Third Party Risk Management

Defending your assets from supply chain cybersecurity risks

What is Third Party Risk Management?

HolistiCyber's third-party risk management (TPRM) is a unique program designed to assess and control cybersecurity risks resulting from conducting business with third parties such as vendors and business partners. It is an end-to-end service, ensuring third parties maintain an acceptable level of cybersecurity while working with the organization, thus reducing chances for data breaches and business downtimes. In the process, regulation and compliance issues are covered. **The goal is to mature the organization's security program and elevate its overall security posture.**

How does this service work for me?

1. **Initial assessment** of current company cybersecurity third-party risk-management policies and threat landscape mapping.
2. **Vendor due diligence** - domain experts, pinpoint where cyber security vulnerabilities exist in the current supply chain and how a cyber offender would exploit them.
3. Create a strategy for **closing security gaps** along with a clear **priority list.**
4. Establish comprehensive **third-party security policies and procedures** for the company based on business priorities and cyber risk appetite.
5. **Manage integrations** needed for the organization to be ready to implement the new policies.
6. **New third-party onboarding** - assessment of third parties against company policies before onboarding and **continuous monitoring** throughout the business relationship to check for cybersecurity gaps.
7. **Scalable and continuous reporting** on changing third-party-related risk levels, fine-tuning, and scaling the strategy as needed.

WHAT SHOULD YOU EXPECT?

- **Tailored and scalable supply chain risk management program.**
- **Zero overhead for clients, fully managed service.**
- **Policies adapted to unique company business needs, priorities, and risk appetite.**
- **Maturing organizational TPRM program in consideration of business requirements, workflows, and priorities.**
- **Assessing key vulnerabilities and strengths.**
- **Implementing effective risk controls.**
- **Clear prioritization of security threats that need to be handled immediately vs. items that do not pose an immediate risk.**
- **Straight-forward remediation and mitigation tactics and workflows.**
- **Elevating company security posture.**

How can enterprises keep up with today's 3rd party cyber risks? By getting ahead of them.

For many companies, third-party risk management has become a compliance requirement, a tick-box exercise demanded by regulators and customers, rather than a crucial tool to assure business continuity and bolster an organization's cybersecurity state. Yet, in recent years, we have seen devastating cyber attacks caused by third-party breaches that warrant a more serious approach, including the 2020 *SolarWinds* attack in the US, which created severe implications for a vast number of organizations, including the

Cybersecurity firm FireEye and the upper echelons of the US Government, including the Department of Homeland Security and the Treasury Department. Another notable example is the July 2021 attack via *Kaseya VSA*'s software platform, one of the most significant ransomware attacks in history, with as many as 1,500 companies affected worldwide. A Swedish retail chain was forced to close more than 800 stores. Such breaches are increasing in frequency and severity, occurring across all industries.

To address today's vast risks, HolistiCyber provides a fully managed service that covers all aspects, from full vendor/service provider vetting, onboarding and management, and on to deep analysis of business needs, threats, and attackers' motivations.

Genuinely understanding the business and its third-party relationships is critical, as this determines the most appropriate data collection methods and contextual interpretations. Our approach ensures the program is always tied to business objectives and that third parties and in-house teams are not bombarded with useless data.

The service is priced per the third party and is scalable (whether an organization works with ten third parties or several thousand).

In-depth analysis is provided on many business and security aspects, ranging from SOC2 assessments to service provider/vendor on-site visits (on the client's behalf).

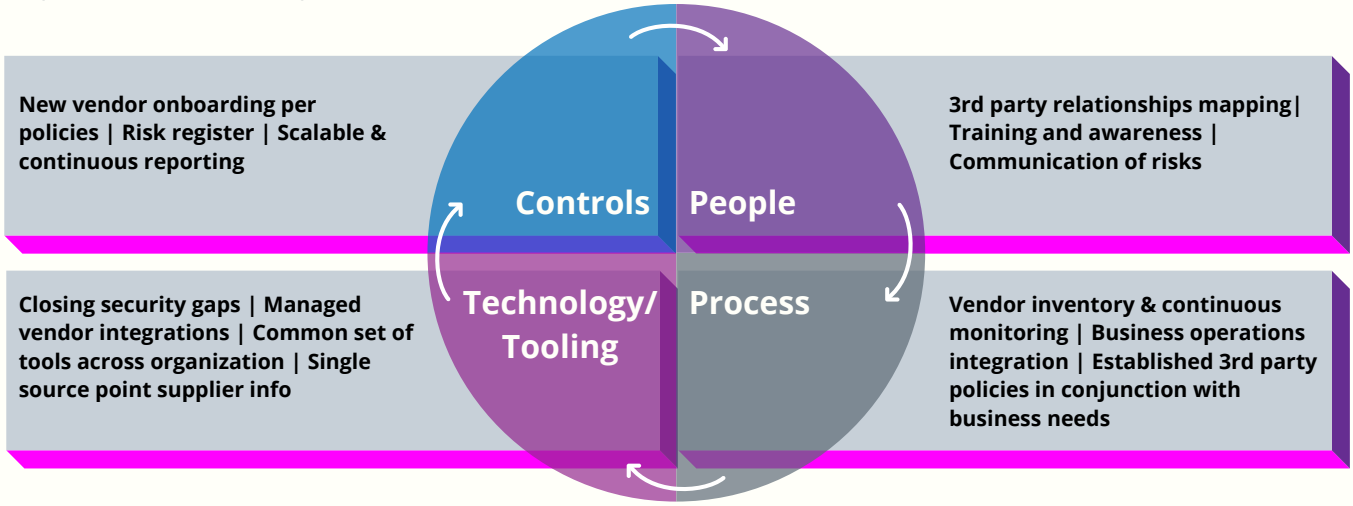

Figure 1: Continuous Third Party Risk Management

Why HolistiCyber?

1. **Nation-state-grade expertise** - our staff of white-hat security experts is composed of former military and government offensive practitioners who can examine the attack surface from the vantage point of the attacker and not only from the company's vantage point. We have a solid grasp of the sophisticated tooling available to today's attackers and access to those attack tools.
2. **Holistic approach** - we tie compliance, remediation, and mitigation solutions to each company's unique business objectives and workflows. Security should complement productivity and growth and avoid hindering them.

"HolistiCyber TPRM team delivered immediate and measurable security impact and profound business benefits and efficiencies. Our in-house security team can now devote time to other essential tasks."

CISO, large healthcare provider, USA