CORY WASHINGTON & CO.

SMARTER RISK. STRONGER BUSINESS.

CWCO-SUP-ITMSP-CHK Rev. 09-2026

IT SERVICES & MSP — COVERAGE CHECKLIST

Pull out your current policy and check the box next to any coverage you can confirm is already in place — anything unchecked is worth a quick conversation with your advisor. Coverage checklist for managed service providers and IT services firms. Priorities reflect typical exposure; confirm against client count and security services.

CORE **PREVALENT** **SITUATIONAL** *— Core: almost always needed · Prevalent: commonly carried by businesses in this class · Situational: depends on specific exposure*

	COVERAGE	WHY THIS BUSINESS NEEDS IT	PRIORITY
☐	**Technology E&O (incl. Network Security Liability)**	Covers client claims when the MSP's services or access cause a breach or outage.	CORE
☐	**First-Party Cyber**	Covers the MSP's own breach response, ransomware, and business interruption.	CORE
☐	**Contingent / Dependent Business Interruption**	Covers losses when an RMM or software vendor is compromised.	PREVALENT
☐	**Commercial General Liability**	Covers bodily injury and property damage at client sites.	CORE
☐	**Crime / Social Engineering**	Covers funds lost to fraud and fake invoices.	PREVALENT

COMMON COVERAGE GAP FOR THIS CLASS

The most commonly missed gap for this class is E&O limits sized for a multi-client event. In the 2021 Kaseya attack, ransomware spread through a remote-management tool to about 50-60 MSPs and up to 1,500 of their clients at once — and each client can bring its own claim. MSPs should confirm their technology E&O includes network security liability, that aggregate limits fit their client count, and that phishing-resistant MFA and segmentation are in place across every client tool.

IMPORTANT — PLEASE READ