www.pipelinepub.com
Volume 22, Issue 1

Third-Party Risk: The Hidden Cybersecurity Weakness for SMBs

By: David Primor

Cybersecurity conversations with small and midsize businesses (SMBs) often start with a review of the key topics such as internal defenses, antivirus, patching, firewalls, and employee training. These are important, of course, but they only cover part of the picture. There is a quieter, harder-to-control vulnerability that is becoming one of the biggest threats to SMB resilience - third-party risk. Vendors and service providers are now woven into almost every aspect of how SMBs operate. Whether it is outsourced IT, cloud applications, payroll, or digital marketing, these external partners often hold sensitive data or have direct access to networks. That means a single vendor with weak security practices can open the door to costly breaches. For SMBs without mature cybersecurity programs, vendor risk is a hidden weak point that is only now coming into sharper focus.

Why Vendor Risk Is Growing

Third-party risk is climbing the threat list for several reasons. First, SMBs are increasingly outsourcing specialized functions to reduce overhead and gain expertise they cannot maintain in-house. While this helps them scale quickly, it also expands the network of vendors and potential points of exposure. A vendor handling payroll or customer data can be far more attractive to attackers than the SMB itself because smaller suppliers often have fewer security controls.

Second, attackers are targeting the supply chain. High-profile breaches over the past decade have shown that cybercriminals can bypass large enterprise defenses by exploiting weaker security at smaller suppliers. For SMBs, this means that their cybersecurity is only as strong as the “weakest” vendor they rely on. Even heavy investment in firewalls and endpoint security can be undone by a single unprotected vendor account.

Third, regulatory and customer expectations are rising. SMBs that handle sensitive data are increasingly expected to demonstrate formal vendor due diligence. This isn’t limited to industries like healthcare, finance, or government contracting. Even small businesses working with enterprise clients or third-party marketplaces are being asked to provide proof of vendor

risk assessments, security certifications, and compliance protocols. Simply put, SMBs can no longer treat vendor security as someone else's problem.

The Opportunity

This is where Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) can make a real difference. Most SMBs lack the staff or expertise to build a strong Third-Party Risk Management (TPRM) program, but MSPs and MSSPs are already trusted to deliver IT and security services and are in a prime position to fill this gap. TPRM is not just a needed service; it is also a business opportunity. By including vendor risk assessments, monitoring, and reporting in their service offerings, MSPs and MSSPs can stand out in a crowded market.

TPRM also opens up new revenue streams. Assessing vendor risk usually uncovers gaps that need attention, like unpatched software, inadequate access controls, or missing policies. In some cases, clients' vendors are so impressed by the assessments that they hire the service provider to manage their own third-party risk.. MSPs and MSSPs can turn vendor risk assessment findings into services such as compliance consulting or cybersecurity advisory. This moves them beyond technical support and into the role of strategic partner, helping SMBs navigate a complex security landscape while also growing their own business.

Making TPRM Practical for SMBs

For years, TPRM was seen as too resource-intensive for smaller businesses. Manually assessing each vendor, repeating the process across multiple clients, and producing audit-ready reports could quickly overwhelm SMB budgets or MSP teams. Traditional approaches were slow, cumbersome, and often impractical for smaller organizations that needed results fast.

Modern approaches, however, make TPRM manageable and repeatable. Today's MSPs can deliver these services efficiently by using guided workflows, reusable templates, automation and even tools built specifically for them. Standardized questionnaires simplify vendor data collection, while centralized management tools track shared vendors across multiple clients to eliminate redundancy. Integrating internal and vendor risk data into a single platform gives MSPs a clear view of how third-party vulnerabilities impact each client's overall security posture.

Advanced tools also make scoring and reporting easier to understand. AI-powered risk models can highlight the most pressing threats, while visual dashboards, heatmaps and straightforward reports help clients quickly see where the biggest risks lie. With this approach, TPRM becomes a repeatable, high-value service that offers both insight and strategic guidance.

Effective Workflow

A successful workflow usually starts with collecting all relevant vendor information, including contracts, policies, and other documentation, and sending out standardized questionnaires based on industry frameworks. Once the data is in, MSPs review supporting evidence like encryption practices, access policies, and incident response protocols. Then, client-specific forms are used to assess vendor responses against the client's priorities and business impact. Vendors are scored and categorized by risk level, and those assessments are aligned with the client's overall risk posture. The final step is generating audit-ready reports and visual dashboards to make risks clear, with regular reassessments scheduled to track changes over

time. This approach gives SMBs insight almost immediately while keeping the process structured and manageable.

TPRM can also reveal other opportunities for MSPs and MSSPs. Vendor assessments often uncover unpatched software, weak access controls, or missing policies. Each of these gaps can lead to projects like compliance consulting, contract review, or deploying additional cybersecurity solutions. By taking a proactive approach, service providers move from technical support to strategic advisory, helping clients manage risk while strengthening their own relationships.

Proactive vendor risk management also builds trust. SMB clients often feel vulnerable when it comes to cyber threats, and having visibility into third-party risks provides reassurance. MSPs and MSSPs that can clearly show vendor risk data and offer actionable recommendations position themselves as indispensable partners rather than just service providers.

Market Momentum and Growth

Analysts now agree that third-party risk is not just a problem for big companies. SMBs are firmly in the spotlight, and demand for accessible, scalable vendor risk management is growing quickly. Research shows that the global TPRM market is expected to expand sharply in the next decade, driven by regulatory requirements, high-profile supply chain breaches, and customer expectations for stronger due diligence.

For MSPs and MSSPs, this creates a dual opportunity to protect clients while growing profitably. Early adopters can gain a significant advantage in a market that is still underserved at the SMB level. By offering streamlined TPRM services, service providers can meet client needs while positioning themselves as trusted, forward-looking advisors.

Why SMBs Can't Ignore Third-Party Risk

The reality is clear - and here. Vendors that support growth and efficiency can also create serious vulnerabilities. Data breaches originating from third-party suppliers are often more damaging than internal failures because they exploit trusted relationships that are overlooked. For SMBs, these breaches can lead to lost revenue, reputational harm, and regulatory penalties, all of which can be devastating for smaller organizations.

As SMBs grow, their vendor ecosystems become more complex. What might have started as a single cloud application or outsourced service can quickly turn into dozens of vendors handling payroll, customer data, IT support, marketing, and more. Without a systematic approach to vendor risk management, SMBs are blind to threats that can compromise their operations.

This is the call to understand how third-party risk has become the hidden cybersecurity weakness for SMBs. Vendors, contractors, and service providers that are a value add as they drive growth and efficiency can also introduce vulnerabilities. And the catch is that most SMBs lack the resources to manage this risk themselves, but MSPs and MSSPs can fill the gap. By integrating TPRM into their offerings with standardized workflows, centralized vendor management, and scalable reporting, service providers can deliver a solution that is practical and profitable.

This allows SMBs to have the confidence they need, knowing that their operations and customer relationships are not compromised by the partners they rely on. Beyond reducing risk, TPRM enables service providers to become strategic advisors, uncovering gaps to shine a

light on solutions while strengthening client trust. For SMBs and the MSPs that serve them, embracing third-party risk management is no longer optional - it's essential for growth, security, and resilience in a digital world where vulnerabilities can appear when least expected.