DATA RESILIENCY

WHY CYBER SECURITY & BACKUP MUST CONVERGE

Building a foundation for operational confidence in a disrupted world

By Velocity Technology Group

Contents

Introduction: Why Data Resiliency matters

Modern organisations must assume disruption. Cyber attacks, cloud outages, human error, misconfiguration and supplier failures are no longer rare events. They are part of normal operating risk.

Many organisations invest heavily in cyber security controls, while others focus primarily on backup and disaster recovery. Increasingly, both approaches prove insufficient on their own. Data Resiliency brings these disciplines together. It focuses on protecting data wherever it exists, reducing the impact of incidents when they occur, and ensuring organisations can recover operations quickly and with confidence.

Data Resiliency is not a single tool. It is an organisational capability that unifies protection, risk reduction and recoverability across the modern estate, including hybrid infrastructure and cloud and SaaS platforms.

Chapter 1

The shift from prevention to resilience

Traditional security models were designed to stop attacks. They were built for static environments, fixed networks and clearly defined perimeters, where systems were predictable and the boundary between “inside” and “outside” was clear.

Today’s reality is different. Identities are the primary control plane, endpoints are mobile and remote, cloud platforms host business-critical services, collaboration systems hold sensitive data, and third-party access is unavoidable. In this environment, disruption does not only come from cyber attacks. Cloud outages, misconfiguration, human error and supplier failures are part of normal operating risk.

This is the critical shift. Modern organisations can be well protected and still be disrupted. Prevention remains essential, but it is no longer sufficient on its own because incidents now include a wider range of causes and compound effects. A single issue can cascade: a user compromise becomes identity misuse, identity misuse becomes access expansion, access expansion becomes operational disruption, and operational disruption becomes a recovery challenge.

No matter how strong prevention controls are, incidents still happen. Resilient organisations assume this and focus on how quickly they can recover when controls fail. That recovery focus is not a surrender. It is a realistic acknowledgement of the complexity of modern IT estates and the speed at which risk can materialise.

This is why Data Resiliency is becoming the new baseline. The goal is not simply to “stop bad things”, but to ensure the organisation can operate through disruption, limit impact and restore normal service predictably.

In practice, this shift changes how leaders think about investment and governance:

- Security becomes about reducing likelihood and blast radius, not just deploying tools.
- Backup becomes about proven recoverability, not just backup jobs completing.
- Resilience becomes an operating capability owned across IT, security and leadership, not a document on a shelf.

Reduce risk

Reducing risk means limiting blast radius through visibility, monitoring, governance and least-privilege access, so that when something goes wrong it does not spread further than it has to. This is where oversight matters, because many failures are not “no security”, they are “security that drifted”, “alerts that were missed”, or “controls that were assumed to work but were never validated”.

This layer is also where organisations build operational discipline: knowing what matters most, tracking posture, and continuously closing gaps rather than reacting only after incidents.

Recover

Recover means restoring data, identities, systems and services quickly, safely and with confidence. If any one of these is missing, resilience breaks down. It is not enough to restore files. Modern organisations must recover operational capability, which often depends on identity, access control, cloud configuration and collaboration platforms.

This is why Data Resiliency emphasises that cloud and SaaS availability is not the same as data recoverability, and why independent protection is required. Backup and Disaster Recovery is no longer a compliance exercise. It is a core business continuity capability that ensures operations can recover quickly and predictably from data loss, system failure or major disruption.

Data Resiliency therefore requires an explicit mindset shift:

- Cloud and SaaS availability is not the same as data recoverability.
- Backups are only meaningful if recovery is fast, reliable and trusted.
- Identity and access recoverability must be treated as first-class resilience requirements, not hidden assumptions.

Chapter 3

Why recovery is a security capability

Recovery is no longer an IT afterthought. It is a core security requirement. Modern attacks aim to disrupt operations, destroy trust in data, and compromise recovery paths. Even outside of cyber incidents, organisations face disruption through system failure, accidental deletion, cloud service interruption, misconfiguration and insider risk.

This changes the role of recovery. It is not only something you do after an incident. It is something you design as part of security, because it determines how bad an incident becomes.

Security controls reduce likelihood. Recovery capability limits impact. The organisations that recover fastest are not the ones with the most tools, but the ones with tested, trusted recovery capability aligned to business priorities.

This is where many strategies fail, because organisations often discover weaknesses only when recovery is required. Common challenges include incomplete or unverified backups, assumptions that cloud and SaaS data is protected by default, and recovery objectives that cannot be met in practice.

A resilient organisation treats recovery as a security capability by ensuring:

Recovery objectives reflect business impact, not technical convenience.

Recovery works across real environments, including on-premises workloads, Azure workloads and Microsoft 365 data.

Recovery planning covers operational scenarios that occur frequently, such as user error, system failure, cloud disruption, insider risk, major incidents and ransomware.

Recovery is validated through testing and reporting, because resilience must be demonstrated, not asserted.

Backup jobs running in the background do not equal resilience. Resilience is the proven ability to restore services and data under pressure, in the right order, without introducing new risk.

In a modern, identity-driven environment, recovery becomes inseparable from security. When organisations accept that reality, they stop treating recovery as a separate “IT function” and start treating it as what it truly is: a business-critical security capability.

Chapter 4

Why cyber security and backup must converge

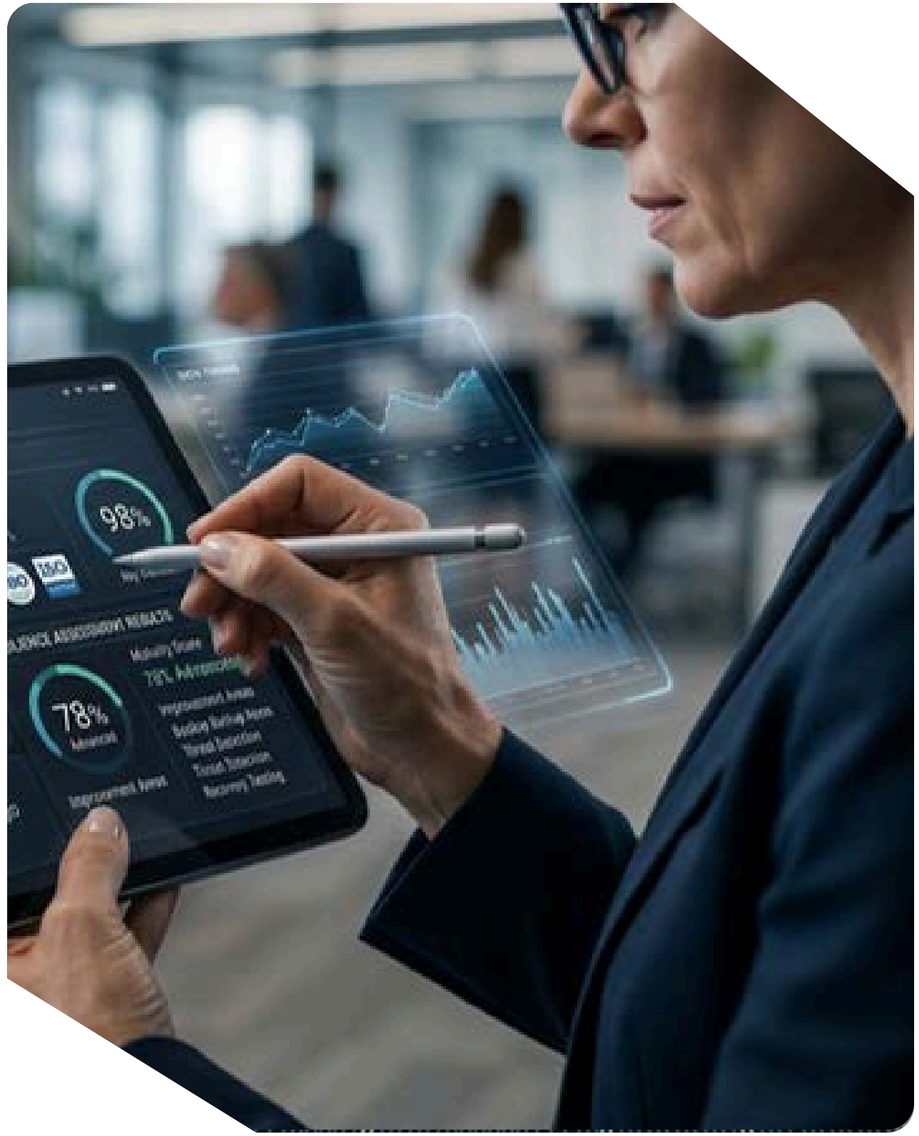
Many organisations treat cyber security as one programme and backup as another. This creates a dangerous gap.

Cyber security programmes often focus on preventing compromise and detecting threats, but do not verify that recovery paths remain usable under attack. Backup programmes often focus on coverage and retention, but do not account for modern identity-driven attacks or the possibility of malicious deletion, encryption, or operational pressure during recovery.

A resilient foundation requires both:

- Controls that reduce the probability and blast radius of incidents across people and identities
- Recovery capability that restores services predictably across on-premises, cloud and SaaS environments

Backup is required far more frequently than most organisations expect, and not only for ransomware. Recovery capability must cover user error, system failure, cloud disruption, insider risk, site-level incidents and ransomware.



Chapter 5

When recovery defines the crisis

Lessons from recent incidents (M&S, JLR, Travelex)

Incidents rarely become crises at the moment of compromise. They become crises when organisations cannot restore operations quickly, safely and confidently. This is where the convergence of cyber security and backup becomes decisive.

To the right are recent, recognisable examples that illustrate a consistent theme: the recovery phase drives the true business impact.

The shared lesson

Across these incidents, the most material business damage occurs during recovery: uncertainty, operational disruption, and the time it takes to restore safe, normal service. Data Resiliency exists to prevent recovery becoming the crisis.

MARKS & SPENCER: DISRUPTION BECOMES A QUANTIFIED PROFIT IMPACT

Marks & Spencer stated that a cyberattack would result in an estimated £300 million impact on group operating profit for the year. The same report noted the incident brought online activity to a standstill and that disruption was expected to continue into July.

Independent analysis also described an estimated £300 million profit hit and reported that the company aimed to have online shopping back to normal by August, illustrating how long recovery can take.

Data Resiliency takeaway: prevention matters, but resilience depends on operational recovery. The longer it takes to restore normal service, the larger the financial, customer and reputational impact becomes.

JAGUAR LAND ROVER: CYBER DISRUPTION BECOMES SUPPLY CHAIN DISRUPTION

The Cyber Monitoring Centre categorised the Jaguar Land Rover incident as a Category 3 systemic event, estimating a UK financial impact of £1.9 billion and stating that it affected over 5,000 UK organisations through supply chain and downstream impact.
It also states the incident impacted JLR's internal IT environment, leading to an IT shutdown and a halt in global manufacturing operations, including major UK plants, with a controlled, phased restart during recovery.

Data Resiliency takeaway: in modern environments, digital disruption can halt physical operations. Recovery is not just "restore IT". It is re-establishing operational continuity across systems, suppliers and downstream dependencies.

TRAVELEX: RANSOMWARE FORCES MANUAL WORKAROUNDS AND EXTENDED RESTORATION

CNBC reported that Travelex experienced a ransomware attack which led the company to take "all our systems offline", and that staff in some locations handled transactions with pen and paper.

CyberScoop reported that nearly two weeks after the incident, Travelex said it had restored some digital capabilities and was making progress with recovery after suspending online services and internal systems.

Data Resiliency takeaway: ransomware is not only a security event. It is an operational continuity event. Recovery timelines can extend into weeks, and workarounds become part of business reality until systems are restored safely.

Chapter 6

Data Resiliency self-assessment checklist (short form)

Use a simple maturity lens to assess proven capability, not planned improvements.
The purpose is clarity. Inflated confidence delays action and increases exposure.

Ask:

- [ ] Are recovery objectives defined and tested against realistic scenarios?
- [ ] Can identities and access controls be recovered if compromised?
- [ ] Are endpoints covered by protection and recoverability at scale?
- [ ] Is Microsoft 365 and collaboration data independently protected, not assumed?
- [ ] Are backups verified, tested and trusted for recovery?
- [ ] Is recovery designed for ransomware as well as everyday failures such as deletion, corruption and outages?

Chapter 7

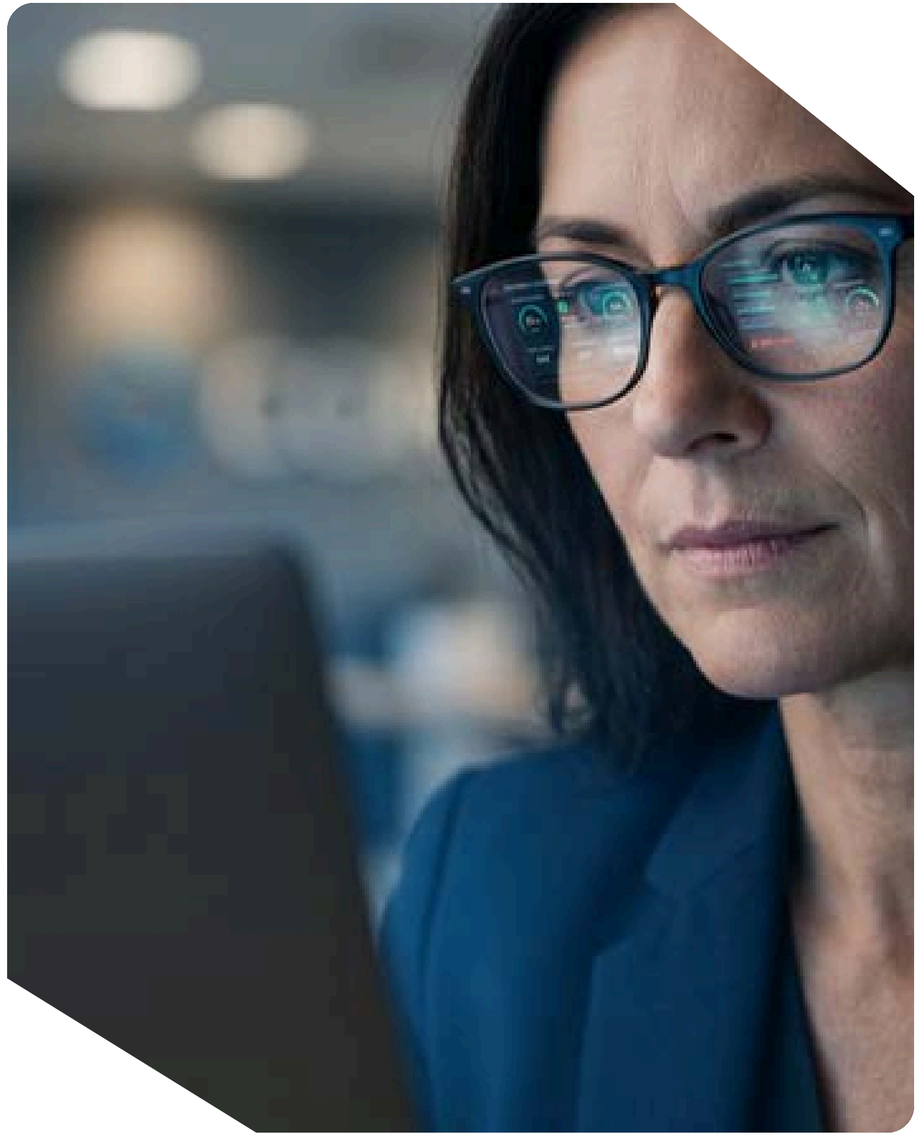
Building a resilient operating model

Data Resiliency is not a technology investment. It is an operating capability that determines how an organisation performs during disruption.

A resilient operating model includes:

- Recovery aligned to business impact, using explicit objectives owned by the business
- Explicit coverage of identity and access recoverability
- Independent protection for cloud and SaaS data (not assumptions)
- Regular testing and reporting of outcomes
- Clear ownership across IT, security and leadership governance

Resilience must be demonstrated, not asserted. Regular, realistic testing should be supported by clear reporting, defined ownership and visible improvement over time.



Chapter 8

How VTG supports a Data Resiliency foundation

Practical convergence, delivered as an operational capability

A Data Resiliency foundation requires cyber security and backup to operate as one discipline. VTG's approach combines:

Holistic cyber security that strengthens the control plane

VTG's cyber security model focuses on reducing organisational risk across people, identity, technology, oversight and compliance.
This includes Human Risk Management, identity consulting and audits, and continuous improvement of security posture through Secure Score monitoring and remediation.

Independent oversight and monitoring to reduce blind spots

Velocity SOS provides independent, continuous oversight designed to detect suspicious activity and support layered defence strategies.

Backup and Disaster Recovery designed for trusted recovery

VTG designs Backup and Disaster Recovery around real environments across on-premises, cloud and SaaS, aligned to business impact and recovery objectives.
It explicitly addresses common failure points such as incomplete or unverified backups and assumptions that cloud and SaaS data is protected by default.
It also plans for a wide range of recovery scenarios including accidental deletion, system failure, cloud disruption, insider risk, major incidents and ransomware.

The outcome

The outcome is a tested, trusted recovery capability that complements cyber controls and provides confidence that the organisation can recover from data-impacting events predictably.

Closing: Turning resilience into confidence

Data Resiliency gives organisations confidence to operate through disruption, recover without panic, protect customer trust and support long-term growth.

The question is no longer “Can we stop everything?”

It is “Can we recover cleanly, confidently and fast enough to protect the business?”

Speak to a Data Resiliency Expert

VE·LOC·I·TY
TECHNOLOGY GROUP

https://thevtg.com
info@thevtg.com