

PROACTIVE DATA SYSTEMS · A BOARD-READY CHECKLIST FOR CISOs

Cyber Recovery Readiness Checklist for CISOs

The seven things that decide whether you come back
after a ransomware attack

By: Muhammad Shariq, General Manager

Most organisations believe they can recover from ransomware because they have backups. Attackers know this. Ransomware now goes for the backup environment first, because a victim who cannot restore is a victim who pays.

Attackers targeted the backup environment in 96% of ransomware incidents, and 84% of victims who paid the ransom still did not get all their data back (Veeam and Sophos ransomware research, 2024 to 2025). Having backups and being able to recover are two different things. The gap between them is where businesses fail.

The question a board should ask is not "do we have backups?" It is "can we prove we can recover, cleanly, in a time the business can survive?" This checklist helps you answer it. It explains the difference between backup and cyber recovery, describes what a sound recovery architecture looks like, and gives you seven dimensions to score, a ransomware recovery checklist and a backup audit in one. You can complete it in an afternoon and take the result to your next board meeting. It also covers the two Indian obligations, CERT-In's six-hour reporting rule and the DPDP breach-notification duty, that turn a recovery failure into a regulatory one.

It is written for CISOs, CIOs and IT heads who are accountable for whether the business comes back after an attack, and for the board members who ask them to prove it. If you want to go straight to the scoring, skip to How Do I Run the Cyber Recovery Readiness Checklist? below.

Proactive Data Systems, a Cisco Preferred Partner across all five architectures with 35 years in Indian enterprise infrastructure, has designed, built and tested cyber recovery environments for Indian enterprises of all sizes. This checklist is the one we use before any of that work starts.

Why "We Have Backups" Is Not an Answer

Backups fail as a recovery plan because the attacker goes after them first. 96% of ransomware attacks now hit the backup repositories, and 76% of those attempts succeed. For thirty years, the answer to "what if we lose the data?" was a backup. That worked when the threat was a failed disk, an accidental deletion or a flood in the server room. Those 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. An attacker does all three.

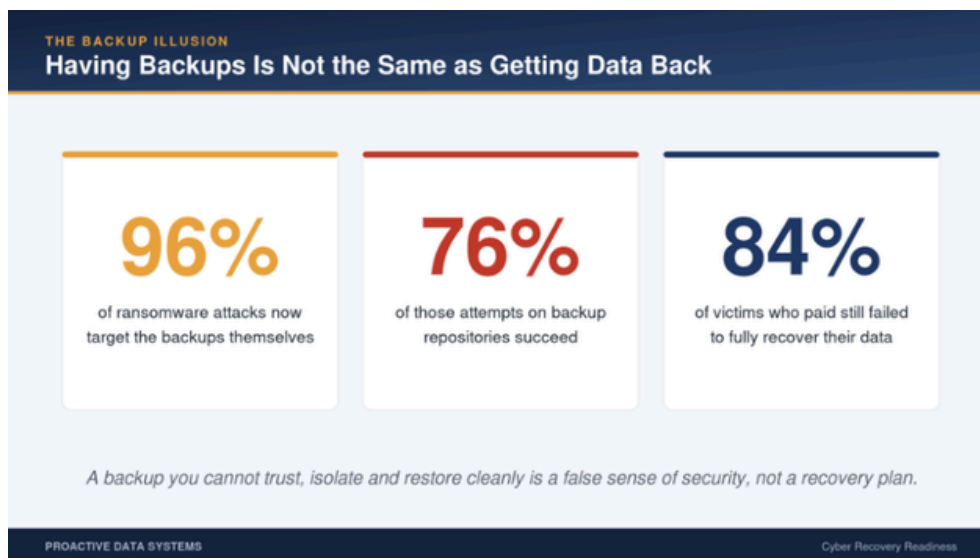


Figure 1. The gap between having backups and getting data back.

Put the three numbers in Figure 1 together, and they say one thing. Attackers go after the backups in almost every case; they usually get in, and paying does not get you your data back. A backup on the same network as production, reachable with the same credentials, visible to an attacker who has spent weeks inside your estate, is not a safety net. It is another target, and usually the first one.

The illusion holds because the backup job keeps reporting success. Nobody restores anything, because nothing has broken. Then everything breaks at once, and the organisation finds out, under maximum pressure, whether its backups were a recovery plan or a compliance checkbox. That is the wrong time to find out. This checklist lets you find out now.

How Is Cyber Recovery Different from Backup?

Cyber recovery differs from backup on one assumption. Backup assumes the copy is safe. Cyber recovery assumes the attacker reached it. Backup is a copy of data made so it can be restored. Cyber recovery is getting the business running again after someone has done everything they can to stop you, including corrupting or deleting the copies you planned to restore from. People use the two words interchangeably. They should not. The difference changes the architecture, the testing, the ownership and the assumptions.

	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

Backup and cyber recovery answer different questions.

The second row matters most. A backup strategy assumes the backup is safe. A cyber recovery strategy assumes it is not, and designs around that. Everything else follows. If you assume the attacker reached your backups, you isolate them. If you assume the restored data carries 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 job. Cyber recovery is a business capability, owned by the board through the CISO.

What Does a Defensible Recovery Architecture Look Like?

A sound recovery architecture has three properties: immutable, air-gapped and recovered clean. If you cannot assume your backups are safe, trustworthy data has to come from somewhere else. The standard answer is an isolated recovery environment, sometimes called a cyber recovery vault. It depends on all three properties. Any one of them on its own is not enough.

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. It is the minimum, not the whole answer.

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

This 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 and checked before they touch production, is what turns a restore into a recovery.



Figure 2. Recover into isolation, prove the data is clean, then return it to production.

None of this needs unusual technology. The platforms to build it, from Veeam, Rubrik, Commvault, Dell and others, are mature. What it needs is a design that assumes an attacker, and a partner who has built and tested one before, not one who has assembled the parts and hoped.

What Are the Seven Dimensions of Cyber Recovery Readiness?

Cyber recovery readiness is not a product you buy or a box you tick. It is seven separate things, and the weakest one decides the outcome. An immutable vault is worth nothing if you have never tested a restore from it. A good recovery plan is worth nothing if nobody knows who is allowed to trigger it at 2 a.m. These are the seven.

	Dimension	Cyber Recovery
1.	Protected Copies	Is at least one copy immutable, air-gapped and 3-2-1-1-0?
2.	Isolation	Is recovery separated from production?
3.	Clean Restore	Do we scan before we restore?
4.	Tested Objectives	Are RTO and RPO proven, not assumed?
5.	Playbook & Roles	Who decides, who acts, and what is our ransom stance?
6.	Regulatory Readiness	Can we meet CERT-In and DPDP on the clock?
7.	Evidence for the Board	Can we show recovery works, not just assert it?

Score each dimension from 0 to 3: 0 is Blind, 1 is Partial, 2 is Managed, 3 is Proven. Read the total, out of 21, against the bands under Reading Your Score.

How Do I Run the Cyber Recovery Readiness Checklist?

Score each of the seven dimensions from 0 (Blind) to 3 (Proven) against the three questions in its table, then add up the total out of 21. This is a ransomware recovery checklist and a backup audit in one. Be honest. The point 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. In a real incident, that is close to having nothing.

The table under Reading Your Score tells you what the number means.

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.

Diagnostic question	Score (0 to 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?	

Checklist table 1 of 7: Protected Copies. Three diagnostic questions, score 0 to 3.

2. Isolation

A recovery environment separated from production, so an attacker who owns your live estate does not own your recovery capability as well.

Diagnostic question	Score (0 to 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?	

Checklist table 2 of 7: Isolation. Three diagnostic questions, score 0 to 3.

3. Clean Restore

The ability, and the habit, of scanning recovered data for reinfection before you trust it, instead of restoring blindly under pressure.

Diagnostic question	Score (0 to 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?	

Checklist table 3 of 7: Clean Restore. Three diagnostic questions, score 0 to 3.

4. Tested Objectives

Recovery time and recovery point objectives agreed with the business and proven by regular exercises, not taken from a vendor data sheet.

Diagnostic question	Score (0 to 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?	

Checklist table 4 of 7: Tested Objectives. Three diagnostic questions, score 0 to 3.

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.

Diagnostic question	Score (0 to 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?	

Checklist table 5 of 7: Playbook & Roles. Three diagnostic questions, score 0 to 3.

6. Regulatory Readiness

The processes to meet CERT-In's six-hour reporting window and the DPDP breach-notification duty when an incident is reportable.

Diagnostic question	Score (0 to 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?	

Checklist table 6 of 7: Regulatory Readiness. Three diagnostic questions, score 0 to 3.

Reading Your Score

Add the seven scores for a total out of 21. The bands are blunt on purpose. 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 to 7	Exposed	You are relying on backups an attacker can reach. Treat this as an urgent, board-level risk
8 to 14	Partial	You have components but not a proven capability. The gaps, not the strengths, are what an attacker will find.
15 to 19	Managed	A real recovery capability. Focus now on testing cadence and closing the last one or two weak dimensions.
20 to 21	Proven	Defensible. Keep it that way with regular exercises and board reporting. Readiness fades if you stop testing.

Checklist table 5 of 7: Playbook & Roles. Three diagnostic questions, score 0 to 3.

The India Layer: CERT-In and DPDP

In India, a ransomware incident is also a reporting obligation on a clock, and the clock is short. Two separate regimes apply at once.

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 clock does not wait for the CISO to be certain. An alert from a managed security provider, a priority SOC ticket or a credible third-party disclosure can start it. 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. One ransomware event can trigger both, on different timelines and to different authorities. That is why regulatory readiness is one of the seven dimensions and not a footnote.

What this means for the CISO: your recovery playbook must include the reporting workflow, pre-drafted templates, named responsible people and legal input, all ready before an incident, because there is no time to assemble them during one. Non-compliance with the CERT-In Directions carries penalties, so this is a board-level exposure on its own.

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

From Score to Assurance

A score is a starting point. What the checklist gives you is a specific list of weak dimensions to fix, in priority order, in place of a general worry about whether you are protected. The organisations that recover well are rarely the ones that spent the most. They are the ones that closed every dimension and tested it, so 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 for CERT-In and DPDP, is specialised work. It needs a partner who has designed, built and rehearsed cyber recovery for organisations like yours, not one who sells backup software and leaves the recovery to chance.

Proactive Data Systems, a Cisco Preferred Partner across all five architectures with 35 years in Indian enterprise infrastructure, 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 also a Dell Platinum Partner and NetApp Preferred Partner, with more than 1,500 organisations served and a 24/7 service desk in India.

Want your score checked?

Ask Proactive for a cyber recovery readiness assessment. We will test your checklist result against your actual estate, run a recovery test, and give you the evidence for your next board meeting.

Frequently Asked Questions

What is cyber recovery readiness?

Cyber recovery readiness is your proven ability to restore the business after a deliberate attack, not only after an accident. It has seven dimensions: protected copies, isolation, clean restore, tested objectives, playbook and roles, regulatory readiness, and evidence for the board. Readiness means each one is in place and tested, not just bought.

How long does the checklist take to complete?

An afternoon. Each of the seven dimensions has three questions and one 0 to 3 score, so a CISO who knows the estate can complete it in two to three hours. It takes longer only if you need to check whether a control has actually been tested.

What score should a CISO aim for?

Twenty or more out of 21 is the only band you can defend at board level. A score of 15 to 19 is a real capability with one or two weak dimensions to close. Below 15, you have components but not a proven ability to recover, and the weakest dimension is where an attacker will find you.

What is the CERT-In six-hour reporting rule?

Under the CERT-In Directions, organisations in India must report specified cyber incidents, ransomware included, within six hours of becoming aware of them. The Directions also require 180-day security log retention and synchronised system clocks. An incident involving personal data may separately trigger a DPDP breach notification.

Is the checklist a substitute for a formal readiness assessment?

No. The checklist is self-scored and tells you where to look. A formal cyber recovery readiness assessment checks the score against your actual estate, runs a recovery test, and produces the evidence the board needs. Use the checklist first, then the assessment to prove the result.

Sources

- Veeam and Sophos ransomware trend research on backup targeting and recovery outcomes, 2024 to 2025.
- Coveware and CrowdStrike ransomware reporting on recovery and payment outcomes, 2024 to 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, Chennai, and Singapore.

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

 www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience