AnchorOne

GOVERNANCE BRIEF

MULTI-FACTOR AUTHENTICATION

The One Control That Stops Most Breaches — When It Is Actually Enforced

MFA is the most widely recommended security control in the industry. It is also the most selectively deployed. Most organizations have enabled it for some users. Almost none have enforced it for every user with no exceptions. The gap between "enabled" and "enforced" is where accounts get compromised.

99.9%	**34%**	**51%**	**65%**
of compromised accounts did not have MFA enabled at the time of breach	MFA adoption rate among SMBs with 26–100 employees — the primary target market	of organizations have suffered financial losses directly attributed to identity-related breaches	of global SMBs do not use MFA and have no plans to implement it

Sources: Microsoft Security Intelligence (2025) · JumpCloud IT Trends Report (2024) · Cisco Duo State of Identity Security (2025) · Cyber Readiness Institute Global MFA Survey (2024)

THE EXEMPTION PROBLEM

When organizations deploy MFA, they rarely deploy it universally. The rollout begins with IT staff, extends to general employees, and then stalls at the individuals with the most organizational authority — and the most access to sensitive data. Partners object. Executives cite inconvenience. Senior staff who have been with the firm for decades are granted informal exceptions that are never formally documented and never revisited.

This pattern is consistent across professional services firms regardless of size or vertical. The result is an identity environment where the accounts with the broadest access to client data, financial records, and privileged systems are the least protected. Attackers understand this. Credential attacks are not random — they target the accounts most likely to yield the highest value access with the fewest controls in the way.

ENABLED IS NOT ENFORCED

There is a meaningful difference between an organization that has MFA available and one that has MFA enforced. Available means users can opt in. Enforced means no user can authenticate without it — no exceptions, no bypass accounts, no legacy protocols that route around it. Nearly half of organizations report they cannot enforce consistent MFA across all users and applications. That gap is not a configuration problem. It is a governance problem. Someone inside the organization has the authority to grant exceptions, and they use it.

Legacy authentication protocols compound this further. Basic Auth, IMAP, and SMTP Auth were designed before MFA existed. They authenticate with a username and password only — and they bypass Conditional Access entirely. An organization can have MFA enforced for every browser login and still be fully exposed through a single account running legacy auth in the background. This is covered separately in the Legacy Authentication governance brief.

WHAT A GOVERNED ENVIRONMENT REQUIRES

Control	Requirement	What It Addresses
MFA — all users	MFA enforced for every user without exception — no bypass accounts, no exemptions for role, tenure, or title	Senior-level exemptions, informal bypass accounts, and selective enforcement that leaves the highest-value identities unprotected
Conditional Access	Every access request evaluated — compliant device and MFA required as a minimum condition	Authentication paths that bypass MFA through policy gaps, exclusions, or unmanaged access points
Passwordless for privileged roles	FIDO2 or Microsoft Authenticator passkey required for all privileged and administrative accounts	Password-based authentication for the accounts with the broadest access to governed resources
Identity risk monitoring	Entra ID Protection active — high-risk sign-ins flagged and acted upon automatically	Compromised credentials operating undetected inside the environment after initial breach

The standard requires MFA for every user. Not most users. Not users below a certain seniority level. Every user. The partner who objects, the executive who finds it inconvenient, the long-tenured employee who has never needed it before — all of them authenticate under the same requirement. There is no exception process. The count of approved exceptions is always zero.

WHAT CARRIERS AND REGULATORS NOW REQUIRE

MFA has moved from a recommended control to a documented underwriting requirement. Nearly 80% of cyber insurance carriers now mandate MFA across all systems as a condition of coverage. CMMC 2.0, enforceable as of November 2025, requires strong authentication for all users accessing controlled unclassified information. The New York Department of Financial Services mandates MFA for financial institutions. PCI DSS 4.0 requires it for all access to payment transaction data. An organization that cannot demonstrate universal MFA enforcement is not meeting the baseline requirement of any of these frameworks simultaneously.

MFA enforcement is not a technical achievement. It is an organizational discipline. The technology has been available for years. What most organizations lack is the authority to enforce it without exception — including against the people inside the organization who believe the rules do not apply to them.

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

— Dan Cull, Founder, AnchorOne