The Vendor as the Vector: Third-Party Risk Management Across Veterinary and Insurance Networks

Bridgham Technology Institute
Bridgham Cyber, LLC
June 2026
Reissued September 2026 under the Bridgham name.

Abstract

Third-party vendors represent the fastest-growing category of initial breach access across the mid-market, yet most $5M to $30M businesses in the veterinary and insurance verticals have no formal inventory of the vendors holding privileged access to their systems. Bridgham Cyber client engagement data, combined with SecurityScorecard vendor risk intelligence, indicates that the average veterinary group or independent insurance agency has between 12 and 18 software vendors with some form of authenticated access to core operational systems. Graph-theoretic analysis of these vendor relationships consistently reveals that two to three vendors account for more than 60 percent of the total third-party data exposure in a given organization. This concentration means that third-party risk, properly understood, is not a broad and unmanageable problem. It is a focused problem amenable to prioritized remediation.

1. Threat Environment

1.1. The Managed Service Provider as Primary Attack Surface

The majority of veterinary practices and independent insurance agencies at the mid-market revenue band engage a managed service provider (MSP) for some or all of their IT infrastructure management. The MSP relationship is operationally necessary and, in many cases, appropriate. It is also, from an adversarial perspective, one of the highest-value targets in the mid-market ecosystem.

A successful compromise of an MSP that serves 40 veterinary practices creates immediate lateral access to all 40 environments simultaneously. The MSP's remote monitoring and management (RMM) tools, which by design have elevated privileges across all client environments, become the adversary's operational infrastructure. The 2021 Kaseya VSA incident, which affected hundreds of MSP clients through a single software supply chain compromise, established the template for this attack pattern. It has been replicated in smaller-scale operations consistently in the years since.

1.2. SaaS Vendor Proliferation and the Unmapped Access Graph

The operational technology stack of a mid-market veterinary group or insurance agency has expanded significantly since 2020. Cloud-based practice management, telemedicine platforms, payment processors, HR and payroll systems, marketing automation, and specialty software for regulatory reporting each introduce an authenticated connection to the organization's data environment. Individually, each integration appears low-risk. Collectively, they constitute an unmapped access graph

that few organizations have formally inventoried.

SecurityScorecard risk data indicates that organizations in the healthcare and financial services categories that have not conducted a formal third-party vendor inventory in the prior 12 months are significantly more likely to have at least one vendor with a critical security finding in their risk profile. The finding is not that the vendor's product is broken. The finding is that the organization does not know what access its vendors hold and therefore cannot respond effectively when a vendor is compromised.

1.3. IT Provider Contractual Gaps and Incident Notification Obligations

Many mid-market organizations have IT provider contracts that predate the current threat environment and contain no provisions for incident notification, security audit rights, or breach response obligations. When an IT provider experiences a security incident affecting client environments, organizations operating under legacy contract structures may not receive notification on a timeline that enables them to respond within applicable regulatory notification windows.

Bridgham Cyber has reviewed IT provider agreements for clients in both the veterinary and insurance verticals. A consistent finding is that fewer than 30 percent of agreements reviewed contain a notification obligation requiring the provider to inform the client within 24 to 72 hours of a confirmed incident. This contractual gap is remediable through a simple amendment. It is not remediable after an incident has occurred.

> ***Key Observation.*** *Third-party risk is not an abstract supply chain concern. It is a concrete operational exposure defined by the specific vendors holding authenticated access to your systems today. The remediation begins with an inventory, not a framework.*

2. Regulatory Update

2.1. FTC Safeguards Rule: Third-Party Oversight Requirements

The FTC Safeguards Rule explicitly requires covered financial institutions, including qualifying insurance agencies, to oversee service provider arrangements. Specifically, the rule requires covered entities to select and retain service providers that maintain appropriate safeguards, require service providers by contract to implement and maintain such safeguards, and periodically assess service providers based on risk.

FTC enforcement actions in 2025 and 2026 have included findings that covered entities failed to conduct adequate oversight of IT service providers, in some cases where the IT provider was the proximate cause of a breach. The enforcement posture reflects the FTC's position that outsourcing IT functions does not transfer regulatory responsibility. The covered entity remains accountable for the

security outcomes produced by its vendor relationships.

2.2. HIPAA Business Associate Agreements: Scope Expansion Under OCR Guidance

The HHS Office for Civil Rights has issued updated guidance clarifying that business associate agreement (BAA) obligations extend to subcontractors of covered business associates. For veterinary practices with any HIPAA-adjacent data handling and for the IT providers and SaaS vendors serving them, this creates a chain of contractual obligation that many organizations have not fully mapped.

The practical implication is that a veterinary practice relying on a cloud-hosted backup provider that stores data containing protected health information must have a BAA in place with that provider, and must be able to demonstrate that the provider's security controls are commensurate with the data they hold. The absence of a BAA where one is required is a per-record violation under current OCR enforcement guidance.

2.3. North Carolina Identity Theft Protection Act: Service Provider Accountability

The NCIDTPA's provisions governing breach notification apply to businesses that own or license personal information. When a business is subject to a breach through a third-party service provider, the notification obligation remains with the business, not the provider, unless the provider is separately covered by the act. This structure places the operational and reputational cost of a vendor-caused breach on the client organization, regardless of contractual indemnification. Contractual remedies may recover costs over time. They do not prevent the breach notification obligation from triggering immediately.

3. Intelligence Briefing

3.1. Deep Dive: Applying Vendor Tiering to Concentrate Third-Party Risk Reduction

The most common reason mid-market organizations do not manage third-party risk is not lack of awareness. It is the perception that vendor risk management requires a dedicated function, a risk management platform, and sustained resource investment. This perception is accurate when applied to enterprise-scale vendor ecosystems of 200 to 500 vendors. It is not accurate for the 12 to 18 vendor environments characteristic of the mid-market practices in our client portfolio.

The following tiering model, adapted from our client engagement methodology, provides a practical framework for concentrating remediation effort on the vendors that represent the majority of third-party risk exposure.

Tier	Definition and Management Standard
Tier 1: Critical	Vendors with authenticated access to systems containing sensitive client or patient data, financial transaction capability, or administrative control over IT infrastructure. Typically 2 to 4 vendors. Examples: MSP, AMS platform, PMS platform, cloud backup provider. Require annual security review, written security addendum or BAA, and defined incident notification obligation.

Tier	Definition and Management Standard
Tier 2: Significant	Vendors with access to operational systems containing business-sensitive but not regulated data. Typically 4 to 8 vendors. Examples: HR/payroll, marketing automation, scheduling software. Require security documentation review at contract renewal and MFA enforcement on vendor-managed credentials.
Tier 3: Standard	Vendors with no authenticated access to sensitive data or with access limited to public-facing systems. Typically 6 to 10 vendors. Require standard vendor due diligence at procurement and periodic review on an 18 to 24 month cycle.

Clients that have implemented this tiering model uniformly report two findings: first, the number of Tier 1 vendors is smaller than anticipated, typically three to five, which makes the compliance and oversight workload manageable. Second, the process of building the inventory surfaces vendor relationships that were not in the institutional memory of current leadership, including legacy integrations that have persisted through staff transitions and platform migrations.

The vendor inventory is a one-time exercise requiring four to six hours for most organizations in our client portfolio. The tiering classification adds two to three hours. The result is a risk-prioritized vendor register that drives remediation activity for the subsequent 12 months.

4. Recommendations

1. **Completing a vendor inventory and applying the tiering model.** Clients are conducting a structured inventory of all vendors with authenticated access to any system containing client, patient, or financial data. The inventory uses the three-tier model described in Section 3. Tier 1 vendors are reviewed immediately for security documentation and contractual notification obligations. This exercise consistently produces a materially different view of organizational risk than leadership held at the start of the engagement.

2. **Amending IT provider agreements to include incident notification obligations.** Clients are requesting a contract amendment from their MSP or IT provider requiring notification within 48 hours of any confirmed security incident affecting the client’s environment or data. The amendment also requires the provider to maintain documentation of their own security program and to provide that documentation upon request. Most IT providers serving the mid-market will accept this amendment without objection. The amendment request itself signals organizational security maturity that influences provider behavior.

3. **Revoking inactive vendor access on a quarterly cycle.** Clients have established a quarterly process to review and revoke authenticated vendor access that is no longer operationally required. Platform integrations accumulate over time as software evaluations, discontinued services, and staff-initiated tool connections persist beyond their operational lifespan. A quarterly access review takes approximately 90 minutes for the relevant IT or operations lead and eliminates a category of access risk that otherwise compounds indefinitely.

Disclaimer

This publication is produced by Bridgham Cyber, LLC for informational and analytical purposes only. It reflects independent research and does not constitute legal, regulatory, compliance, or investment advice, nor a solicitation of any kind. The analysis draws on sources believed to be reliable at the time of writing, and no warranty is made as to their accuracy or completeness. Reproduction or redistribution, in whole or in part, requires attribution to Bridgham Cyber, LLC.