REDEFINING CYBER RECOVERY

Introducing Mean Time To Clean Recovery

By **Duncan Bradley,** Kyndryl Security & Resiliency Practice Leader and **Darren Thomson**, Field CTO, Commvault

READIVERSE

Executive Summary

Commvault® + kyndryl

Cyber resilience – and in particular, the ability to recover critical business systems following a catastrophic cyber incident – is no longer just a technical challenge. It is a critical business imperative owned by the business and operated through IT infrastructure and security teams.

Modern cyberattacks are designed not only to disrupt business but to destabilize recovery itself. Attackers have evolved. They are no longer simply stealing data or causing outages. They are quietly corrupting the very systems and backups that organizations rely on to recover.

As a result, many businesses discover the worst possible truth when they attempt to restore operations: Their backups and disaster recovery systems are encrypted, infected, or silently compromised.

Despite this, many organizations still rely on traditional metrics such as recovery time objective (RTO) and recovery point objective (RPO) to measure their recovery capabilities. These metrics assume that there is a clean environment to recover to and that recovery data is intact and trustworthy. But in the modern threat landscape, this assumption no longer holds.

This whitepaper introduces a new, board-relevant concept: Mean Time to Clean Recovery (MTCR).

MTCR measures not how fast a particular system can be brought back online, but how quickly an organization can restore its critical business services (referred to in this paper as minimum viable company, or MVC) using verified clean data.

It is the missing link between cybersecurity and business continuity, and it highlights a pressing truth: Many organizations today face a cyber resilience gap – a dangerous disconnect between disaster recovery readiness and actual recovery assurance.

Executive Summary

Commvault + kyndryl

For senior executives, MTCR offers an opportunity to reshape how recovery is understood, managed, and planned for. It reframes resilience from a purely IT-led function into a strategic business capability that spans cybersecurity, operations,
and risk.

Importantly, it challenges leaders to push their IT teams to move beyond "restore speed" and start thinking in terms of data trust, system integrity, and clean recovery timelines.

MTCR as an evolving business management concept should matter to the boardroom for the following reasons:

- It addresses the board's growing concern: "If we suffer a breach, how do we know we're not restoring compromised data?"
- It changes the narrative from IT recovery metrics to business service continuity.
- It promotes alignment between cybersecurity, infrastructure, and business leadership.
- It enables risk-based prioritization of critical services, supporting regulatory obligations (DORA, NIS2, UK Cyber Resilience Act) and improving audit and insurance readiness.

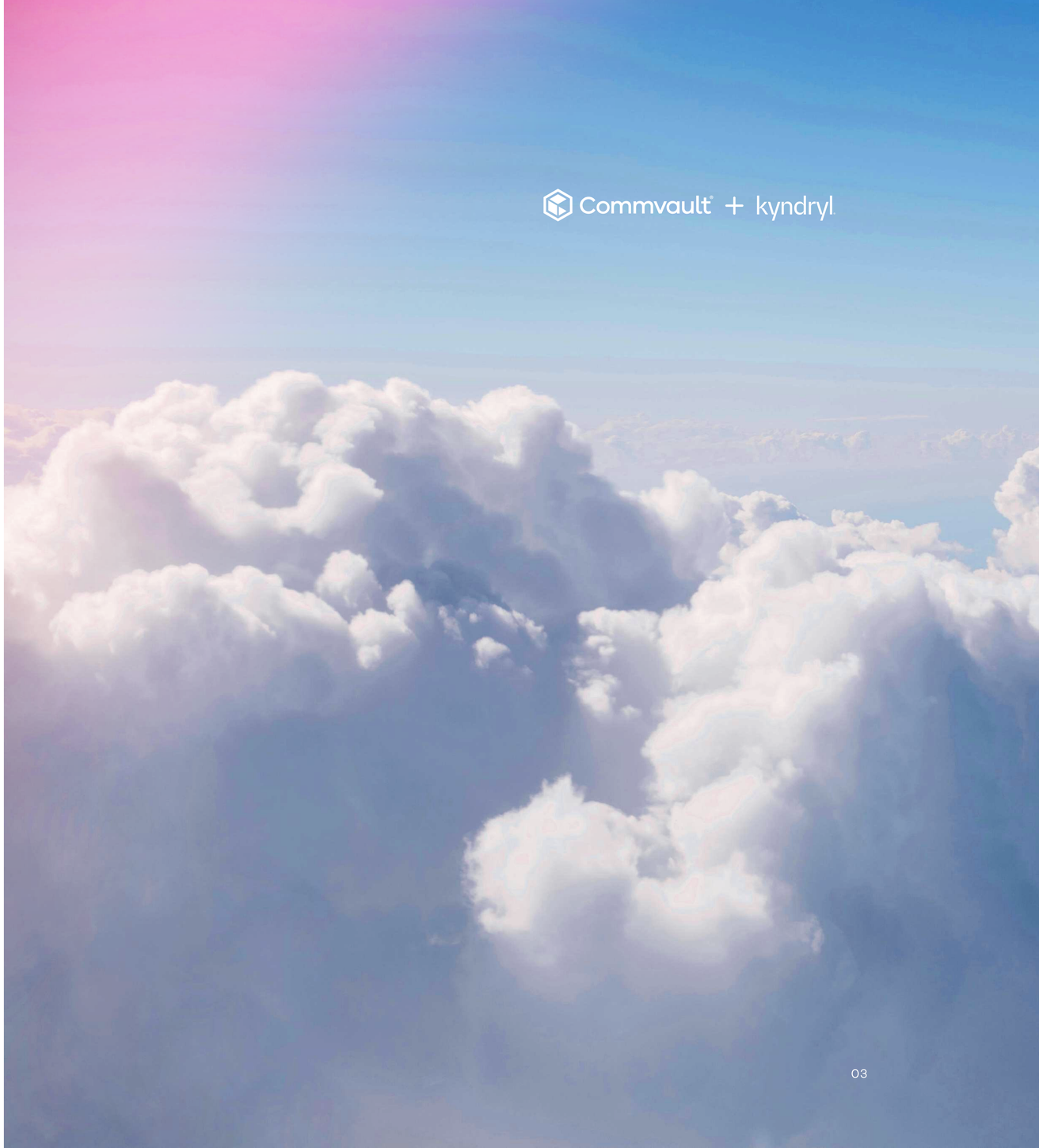
Business executives must now challenge their IT and cybersecurity leaders to think differently:

- Are we recovering with speed but risking reinfection?
- Do we know which systems and datasets are clean and usable after an attack?
- Have we tested our ability to restore the business processes – not just the servers or data?

MTCR encourages senior leaders to drive collaboration between SysOps and SecOps teams, transforming recovery from a fragmented operational task into a coordinated, strategic function. It highlights the need for collaborative planning, shared accountability, and integrated testing – because clean recovery is no longer a nice-to-have, it's a board-level mandate.

Executive Summary

Given that the true cost of reinfection is reputational, operational, and financial, MTCR is the new business standard for recovery success. Boards that embrace this thinking will not only be better protected but better prepared to respond with confidence when the worst happens.



The Cyber Resilience Gap

Commvault + kyndryl

Cyber threats continue to evolve in both in scale and complexity. From ransomware to data wipers and supply chain manipulation, organizations are increasingly dealing with attacks that not only disrupt operations but also poison the vital tools used for recovery.

Backup and recovery systems, once assumed safe, are often compromised or hold dormant threats only to be discovered at the worst possible time – when you need to recover.

Despite this, many recovery strategies still revolve around RTO and RPO. These metrics assume that recovery data is usable, intact, and trustworthy. In reality, this data has often become infected, encrypted, or subtly altered during a cyberattack. Restoring them without proper validation can reintroduce a threat – or worse, entrench it.

All of this can have a profound impact on recovery times, with organizations entering into a "trial and error" cycle while attempting to find the last clean backup.

The only conclusion that we can draw from all of this is that most organizations have a cyber resilience gap today and that their backup infrastructures lack modern cyber resilience features to secure, validate, and recover their organizational data at scale.

To make even clearer the distinction between an organization that has embraced a mature approach to cyber resilience and one that still shows gaps in approach, consider the following:

A Mature Cyber Resilient Organization Would Likely

Detect the breach quickly with SysOps and SecOps teams working collaboratively.

Isolate affected systems as a matter of standard process.

Perform recovery of prioritized systems from proven and clean backup data.

Resume operations with minimal downtime following initial restore.

An Organization with Cyber Resiliency Gaps Might

Take days to detect a breach.

Discover backups are compromised only after the breach.

Have no clear recovery plan.

Suffer prolonged downtime and reputational damage.

Even a cursory look into cyber breaches that occur quickly reveals that most affected organizations fall into the second camp. Rapid transformation is required in order to enable businesses to "bounce back" should a cyber catastrophe occur.

Start thinking in terms of data trust, system integrity, and clean recovery timelines.

Rapid transformation is required in order to enable businesses to "bounce back" should a cyber catastrophe occur.

Introducing mean time to clean recovery process

Commvault + kyndryl

MTCR is defined as the average time required to restore previously defined critical business applications, their foundational systems, infrastructures, and associated clean, validated data following a cyber event. It represents a shift from focusing solely on how fast and how recent the data is, to verifying how trustworthy the data is before it re-enters a production environment.

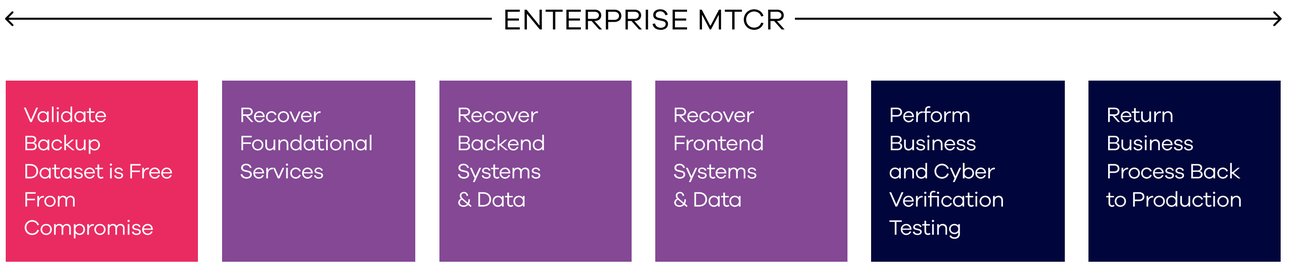
To achieve clean restoration of important business services, we must include aspects of recovery that are often missed as part of traditional disaster recovery techniques. These include but are not exclusive to:

- Performing forensic scans and integrity checks on infrastructure components, applications, and data.
- Identifying whether data is safe to restore.
- Validating systems and application behavior in sandbox environments.
- Isolating clean versions from infected or altered datasets.

Importantly, MTCR complements RTO and RPO. Together, the old concepts and the new can form a triad of modern recovery assurance, leading to improved cyber resilience and, very importantly, improved business recovery times.

The concept of MTCR shifts focus to a more mature and dependable approach to recovery. It assumes that compromise has occurred and that time is needed to validate, verify, and trust the data before it is restored.

MTCR introduces a set of activities that, when executed methodically, provides confidence that the recovery data is free from embedded threats. This may involve scanning backups with multiple malware detection engines, running restored instances in isolated sandboxes, and verifying logs and behavioral indicators. It also may include consulting with threat intelligence teams to account for emerging malware signatures or TTPs (Tactics, Techniques, and Procedures).



MTCR formalizes a previously informal or ad-hoc process.

By making the clean data check part of the recovery metric, organizations can build repeatable, auditable processes that align IT, cybersecurity, and business continuity disciplines.

Implementing MTCR: Practical Considerations

Commvault + kyndryl

Cyber resilience frameworks such as NIST, NSCS CAF Enhanced, and ISO 27001 and regulations such as DORA, NIS2, and the upcoming UK Cyber Resilience Act are evolving to reflect the need for assurance in recovery. MTCR fits naturally into these frameworks by introducing enhancements to the response and recovery phases (in the case of NIST).

MTCR should be seen as a business concept, not a measure of IT delivery success. This allows business leaders to define realistic recovery objectives for when critical business services need to be recovered from proven clean data. Importantly, the entire technology stack covering an entire business service needs to be considered.

The Five Pillars of MTCR Implementation

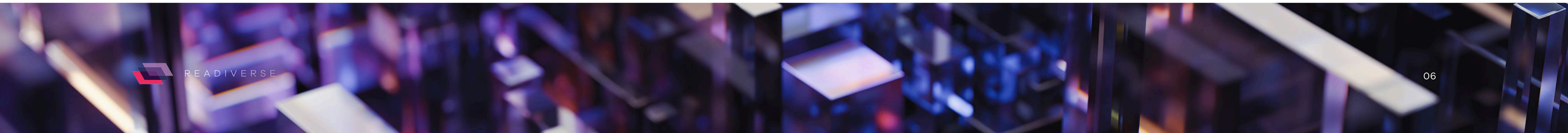
01 Establish clean recovery environments.
Modern attacks require isolated recovery environments (IREs) or "cleanrooms" – compute and data storage infrastructure physically or virtually separated from production environments. Without an IRE, MTCR timelines extend to days or weeks as forensic teams certify complex hybrid environments as "clean."

02 Identify and validate clean data.
Attackers often compromize environments for weeks before launching attacks, seeding payloads in backup sets. Indicators of Compromise (IOC) scanners and anomaly detection engines must automatically scan backup sets to identify clean restoration points, avoiding the trial-and-error cycle of testing multiple backups.

03 Enable adequate recovery performance.
Enterprise backup solutions have become commodity tools designed for compliance, not catastrophic recovery. Organizations face the stark reality of highly consolidated business processes s upported by low-cost backup systems that can take 10+ hours per TB to restore, scaling to weeks for enterprise-sized services.

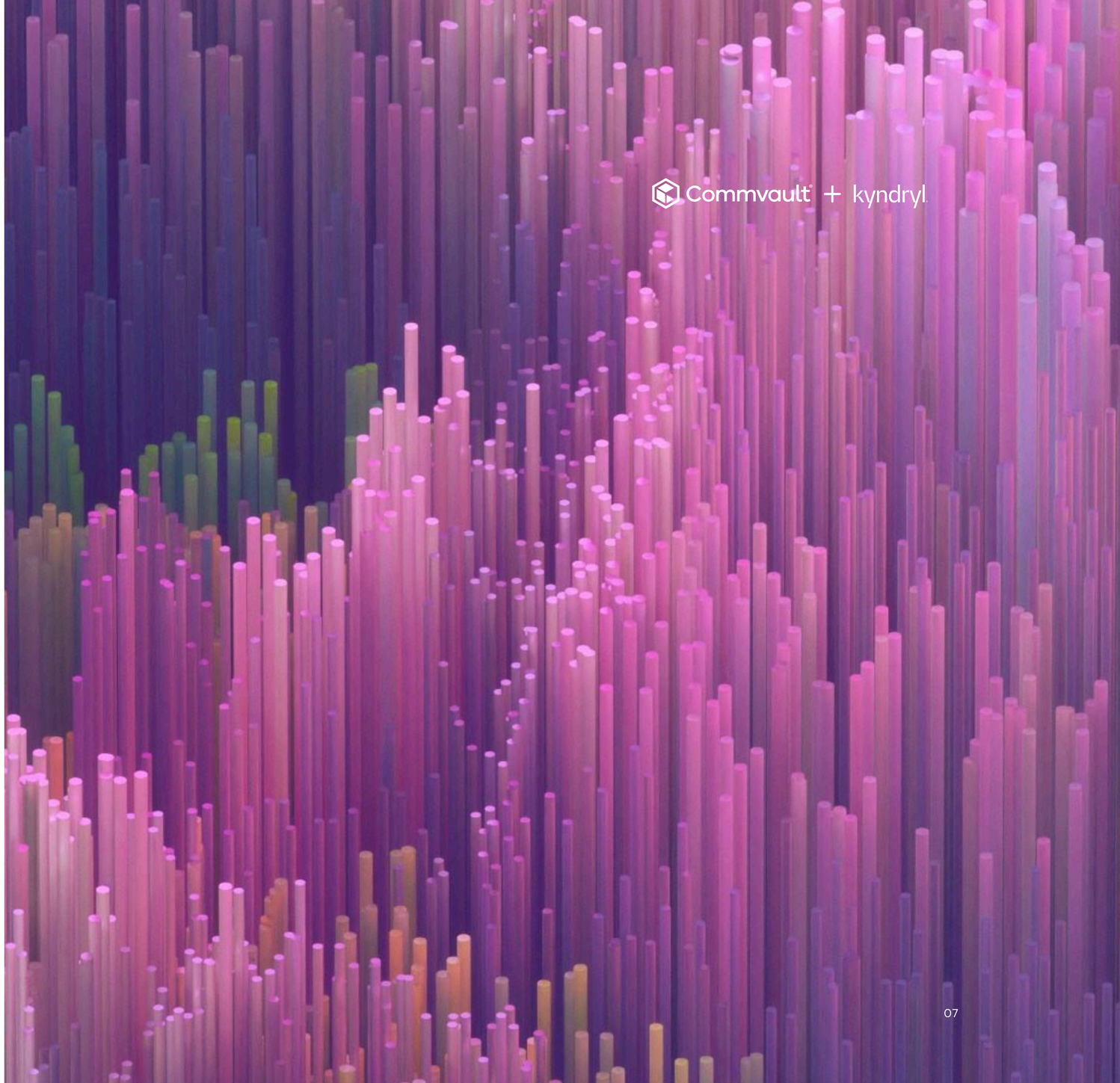
04 Maintain data integrity across platforms.
Recovery involving systems with different backup timestamps creates data integrity challenges across hybrid environments. Effective cyber recovery plans must address sequencing, interdependencies, and require application teams to validate recovered systems – factoring in team availability during crisis scenarios.

05 Define and test acceptance criteria.
Organizations must pre-define their MVC – all services and functionality needed to "stay alive" after an attack. Clear, comprehensive test criteria for service acceptance prevents rushing to restore without proper validation, which can reintroduce attack remnants.



For almost all organizations, implementing MTCR represents significant change. While many have mature disaster recovery plans for physical disasters, most lack enterprise-wide cyber recovery plans that address data cleanliness and integrity following cyberattacks.

An enterprise-wide cyber recovery plan defines how an organization will recover critical business services, associated sequencing, and testing procedures to confirm successful restoration. A mature cyber recovery plan enables organizations to recover critical business systems supporting their MVC.



Benefits of Adopting MTCR

MTCR provides a strategic tool for building cyber resilience. It facilitates proper discussion between boards of directors, business process owners, and IT teams. It also puts into context the complex challenges of recovering the data and systems that support critical business services while setting realistic expectations about recovery timelines.

Organizations that adopt MTCR gain reduced risk posture and stronger resilience maturity, not just in technical recovery but also in stakeholder confidence, audit readiness, and cyber insurance negotiations.

Boards are now reguarly asking harder questions about recovery: “Can we trust the data we’re restoring? Can we REALLY recover in a reasonable amount of time following breach?” MTCR offers a concrete way to answer these questions even if the initial answers are hard to hear.

For CISOs and CIOs, MTCR becomes a metric that bridges risk and operations. For CFOs, it reduces the potential cost of reinfection and unnecessarily prolonged downtime. For IT teams (both SysOps and SecOps), it creates a framework that justifies investment in backup validation, sandboxing, and forensic tooling.

Adopting MTCR leads to:

- Greater confidence in recovery outcomes.
- Reduced risk of reinfection or data corruption.
- Tighter aligment between IT and security teams.
- Improved readiness for audits, compliance, and cyber insurance.
- A differentiated cyber posture that speaks the language of both operations and risk.

Strategic Implementation Framework

Commvault + kyndryl

Embedding MTCR within an organization is a transformational initiative. It is a deliberate shift in mindset from “how fast can we restore?” to “how fast can we trust what we restore?” It is not an IT project. It is a cross-functional program spanning governance, architecture, incident response, and business continuity.

To institutionalize MTCR, senior leaders must take five key actions:

Organizations that adopt MTCR gain reduced risk posture and stronger resilience maturity, not just in technical recovery but also in stakeholder confidence, audit readiness, and cyber insurance negotiations.

Elevate MTCR to the boardroom.
Make MTCR a core part of cyber resilience KPIs.
The board should understand what clean recovery means, how it differs from traditional DR, and why it matters in a modern regulatory and threat landscape.

Define the MVC.
Map and document the critical business services that must survive any cyber catastrophe. Identifying dependencies, sequencing, and minimum viable functionality. Recovery of these should be your MTCR benchmark.

Create unified recovery governance.
SysOps and SecOps must not operate in silos. Recovery processes should be co-owned, jointly tested, and consistently reviewed. CIOs and CISOs must co-sponsor clean recovery plans and exercises.

Fund the cyber resilience stack.
Cyber recovery requires more than backup hardware. It demands sandboxing, anomaly detection, forensic tooling, and isolated recovery environments. MTCR is unachievable without investment in a full-spectrum cyber resilience platform.

Operationalize the process.
Move MTCR from whiteboard to playbook. Document clean recovery procedures, define roles, automate IOC scanning, and set MTCR targets by business service. MTCR must become a tested, repeatable process, not an aspiration.

The Road Ahead: MTCR and the Future of Cyber Resilience

Commvault + kyndryl

The path to cyber resilience is no longer defined by perimeter defense or traditional backup reliability alone. Since adversaries can now weaponize not just your data but also the infrastructure and processes designed to restore it, recovery must evolve. MTCR provides the business-aligned lens through which this evolution must happen.

Just as DevSecOps redefined collaboration across development and security, MTCR can be the catalyst for breaking down operational silos in the era of resilience. It creates a shared language where the board, CISO, CIO, and business process owner can talk about risk in real-world, outcome-oriented terms.

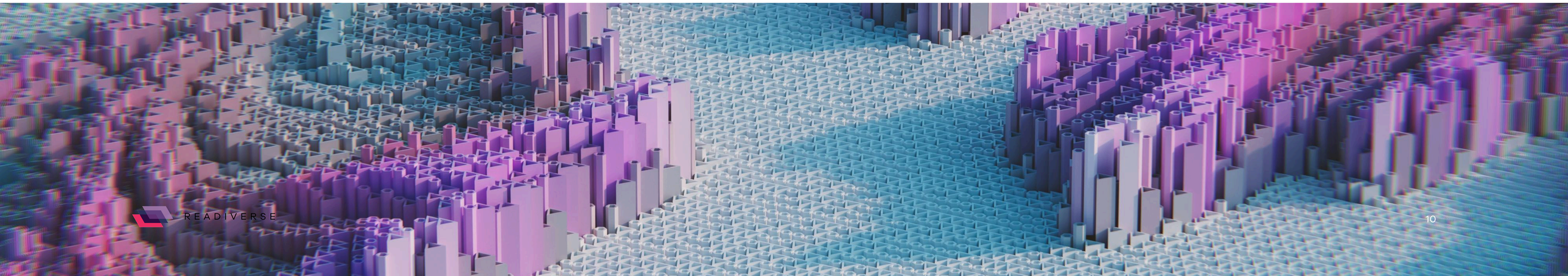
The adoption of MTCR will shift recovery conversations from vague assurance ("we have backups") to measurable confidence ("we know how long it will take to restore service from clean data"). It reframes compliance from checklist to capability. Most importantly, it removes ambiguity from one of the most critical business questions of our time: "How ready are we to come back from a cyber disaster?"

MTCR is not a niche metric. It is the clearest expression yet of what it means to be cyber resilient in an era

- of pervasive compromise. It empowers organizations to:
- Respond to ransomware without panic.
- Rebuild with integrity, not guesswork.
- Restore operations in hours or days, not weeks.
- Demonstrate resilience to customers, regulators, and insurers.
- Avoid the crippling cost of reinfection and reputational loss.

Recovery is no longer the final chapter in an incident. It is the true test of your cyber resilience strategy. Those that embrace MTCR will not only recover faster, they will recover smarter, cleaner, and more credibly.

As an executive leader, you have a choice. Will you allow your organization to be measured by outdated recovery assumptions? Or will you lead the charge toward a new, strategic era of clean recovery, one that defines your organization's resilience in the moments that matter most?



About the Authors

Duncan Bradley, Associate Partner, Kyndryl Security & Resiliency Practice Leader

Duncan Bradley, with over 28 years of experience, has a proven track record in supporting large global enterprise customers across the US, Europe, and Asia. His global experience in cyber resilience makes him a valued asset in advising on "Protect & Detect" as well as "Respond & Recover" strategies to ensure customers are prepared before real-life events occur. As a thought leader in modern cyber tolerant recovery solutions, he advises Kyndryl's strategic customers on ensuring data recoverability is built into their enterprise systems designs to prepare them to recover from the modern cyber threats they face.

Darren Thomson, Field CTO, Commvault

Darren Thomson is the field chief technology officer for EMEA and India at Commvault. In his role, Thomson is helping to shape a new era of data protection and deliver industry-leading threat detection and rapid recovery capabilities.

Before joining Commvault in January 2024, Thomson led the product marketing organization at identity and access management company One Identity. Prior to this, he helped shape the cyber insurance industry through his work at CyberCube and Lloyds of London, after spending many years gaining experience in senior executive roles at Symantec and Veritas.