

A BOARD-READY WHITEPAPER FOR CISOs

Cyber Recovery Readiness

The Seven Things That Decide Whether You Come Back

Why “we have backups” is not an answer, and a board-ready checklist to find out where you really stand before an attacker does.

Author: Muhammad Shariq, General Manager

Data Protection & Cyber Recovery, Proactive Data Systems

FOR THE BOARD AND THE CISO

Executive Summary

Most organisations believe they can recover from a ransomware attack because they have backups. That belief is the single most dangerous assumption in enterprise security today, because the attacker has read the same playbook. Modern ransomware does not simply encrypt production. It hunts down the backups first, because a victim who cannot restore is a victim who pays.

The data is unambiguous. The overwhelming majority of ransomware attacks now target the backup environment itself, and most of those attempts succeed. Even among organisations that pay the ransom, a large majority still fail to recover all of their data. The uncomfortable conclusion is that having backups and being able to recover are two different things, and the gap between them is where businesses fail.

This whitepaper reframes the question a board should be asking. Not “do we have backups?” but “can we prove we can recover, cleanly and within a time the business can survive?” It sets out the difference between backup and cyber recovery, explains what a defensible recovery architecture looks like, and gives you a seven-dimension readiness checklist you can score in an afternoon and take to your next board meeting. It also covers the India-specific obligations, CERT-In’s six-hour reporting rule and the DPDP breach-notification duty, that turn a recovery failure into a regulatory one.

SECTION 1

The Backup Illusion

For thirty years, the answer to “what if we lose the data?” was a backup. It was a sound answer when the threat was a failed disk, a fat-fingered deletion or a flood in the server room. Those threats are accidents. They do not adapt, they do not target your recovery capability, and they do not wait until your backups are compromised before they strike. A modern attacker does all three.

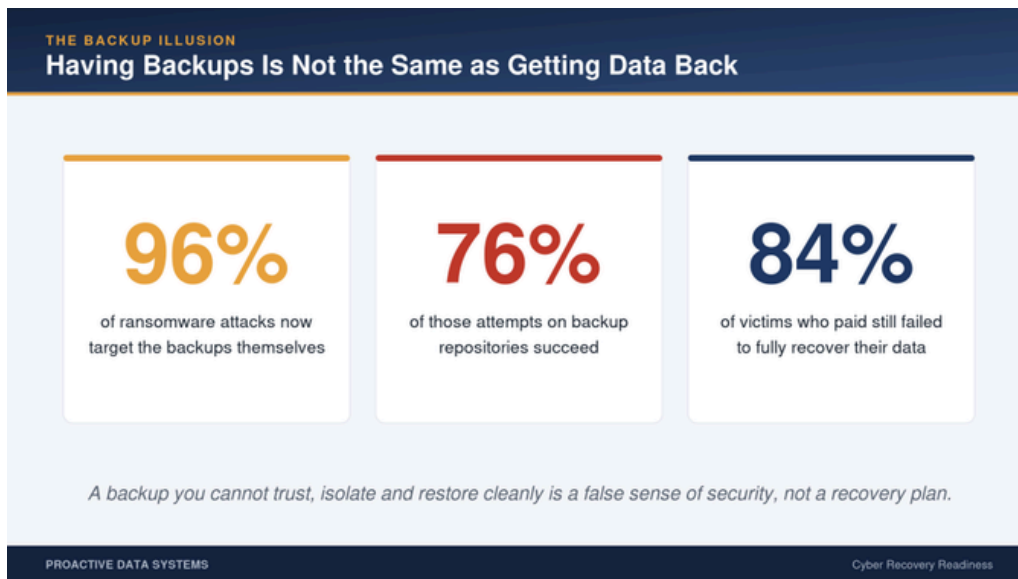


Figure 1. The gap between having backups and getting data back

Read those numbers as a single sentence. Attackers go after the backups in almost every case, they usually get in, and paying does not buy recovery. A backup sitting on the same network as production, reachable with the same credentials, visible to the same attacker who spent weeks inside your estate, is not a safety net. It is another target, and often the first one.

The illusion is comforting precisely because the backup job keeps reporting success. Green ticks accumulate. Nobody restores anything, because nothing has broken. Then the day comes when everything has broken at once, and the organisation discovers, for the first time and under maximum pressure, whether its backups were ever a recovery plan or merely a compliance checkbox. That is the worst possible moment to find out.

SECTION 2

Backup Is Not Cyber Recovery

The two words are often used interchangeably. They should not be. Backup is a copy of data made so it can be restored. Cyber recovery is the discipline of getting a business running again after a deliberate, intelligent adversary has done everything in their power to stop you, including corrupting or deleting the very copies you planned to restore from. The difference is not semantic. It changes the architecture, the testing, the ownership and the assumptions.

A DEFINITIONAL RESET Backup vs Cyber Recovery: Not the Same Discipline		
	BACKUP	CYBER RECOVERY
Designed for	Hardware failure, deletion, disaster	A deliberate, adaptive human attacker
Assumes	The backup is safe and clean	The attacker went after the backup too
Isolation	Often on the same network	Immutable and air-gapped from production
Before restore	Restore and hope	Scan and validate for reinfection first
Proof	Backup job reported success	A tested, timed, clean recovery
Owned by	IT operations	The board, via the CISO
PROACTIVE DATA SYSTEMS		Cyber Recovery Readiness

Figure 2. Backup and cyber recovery answer different questions.

The most important row in that table is the second one. A backup strategy assumes the backup is safe. A cyber recovery strategy assumes it is not, and designs around that assumption. Everything else follows. If you assume the attacker reached your backups, you isolate them. If you assume the restored data might carry the same malware that took you down, you scan it before you trust it. If you assume recovery is a business decision with legal and financial consequences, you take it out of the server room and put it in front of the board. Backup is an IT task. Cyber recovery is a business capability.

SECTION 3

What Good Looks Like

If you cannot assume your backups are safe, where does trustworthy data come from? The answer that has emerged as the standard for serious organisations is the isolated recovery environment, sometimes called a cyber recovery vault. It rests on three ideas that work together, and each is useless without the others.

Immutable

An immutable copy cannot be altered or deleted for a defined retention period, by anyone, including an administrator whose credentials the attacker has stolen. This is what stops ransomware from encrypting or wiping the backup along with everything else. Immutability is the floor, not the ceiling.

Air-gapped

Immutability protects the data from being changed. An air gap protects it from being reached. The recovery copy sits with no live network path to production, the internet, or any machine the attacker can touch. Data flows in on a controlled, one-way basis and nothing flows out until it has been checked. Only copies that are both immutable and air-gapped reliably survive a serious attack.

Recovered clean

The final idea is the one most organisations miss. The malware that encrypted your production estate may have been dormant in your systems, and therefore in your backups, for weeks before it detonated. Restore blindly and you can reinfect yourself with your own recovery data. A clean room, an isolated space where recovered systems are scanned, validated and proven free of threats before they touch production, is what turns a restore into a recovery.

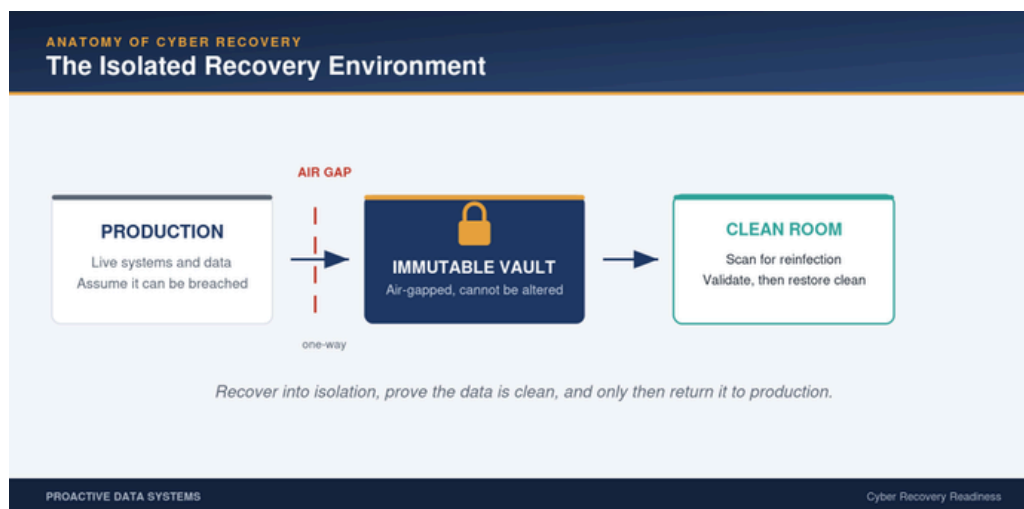


Figure 3. Recover into isolation, prove the data is clean, then return it to production.

None of this requires exotic technology; the platforms to build it, from Veeam, Rubrik, Commvault, Dell and others, are mature and proven. What it requires is a design that treats recovery as adversarial by default, and a partner who has built and tested one before rather than assembled the parts and hoped.

SECTION 4

The Seven Dimensions of Readiness

Cyber recovery readiness is not a single product you buy or a box you tick. It is a capability made of seven distinct dimensions, and a chain is only as strong as its weakest. An immutable vault is worthless if you have never tested a restore from it. A perfect recovery plan is worthless if nobody knows who is authorised to trigger it at 2 a.m. The seven dimensions below are the ones that, together, decide whether you come back.



Figure 4. The seven dimensions, each scored from 0 (Blind) to 3 (Proven).

1. Protected Copies. At least one copy of critical data that is immutable, air-gapped and follows the 3-2-1-1-0 rule: three copies, on two media, one off-site, one immutable or offline, and zero errors on a verified restore test.

2. Isolation. A recovery environment that is genuinely separated from production, so an attacker who owns your live estate does not automatically own your recovery capability too.

3. Clean Restore. The ability, and the habit, of scanning and validating recovered data for reinfection before it is trusted, rather than restoring blindly under pressure.

4. Tested Objectives. Recovery time and recovery point objectives that are agreed with the business and, crucially, proven by regular exercises, not assumed from a vendor data sheet.

5. Playbook & Roles. A written incident playbook that names who decides, who acts and who communicates, including a pre-agreed position on whether the organisation will pay a ransom.

6. Regulatory Readiness. The processes to meet CERT-In's six-hour reporting window and the DPDP breach-notification duty when, not if, an incident is reportable.

7. Evidence for the Board. The reports, test results and metrics that let the CISO show the board that recovery works, rather than assert that it should.

SECTION 5 · THE ASSESSMENT

The Cyber Recovery Readiness Checklist

This is the working heart of the whitepaper. For each of the seven dimensions, ask the diagnostic questions below and score the dimension from 0 to 3 using the anchors in Figure 4. Be honest; the point of the exercise is to find the weak link before an attacker does. An organisation that scores 3 on protected copies but 0 on tested objectives has an expensive vault and no proof it works, which in a real incident is close to having nothing.

Score each dimension, then total it. The summary table at the end tells you how to read the number.

1. Protected Copies

Diagnostic question	Score 0–3
Do we hold at least one immutable copy of critical data that cannot be deleted or altered within its retention period?	
Is at least one copy air-gapped, with no live network path from production?	
Can we point to the 3-2-1-1-0 rule being met for our most critical systems?	

2. Isolation

Diagnostic question	Score 0–3
Is our recovery environment separated from production, with its own authentication and access controls?	
Would an attacker who compromised our domain administrator credentials also gain control of our backups?	
Is access to the recovery environment limited to a small, named, monitored group?	

3. Clean Restore

Diagnostic question	Score 0–3
Do we scan recovered systems and data for malware before returning them to production?	
Do we have an isolated clean room, or equivalent, in which to validate recovery?	
Do we have a defined process to identify the last known-clean recovery point?	

4. Tested Objectives

Diagnostic question	Score 0–3
Have we agreed recovery time (RTO) and recovery point (RPO) objectives with the business for our critical systems?	
Have we actually tested a full recovery in the last twelve months, and did it meet those objectives?	
Do we record the measured recovery time from each test, rather than the target?	

5. Playbook & Roles

Diagnostic question	Score 0–3
Do we have a written cyber incident and recovery playbook that is current and accessible offline?	
Does it name who is authorised to declare an incident and to trigger recovery?	
Have we pre-decided our position on ransom payment, with legal and executive input?	

6. Regulatory Readiness

Diagnostic question	Score 0–3
Can we detect, classify and report a qualifying incident to CERT-In within six hours of becoming aware of it?	
Do we know which incidents also trigger a DPDP breach notification to the Data Protection Board and affected individuals?	
Are our security logs retained for at least 180 days, with synchronised clocks?	

7. Evidence for the Board

Diagnostic question	Score 0–3
Can the CISO show the board a current, evidenced view of recovery readiness?	
Do we report tested recovery results, not just backup success rates?	
Is cyber recovery reviewed at board level with the same seriousness as financial risk?	

Reading Your Score

Total the seven dimension scores for a figure out of 21. The bands below are deliberately blunt, because cyber recovery is one of the few areas of security where a near miss and a hit produce the same outcome.

Total	Where you stand	What it means
0–7	Exposed	You are relying on backups an attacker can reach. Treat this as an urgent, board-level risk.
8–14	Partial	You have components but not a proven capability. The gaps, not the strengths, are what an attacker will find.
15–19	Managed	A real recovery capability. Focus now on testing cadence and closing the last one or two weak dimensions.
20–21	Proven	Defensible. Keep it that way with regular exercises and board reporting; readiness decays without use.

SECTION 6

The India Layer: CERT-In and DPDP

In India, a ransomware incident is not only an operational crisis. It is a reporting obligation on a clock, and the clock is short. Two regimes apply at once, and they are distinct.

CERT-In: the six-hour rule

Under the CERT-In Directions, organisations must report specified cyber incidents, ransomware explicitly among them, within six hours of noticing or becoming aware of them. Six hours is not long enough to improvise. The trigger is not limited to the CISO's certainty; an alert from a managed security provider, a priority SOC ticket or a credible third-party disclosure can start the clock. If your detection, classification and escalation chain takes longer than a couple of hours, you are already at risk of breaching it. The Directions also require security logs to be retained for 180 days and system clocks to be synchronised to trusted time sources.

DPDP: the breach-notification duty

The Digital Personal Data Protection framework adds a second, overlapping duty. Where an incident involves personal data, the organisation, as data fiduciary, must notify both the Data Protection Board and the affected individuals. CERT-In is concerned with national cyber security and incident response; DPDP is concerned with individuals' rights. A single ransomware event can trigger both, on different timelines and to different authorities, which is exactly why regulatory readiness is a dimension of recovery and not a footnote to it.

The practical implication for the CISO is simple and demanding. Your recovery playbook must include the reporting workflow, pre-drafted templates, named responsible people and legal input, ready before an incident, because there is no time to assemble them during one. Non-compliance with the CERT-In Directions carries penal consequences, so this is a board-level exposure in its own right.

This whitepaper is general guidance, not legal advice. Confirm your specific obligations under the CERT-In Directions and the DPDP Act and Rules with qualified counsel.

WHAT TO DO NEXT

From Assessment to Assurance

A score is a starting point, not a verdict. The value of this checklist is that it turns a vague anxiety, “are we actually protected?”, into a specific list of weak dimensions you can fix in priority order. The organisations that recover well are rarely the ones that spent the most. They are the ones that closed every dimension of the chain and, above all, tested it, so that the first real recovery is not the first recovery they have ever done.

Building that capability, an immutable and air-gapped recovery vault, a clean room to recover into, tested recovery objectives, and the reporting workflow to stay on the right side of CERT-In and DPDP, is specialised work. It rewards a partner who has designed, built and rehearsed cyber recovery for organisations like yours, rather than one who sells backup software and leaves the recovery to chance.

Proactive Data Systems designs and operates cyber recovery for Indian enterprises, immutable and air-gapped data protection, isolated recovery environments, tested recovery, and the incident-reporting readiness that CERT-In and DPDP now demand. We are a Cisco Preferred Cloud and AI Partner, Dell Platinum Partner and NetApp Preferred Partner, with 35 years in enterprise IT, more than 1,500 organisations served, and a 24/7 service desk in India. To pressure-test your own readiness against this checklist, you can ask Proactive for a cyber recovery readiness assessment.

Sources

- Veeam and Sophos ransomware trend research on backup targeting and recovery outcomes, 2024–2025.
- Coveware and CrowdStrike ransomware reporting on recovery and payment outcomes, 2024–2025.
- Vendor and cloud-provider guidance on isolated recovery environments and clean-room recovery, 2025.
- CERT-In Directions on incident reporting (six-hour rule; 180-day log retention).
- The Digital Personal Data Protection Act, 2023 and Rules; breach-notification duties.

Figures are drawn from published industry research and vary by source, methodology and year; verify current data before citing externally.

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us
at pro@proactive.co.in

 www.proactive.co.in

PROACTIVE[™]
Enhancing Digital Experience

© 2026 Proactive Data Systems Pvt Ltd. All rights reserved.

This report is for informational purposes only. It does not constitute legal or regulatory advice. Statistical claims are attributed to named sources; readers should refer to original sources for complete methodology and context.