Ransomware Has Changed Third-Party Risk Management:

From Information Protection Risk to Business Continuity Crisis

HITRUST®

Organizations rely on a complex web of third-party vendors, suppliers, and service providers to keep their operations running smoothly. As the digital footprint expands, so does the attack surface for cybercriminals. While data breaches have long been a concern, a newer and more disruptive threat has emerged: ransomware. Rather than simply stealing data, ransomware can bring entire business operations — and even entire supply chains — to a grinding halt. This escalation in both frequency and severity has shifted the Third-Party Risk Management (TPRM) landscape. TPRM leaders must now manage the risks of data compromise and also the possibility that a partner's ransomware incident could paralyze critical business functions, holding operations hostage and causing widespread disruption.

A stark example is the 2024 incident, where a critical healthcare service provider suffered a major ransomware attack. Beyond exposing sensitive data, the resulting operational downtime disrupted patient care services, billing workflows, and critical partner integrations. The cascading effects were felt not only by the organization attacked but also by a network of hospitals, practices, and other healthcare providers, underscoring the alarming new reality:

Ransomware is as much a business continuity crisis as it is an information protection risk.

This eBook explores the urgent need to adapt TPRM strategies to this evolving threat. We will examine why standard approaches such as SOC 2 and questionnaires often fall short in mitigating the modern ransomware menace. We will outline practical steps to bolster business continuity planning, integrate cybersecurity with operational resilience, and leverage HITRUST for more robust third-party risk mitigation. The question is not if another disruption will occur but *when* — and whether your organization will be ready.

The Expanding Ransomware Threat Landscape

Ransomware by the Numbers

Ransomware attacks have surged in frequency and severity over the past five years. It has become the most common action in breaches, according to Verizon's 2025 Data Breach Investigations Report.

44% of breaches involve ransomware.

IBM's 2024 Cost of a Data Breach Report states the average cost for a ransomware attack as USD 4.9 million.

Ransomware leads to downtime, triggering operational bottlenecks and lost business opportunities, followed by legal consequences and reputational damage.

Third Parties: The "Soft Underbelly"

Attackers increasingly target third-party vendors, knowing these organizations often have weaker cyber defenses compared to large enterprises. A vulnerability in one vendor's environment can grant criminals a foothold in multiple client networks. Ransomware operators then move laterally across interconnected platforms, launching coordinated attacks that can devastate entire supply chains.

Shift from Data Theft to Service Disruption

Early ransomware attacks primarily involved encrypting data and demanding payment for its decryption. Today, malicious actors realize they can inflict even greater damage and extract higher ransoms by halting critical systems and services and exfiltrating data. For organizations and their third parties, a day of downtime can be more financially ruinous than a data breach alone.

The Limitations of Traditional TPRM Approaches

Why Standard Compliance Measures Are No Longer Enough

SOC 2 reports and other compliance audits were never designed to address the operational impact of a large-scale ransomware incident. While these assessments focus on the existence of security controls, they offer limited insights into how well-prepared an organization is and how quickly it can recover from a full-scale shutdown.

The Failure of Questionnaire-Based Vendor Assessments

Many TPRM programs still rely heavily on static questionnaires. These tools offer only a snapshot of a vendor's security posture at a specific moment in time. They rarely capture real-time changes in threat environments, technology stacks, or organizational risk factors. The answers are often subjective, not validated, and limited in information. As ransomware attacks become more frequent and agile, a self-attested, point-in-time checklist fails to provide ongoing assurance.

Challenges in Risk Quantification

Understanding how a disruption at a single vendor might cascade through an interconnected supply chain is difficult. Standard risk heat maps and manually updated spreadsheets cannot keep pace with the evolving threat landscape. This gap often leads to an underestimation of potential downtime and a lack of robust contingency plans.

The New TPRM Model — Proactive Resilience

Cybersecurity and Business Continuity Integration

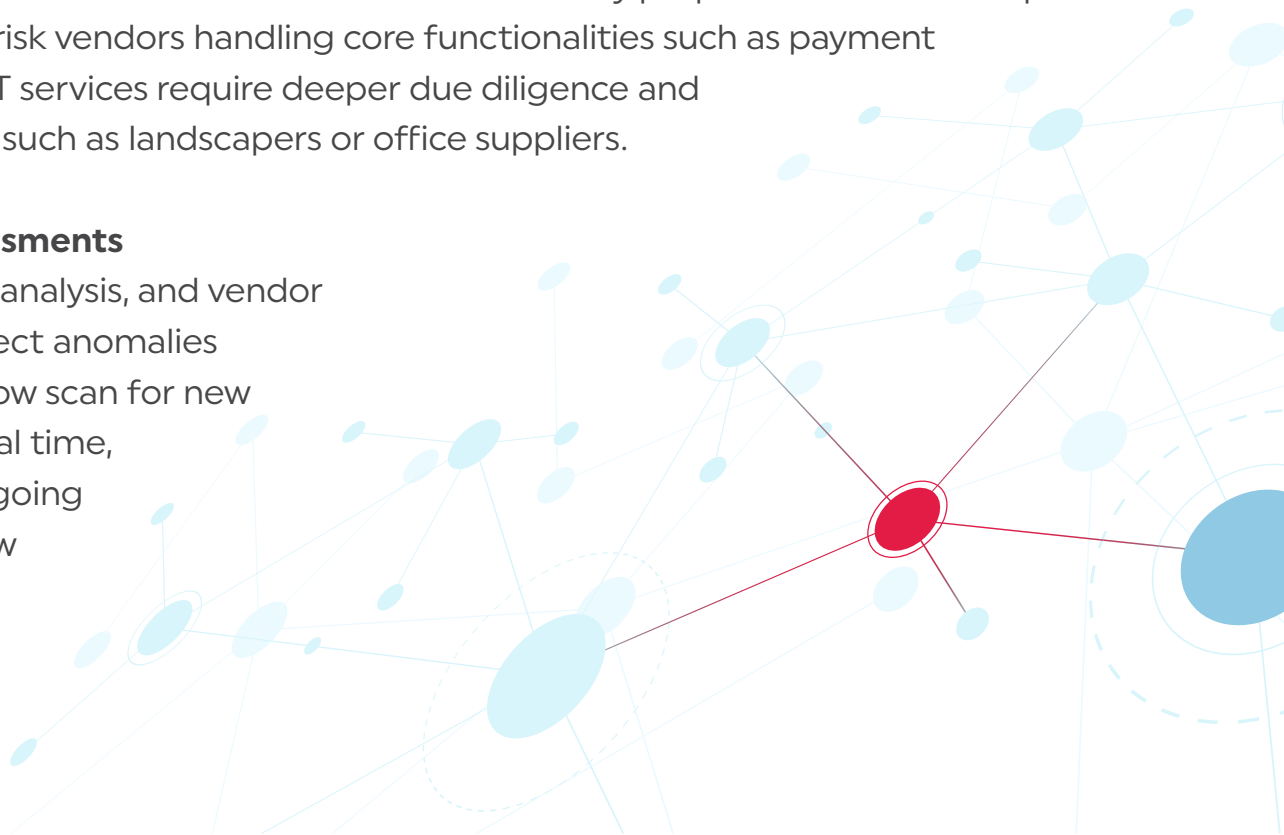
A forward-thinking TPRM strategy integrates cybersecurity practices with robust business continuity and disaster recovery planning. Organizations must ensure that their vendors have the right controls to reduce risk. They must also confirm that partners have the resilience to maintain or quickly restore critical services in the face of ransomware.

Structured Approach to Vendor Risk Tiers

Assigning risk tiers to vendors allows organizations to allocate resources and scrutiny proportionate to the impact a third party could have on operations. High-risk vendors handling core functionalities such as payment processing, patient management, or critical IT services require deeper due diligence and continuous monitoring than low-risk vendors such as landscapers or office suppliers.

Continuous Monitoring and Adaptive Assessments

Real-time threat intelligence, network traffic analysis, and vendor performance metrics help TPRM leaders detect anomalies before they escalate. Automated tools can now scan for new vulnerabilities or suspicious activity in near real time, triggering adaptive risk assessments. This ongoing vigilance is crucial in responding swiftly to new ransomware threats as they arise.



HITRUST's Role in Cybersecurity TPRM

HITRUST Inherent Risk Questionnaire (IRQ) and Rapid Assessment

Designed to help organizations quickly identify a vendor's level of inherent risk, the HITRUST IRQ streamlines due diligence by highlighting red flags that might indicate vulnerability to ransomware. Rapid assessments further allow for a timely yet comprehensive review of a vendor's readiness against critical threats.

HITRUST Assessment XChange

For many organizations, gathering risk data from hundreds (or thousands) of vendors can be overwhelming. HITRUST's Assessment XChange centralizes vendor risk data, facilitating efficient qualification and re-qualification processes. TPRM leaders gain a clear, comparative view of each vendor's resilience posture by using standardized scoring and consistent metrics. The HITRUST Assessment XChange App also integrates with leading GRC applications like ServiceNow to make effective vendor risk management more efficient.

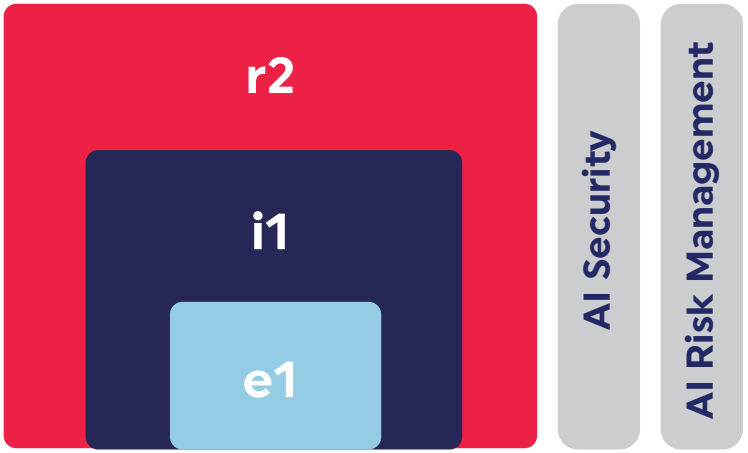
HITRUST Score

Unlike standalone compliance certifications, HITRUST offers actionable insights into a vendor's security and resilience. The scoring methodology considers the maturity of controls, ongoing compliance, and the organization's capacity for rapid response — key factors in defending against ransomware.

Tiered Assurance Model

HITRUST can help identify critical vendors and assign them to the highest tier, requiring more rigorous evaluations than other low-risk vendors. Leverage HITRUST's different assessment options for scalable risk mitigation.

- **e1** Focuses on essential cybersecurity hygiene for low-risk vendors
- **i1** Adds deeper security and privacy requirements for medium-risk vendors
- **r2** Offers the most comprehensive and rigorous assessment for high-impact service providers



All assessments are based on the HITRUST framework, which harmonizes more than 60 authoritative sources, including HIPAA, ISO, and NIST. The framework evolves with near-real-time threat intelligence data to keep organizations ahead of emerging threats.

Conclusion: Preparing for the Next Disruption

Ransomware-driven disruptions are not a passing trend; they are an evolving threat likely to intensify. As criminal groups become more sophisticated and well-funded, even the most vigilant organizations can be vulnerable — particularly through third parties. Consequently, TPRM strategies must evolve to prioritize business continuity, operational resiliency, and rapid response capabilities alongside standard information protection measures.

Whether you're safeguarding patient data in healthcare or ensuring uninterrupted payment processing in finance, the message is clear: **Elevate your TPRM approach now.** By integrating continuous monitoring, adopting tiered assurance models, and leveraging frameworks like HITRUST, you can build a more resilient supply chain — one capable of withstanding and recovering from the next inevitable ransomware attack.

The stakes are higher than ever; the time to act is now. **Will you be ready?**

Learn more: https://hitrustalliance.net/third-party-risk-management