AnchorOne

GOVERNANCE BRIEF

IMMUTABLE BACKUP

The First Asset Threat Actors Compromise in a Ransomware Event

Most organizations believe they have a backup. Ransomware attackers count on that belief being wrong. Retention policies preserve deleted items — not encrypted ones. Backups that can be modified or deleted by a threat actor with admin credentials are not backups. And a backup that has never been tested for recovery is an assumption, not a guarantee.

68%	1 in 3	75%	21–24
of ransomware attacks specifically target and attempt to corrupt or delete backup data	SMBs discover their most recent backup is unusable at the moment of recovery	of SMBs say they could not continue operating if hit with ransomware	days average ransomware recovery time using conventional backup approaches

Sources: Infrascale Ransomware Recovery Report (2026) · CrashPlan Data Loss Statistics (2026) · BD Emerson SMB Research · Spin.AI Microsoft 365 Backup Analysis (2026)

THE RETENTION POLICY MISCONCEPTION

Microsoft 365 includes retention policies for Exchange, SharePoint, OneDrive, and Teams. These policies preserve deleted or modified items within a defined retention window. They are a compliance tool — not a backup. When ransomware encrypts a file in SharePoint, the encrypted version is what is retained. When a threat actor operating under valid credentials deletes mailbox content, retention may preserve a copy — but that copy exists within the same tenant the attacker already controls. Retention does not create an independent, isolated recovery point. It preserves state inside the environment that is already compromised.

This distinction is not technical nuance. It is the difference between an organization that can recover from a ransomware event in hours and one that discovers — at the moment it matters most — that it has no usable copy of its data outside the compromised environment.

WHAT THREAT ACTORS DO TO BACKUPS

Ransomware operators understand backup infrastructure. In the majority of attacks, locating and destroying backup copies is a deliberate step in the attack sequence — not an afterthought. A threat actor who gains admin-level access to a Microsoft 365 tenant can delete backup jobs, corrupt retention policies, and remove recovery points before the encryption payload deploys. By the time the organization discovers the attack, the backup the organization believed it had no longer exists.

Immutability is the only technical control that addresses this directly. An immutable backup cannot be modified or deleted — not by ransomware, not by a threat actor operating with admin credentials, and not by an administrator acting under duress during an extortion event. The data exists in a state that neither the attacker nor the organization can alter within the defined retention window.

WHAT A GOVERNED ENVIRONMENT REQUIRES

Control	Requirement	What It Addresses
M365 Backup — all workloads	Daily backup active for Exchange, SharePoint, OneDrive, and Teams — all jobs completing successfully	Every governed workload has an independent, current recovery point outside Microsoft retention policies
Immutable storage	Backup data cannot be modified or deleted by ransomware, admin action, or threat actor with tenant access	A clean recovery point exists regardless of what a threat actor does to the live environment
Quarterly restore testing	Restore test completed every 90 days for all M365 workloads — results documented and verified	Recovery capability is verified before it is needed, not assumed at the moment of crisis
Recovery SLAs defined	Recovery time and recovery point objectives documented before an incident occurs	The organization knows exactly what it can recover, from what point in time, and within what window

Quarterly restore testing is not optional. A backup that has never been tested is an assumption. Assumptions do not recover law firm client files, financial advisor client records, or years of matter history on a Sunday morning after a ransomware event. The test exists so the organization knows — before the event — exactly what can be recovered and within what timeframe.

WHAT CARRIERS NOW VERIFY

Cyber insurance underwriters have moved immutable backup from a recommended control to a documented underwriting requirement. Nearly three quarters of carriers now require immutable, air-gapped backup with documented testing results as a condition of coverage. They ask not whether backup exists, but whether it is immutable, whether it covers all workloads, and when it was last successfully tested. An organization that answers these questions with silence or uncertainty is presenting the same risk profile as an organization with no backup at all.

A governed environment does not answer these questions under pressure at renewal. Immutable backup is active on every workload. Restore tests are completed quarterly and documented. Recovery SLAs are defined before they are needed. The evidence exists because the control is enforced — not assembled because an underwriter asked for it.

This brief is part of AnchorOne's Spring 2026 governance series.

— Dan Cull, Founder, AnchorOne