Cyber Resilience Workshop

Attendee Pack

READIVERSE

Commvault®

TABLE OF CONTENTS

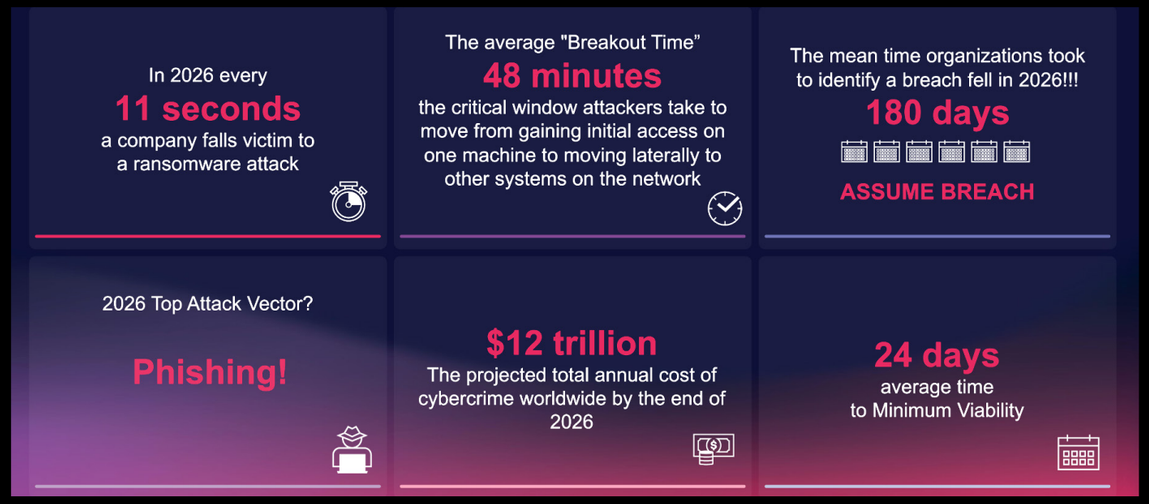
WHAT IS CYBER RESILIENCE?

Cyber resilience is best understood as an organizational capability—not a backup feature. NIST defines **cyber resiliency** as "the ability to **anticipate, withstand, recover from, and adapt** to adverse conditions, stresses, attacks, or compromises affecting cyber-enabled systems." [1]

This matters because many organizations can restore data but still fail to restore **trusted operations** (e.g., identity, access, clean infrastructure, validated applications) fast enough to meet business needs, or they restore too quickly and reintroduce compromise.

To be cyber resilient, organizations must look beyond backup and disaster recovery. Organizations must assume:
- You will be attacked
- Defenses will fail
- Recovery must be planned for chaos, not perfection

The new reality facing organizations is with the rapid implementation of AI we are facing increasingly difficult, modern threats which may include:
- Ransomware
- Phishing
- Insider threats
- AI poisoning
- Supply chain compromise



Sources:
- In 2026 every **11 seconds**, a company falls victim to a ransomware attack. Ransomware Will Strike Every 2 Seconds By 2031 | Ransomware Clock
- **48 minutes** is the average **"Breakout Time"**—the critical window attackers take to move from gaining initial access on one machine to moving **laterally** to other systems on the network. CrowdStrike 2025 Global Threat Report
- The mean time organizations took to identify a breach fell in 2025 to **181 days**. **Always Assume Breach!** (do the math) | 2025 IBM cost of a data breach report
- Phishing is still the #1 top attack vector, closely followed by hacking, supply chain compromise, and malicious insider threats. 2025 IBM cost of a data breach report | Deloitte Cyber Threat Trends Report 2025
- $12 Trillion is the projected **total annual cost of cybercrime worldwide by the end of 2026, making cyber crime the third largest economy in the world,** behind USA and China. 2025 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics

WHAT IS CYBER RESILIENCE?

24 days is the average time to MINIMAL VAIBLE RECOVERY (MVR)

MVR shifts focus from "restore everything" to: "Restore what keeps the business alive."

Restore only:
- The critical systems and data required to operate
- In the correct order
- Within an acceptable time window
- Enabling the business to function while full recovery continues

Common cyber recovery myths that today no longer hold up and are dangerous assumptions.

Myth	Reality
"Our firewall keeps us safe."	Threats bypass perimeter defenses.
"Our DR plan covers cyber recovery."	Traditional DR ≠ cyber recovery.
"RTO/RPO define success."	Clean recovery + integrity validation matter more.
"Backups will always be there."	Backups are often targeted first.
"Immutable storage is enough."	Immutability without isolation is insufficient.
"Paying ransom guarantees data return."	There is no guarantee.
"Cyber insurance covers everything."	Policies often have exclusions and conditions.

Teams need to be clear and aligned:
1. **Clarity on what "good" looks like** (clean, available, prioritized, validated recovery),
2. **A Cyber Resilience plan structure** that assigns roles, decisions, and evidence, and
3. **A repeatable proving loop** (tabletop + technical recovery testing + continuous improvement).

Key takeaway: Data recovery is only half the battle. Recovery must ensure:
- Clean data
- Secure restore environments
- Validated integrity
- Business continuity

NIST's Cybersecurity Framework (CSF) 2.0 supports this outcomes-first approach by providing a risk-management taxonomy (including governance) that organizations can tailor; it does not prescribe specific implementations, but it helps align stakeholders on outcomes and maturity. [2]

RECOVERY TYPES EXPLAINED

The Cyber Resilience Workshop explained the differences between the different types of recovery.

	Operational Recovery	Disaster Recovery	Cyber Recovery
Scope	Individual components	Site-specific systems and infrastructure	Cyberattacks
Examples	Recovering deleted files, application crashes	Server room fire, earthquake, flood	Data breach, ransomware attack, malware infection
Goals	Decrease downtime, resume normal operations	Business continuity, protect critical data, recover quickly	Minimize cyberattack damage, reduce data loss, recover only clean data
Methods	Granular backups, point-in-time recovery	Full system backups.	SIEM, cyber recovery plan, anomaly detection, Cleanroom, full system.
Recovery Copy	Primary copy of data for fast, local recovery.	Secondary copy of data off-site for recovery from site-wide failures.	Tertiary copy of data air-gapped, immutable, indelible, and on someone else's infrastructure.

Recovery Type	Focus	Goal
Operational recovery	Deleted files, crashes	Resume normal operations
Disaster recovery	Site failure (fire, flood)	Restore infrastructure
Cyber recovery	Ransomware, breach	Recover only clean data

Recovery Copy Model
- Primary copy – local fast recovery
- Secondary copy – offsite site-level recovery
- Tertiary copy – air-gapped, immutable, isolated recovery

CYBER RECOVERY VALIDATION GOAL

Recover critical data from a secure, clean backup source into an isolated environment, perform forensic analysis to prove integrity and cleanliness, and confirm the recovered data is fit for production use.

GLOBAL STANDARDS AND REGULATORY DRIVERS

- **US:** NIST CSF 2.0, CISA, CMMC 2.0
- **EU:** NIS2, DORA
- **APAC:** RBI, MAS TRM, APRA CPS 234
- **Canada:** OSFI B-13
- **Japan:** FISC
- ISO/IEC 27001 (global standard)

RECOVERY TYPES EXPLAINED

INCIDENT RESPONSE AND RECOVERY TIMELINE

This timeline aligns with:

1. NIST SP 800-61r2's lifecycle framing (prepare, detect/analyze, contain/eradicate/ recover, post-incident), [14]
2. CISA's ransomware response checklist priorities (isolation, triage, evidence collection, team coordination), [25]

THE FOUR PILLARS OF CYBER RESILIENCE

Resilience leaders must have a proven and reliable CR Plan to assist with "decide and do" while under extreme pressure — Commvault suggests organizations should follow key milestones with "actionable" steps, we call these: The 4 Pillars of Cyber Resilience.

1. Logical Air-Gap and Immutable Storage:
The "air gap" concept is precise—and easily undermined by automation.
NIST defines an air gap as an interface where systems are not physically connected and any logical connection is not automated; data transfer occurs only manually under human control. [9]

An air –gap must have:
a. No physical connection to environment
b. No automated logical connection
c. Manual data transfer under human control
d. Enforced write-once, read-many protection
e. Restricted administrative access

Key lesson: "Offsite" does not automatically mean safe.

Action: verify whether your "offsite" or "isolated" backups are truly separated from compromised identity/admin planes. If your backup administrative path is reachable from production identity, treat it as potentially compromiseable and plan for a tiered copy strategy that includes a strongly protected, immutable, separated copy (a common pattern emphasized in Commvault's "air-gapped copies" guidance for minimum viability). [10]

Immutability alone is not a complete cyber recovery strategy.
Immutability helps prevent alteration or deletion, but cyber recovery also requires: identifying a last-known-good point, validating data cleanliness, and recovering into a space where compromise cannot immediately re-spread. Commvault guidance for minimum viability explicitly recommends air-gapped copies, frequent testing, establishing last-known-good practices, and isolated forensics/cleanroom usage. [11]

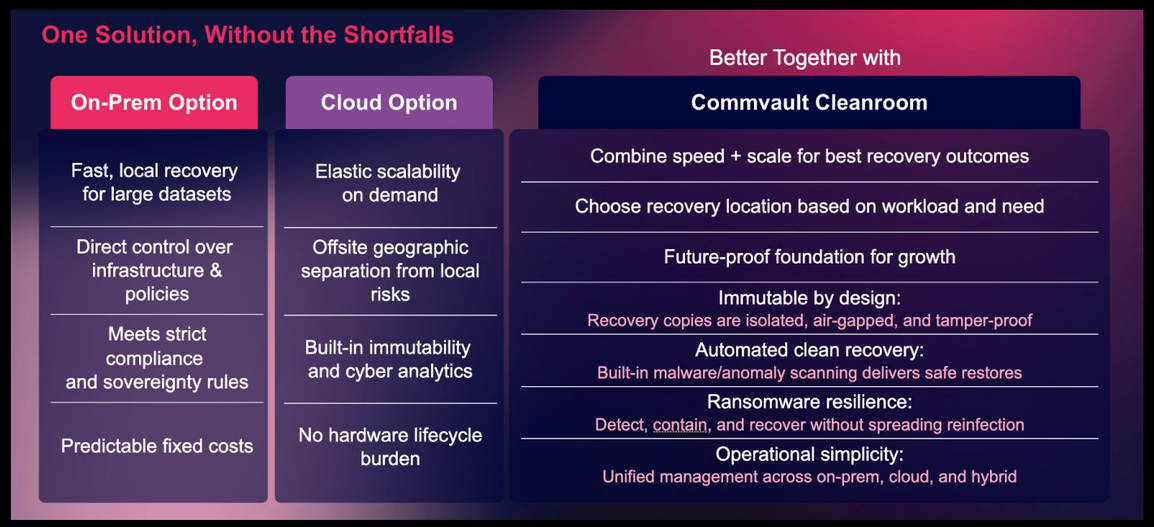
Action: pair "immutable storage" controls with a defined **clean-point selection and approval** step reflected in the workbook's "Last-known Safe Point" and "Cyber Recovery Approval Plan" fields. [3]

2. Isolated Recovery Environment (IRE)

An IRE is a secure, separate network environment designed to restore critical systems and data after a cyberattack. An IRE is a control boundary and should be used for both recovery and forensics:
- Restore clean backups
- Prevent reinfection
- Validate integrity
- Enable production failover
- NIST Definition

Action: treat "where will we restore?" as a high priority decision: the CR Plan template workbook explicitly prompts restoration targets as either in-place or IRE / Cleanroom. [13]

Commvault has a cleanroom / isolated recovery environment as a secure environment used for continuous testing, forensic investigation, and recovery into an isolated target when production integrity is uncertain. [12]



THE FOUR PILLARS OF CYBER RESILIENCE

3. Cyber Recovery (CR) Plan

Definition (NIST-aligned):
A documented set of procedures developed to restore and maintain resilience after a cybersecurity event. NIST SP 800-61r2 emphasizes establishing an incident response capability to detect incidents rapidly, minimize loss, mitigate exploited weaknesses, and restore services—covering preparation through lessons learned. [14]

A CR plan must include:
- Defined recovery roles ("cyber first responders")
- Hardened data protection environment
- Validated prerequisites
- Tested recovery dependencies
- Defined minimum viable recovery scope

Action: design your plan so it produces evidence (clean restore points, approval records, validation status), not just steps. This aligns with NIST SP 800-184's emphasis on recovery planning, playbooks, testing, and improvement after a cybersecurity event. [8]

Ensure your cyber recovery plan is a team sport, with named owners and alternates, plus offline contact methods—exactly what the Commvault workbook structure suggests (IT Director/Owner, Security Director, Coordinator/PM, Recovery Team, Forensic Analysis Team, and alternates). [3]

Align on CR definitions: Use consistent language across IT, security, and leadership
- Cyber resiliency: ability to anticipate, withstand, recover, and adapt. [1]
- Air gap: not physically connected; logical connection not automated; manual transfer under human control. [9]
- Incident handling lifecycle (practical anchor): preparation → detection/analysis → containment/eradication/recovery → post-incident lessons learned. [14]
- Cleanroom / isolated recovery environment: isolated place to test recovery, perform forensics, and recover clean data when production integrity is uncertain. [12]

4. Cyber Recovery (CR) Plan

The "Principles of Chaos Engineering" define chaos engineering as disciplined experimentation to build confidence in a system's ability to withstand turbulent conditions in production. [16]

Resilience is broader than recovery speed: it is trusted restoration under adversary conditions. NIST's definition explicitly includes "adapt" after recovery, which implies learning and improving—not merely returning to a prior state. [7]

Tabletop exercises and "chaos" validation are not optional maturity steps; they are how resilience is proven. Chaos testing validates that systems can withstand real-world attack failures — not just that they work under ideal conditions.

THE FOUR PILLARS OF CYBER RESILIENCE

Conducting tabletop exercises with ever changing cybersecurity scenarios (e.g., ransomware, insider threats, phishing), with objectives, scenarios, and discussion questions—makes it easier to operationalize recurring cyber resilience practices. "Tabletop exercises are a crucial component of a comprehensive cybersecurity strategy..."

NIST SP 800-161: CISA Statement: "Organizations that conduct exercises:
Contain and recover more quickly, and experience lower financial losses due to reduced downtime and data breaches.

A NOTE ON CYBER INSURANCE

Ransom payment and insurance are not reliable recovery mechanisms.

The FBI explicitly states it does not support paying ransom and warns that paying **does not guarantee** that you will get your data back. [17]

Cyber insurance can help offset some costs, but government and supervisory bodies note limits and exclusions—especially for systemic or "cyber war" categories—and the GAO highlights insurers taking steps to limit exposure to systemic attacks. [18]

Recovery Type	Focus	Goal
Operational recovery	Deleted files, crashes	Resume normal operations
Disaster recovery	Site failure (fire, flood)	Restore infrastructure
Cyber recovery	Ransomware, breach	Recover only clean data

COMMVAULT STEP-BY-STEP GUIDANCE: BUILD A CYBER RESILIENCE PLAN

Commvault has created the CR Plan Template to align to globally adopted primary guidance for incident handling and recovery planning: NIST SP 800-61r2 and NIST SP 800-184, and incorporates CISA/FBI operational guidance relevant to ransomware response and exercises. [4] [19]

Action: Attendees of the CRW are encouraged to download the **Commvault Cyber Resilience Plan Template** to provide guidance to create your organization's CR Plan.

Download

Resources:
- NIST cyber resiliency and air gap definitions (CSRC glossary)
- NIST CSF 2.0, NIST SP 800-61r2 (Incident Handling)
- NIST SP 800-184 (Event Recovery)
- CISA ransomware response checklists/exercises, and FBI guidance on ransom payment risk. [5]

Layout of the Commvault CR Plan template and instructions how to complete each section:

Section	Objective	Questions to complete	Questions to complete
Scope, assumptions, and minimum viability (added; bridges workshop → workbook)	Define what recovery must accomplish **first**, not eventually; establish how success will be measured	What business outcome must be restored first (e.g., order processing, patient care, trading)? What is the "minimum viable" set of apps/data/people to operate? What dependencies are often overlooked (identity, DNS, email, privileged access tooling)? What is the target time window for minimum viability? (Use a single agreed time unit for all teams.)	A one-paragraph mission statement + an initial "minimum viability stack" list (Top 10 services) aligned to Commvault's minimum viability framing (people/process/tech). [20]
Cyber Recovery Team (workbook: team roles & contacts)	Establish decision authority, alternates, and out-of-band communications	Who is the plan **owner**? Who declares activation? Who leads security determination of breach scope? Who coordinates cross-functional workstreams? Who restores systems? Who validates cleanliness? What is the communication method if "all systems are down"?	Completed team matrix with roles/responsibilities and emergency contact paths (including alternates). [3]
Vendors and critical external contacts (workbook: vendor table)	Ensure fast escalation and reduce "lost time" searching for contract and support info	What vendors are required to recover (backup platform, cloud storage, identity provider, IR retainer, forensics firm)? What are support numbers, account IDs, and entitlements? Do we have a "break glass" contract path if the primary procurement system is down?	Completed vendor list with support access instructions and key account identifiers, contact details. [21]
Awareness of attack (workbook: initial forensics and key facts)	Create a structured intake that supports containment, evidence preservation, clean-point selection, and leadership decisions	What is known about the incident (who/when/what they want)? What anomalies suggest dwell time? Which servers/apps are impacted and in what order must they be restored? What is the **last-known safe point** and who approves it? Is identity management compromised (which roles, degree of infiltration)? When should backup data aging be halted?	A single "incident facts & recovery triage" page that can be used during an event, with named approvers and timestamps. [22]
Recovery execution (workbook: recovery status tracking)	Track restoration readiness, targets, identity status, and validation so recovery does not reintroduce compromise	For each prioritized system: what's the machine name/owner/location? Is it production-ready (or needs remediation)? Will we restore **in-place** or into an **isolated recovery environment/cleanroom**? What is the identity management status and next step (rebuild/restore)? What is restoration/validation status and date?	A prioritized recovery board (spreadsheet or ticket view) that aligns each system to restore targets and validation evidence. [13]
Reintegration and production cutover (workbook: approvals)	Prevent premature reconnect; ensure leadership and security explicitly accept risk	What are the reintegration gates? Who approves return to production? What is the observability/monitoring period? What residual risks remain? What communications must occur (internal/external/regulatory) before cutover?	A reintegration checklist with named approvers and recorded decisions (time-stamped). [23]
Proving loop: tabletop + technical recovery + improvement (added; bridges workbook → operational reality)	Convert the plan from a document into a capability through recurring exercises and measured improvements	Which scenario(s) will we exercise first (ransomware, identity compromise, insider threat)? What are the success criteria (minimum viability restored, clean verified, reintegration approved)? How often will we test? What evidence is produced and stored? What gaps become funded backlog items?	An exercise schedule + metrics + backlog of resilience improvements. Use CISA exercise packages and/or ransomware checklists as structured prompts. [24]

COMMVAULT STEP-BY-STEP GUIDANCE: BUILD A CYBER RESILIENCE PLAN

© Commvault – Cyber Resilience Workshop Attendee Pack 2026

THE 1 PAGE CR PLAN ACTIVATION CHECKLIST

The Checklist is your "must-do" oriented steps and maps to the Commvault CR Plan Template's structure (team → awareness → recovery → reintegration), and integrates the proving loop.

Before an incident (preparedness)

- ☐ Define and document "minimum viability" (people + process + technology that must come back first). [20]
- ☐ Confirm at least one highly protected copy strategy that supports recovery even if production/admin identity is compromised (air-gapped + immutable concept). [10]
- ☐ Name the Cyber Recovery Team roles and alternates; validate offline contact methods. [3]
- ☐ Maintain a vendor/support list with account details accessible if core systems are down. [21]
- ☐ Schedule tabletop exercises using structured packages and questions; capture outcomes as backlog. [15]

When you suspect ransomware / cyber compromise (first decisions)

- ☐ Determine impacted systems and isolate immediately; if unable to disconnect, power down only as necessary (acknowledge evidence tradeoffs). [25]
- ☐ Activate incident response and the cyber recovery plan owners; start a single incident log. [26]
- ☐ Preserve evidence (e.g., system images/memory captures) and coordinate forensics. [27]
- ☐ Record "awareness of attack" facts: what happened, when, what the actor wants, suspected dwell time indicators. [3]
- ☐ Identify and approve last-known safe recovery point(s); document approver, timestamp, and rationale. [28]

Recovery and validation (restoring without reinfection)

- ☐ Decide restore target: in-place vs isolated recovery environment/cleanroom. [13]
- ☐ Restore secure access/identity services early (often a gating dependency). [29]
- ☐ Track recovery status + validation status for each prioritized system; do not promote "restored" to "ready" without validation evidence. [30]

Reintegration and after-action improvement

- ☐ Require explicit approvals to reconnect or resume production operations; document residual risk acceptance. [30]
- ☐ Capture lessons learned and feed improvements into the next exercise cycle; treat resilience as continuous. [31]
- ☐ Do not assume paying ransom solves recovery; it does not guarantee data return and is discouraged by the FBI. [17]
- ☐ Do not assume cyber insurance covers everything; systemic exclusions/limitations exist and vary. [18]

ROLES/RESPONSIBILITIES AND PRIORITIZED ACTIONS

This is phrased as "who does what by when," using the workbook's roles as the core operating model (IT Director/Owner, Security Director, Coordinator/PM, Recovery Team, Forensic Analysis Team, plus alternates). [3]

Short-term priorities
Ownership and structure come first because they are the gating factor for every technical improvement. NIST emphasizes preparation as the first phase of incident handling and stresses organizing an incident response capability. [14]

Primary actions: complete the Cyber Recovery Team matrix and offline contact method; complete vendor access list; define minimum viability; run first tabletop exercise (ransomware scenario) using CISA materials; ensure the organization's ransom/insurance assumptions are not treated as recovery strategy. [32]

Mid-term priorities
Shift from "plan drafted" to "capability proven." Commvault cleanroom guidance supports continuous testing and isolated recovery/forensics, which is the practical foundation for proving recovery without reinfection. [12]

Primary actions: establish or validate an isolated recovery environment/cleanroom target; implement and test clean recovery points; integrate recovery validation into routine operations; refine reintegration approvals; run at least one technical recovery test that restores minimum viability services. [33]

Long-term priorities
Mature governance and measurement. CSF 2.0 supports using profiles and tiers to communicate current and target maturity and to drive continuous improvement. [2]

Primary actions: formalize KPIs (including "clean recovery point age" and validated recovery time to minimum viability), expand exercise scope, integrate threat-informed defense learnings (e.g., MITRE ATT&CK for adversary behavior modeling), and align evidence/controls to applicable regulatory obligations (e.g., SEC incident disclosure expectations for public issuers). [34]

CR PLAN: COMPONENT ALIGNMENT TABLE

Plan component	Workshop Reminder	What "done" looks like (evidence)
Governance, minimum viability, and recovery success criteria	Minimum viability concept; resilience beyond backup	Minimum viability stack identified; target time window agreed; evidence locations defined. [35]
Cyber Recovery Team Named owners, alternates, and offline comms	"Planning is essential" reality; cross-functional execution	Filled role matrix + tested out-of-band contact method + alternates assigned. [36]
Vendors External dependencies and escalation paths	"Prepared until we're not" (avoid time loss)	Vendor contacts, contract IDs, and recovery-critical services listed and accessible offline. [3]
Awareness of Attack Incident facts, triage, safe point approval, identity compromise assessment	Detect/respond focus; last-known good; identity as a gating dependency	Time-stamped incident facts; safe point approval captured; identity infiltration assessment recorded. [37]
Recovery Restoration targeting (in-place vs IRE/cleanroom), status tracking, validation	Isolated recovery environment + validation; "recover only clean data"	Restore target documented; recovery + validation status tracked for each critical system; forensics evidence stored. [38]
ReIntegration Controlled return to production and risk acceptance	Adapt/learn; avoid reintroducing compromise	Reintegration approvals recorded; post-cutover monitoring plan executed; lessons learned documented. [30]
Consistency Exercises, chaos validation, and continuous improvement	Tabletop + chaos testing as ongoing testing and proof	Exercise calendar exists; after-action reports and improvement backlog maintained; repeat testing. [39]

REDUCE THE MEAN TIME TO CLEAN RECOVERY

If you follow the 4 pillars of cyber reslience you will see a decrease of mean time to clean recovery by 2.7%.

Commvault covers such a broad range of workloads it's common for organizations to consolidate from multiple systems to a centralized single platform with Commvault. On a recent Commvault customer survey, 54% of respondents consolidated to Commvault from 2 systems. 32% consolidated from 3 or more.

Consolidation to a centralized, unified resilience platform, especially with our unique innovation that accelerates rebuilding AND recovery … add it all together and it delivers the fastest mean time to recover, 2.7x faster recovery across the entire rebuild and recovery timeline.

"Commvault gives us the power to protect our data from various sources and formats from a single interface, drastically reducing the costs and efforts required for backups. Moreover, its proven recovery capabilities have saved us multiple times from ransomware attacks which could have been devastating." Ryan Sinnwell, the Weitz Company

Customer Case Study
Recently, an American logistics company was hit by a ransomware attack. Fortunately, they partnered with Commvault's IR team and were able to avoid a payout, continue operations, and recovered in 72 hours, not the 2 weeks the team thought. And on top of that they recovered 100% of the data. Commvault's fleet of engineers expedited recovery and allowed the customer's team to take much-needed breaks. After the attack the IR team worked with the logistics company to implement best-in-class cyber resilience measures, so they'd recover even faster from their next attack.

Customer Story: Sony
Sony's comprehensive data protection strategy encompasses a layered defense system, including early warning, threat scanning, remediation, intelligent quarantining, and clean recovery validation. These measures enable Sony to detect threats earlier, recover more quickly, and minimize downtime, ensuring continuous business operations and regulatory compliance.

Based on a recent Commvault customer survey, 54% of respondents consolidated to Commvault from 2 or more systems. 32% consolidated from 3 or more. From that same survey we found that due to vendor/ solution consolidation and simplification, as well as with Commvault's technological approach to recovery, 67% of customers reported seeing a 2x increase in data recovery speed. 34% reported seeing at least a 5x improvement with 19% saying Commvault was 10x faster at data recovery than with their previous solutions.

YOUR CYBER RESILIENCE JOURNEY WITH COMMVAULT – NEXT STEPS

READIVERSE

Are you really prepared? Be sure. Here are a few suggestions:

Host the Cyber Resilience Workshop for your company
https://www.readiverse.com/

Build your Cyber Resilience Program
Use Commvault Cyber Resilience Plan Template and build with your teams to align on your organization's strategy for preventing and recovering from cyber incidents.

Conduct a Commvault Cyber Resilience Assessment at your company
https://www.commvault.com/becoming-cyber-ready/cyber-resilience-services

Perform a critical capabilities review with Commvault Professional Services
https://www.commvault.com/becoming-cyber-ready/cyber-resilience-services

Cyber Resilience Education and Certification courses
https://www.readiverse.com/academy

To learn more, visit **commvault.com**

Commvault® | commvault.com | 888.746.3849

APPENDIX: SOURCES AND RESOURCE LINKS

The list below prioritizes official and primary sources used in Commvault Cyber Resilience Workshop and Commvault Cyber Resilience Plan Template and this takeaway, plus key regulatory references organizations should monitor.

https://www.commvault.com/download-pdf/11825/
https://www.commvault.com/becoming-cyber-ready/readiverse
https://docs.commvault.com/saas/cleanroom_recovery_for_cyber_resilience.html
https://www.commvault.com/platform/recovery-reserve
https://www.commvault.com/becoming-cyber-ready/cyber-resilience-services
https://csrc.nist.gov/glossary/term/cyber_resiliency
https://csrc.nist.gov/glossary/term/air_gap
https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
https://www.nist.gov/publications/computer-security-incident-handling-guide
https://www.nist.gov/publications/guide-cybersecurity-event-recovery
https://www.cisa.gov/ransomware-response-checklist
https://www.cisa.gov/about/divisions-offices/cisa-exercises
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware
https://ransomwareclock.org/?utm_source=chatgpt.com
https://principlesofchaos.org/
https://www.gao.gov/products/gao-22-104256
https://www.eiopa.europa.eu/eiopa-publishes-supervisory-statements-exclusions-related-systemic-events-and-management-non-2022-09-22_en
https://www.mitre.org/focus-areas/cybersecurity/mitre-attack
https://www.sec.gov/corpfin/secg-cybersecurity
https://business.defense.gov/Programs/Cyber-Security-Resources/CMMC-20/
https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
https://op.europa.eu/en/publication-detail/-/publication/dc8116a1-3fe6-11ef-865a-01aa75ed71a1/
https://www.iso.org/standard/27001

APPENDIX: SOURCES AND RESOURCE LINKS

Appendix: Sources Cited in this Document:

[1] [5] [7] [41] https://csrc.nist.gov/glossary/term/cyber_resiliency
[2] https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
[3] [6] [13] [19] [21] [22] [23] [28] [30] [32] [36] [37] [38] https://www.commvault.com/download-pdf/11825/
[4] [14] [26] [40] https://www.nist.gov/publications/computer-security-incident-handling-guide
[8] [31] https://www.nist.gov/publications/guide-cybersecurity-event-recovery
[9] https://csrc.nist.gov/glossary/term/air_gap
[10] [11] [33] https://www.commvault.com/minimum-viability/minimum-viability-guide
[12] https://docs.commvault.com/saas/cleanroom_recovery_for_cyber_resilience.html
[15] [24] [39] [42] https://www.cisa.gov/about/divisions-offices/cisa-exercises
[16] https://principlesofchaos.org/
[17] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware
[18] https://www.gao.gov/products/gao-22-104256
[20] [35] https://www.commvault.com/explore/minimum-viability
[25] [27] https://www.cisa.gov/ransomware-response-checklist
[29] https://www.commvault.com/minimum-viability
[34] https://www.mitre.org/focus-areas/cybersecurity/mitre-attack
[41] Core definitions (cyber resiliency, air gap) come from NIST CSRC glossary entries.
[40] Incident handling and recovery planning guidance come from NIST SP 800-61r2 and NIST SP 800-184, respectively.
[42] Exercises and ransomware operational checklists come from CISA and FBI

commvault.com | 888.746.3849