itSimple
बैकअप सरल है

Tech Business Connect 2026
11 – 12 September 2026 | Delhi

CYBER RESILIENCE REPORT

Key insights on organisational readiness to recover from cyber attacks



81%

STILL AT RISK OR DEVELOPING

35%

PARTIAL IMPLEMENTATION IS THE NORM

4%

FULLY IN PLACE OR DEMONSTRATED

© itSimple 2026

ITS Technology Solution Private Limited

B194 (Ground Floor), Sector 19,

Noida, UP – 201302, India

© itSimple 2026

1. Executive Summary

This survey was conducted on 11th and 12th September 2026 at the Tech Business Connect event in Delhi.

The survey comprised four pillars and 16 questions, scored 0, 2 or 4.

This report contains the results and interpretation.

The Average CR Score is 35/64, placing the respondent group in the **'At Risk'** band. This indicates that, overall, some recovery capabilities are in place, but they are not yet consistently connected, evidenced, and demonstrated.

8% participating organisations are at 'Critical' level i.e., they do not have evidence of work done.

46% participating organisations are at 'At Risk' level i.e., some work is done but in silos and is not aligned.

35% participating organisations are at 'Developing' level i.e., they have good practices in place, but claims are to be substantiated with evidence.

Only 7% participating organisations are at 'Resilient' level i.e., evidence of tested claims exist and gaps are closable.

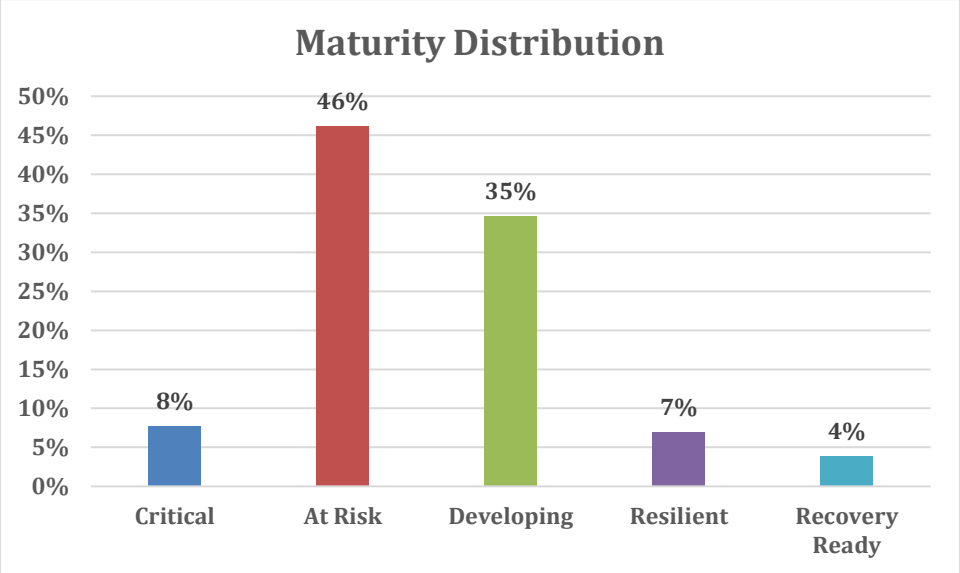
Only 4% participating organisations are at 'Recovery Ready' level, i.e., demonstrated capabilities exist with evidence.

© itSimple 2026

2. CR Score Framework

Band	Score	Definition
Critical	0–19	A belief held in good faith. Nothing proven.
At Risk	20–39	Pieces exist, but do not connect. The most common result.
Developing	40–51	A practice is forming. What remains is evidence and timing.
Resilient	52–57	Tested and largely proven. Gaps are specific and closable.
Recovery Ready	58–64	Rare. Demonstrated rather than described.

3. Maturity Distribution



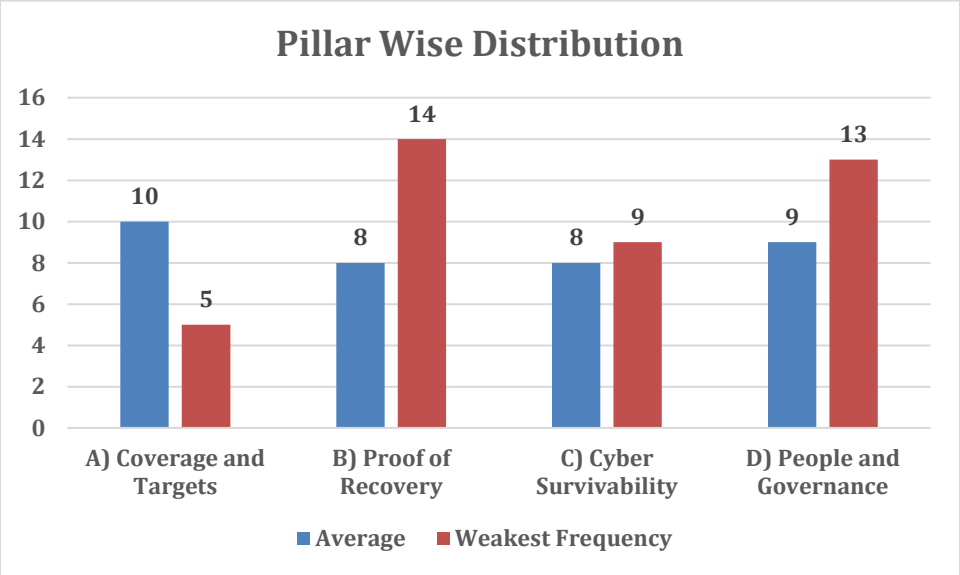
Maturity Distribution

The maturity distribution shows a clear concentration in the middle bands: **46% are At Risk** and **35% are Developing. This means 81%** of the assessed organisations are yet to **demonstrate a consistently proven recovery capability**. **Only 11% fall into the Resilient or Recovery Ready** bands, indicating that **demonstrated recovery capability remains relatively uncommon**.

© itSimple 2026

4. Pillar Performance

Pillar Name	Average Score	Weakest Frequency
A) Coverage and Targets	10	5
B) Proof of Recovery	8	14
C) Cyber Survivability	8	9
D) People and Governance	9	13

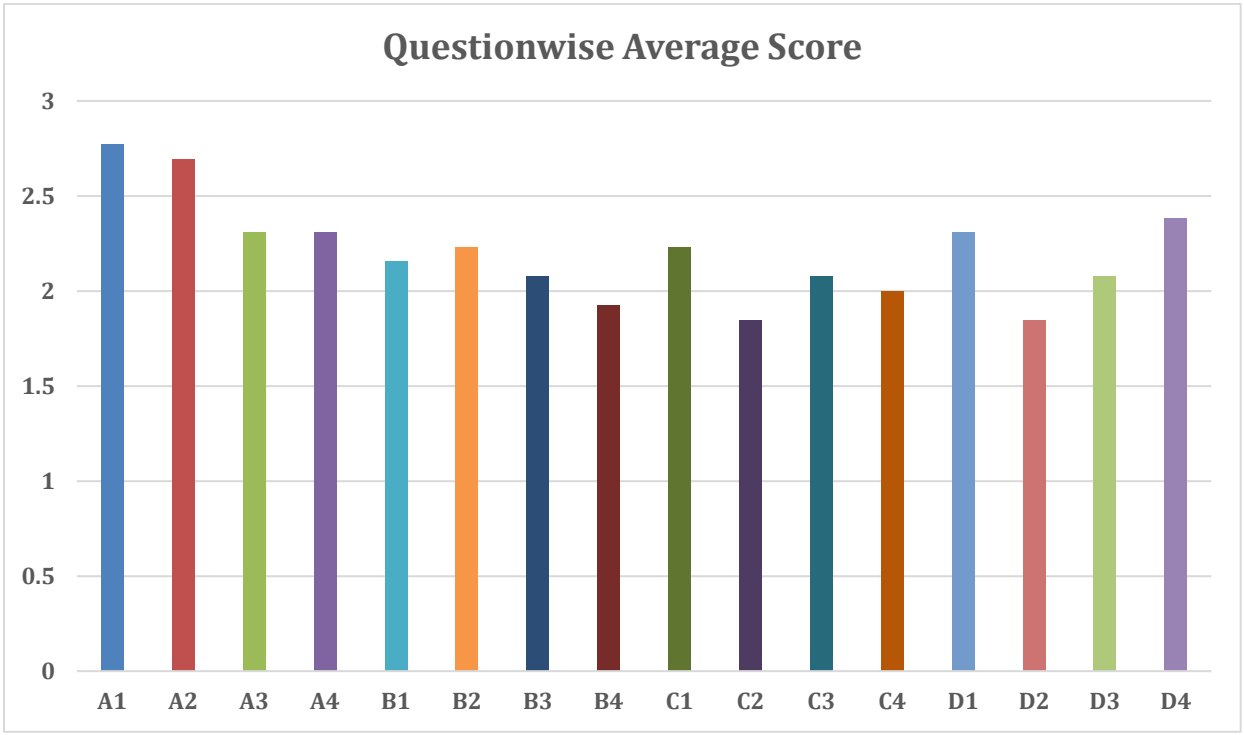


Pillarwise Distribution

The results show that **Coverage and Targets (A) is relatively stronger** across the respondent group, while **Proof of Recovery (B) and Cyber Survivability (C) have the lowest average scores**. Looking at individual respondents, however, **Proof of Recovery (B) most frequently emerges as the weakest pillar**, followed by **People and Governance (D)**. Together, these findings suggest that the key challenge is moving beyond having recovery arrangements defined to consistently proving recovery capability and ensuring that people, processes, and governance can execute it when required.

© itSimple 2026

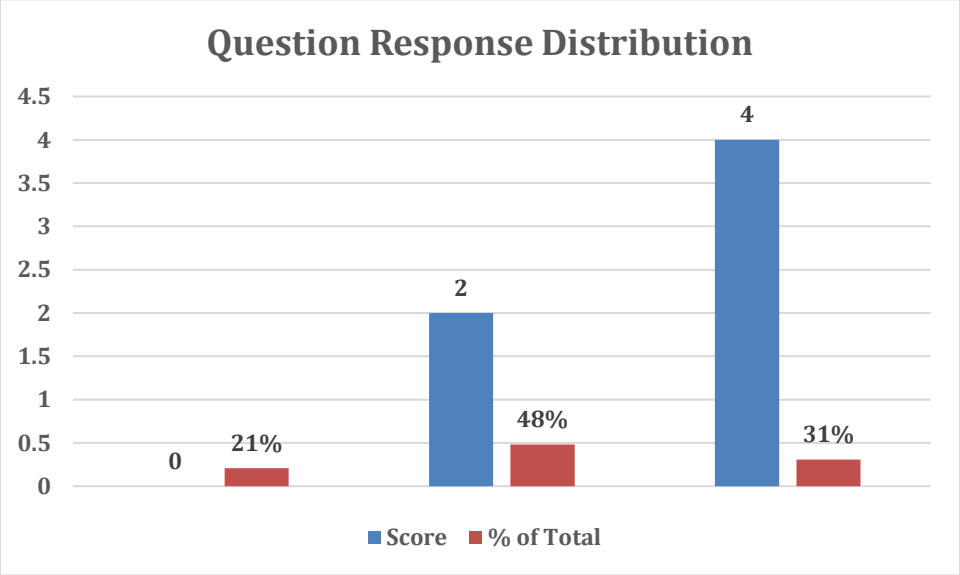
5. Question-Level Analysis



Question wise Average Score

Question-wise analysis takes the assessment one level deeper, showing which specific practices are driving the pillar scores. The results reveal a consistent pattern: A1, relating to coverage of business-critical applications, records the **highest average score (2.77)**, aligning with A being the strongest pillar overall. At the other end, C2—whether recovery can continue when production systems or credentials are compromised—records one of the **lowest scores (1.85)**, consistent with C having the **lowest pillar average**. D2 and B4 also score among the lowest, highlighting challenges around recovery personnel and identifying a clean recovery point after a cyber incident. Overall, the findings suggest that organisations are relatively more confident about having recovery arrangements defined than about executing and proving recovery when conditions are adverse.

© itSimple 2026



Question Response Distribution

Across the 416 individual question responses, **almost half (48%) scored 2**, indicating that partial implementation is the dominant pattern across the respondent group. While **31% of responses indicate practices that are fully in place or demonstrated**, **21% show no evidence** of the practice being in place. The distribution therefore suggests that the primary challenge is not simply the absence of resilience capabilities, but the transition from partially implemented arrangements to consistently demonstrated and recoverable capability.

6. Weakest-Pillar Diagnostic Journey

CR Score → Resilience Band → Weakest Pillar → Targeted Action

Weakest Pillar	Targeted Action	Diagnostic intent
A – Coverage and Targets	Workload criticality mapping — Classifying what the business cannot live without, with targets agreed outside IT.	Clarify critical workloads and agreed targets. BIAs conducted and outputs (RTO, RPO, Dependencies) agreed with Business.
B – Proof of Recovery	Restore drills and validation — Structured tests on selected workloads, with timing, evidence, and a findings report.	Produce evidence of actual restoration. Follow actions to closure after improvements and reruns/ retests.
C – Cyber Survivability	3-2-1-1-0 readiness review — Copies verified by restore	Verify clean recovery after cyber compromise. Recovery

Weakest Pillar	Targeted Action	Diagnostic intent
	rather than policy, plus a clean recovery path.	not just of data, applications, and systems, but of the business as well.
D – People and Governance	Runbook and recovery playbook — Documents a second person can follow, and roles agreed before the cyber-attack.	Make recovery executable beyond one individual through lessons learnt and competency enhancement through learning and sharing.

7. Key Actionable Takeaways

1. Move from "having recovery" to "proving recovery"

With **81%** of respondents falling in the **'At Risk' or 'Developing'** bands, the immediate priority is to move beyond documented arrangements and demonstrate that recovery capabilities actually work when required. This would also need strenthening Pillar D 'People and Governance' through **meaningful Play Books and Run Books.**

2. Make recovery capability executable — not dependent on assumptions

The weakest areas point to three practical priorities: **prove restoration, establish clean recovery paths after cyber compromise, and ensure trained people can execute recovery when key individuals or systems are unavailable.**

3. Focus improvement where the weakness actually sits

Use the diagnostic journey:

CR Score → Resilience Band → Weakest Pillar → Targeted Action

This allows improvement efforts to be targeted rather than applying the same resilience program to everyone.

4. Treat evidence as the measure of maturity

The results suggest that the key transition is from **partial implementation to demonstrated capability**. Recovery claims should therefore increasingly be supported by **tests, evidence, findings and retests**.

5. Prioritise the weakest link, not the average

Overall scores can hide specific weaknesses. Management attention should therefore focus on the **weakest pillar and the specific practices behind it**, rather than relying only on the overall CR Score.

6. Apply PDCA cycle to this exercise

This is not one-time activity. It is recommended that improvement actions are drawn, acted upon and results are checked for effectiveness. An ideal frequency for such re-runs may be quarterly.

© itSimple 2026

The objective is not simply to improve the CR Score. The objective is to build Cyber Recovery Capability that can be demonstrated for your MVO (Minimum Viable Organisation) when normal conditions no longer exist.

Note: The report has been produced based on data as filled in by the participants during the event. No adjustments have been made. Privacy and confidentiality have been maintained as promised during data collection.

While all care has been taken towards accuracy in analysis and interpretation of data, the authors will not be liable to any consequences due to unintentional errors or noise in data and report.

itSimple
Life is Simple

Secure. Compliant. Sovereign.

Backed by deep expertise and uncompromising commitment.



Sovereign & Compliant

DPDP 2025, RBI & regulatory compliant.

Trusted Technology

Enterprise-grade platforms with proven reliability.

Always Available

24×7 monitoring, response and support.

End-to-End Expertise

From backup strategy to successful restoration.

Business Outcome Focused

Reduce downtime. Ensure continuity.

Partnership Driven

Built on trust, transparency and results.

Let's Build Your Resilience Together

Modernising, migrating, or preparing — we keep you one step ahead.

- Free Consultation & Assessment
- Tailored Solution Roadmap
- Stronger Resilience. Lower Risk.

Scan to Connect

+91 20 6743 0000 | info@itsimple.in | www.itsimple.in

Offices: INDIA | Serving 20+ Countries

Data Resilience Delivered
Built for enterprise. Proven in practice.

13+ Years
Of delivering data resilience solutions.

300+ Clients
Across critical industries and sectors.

20+ Countries
Global reach. Local expertise.