 18% of SMBs skip critical software updates entirely (Flow Specialty, 2025). Only 34% of SMB owners have a formal incident response plan developed with professional assistance (Guardz, 2025). Cyber insurance adoption among the smallest businesses remains between 10% and 17%, and approximately 40% of claims filed are denied, with 82% of those denials involving organizations without proper MFA documentation.

Internal Benchmark

MFA adoption across the managed client base stands at 63%. EDR/MDR coverage is 53%. Patch compliance is 94% for endpoints, 99% for servers, 99% for firewalls, and 100% for M365 and core SaaS applications. In Q4 2025, 12,977 ransomware attempts were blocked. 379 security incidents required escalation.

The Delta

MFA and patching represent the most significant advantages of the managed environment. The 63% MFA adoption rate is approximately 1.7 times the industry average. Patch compliance at 94-100% is transformative when measured against an industry where 60% of breaches originate from unpatched vulnerabilities and 77% of organizations take more than a week to patch. The enforcement model — 100% patch enforcement across all categories — eliminates the most common ransomware entry vector for participating clients.

The 12,977 blocked ransomware attempts in a single quarter provide operational context for the Verizon DBIR's finding that 88% of SMB breaches involve ransomware. These are not theoretical threats, but active, persistent ones that are hitting even well-defended environments at scale. The 379 security escalations indicate that automated defenses catch the vast majority of attempts, but a meaningful volume still requires human analysis and response.

> "Nearly 13,000 blocked attempts in a single quarter should settle any debate about whether SMBs are being targeted," said Ben Silver, Chief Operating Officer. "These are not hypothetical risks. They are hitting the perimeter constantly."

Gaps remain, however. The 63% MFA rate, while strong relative to the industry, still leaves 37% of users without this foundational control. EDR/MDR at 53% means nearly half of endpoints lack advanced threat detection. These are areas where incremental improvements yield outsized risk reduction.

Metric	Internal Benchmark	Industry Benchmark
MFA adoption	63%	34–40%
EDR/MDR coverage	53%	25–40% (estimated)
Endpoint patch compliance	94%	~40–60% within 30 days
Server patch compliance	99%	Variable; 77% take >1 week
Firewall patch compliance	99%	Not widely benchmarked
M365/SaaS compliance	100%	Not widely benchmarked
Ransomware attempts blocked (Q4)	12,977	N/A (no comparable metric)
Security escalations (Q4)	379	N/A

Quick Fact

99.9% of compromised accounts did not have MFA enabled. At 63%, the managed client base is nearly double the industry adoption rate — but 37% of users remain exposed. (Microsoft / Internal data)

4d. Operational Maturity

Industry Benchmark

Operational maturity in SMB IT is shaped by a fragmented service provider landscape and a severe talent shortage.

> "There are estimates of 10,000 to 40,000 MSPs in the United States, and 27% of them have between one and five employees," said Jim Griffith, CEO. "The barriers to entry are low. Anyone with a few years of technical experience, a website, and remote connection software can claim to offer managed services. But IT services need to be available 24/7 — with redundancy. SMB owners need to become discerning buyers."
>
> "Anyone with a few solar panels and a battery system could theoretically resell power. As a business owner, would you rely on that company to keep the lights on every day? The same is true for IT."

Help desk responsiveness benchmarks show that the average mean time to resolution exceeds 30 hours without AI or automation assistance, while organizations leveraging automation achieve under 15 hours (Moveworks, 2024). First-call resolution rates average 70% across all industries and 74% for IT service desks (SQM Group/MetricNet, 2025). The IT staffing ratio for small businesses averages 1:18 — one IT staff member per 18 employees — compared to approximately 1:70 in large enterprises. 76% of MSPs report difficulty hiring qualified technicians, and there are 470,000 unfilled U.S. cybersecurity positions (CompTIA Cyberseek, 2024).

Standardized documentation and process discipline remain uncommon. Devolutions' 2025 report found that 52% of SMBs still manage privileged access manually using spreadsheets or shared vaults. Only an estimated 20-30% of SMBs have formal incident response plans, and roughly 30-40% maintain written IT security policies.

Internal Benchmark

Patch enforcement across the managed client base is 100% for endpoints, servers, firewalls, and M365 applications. This is, in our view, the single strongest operational metric in the index. Help desk responsiveness data, including average and median ticket resolution times, percentage of tickets resolved remotely versus onsite, and SLA compliance rates, is not yet available for this edition and will be incorporated in Q2 2026.

The Delta

Universal patch enforcement is a direct reflection of operational discipline. In an industry where 77% of organizations take more than a week to deploy patches and 60% of breaches originate from unpatched vulnerabilities, maintaining 100% compliance across all system categories eliminates the most common and most preventable attack vector.

The MSP market fragmentation data provides important context for interpreting these results, with the operational outcomes documented in this index reflecting the capabilities of a scaled MSP with dedicated teams for help desk, remote monitoring, project work, and technology roadmap services.

These capabilities are not universal across the MSP market. SMBs evaluating IT partners should ask direct questions:

- How many employees do you have?
- Do you actually staff all 168 hours per week for 24/7 support?
- Are there dedicated teams for distinct functions?

The answers will separate providers capable of delivering these outcomes from those that cannot.

Quick Fact

27% of MSPs in the United States have between 1 and 5 employees. The barriers to claiming MSP status are low, but the requirements for delivering enterprise-grade support at scale are not. (ConnectWise / Internal data)

Note: *Help desk responsiveness metrics will be incorporated in Q2 2026 as internal measurement standardization is completed. This pillar will expand significantly in future editions.*

4e. Financial Impact

Industry Benchmark

The financial consequences of IT failures disproportionately affect SMBs, where margins are thin and cash reserves are limited. ITIC's 2024 survey found that 57% of SMBs report downtime costs of $100,000 or more per hour. For SMBs in the 10-200 employee range, hourly downtime costs fall between $7,600 and $25,600, with $12,500 per hour as the base modeling scenario used in this index. This base reflects fully loaded compensation of $60 per hour (midpoint of a $45-$95 range, inclusive of wages, benefits, and overhead) combined with revenue-per-hour losses for a 50-employee firm generating $10 million in annual revenue. Annualized across the industry-average 14 hours of unplanned downtime, direct losses reach an estimated $175,000 per year at the base scenario (sensitivity range: $105,000-$280,000) before accounting for recovery labor, compliance penalties, or reputational damage.

Ransomware recovery costs have escalated dramatically, too. Sophos reports an average recovery cost of $1.53 million in 2025. For SMBs specifically, practical financial exposure ranges from $250,000 to $1.5 million for minor to moderate incidents, and $1.5 million to $5 million for major events. NetDiligence's analysis of more than 10,000 cyber insurance claims found the average small-business claim reached $264,000 in 2025, up 30% from the prior year. Average operational disruption lasts 24 days before full restoration.

Meanwhile, the median U.S. SMB holds approximately $12,100 in cash reserves (Bluevine, 2025) against an average cyber claim of $264,000 — a 22:1 insolvency gap that widened 30% year-over-year. The National Cyber Security Alliance's benchmark that 60% of small companies close within six months of a major cyber incident has been directionally corroborated by more recent data, which shows that nearly one in five SMBs that suffered a cyberattack subsequently filed for bankruptcy or closed (Mastercard Global SMB Survey, 2025).

The economic comparison between proactive and reactive IT models is similarly clear. Break-fix support runs $150-$350 per hour with unpredictable billing, and managed IT averages $100-$250 per user per month. For a 50-employee firm, managed IT costs roughly $60,000-$84,000 annually versus $185,000+ for a basic two-person in-house team. Gartner estimates that emergency reactive work costs approximately 30% more than proactive scheduled maintenance. Cyber insurance premiums for SMBs average $1,500–$1,740 per year for $1 million in coverage, but approximately 40% of claims are denied, with 82% of denials involving organizations without verified MFA.

Internal Benchmark (Modeled)

Applying the base scenario of $12,500 per hour to internal operational data: at 0.294 outages per quarter with an average duration of 132 minutes, a 50-employee client faces approximately 2.6 hours of downtime per year. That translates to roughly $32,500 in modeled annual downtime cost. At the sensitivity floor of $7,500 per hour, the figure drops to approximately $19,500; at the upper bound of $20,000 per hour, it reaches $52,000. By comparison, an SMB experiencing the industry-average 14 hours of downtime per year faces approximately $175,000 in direct costs at the base scenario.

“Downtime cost modeling should always be expressed as a range, not a point estimate,” said Sam Mahn, Chief Financial Officer of Corporate Technologies. At the base scenario of $12,500 per hour, even a managed environment with minimal outages carries measurable exposure. The difference is that the exposure is predictable, not an open-ended variable that spikes every time something breaks.”

The Delta

The managed model reduces modeled downtime cost by approximately 80% at the base scenario relative to industry averages. The annual cost differential of roughly $142,000 exceeds the typical cost of managed IT coverage for a firm of this size. In other words, the downtime savings alone can offset the investment in proactive IT management.

Beyond the absolute cost reduction, standardization across endpoints, backups, patching, and identity management narrows the variance in IT spending month-over-month, thereby reducing incident-driven cost spikes and improving budget forecast accuracy.

“The financial case for standardization isn’t just about reducing the total cost, but also reducing variance,” Mahn said. “When you narrow incident-driven spending and move to a predictable model, you improve forecast accuracy. That shift from reactivity to predictability is worth just as much to a CFO as the raw cost savings.”

This financial model is conservative, however, and accounts only for direct revenue and productivity losses during the outage itself. It doesn’t include recovery labor, data reconstruction, compliance penalties, customer attrition, or reputational damage — all of which increase the true cost of downtime substantially. It also doesn’t model the avoided cost of a ransomware incident, where SMB-specific recovery costs of $250,000 to $1.5 million for a minor-to-moderate event would represent a significant multiple of the annual managed IT investment.

Metric	Managed Environment	Industry Average
Annual downtime hours	~2.6	~14
Direct cost per hour (50 employees)	$6,600	$6,600
Annual modeled downtime cost	~$32,500 (base)	~$175,000 (base)
Annual managed IT cost (50 users)	$60,000–$84,000	N/A (break-fix: unpredictable)
Average ransomware recovery (SMB)	Avoided/mitigated	$120,000–$254,000
Median SMB cash reserves	$12,100	$12,100
Average cyber insurance claim	$264,000	$264,000

Quick Fact

The median U.S. SMB holds $12,100 in cash reserves. The average cyber insurance claim for a small business reached $264,000 in 2025. That is a 22:1 insolvency gap. (MoneyGeek / NetDiligence)

5. Key Findings & Trends

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

1. The confidence-readiness gap is the defining characteristic of SMBs.

71% of SMBs express confidence in their cyber readiness; 22% are actually prepared. Operational data is the only reliable instrument for closing this gap. Self-reported surveys consistently overstate security posture, and plans without execution provide no measurable protection.

2. Ransomware has fundamentally restructured the SMB threat profile.

It appears in 88% of SMB data breaches, targets backup infrastructure in 93-96% of cases, strikes disproportionately on weekends and holidays when defenses are weakest, and imposes recovery timelines measured in weeks. This is not a nuisance risk. It is a business continuity crisis.

3. Foundational controls remain dramatically underdeployed across the industry.

MFA at 34-40%. Documented disaster recovery plans at 25%. Tested restores under 54%. Even within the managed environment, immutable backup coverage at 11% and RPO/RTO documentation at 5% reveal that structured support does not automatically close every gap. The operational discipline exists for patching and threat blocking; it has not yet fully extended to recovery planning.

4. The financial margin for error among SMBs is effectively zero.

Median cash reserves of $12,100 against practical breach exposure starting at $250,000 leave no buffer for a significant incident. One in five SMBs that suffer a cyberattack subsequently file for bankruptcy or close.

5. Managed environments outperform industry benchmarks materially, but gaps persist.

Four times fewer outages, nearly double the MFA adoption rate, near-universal patch compliance, and 80-88% reduction in modeled downtime costs. These are measurable outcomes of structured IT management. The gaps that remain (RPO/RTO documentation, immutable backup coverage, full MFA deployment) represent the highest-value improvement targets for the next quarter.

> "The reliance on technology for SMB success is only going to increase," said CEO Jim Griffith. "Choosing the right IT partner — one with the scale, redundancy, and operational discipline to deliver — will be 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. 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. What follows is a three-tier maturity framework that provides a practical benchmark for where an organization stands today and what it should be working toward next.

> "IT services for the SMB market should be identical to what enterprise businesses experience. With the right partner, that's achievable regardless of company size. What matters is the size and capability of the MSP, not the size of the client,” says CEO Jim Griffith.

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 running 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; at 63%, the managed client base in this index is ahead of the industry average but still short of full coverage. Patching should be deployed within 30 days of release for operating systems and core applications.

A basic incident response plan should exist in writing, with contact information and initial response steps defined. Additionally, a cyber insurance policy should be in place with coverage validated against the organization's actual security posture, not purchased and forgotten.

This tier is the fundamental baseline. It doesn’t make an organization resilient, but it can make it recoverable.

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 based on the fact that a backup job was completed.

EDR or MDR is deployed across all endpoints, not just servers or executive devices, and monitoring runs 24/7 with defined escalation paths and response SLAs that are tracked and reported. Help desk performance is measured against concrete metrics: ticket resolution time, first-call resolution rate, and SLA compliance. Privileged access is managed through a centralized system rather than the spreadsheets and shared vaults that Devolutions found 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

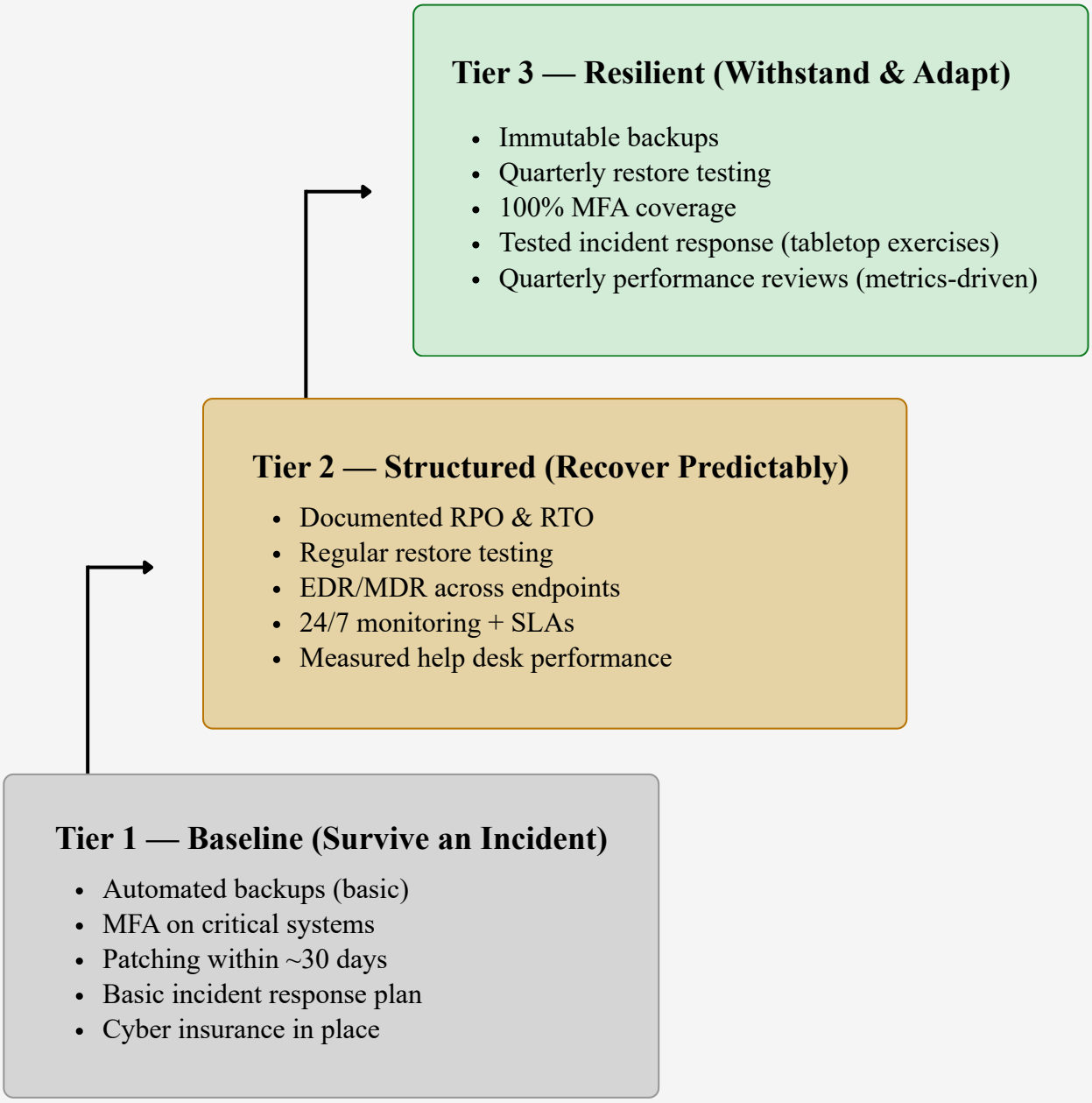
Tier 3 organizations treat resilience as an operational discipline, not a project. Backups are immutable — meaning ransomware cannot encrypt, alter, or delete them — and restore testing is conducted quarterly with results documented.

MFA coverage reaches 100% of users and systems, eliminating the residual exposure that persists at lower adoption rates. The incident response plan is not just documented but tested annually through tabletop exercises that simulate realistic scenarios, including ransomware, data exfiltration, and extended outages. 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. Written IT security policies are reviewed annually against NIST CSF or an equivalent framework. This means that the organization measures its own defenses and improves them systematically.

Most SMBs in this index currently operate between Tier 1 and Tier 2. The internal data shows strong performance on automation, patching, and threat blocking, but significant gaps in recovery documentation, immutable backup coverage, and universal MFA deployment. Closing those gaps is the path from Tier 1 to Tier 3 — and it’s measurable quarter over quarter.

SMB Maturity Model
From Survival to Resilience



7. Practical Recommendations by Maturity Level

The data in this index points 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. Universal MFA. Monthly reporting from IT providers. These are not advanced capabilities but baseline operational hygiene, and the majority of SMBs haven't implemented them.

The following 90-day action plan is designed for organizations at any maturity level. It's sequenced deliberately, with the first phase addressing the gaps most likely to determine whether an organization survives an incident at all. The second phase builds the procedural structure that turns tools into reliable processes. The third phase establishes the verification and measurement discipline that sustains resilience over time. Each phase builds on the previous one.

Days 0–30: Close the Critical Gaps

The first 30 days should focus on 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. The goal of this phase is not to solve every problem but to identify exactly where the organization stands.

Start with MFA. Audit coverage across every system that touches sensitive data, email, financial applications, and remote access. The index data shows the managed client base at 63% adoption, which is nearly double the industry average, but still leaves more than a third of users exposed. The target is 100%. Every account without MFA is an open door, and Microsoft's data is unambiguous: 99.9% of compromised accounts lacked it.

Move to backups. Verify that automated backups are running on a defined schedule and confirm that off-site or cloud replication is active. Don't assume — check. The 71% automation rate in the managed environment is strong relative to the industry, but 29% without automation means those backups depend on a human being remembering to run them.

Then document recovery objectives. RPO and RTO targets should exist in writing for every business-critical system. At 5%, the managed client base has the widest gap in the entire index on this metric. Even rough initial targets — "we can tolerate four hours of data loss" or "our billing system needs to be back within six hours" — are materially better than undocumented assumptions that have never been tested.

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

Key actions:

- ✓ Audit MFA coverage across all systems accessing sensitive data, email, and financial applications. Target 100%.
- ✓ Verify automated backup status and confirm off-site or cloud replication is active.
- ✓ Document RPO and RTO targets for all business-critical systems, even as initial rough estimates.
- ✓ Request a monthly operational report from the IT provider showing actual patch, backup, and monitoring activity.

Days 31–60: Build the Structure

With visibility established, the second phase focuses on testing assumptions and building the procedural framework that most SMBs lack entirely. The industry data is clear on why this matters: 60% of organizations believe they can recover from downtime within hours, but only 35% actually can. The only way to know which category an organization falls into is to test.

Execute a full restore from backup — not a recovery, but a system-level restore that simulates an actual outage or ransomware scenario. Document the results in detail:

- How long did recovery take?
- Was the data complete?
- What failed?
- What worked?

This single exercise will reveal more about the organization's actual resilience posture than any survey or self-assessment. Given that 93-96% of ransomware attacks now target backup repositories, this is also the moment to evaluate whether current backups would survive an attack or whether they would be encrypted alongside production systems.

Draft or update a formal incident response plan; 34% of SMBs have one developed with professional assistance. The plan should define roles, escalation paths, communication procedures, and the specific steps that occur in the first hour, first four hours, and first 24 hours of an incident. A plan that exists only as a vague intention to "call IT" is not a plan.

Also, review the current cyber insurance policy against the organization's actual security posture. Approximately 40% of cyber insurance claims are denied, and 82% of those denials involve organizations that could not demonstrate MFA compliance. Verify that MFA documentation, backup verification records, and access control evidence meet the insurer's specific requirements for claim eligibility.

Key actions:

Execute a full system-level restore test and document time to recovery, data completeness, and any failures.

Evaluate EDR/MDR coverage across all endpoints and identify unprotected devices.

Draft or update a formal incident response plan with defined roles, escalation paths, and hour-by-hour procedures.

Review cyber insurance policy against actual security posture; verify MFA and backup documentation meet insurer requirements.

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 a plan that was created once and never revisited. Your incident response procedures go stale as staff turnover changes who holds critical knowledge, and backup operations drift. The goal of this phase is to establish the recurring measurement and verification cadence that prevents that decay.

Conduct a tabletop exercise simulating a ransomware incident. Walk through the scenario with the people who would actually respond: who makes the call to isolate systems, who contacts the insurance carrier, who communicates with clients, and how long the business can operate without its primary systems. This exercise consistently reveals gaps that documentation alone misses, particularly around communication, decision authority, and the practical logistics of operating during an extended outage.

Establish a quarterly cadence for restore testing and document results each cycle. A single successful test is a data point, but doing this quarterly sets a trend. Over time, this cadence builds institutional confidence that recovery procedures actually work and provides evidence for cyber insurance compliance.

For organizations working with a managed service provider, this is the moment to evaluate whether the provider has the scale and structure to deliver on the outcomes documented in this index.

The MSP market includes an estimated 40,000-45,000 providers, and 27% of them have between one and five employees. 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 for 24/7 support?
- Are there dedicated, specialized teams for help desk, remote monitoring, project work, and technology roadmap services?

Key actions:

- Conduct a tabletop exercise simulating a ransomware scenario with all relevant stakeholders.
- Establish quarterly restore testing with documented results each cycle.
- Benchmark the current environment against this index's pillar metrics and identify remaining gaps.
- Evaluate MSP capability: headcount, actual 24/7 staffing, dedicated functional teams.

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

The following eight statements correspond to the foundational controls and processes measured across all 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.
- Automated backups are running with off-site 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 , 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 suggests 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.

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.

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

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:

- 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 (midpoint of a $45-$95 range), inclusive of wages, benefits, and overhead. For a 50-employee firm at $10 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 MoneyGeek as cited in the text.

Financial modeling assumptions and cost ranges in this report were reviewed by Sam Mahn, Chief Financial Officer, who validated the base scenario parameters, sensitivity ranges, and guardrails applied to all financial claims.

All downtime and breach cost figures are expressed as ranges with stated assumptions and shouldn’t be interpreted as outcome guarantees.

8c. External Sources

Verizon 2025 Data Breach Investigations Report

IBM 2024 Cost of a Data Breach Report

Sophos 2025 State of Ransomware Report

Kaseya/Unitrends 2025 State of Backup and Recovery Report

ITIC 2024 Hourly Cost of Downtime Survey

- https://itic-corp.com/itic-2024-hourly-cost-of-downtime-report/
- https://itic-corp.com/itic-2024-hourly-cost-of-downtime-part-2/

ConnectWise 2025 SMB Cybersecurity Report

Devolutions 2025 State of IT Security in SMBs

CrowdStrike 2025 State of SMB Cybersecurity

Semperis 2025 Ransomware Holiday Risk Report

JumpCloud 2024 MFA Statistics

Cyber Readiness Institute 2024 MFA Survey

Guardz 2025 SMB Cybersecurity Report

Infrascale 2025 Ransomware Recovery Playbook

Automox 2024 Vulnerability Report

Flow Specialty 2025 SMB Cyber Risk Trends

CompTIA 2025 State of Cybersecurity

NAIC 2025 Cybersecurity Insurance Market Report

Mastercard 2025 Global SMB Survey

Hiscox 2025 Cyber Readiness Report

Marsh 2024 Cyber Insurance Market Update

Palo Alto Networks MTTR Benchmarks

SQM Group 2025 First Call Resolution Benchmarks

Moveworks 2024 Help Desk Metrics

Freshservice 2024 ITSM Benchmark Report

Techaisle 2025 SMB Cybersecurity Paradox Analysis

8d. Disclaimers

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

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 regulatory fine ranges, 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.