SOLUTION BUILDERS®

A SOLUTION BUILDERS PLAYBOOK
2026 EDITION

A PLAYBOOK FOR BUSINESSES THAT CANNOT AFFORD DOWNTIME

The Business Continuity Playbook.

Why backups fail when you need them, RTO and RPO in plain language, immutable copies that beat ransomware and a disaster recovery test you can run this week.

INSIDE THE PLAYBOOK

01 Why backups fail
02 RTO and RPO decoded
03 Immutable copies
04 The 90 minute test

Published by Solution Builders
Bloomington, Minnesota · www.solutionbuilders.com

30+	Top 1%	98%
YEARS	OF MSPS	CSAT

WHAT'S INSIDE

Recovery, not just backup.

A backup you have never tested is a hope, not a plan. Most companies own backup software and still lose days when a server dies or ransomware lands, because nobody checked whether the copies would come back. This playbook is about making the next bad day a hiccup instead of a headline.

01 **Why most backups fail when you need them.**
Silent job failures, restores nobody has tried, copies on the attacker's network and a Microsoft 365 tenant nobody backs up. How to find the gap first.
PAGE 03

02 **RTO and RPO, explained simply.**
Two numbers decide every recovery decision. What they mean, how to set them with the business, and how to tier your systems so you pay for speed only where it matters.
PAGE 06

03 **Beating ransomware with immutable copies.**
Attackers go after backups first, because a company with no copies pays. The 3, 2, 1 rule with one addition, and the design choices that decide whether you negotiate or restore.
PAGE 09

04 **A disaster recovery test you can run today.**
A 60 minute tabletop and one real restore. The agenda, the roles, the scenario script, the scorecard, and what to do with the gaps it will absolutely find.
PAGE 12

WHO IT IS FOR
Owners, COOs, CFOs, IT directors and IT managers at companies with 25 to 500 people who want a dead server or a ransom note to be a bad afternoon, not a bad quarter.

HOW TO USE IT
Chapters 01 and 02 diagnose the problem and set your targets. Chapter 03 is the design. Chapter 04 is a 90 minute test your leadership team can run next week.

READING TIME
About 25 minutes cover to cover. The recovery tier table in chapter 02 and the test scorecard in chapter 04 are built to print and fill in.

SOLUTION BUILDERS®

01

Why most backups fail when you need them.

Nearly every company has backups. Far fewer have recovery. The difference shows up at the worst moment: a green dashboard, a confident vendor and a restore that stalls, comes back corrupt or turns out to be three weeks old. This chapter names the quiet failures so you can find yours first.

32%
of breaches now involve ransomware or extortion, the most common reason a restore gets tested for real

68%
of ransomware victims relied on backups to get their data back. Backups only help if they restore

258
days on average to identify and contain a breach. Two weeks of retention cannot reach back that far

30 days
and a deleted Microsoft 365 mailbox is gone for good. Retention is not backup

Backups rarely fail loudly. They fail quietly.

A failed backup does not send up a flare. It sends an email to a mailbox nobody reads, or it reports success on a job that skipped the one database that matters. Here are the five failures we find most often, in the order we usually find them.

01 **Jobs that fail silently**

A job errors out, retries, and the dashboard stays green. Weeks later the newest usable copy is a month old. Nobody notices until the day of the restore.

02 **Restores nobody has tried**

A backup is a theory until you restore from it. Corrupt catalogs, missing encryption keys and the wrong hardware drivers all hide until the first real attempt.

03 **Copies on the same network**

If the backup server shares credentials and a network with production, the attacker who encrypts production encrypts the backups ten minutes later.

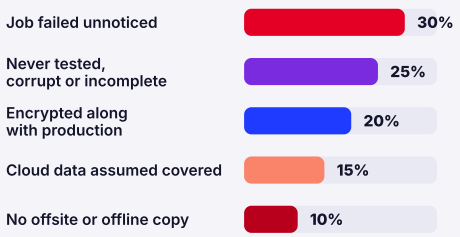
04 **Microsoft 365 is not backed up**

Microsoft keeps the service running. Your data is your responsibility. Retention windows and recycle bins are not backup, and they expire quietly.

05 **No copy outside the building**

Fire, flood, theft and a bad firmware update do not care how many copies sit in the same rack. At least one copy has to live somewhere else.

Why restores fail in practice



Illustrative split, based on what Solution Builders engineers find in recovery assessments. Not a published statistic.

The green dashboard problem

Backup software reports whether a job ran, not whether the business could come back from it. Treat a green checkmark as the start of the question, not the answer to it.

> **The most dangerous backup is the one everyone believes in.**
>
> SOLUTION BUILDERS RECOVERY PRACTICE

Backup is a product. Recovery is a practice.

You can buy backup in an afternoon. Recovery is something your team does on a schedule. Run this audit with your IT team or provider this week. A fail is not a crisis. It is a to do list.

BACKUP MINDSET

What usually exists

- Jobs run nightly. Nobody reads the alerts.
- Copies sit on a NAS in the server room.
- The cloud covers Microsoft 365, surely.
- The last restore test was the install day.

RECOVERY MINDSET

What should exist

- Every failed job becomes a ticket.
- One copy is offsite. One cannot be deleted.
- Microsoft 365 has its own backup platform.
- A timed restore every quarter, on file.

The five minute backup audit

ASK	FAIL LOOKS LIKE	PASS LOOKS LIKE
Did last night's jobs run?	Nobody is sure	A ticket opens on every failure
When did we last restore a server?	"We have never needed to"	Within 90 days, timed
Can one admin delete every copy?	Yes, from one console	No, one copy is immutable
Is Microsoft 365 backed up?	"It is in the cloud"	Mail, files and Teams, daily
Where is the offsite copy?	Same building or host	Other region, own credentials

If you fail a row

- [x] Pull 30 days of job logs and count the failures.
- [x] Book a restore test now. One server, one mailbox.
- [x] Ask your provider to show you the immutable copy on screen, not describe it.
- [x] Write down who can run a restore and where the runbook lives. One name is a gap.

> **An untimed restore is an unkept promise.**
>
> SOLUTION BUILDERS RECOVERY PRACTICE

Sources: Verizon 2024 Data Breach Investigations Report; Sophos, The State of Ransomware 2024; IBM Cost of a Data Breach Report 2024; Microsoft Learn, deleted user and mailbox retention.

SOLUTION BUILDERS®

02

RTO and RPO, explained simply.

Recovery planning has exactly two numbers that matter, and most companies have never written either one down. Recovery point objective is how much work you can afford to lose. Recovery time objective is how long you can afford to wait. Settle them first and every other decision gets easier.

54%
of organizations say their most recent serious outage cost more than $100,000

35%
of ransomware victims needed more than a month to fully recover

24 hrs
of work a once a night backup can lose. That is your real recovery point, whether you chose it or not

2
numbers to agree on for every system, RPO and RTO. Agree on them with the business, not just with IT

RPO is how much you lose. RTO is how long you wait.

Picture the moment a server dies. Everything between the last good backup and that moment is gone. That gap is your recovery point. Everything between that moment and people working again is downtime. That span is your recovery time. Both are choices, and both have a price.

LAST GOOD COPY

The recovery point

Nightly at 11 p.m. means the point sits up to 24 hours behind. Hourly means 60 minutes.

THE INCIDENT

Something breaks

A failed disk, a bad update or a ransom note. The clock starts whether you notice or not.

DECLARED

Someone decides

Recovery begins only when a named person calls it. Hesitation here is pure downtime.

RESTORED

Systems are back

Data is recovered to the recovery point and users can log in. The RTO clock stops here.

CAUGHT UP

Lost work is redone

Everything between the recovery point and the incident gets keyed in again or reconciled.

Set them with four questions

01 **What does an hour of this system cost?**

Count idle payroll, lost orders, overtime and penalties. If nobody can estimate it, the system is not as critical as it feels.

02 **How much work could we redo by hand?**

If the team can rekey a morning of orders from paper, a four hour RPO is fine. If not, you need replication, not backup.

03 **What else is waiting on it?**

A file server nobody thinks about is often the thing the ERP, the payroll run and the shop floor all depend on. Map the dependencies.

04 **What are we willing to pay?**

Shorter RPO and RTO cost more in storage, licenses and engineering. The business picks the trade. IT delivers it.

The nightly backup trap

A nightly backup sounds safe until you do the math. A failure at 4 p.m. on a busy Tuesday erases a full day of invoices, orders and email, and the restore to new hardware eats most of Wednesday. Two days gone, and nobody chose that.

How long full recovery from ransomware took



Share of organizations hit by ransomware. Source: Sophos, The State of Ransomware 2024.

Not every system deserves a one hour recovery.

Paying for a 15 minute recovery on every server is how continuity budgets die. Sort your systems into tiers, give each tier a target and spend where downtime hurts. This table is a starting point. Yours will differ, and that is the point.

Illustrative recovery targets by tier

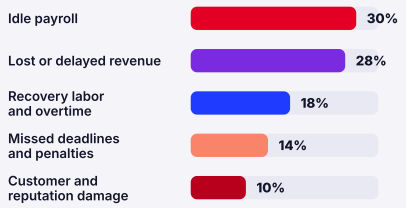
SYSTEM	RPO	RTO	TIER
ERP or line of business app	15 min	4 hrs	1
Microsoft 365 mail, files, Teams	4 hrs	4 hrs	1
Accounting and payroll	1 hr	8 hrs	2
File server and shared drives	4 hrs	8 hrs	2
Phone system, cloud hosted	n/a	1 hr	2
Workstations and laptops	24 hrs	2 days	3
Test and archive systems	7 days	Flexible	3

Illustrative targets for a 100 person company. Set yours with each department lead, then test against them.

How to read the tiers

- **Tier 1** gets replication or hourly snapshots and a rehearsed, documented restore. The money goes here first.
- **Tier 2** gets daily backup with an immutable copy and a timed restore twice a year.
- **Tier 3** gets standard backup and a reimage. Nobody should pay for replication here.

Where a day of downtime costs you



Illustrative split for a 100 person services firm. Build your own with the formula below.

Do the math once

Hourly cost of downtime equals hourly revenue plus the hourly payroll of everyone who stops, multiplied by the share of the business that halts. Write the number down. It settles every RTO argument in the room.

> **If finance has not signed the RTO, IT does not have one. It has a guess.**
>
> SOLUTION BUILDERS RECOVERY PRACTICE

Sources: Uptime Institute Annual Outage Analysis 2024; Sophos, The State of Ransomware 2024. Recovery targets and the downtime cost split are illustrative planning assumptions.

SOLUTION BUILDERS®

03

Beating ransomware with immutable copies.

Modern ransomware crews do not start by encrypting your files. They start by finding and destroying your backups. Then they encrypt, then they call. If one copy of your data cannot be changed or deleted by anyone, including your own administrators, that call ends very differently. This chapter is about that copy.

94%
of organizations hit by ransomware saw attackers attempt to compromise their backups

57%
of those attempts succeeded. The attackers reached the copies before the restore did

2x
as likely to pay the ransom when backups were compromised, 67% versus 36%

8x
higher median recovery cost when backups were compromised, $3M versus $375K

Attackers go after the backups first.

A ransomware operator who finds your backup console wins twice. They get your data, and they take away your only alternative to paying. The sequence is predictable, and so is the defense. Here is the week before the ransom note, and the rule that defeats it.

DAY 0

A login is phished

An employee enters a password on a lookalike Microsoft page. The attacker now has a foothold.

DAY 1 TO 5

They look around

Admin accounts, the backup server, the console password saved in a browser. Quiet and patient.

DAY 6

Backups are deleted

Retention is set to zero, jobs are disabled and cloud copies are purged with your own credentials.

DAY 7

Everything is encrypted

Production goes dark in the early hours of a weekend. The note names a price and a deadline.

DAY 8

Negotiate or restore

With no clean copy, the choices are pay or rebuild from nothing. With one, you restore.

The rule: 3, 2, 1, 1, 0

01 **3 copies**

Production plus two backups. One failure or one mistake should never leave you with zero.

02 **2 different media**

Local disk plus cloud object storage, or disk plus an appliance. Different failure modes.

03 **1 offsite**

Another building, region or cloud. Fire and flood do not care how many copies share a room.

04 **1 immutable**

A copy nobody can alter or delete for a fixed period, admins included. The attacker cannot reach it.

05 **0 errors**

A verified, tested restore. A copy nobody has restored does not count. Most companies skip this.

What immutable actually means

Object lock in cloud storage or a hardened repository that accepts new data and refuses deletes until a timer expires. Not a password. Not a permission. A property of the storage itself that no stolen credential can override.

$0

ransom paid by a 42 user firm whose clean copies held

100%

of its data recovered, with containment in 22 minutes

> **You do not negotiate with someone who cannot touch your copies.**
>
> SOLUTION BUILDERS RECOVERY PRACTICE

Design choices that decide whether you pay or restore.

Immutability is the headline, but it is one of several choices. Separate credentials, a separate network path, retention that predates the intruder and a restore your team has practiced each close a door the attacker will try. Here is the design, weak to strong.

Backup design, weak to strong

CHOICE	WEAK	STRONG
Where copies live	Same host or network	Separate network plus cloud object lock
Who can delete	Any domain admin	Nobody until the lock expires
Credentials	Domain joined shared admin	Separate identity, hardware MFA
Retention	7 to 14 days	30 to 90 days, monthly points for a year
Microsoft 365	Recycle bin and retention policy	Third party backup, three times daily
Restore proof	Green job status	Quarterly timed restore, logged

Why 258 days matters here

Breaches take months to spot. With 14 days of retention, every copy you own may already carry the attacker's tools. Keep monthly recovery points for a year so a clean one exists.

Rolling it out

1. **Lock the cloud copy**
   Turn on object lock on the offsite copy, 30 days minimum. Most platforms do it in an afternoon.
2. **Split the identity**
   Give backup its own admin identity outside the domain, with hardware MFA and no domain trust.
3. **Back up Microsoft 365**
   Add third party backup for mail, OneDrive, SharePoint and Teams, three times a day, separate tenant.
4. **Prove it**
   Restore a server and a mailbox from the immutable copy, not the local one. Time it. File the result.

30 days
minimum lock on the offsite copy

1 year
of monthly points, so a clean copy predates the intruder

Sources: Sophos, The State of Ransomware 2024 and The Impact of Compromised Backups on Ransomware Outcomes 2024; IBM Cost of a Data Breach Report 2024 (time to identify and contain); CISA #StopRansomware Guide (offline, encrypted and immutable backups). The attack timeline is a composite drawn from Solution Builders incident response engagements.

SOLUTION BUILDERS®

04

A disaster recovery test you can run today.

You do not need a weekend, a consultant or a second data center to test recovery. You need 90 minutes, four people in a room and one restore that actually runs. This chapter gives you the agenda, the scorecard and the follow up that turns what you find into a plan.

90 min
is all the first test takes: a 60 minute tabletop plus one timed restore

4
people at the table: executive sponsor, IT lead, operations lead and communications owner

1
server and one mailbox restored end to end, with the clock running and the time written down

22 min
from alert to containment for a 42 user firm that had rehearsed. Practice is the difference

Ninety minutes, four people, one real restore.

A tabletop is a conversation with a clock. You read a scenario aloud and the room says what it would do and who would do it. The gaps appear fast. Then you leave the room and restore something, because talking is not the test.

0:00 — Set the scene
The sponsor reads the scenario aloud. Payroll and the file server are encrypted. It is Friday at 4 p.m.

0:10 — The first hour
Who notices, who declares, who gets called. Does the contact list work with email down?

0:30 — The decisions
Pay or restore. Which systems come back first. What we tell customers, and who says it.

0:50 — The recovery
Walk the restore order against the tier table. Where is the runbook, and who holds the keys?

1:00 — The real restore
Leave the room. Restore one server and one mailbox from the offsite copy. Time it.

Before the meeting

- [x] Print the tier table from chapter 02 and the backup audit from chapter 01. Both are inputs.
- [x] Pick a server and a mailbox that matter, not a test box, and an isolated restore target. Never production.
- [x] Put the incident contact list on paper. Assume email, Teams and the phone system are all down.
- [x] Give someone the job of scribe. Every "we would probably" gets written down as a gap.

60 min
of talking before anyone touches a keyboard

30 min
for one real restore, clock running

Roles at the table

ROLE	OWNS DURING A REAL INCIDENT
Executive sponsor	Declares, approves spend, decides pay or restore
IT lead	Runs the restore and owns the runbook
Operations lead	Keeps the business moving on paper
Communications owner	Talks to staff, customers, insurer, press

The scenario script

"It is Friday at 4 p.m. Payroll runs Monday. The file server and the ERP are encrypted. The note asks for $400,000 in 72 hours. The backup console is not responding." Read it aloud, then let the room answer.

Score the test, then fix the three worst gaps.

Every first test finds gaps. That is the point, not a failure. Score the twelve items below, write the number in the box and pick the three gaps that would hurt most on a real Friday. Then put owners and dates on them and book the next test.

Detection and decisions

- [ ] An alert for the failure reached a named person within 15 minutes, outside business hours.
- [ ] One person had clear authority to declare the incident and did so without calling a meeting.
- [ ] The contact list worked with email, Teams and the phone system assumed down.
- [ ] The room agreed on the restore order without looking it up or arguing about it.
- [ ] Someone could say, within a day, how much data would be lost. The RPO was known.
- [ ] Staff, customers and the insurer each had a named person and a first message ready.

Recovery and proof

- [ ] The restore ran from the offsite or immutable copy, not from the local one.
- [ ] The server came back inside its RTO from the tier table, measured with a clock.
- [ ] The mailbox came back with folders, calendar and permissions intact.
- [ ] Two people could have run the restore from the runbook without the person who wrote it.
- [ ] The restore target was isolated, so a dormant payload could not reach production.
- [ ] Every "we would probably" was written down as a gap with an owner and a date.

_____ / 12

Score yourself

Count the items that passed cleanly. Half credit does not count.

What your score means

SCORE	WHERE YOU STAND
0 to 4	Exposed. A real incident becomes a rebuild. Start with the immutable copy.
5 to 8	Typical. You would recover, slowly and at a price. Fix the three worst gaps, retest in 90 days.
9 to 12	Ready. Move to quarterly restores and test a full site failure next.

Make it a habit

One test is a snapshot. Four a year is a program. Book the next one before you leave the room, rotate the scenario and keep every scorecard. Trend lines convince boards and insurers.

Sources: CISA Cybersecurity Tabletop Exercise Packages; NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide. Case figures from a Solution Builders client engagement, 42 users, professional services.

Continuity that has already been rehearsed.

Solution Builders has kept Minnesota businesses running since 1995. Our continuity practice is built on the RISE framework, delivered by 50+ engineers, watched by a 24/7 security operations center and audited to SOC 2 Type II.

R

Resilient

Immutable, offsite copies of servers, cloud workloads and Microsoft 365, with restores we time every quarter.

I

Integrated

Recovery designed into your infrastructure and cloud, with runbooks your team and ours both own.

S

Secure

24/7 detection that isolates ransomware before it reaches the copies, plus evidence your insurer will ask for.

E

Evolving

AI adoption on data that is governed, backed up and recoverable from day one.

01

Recovery Readiness Snapshot

A 30 minute conversation. You get a candid read on your backups, your real RTO and the three gaps to close first.

FREE · 30 MINUTES

02

Business Continuity Assessment

Two weeks covering backup design, recovery tiers and a facilitated 90 minute test with your leadership team, with a scored report and a 90 day plan.

FIXED FEE · 2 WEEKS

03

Managed Backup and Disaster Recovery

Everything in this playbook, run for you: immutable copies, Microsoft 365 backup, monitored jobs, quarterly timed restores and an annual tabletop.

MONTHLY · ONGOING

Find out what your restore would really take.

Book a free Recovery Readiness Snapshot with a Solution Builders solution architect. No pitch, just a clear read on whether your copies would come back.

Book my readiness snapshot

THE SHORT VERSION

Three things to remember.

If this playbook disappears into a drawer, keep these three ideas. They are the difference between a company that has an outage and a company that has a story about one.

01 **A backup is a hope until it restores.**

Monitor every job, restore a server and a mailbox every quarter, and write the time down. Microsoft 365 needs its own backup.

02 **Pick your two numbers on purpose.**

RPO is how much you lose. RTO is how long you wait. Set both per system with the business, then spend only where downtime hurts.

03 **Keep one copy nobody can touch.**

Attackers go after backups first. One immutable, offsite copy with separate credentials turns a ransom note into a restore job.

SOLUTION BUILDERS®

START THE CONVERSATION

www.solutionbuilders.com

(952) 854-8188 · 1550 American Blvd East, Suite 900, Bloomington, MN 55425
Your technology partner since 1995

Book a free assessment

© 2026 Solution Builders, Inc. All rights reserved. Product names and marks are the property of their respective owners. Figures marked illustrative are planning estimates, not guarantees.