TPRM IS BROKEN

CORL TECHNOLOGIES | HITRUST

Using Collaboration to Remodel Vendor Risk Programs

HITRUST and CORL are committed to collaborating with the industry to solve the toughest and most complex challenges facing healthcare cybersecurity programs.

Third-Party Risk Management (TPRM) has become one of the most daunting challenges for healthcare leaders as breaches mount, reliance on third parties for critical business functions expands, and the supply chain continues to get pummeled by our cyber-adversaries[1].

Our companies have listened attentively to our clients and colleagues and one message has come across loud and clear: **TPRM is broken.**

VENDOR BREACHES ARE DETERIORATING HEALTHCARE'S DIGITAL FOUNDATIONS

55%
percentage of healthcare organizations suffered a third-party data breach in the past year[2]

$10.1m
average cost of a breach for healthcare organizations[3]

100
number of covered entities impacted by the recent breach of Avamere vendor

1.1 million
patients impacted by breach of OneTouchPoint vendor involving over 37 prominent healthcare organizations

2.8 GB
amount of data stolen in a recent cyber breach from Cisco, a prominent provider of network services for healthcare organizations

>1,000
average number of vendors under contract by each healthcare provider in the U.S.

49%
of organizations have a comprehensive inventory of all third parties that have access to their systems[4]

TOP CHALLENGES FACING HEALTHCARE TPRM PROGRAMS

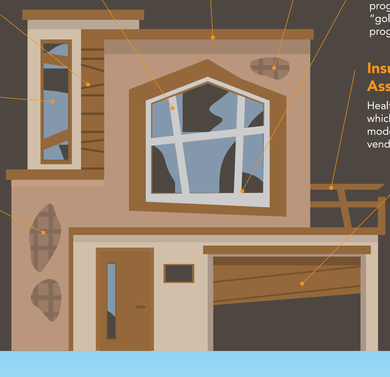
Too Much, Too Fast
TPRM teams can't keep up with the volume of inbound vendor assessments or the expectations for rapid turnaround times.

Limited Follow-Through on Remediation
TPRM teams have limited bandwidth to follow up and track remediation of vendor risks, leaving many exposures unresolved.

Vendors are Overwhelmed
Questionnaires and audits have become part of every customer conversation, and there is a high variance of customer expectations.

Lack of Resources
TPRM teams lack resources to scale assessments to audit and report on the entire vendor population.

Lack of Standards
There is a high variance of TPRM program approaches and no defined "gold standard" for healthcare TPRM programs.



Partial Inventories
Healthcare Organizations inventories do not cover the full population of vendors that the business relies on for operations.

Insufficient Adoption of Assurance Models
Healthcare leaders can't agree on which certifications and assurance models are sufficient to demonstrate vendor security posture.

TPRM Solutions are Incomplete
Point solutions for TPRM often fail to assess the specific scope, products, & implementation factors that drive organizational risk.

Inadequate Risk Reporting
TPRM programs are able to report risks across the entire vendor portfolio in a way that both technical and non-technical stakeholders can understand.

WORKING TOGETHER TO REMODEL HEALTHCARE TPRM PROGRAMS

Healthy security program indicators
Embracing the concept of security health program indicators and focusing on cyber resilience is a rising tide that lifts all boatsmechanisms

Elevate the risk management conversation
Changing the conversation from one that is deeply technical and confusing to one that is easily understood by business and clinical leaders

Third-party assurance
Valuing the inherited trust the industry can provide through rigorous third-party assurance mechanisms

Continuous remediation
Driving constant security improvement through continuous monitoring and remediation

Inherent risk standardization
Creating norms around inherent risk and vendor tiering in the TPRM ecosystem

Stacking Hands
Solving big challenges and making large-scale changes requires participation from leaders across the TPRM ecosystem

HITRUST and CORL are making investments in the future of TPRM and will join the knowledge, insights, and ingenuity of TPRM leaders from the nation's leading healthcare entities. Stay tuned for additional updates; you won't want to miss out on the opportunity to be involved in supporting this mission.

HITRUST

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks, related assessment and assurance methodologies.

Visit https://hitrustalliance.net/ for more information.

VISIT HITRUST

CORL TECHNOLOGIES

About CORL

CORL is a service-centered solution for vendor risk management, compliance, and governance that is 100% focused on the unique needs of the healthcare space. Driven by the belief that third-party vendor risk should be about business acceleration and not business prevention, we are the only platform and partner on the market to enable the velocity and validation needed for healthcare organizations to simultaneously achieve their digital goals and contain their digital risks

Visit corltech.com and follow us on LinkedIn.

VISIT CORL

[1] https://www.hipaajournal.com/55-of-healthcare-organizations-suffered-a-third-party-data-breach-in-the-past-year/
[2] 55% of Healthcare Organizations Suffered a Third-Party Data Breach in the Past Year
[3] 2023 Cost of a Data Breach Report
[4] 55% of Healthcare Organizations Suffered a Third-Party Data Breach in the Past Year

CORL TECHNOLOGIES

VISIT CORLTECH.COM AND FOLLOW US ON LINKEDIN