

Reducing Cybersecurity Risk by Automating Continuous Vendor Assessment

John Chisum, Dir., Solutions Consulting
RiskRecon



Today's Agenda

- Questions and challenges for today's third-party risk practitioner
- Perception vs preparedness: The impact of a third-party breach
- Unique approach leveraging automation
 - Discovery
 - True Risk Prioritization
- Functional use cases to evolve and scale a program with automation and innovation
 - Risk Assessment
 - Triage Critical Exposures
 - Act on Risk and Verify Action
 - High-risk Vendor Monitoring

What Questions are Being Asked?

- Challenges / Concerns Around Tactical Information
 - What is my third-party risk exposure today?
 - What information is no longer available, because onsite reviews cannot be scheduled?
 - Do my critical vendors have an accurate assessment in place?
 - How do my vendors reduce/manage risk of my data?
 - Is my third-party risk exposure getting better or worse?
 - Are any of my vendors operating systems in OFAC countries?
- Technical Security Information Questions Tough to Answer
 - Do my vendors encrypt sensitive data in transit?
 - Do my vendors manage software vulnerabilities well?
 - Who are my 4th Party Vendors?

What Challenges are Third-party Risk Professionals Facing?

Visibility

Limited objective info on vendors in some or all risk tiers

Limited situational awareness on 4th party hosts and geo-location risk

Productivity

Program is too manual and resource intensive

Assessment backlog too high

Exceeding internal SLAs

Risk Outcomes

Over-reliance on attestation

No risk prioritization of findings & scores

Out of cycle surprises

No objective confirmation of completed fixes

Vendor Satisfaction

Suppliers frustrated with one-size-fits all approach

Suppliers frustrated with growing demands on their time

Measurement & Reporting

Difficult to track and quantify program's impact on true risk reduction

Difficult to perform ad-hoc analyses on IT and security findings

A Wall Street Journal Pro risk & security survey...



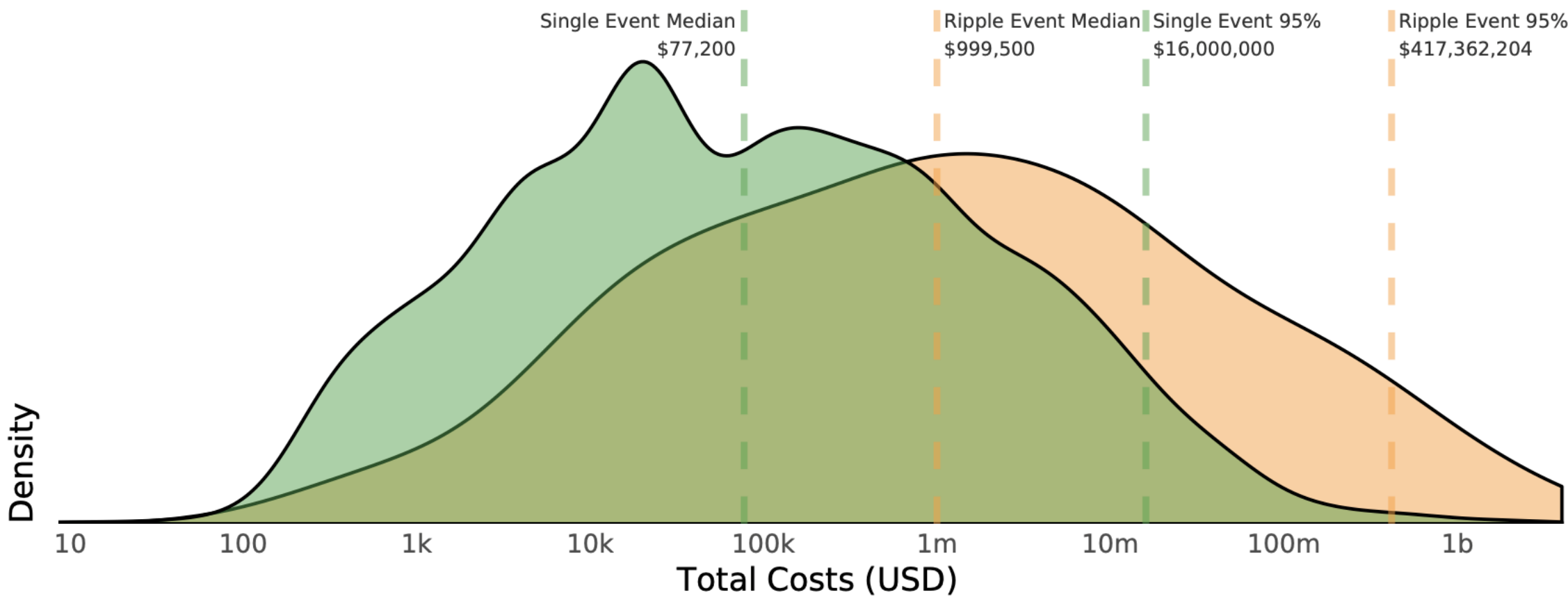
The Perception of Risk Outweighs the Preparedness

- 70% of organizations see third-party or supply chain risk as a major threat, yet less than 60% feel prepared to deal with it.
- Only 62% of businesses with more than \$250M revenue were able to qualify and quantify their risk to or from their suppliers
- 6 out of 10 risk professionals in the financial services industry state they are managing risk well.

Wall Street Journal Pro Research, Cybersecurity Online Survey of 389 enterprises conducted December 2019 – March 2020

The Financial Impact of Multi-party Data Loss (third-party)

FIGURE 12: DISTRIBUTION OF TOTAL LOSSES FOR SINGLE-PARTY INCIDENTS VS. MULTI-PARTY INCIDENTS

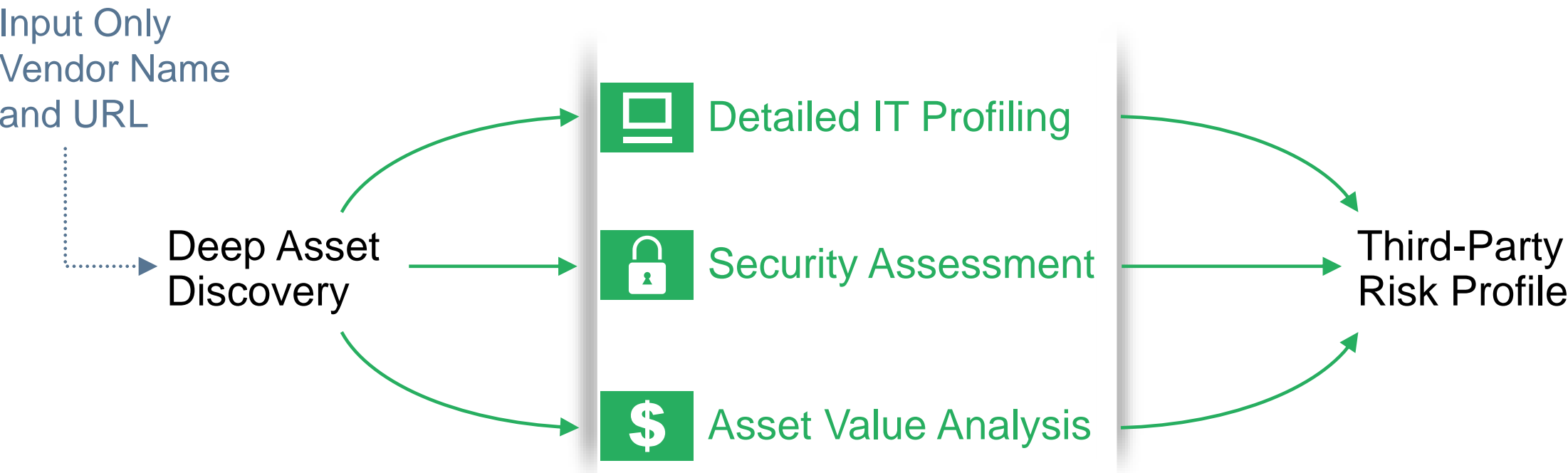


Our Approach to Third-party Risk

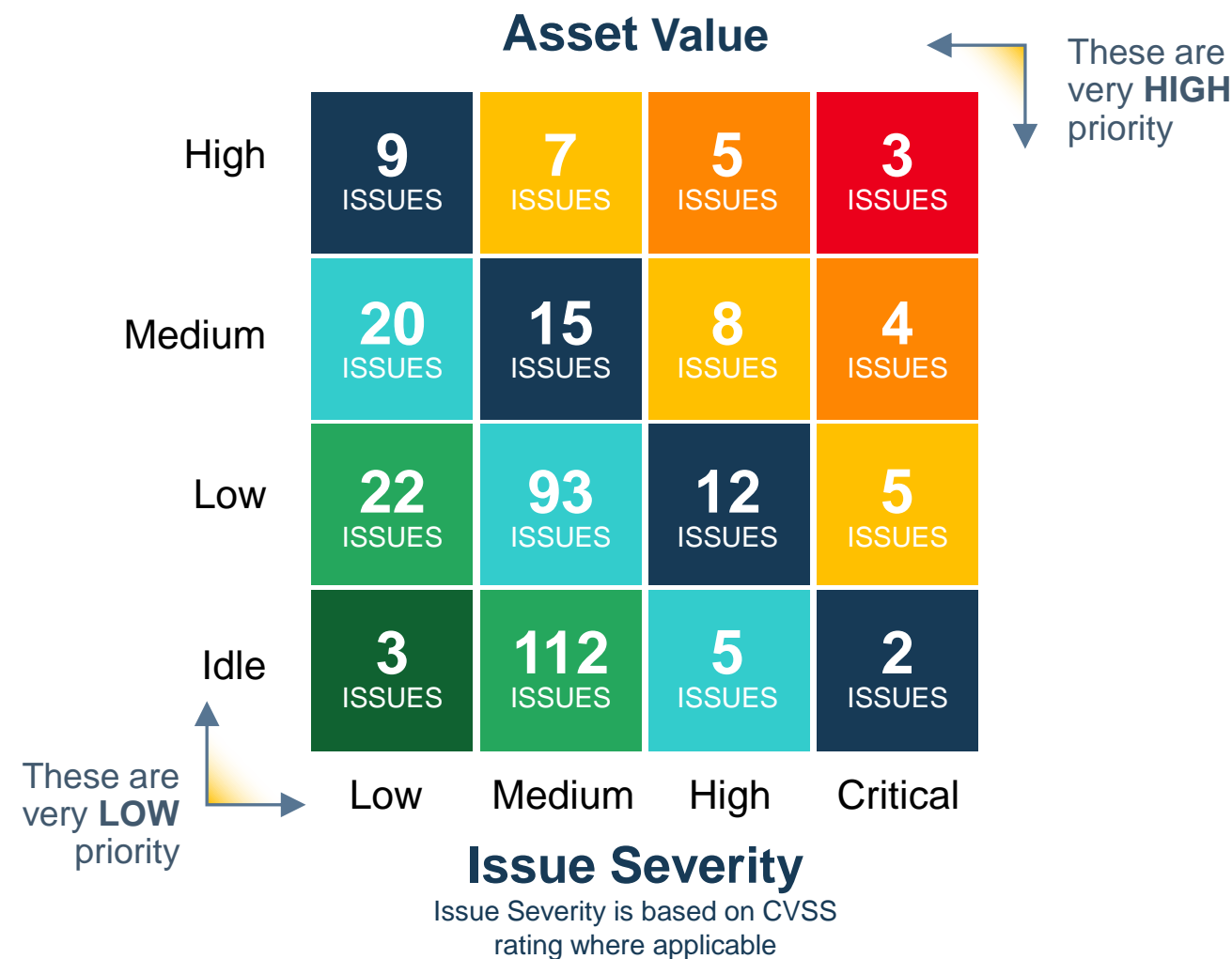
Understanding and Acting on Third-party Risk



Automation to discover assets & measure security posture



Automated Asset Valuation | Risk Prioritization

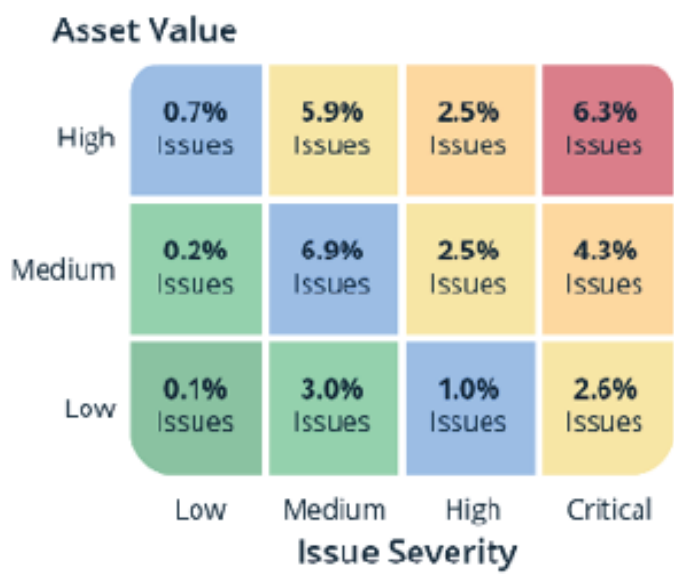


Asset Value Legend

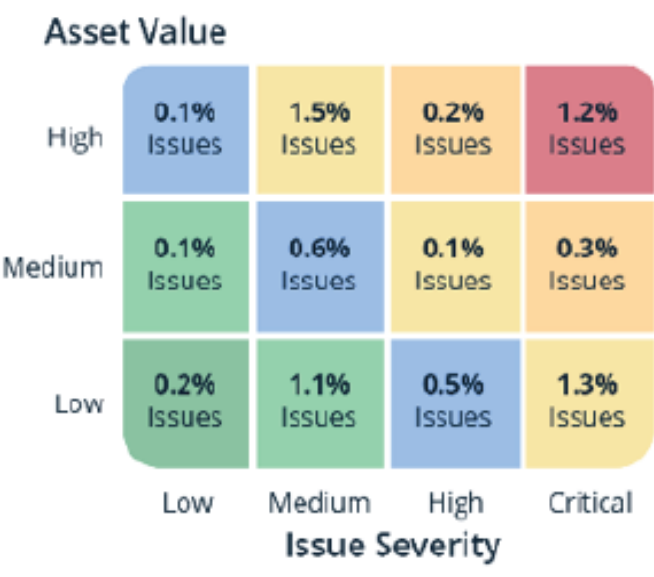
- High**
Systems that collect sensitive data
- Medium**
Brochure sites that are network neighbors to high value systems
- Low**
Brochure sites that are not network neighbors to any system
- Idle**
Parked domains and domain parking websites

The Data Reveals Who Manages Risk Well

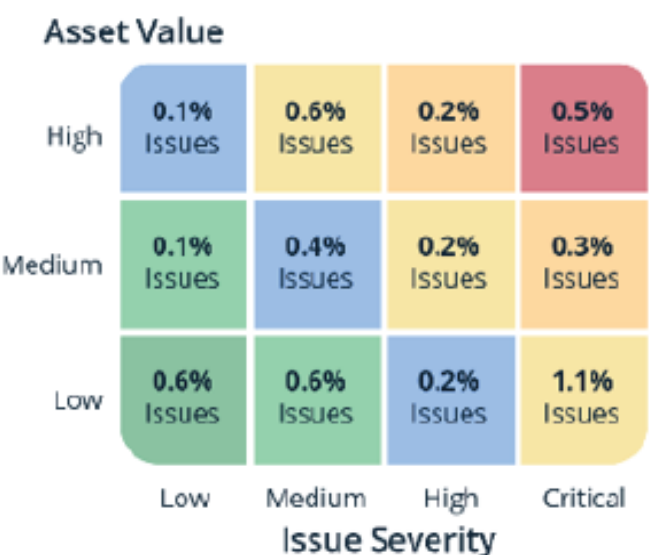
Universities



Healthcare

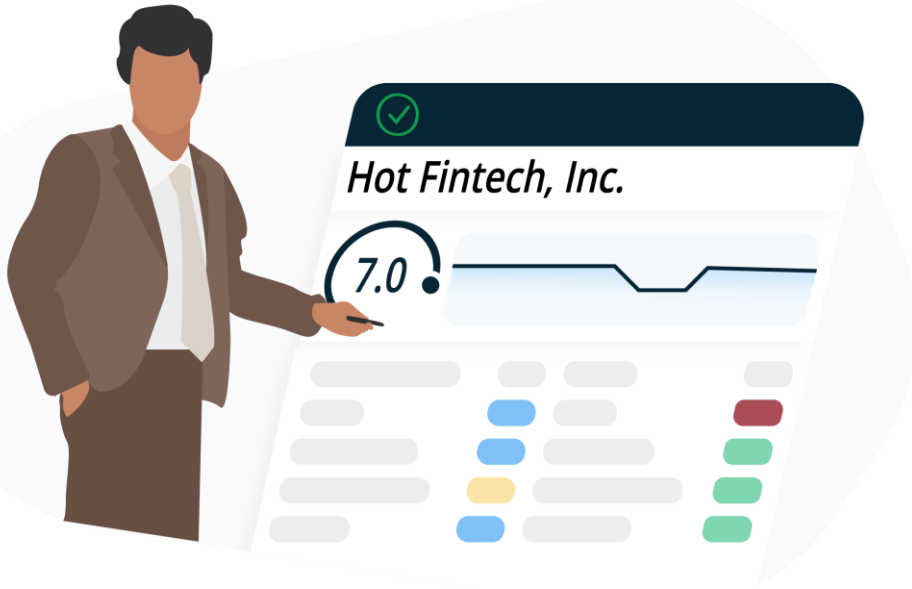


Banking



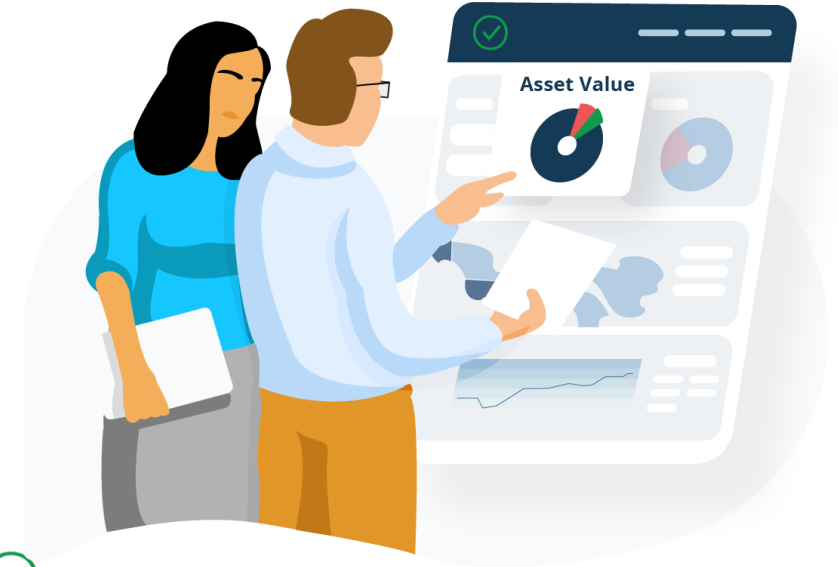
Use Cases / Case Studies

Use Case 1: Conducting An Assessment



Plan assessments based on knowledge of areas of strength and weakness.

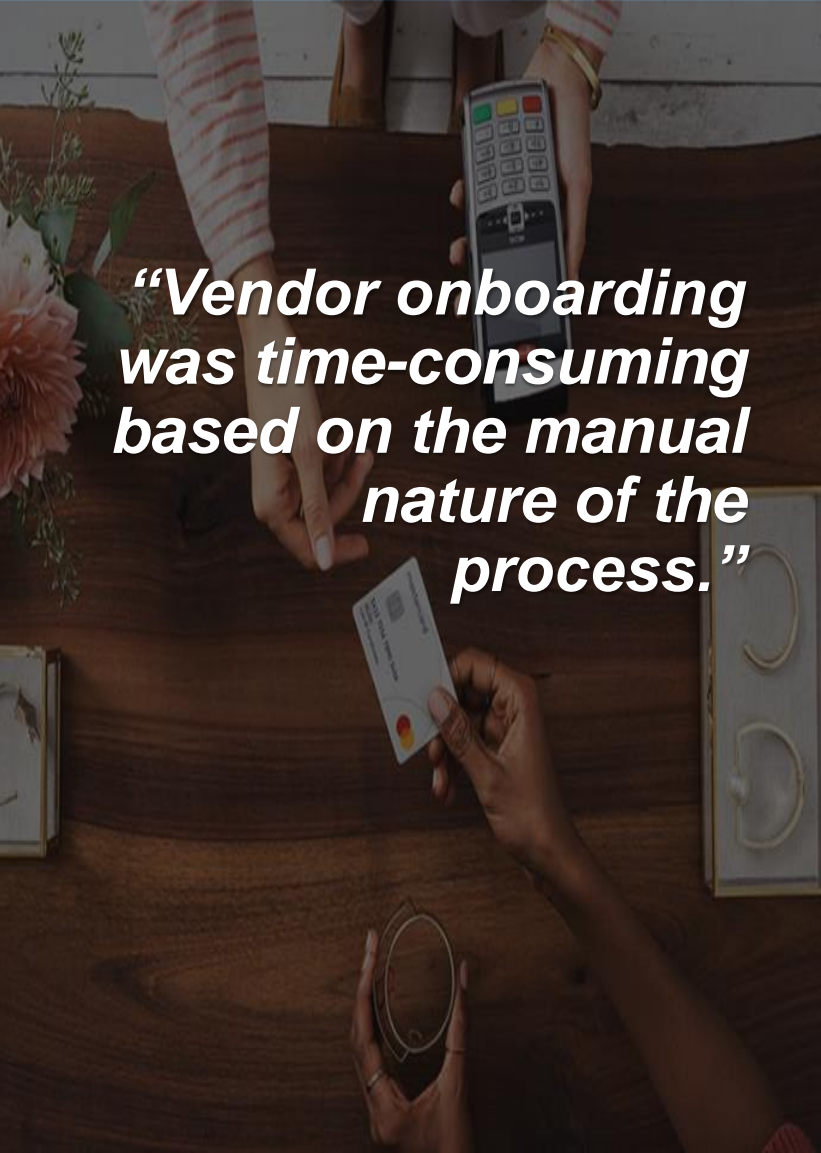
Automatically verify questionnaire responses with objective data.



Improve vendor performance through auto generated, evidence-based risk action plans.

Priority: Vendor Onboarding

Customer Profile



“Vendor onboarding was time-consuming based on the manual nature of the process.”

- **U.S. - based retailer**
- **A two-person team:**
 - Overburdened by the annual vendor assessment
 - Challenged with arduous onboarding process
- **Program maturity: Emerging**
- **Goal:** Improve efficiency and team capacity
- **Needed to answer the question:** Is my vendor really managing risk well, or are they just good at answering questionnaires?

On the process improvement:

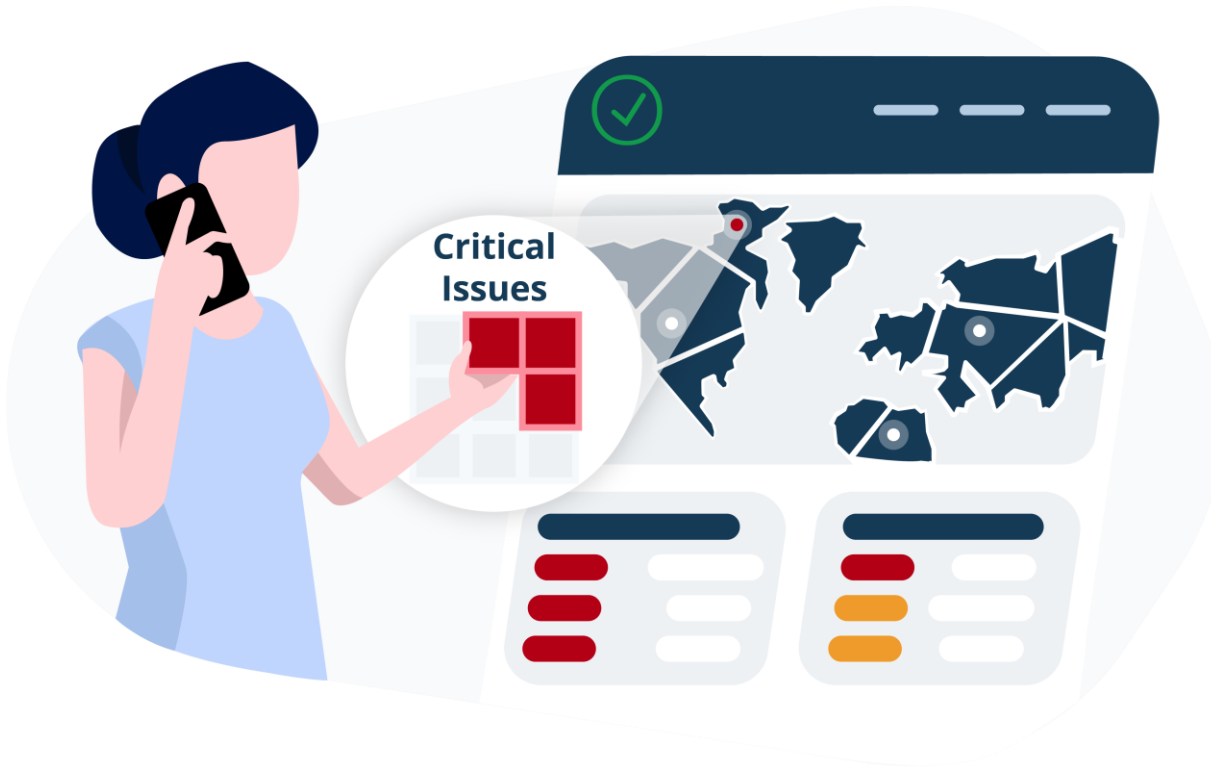


“We were able to objectively assess the range of vendors we wanted, how we wanted and could monitor with continuous capability for those out of policy.”

Implementation and Results

- Use one-time reports for initial review of all new vendors. (during onboarding process)
- For high performing vendors, send modified assessment.
- For low performing vendors send full assessment.
- Leverage RiskRecon's compliance module for validation.
- Add non-compliant vendors to continuous monitoring.

Use Case 2: Triage Critical Exposures



Survey all vendors, or target the ones you know are running exposed technology?

- Drown
- Shellshock
- NotPetya
- Pulse SSL VPN

Managing Vendor Vulnerabilities

“If a vendor vulnerability was discovered that could impact us internally, we needed a quick way to assess accurately to take action.”

Customer Profile

- **U.S. – based regional bank**
- **Challenges**
 - No effective way of responding to vulnerabilities that might impact vendors.
 - Vendor outreach process was inefficient, time-consuming and not particularly effective.
- **Program maturity: Common**
- **Goals:** Redefine process for vulnerability response and quickly provide status and tracking of impact to management.
- **Needed to answer the question:** Which of my vendors most likely is exposed to the [fill in the blank] zero-day vulnerability?

On the improving triage...



“Having a measurable set of outcomes with demonstrable triage success helped us manage the process and gain management support.”

Implementation and Results

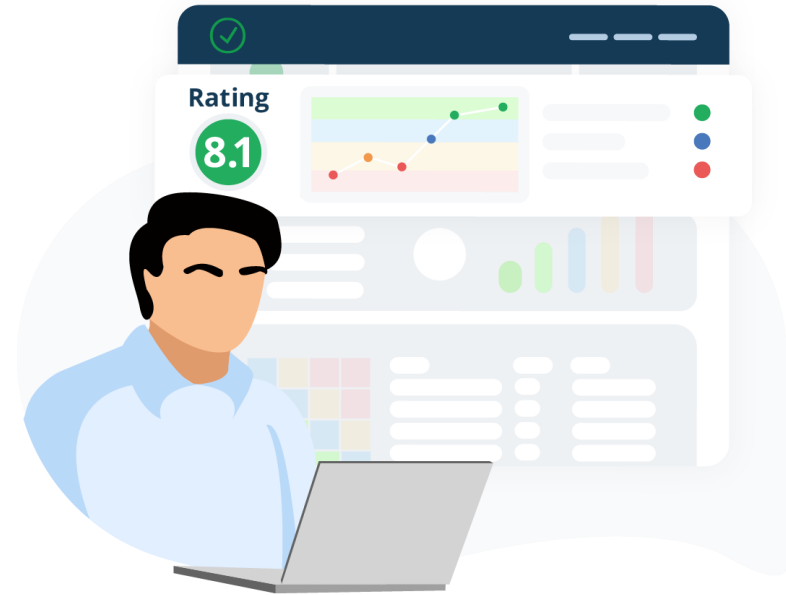
- Monitor vendors on a continuous basis.
- Leverage RiskRecon software and Hosting Provider Search capability to quickly identify the subset of vendors potentially impacted by unexpected vulnerabilities.
- Directly address at-risk vendors with RiskRecon detail.
- Report to management on vendor response and risk mitigation.

Use Case 3: Act on Risks and Verify Action

Share evidence-based action plans that automatically target material risks.



Automatically monitor the vendor's performance to verify that the issues are being addressed.



In Between Assessments...

“Our challenge was understanding the risk stemming from vendor behavior that created dangerous conditions in between our assessments.”

Customer Profile

- **Global Energy Company**
- **Challenge:** Visibility into risk behavior of critical vendors (between assessment cycles) was insufficient based on their established risk tolerances.
- **Program maturity: Pioneering**
- **Goals:**
 - Identify and act on risk as they occur.
 - Demonstrably improve overall risk posture.
- **Needed to answer the question:** How can I assist my vendor in improving security posture and how do I know if they are successful?

Vendor Collaboration to Fix Issues Discovered

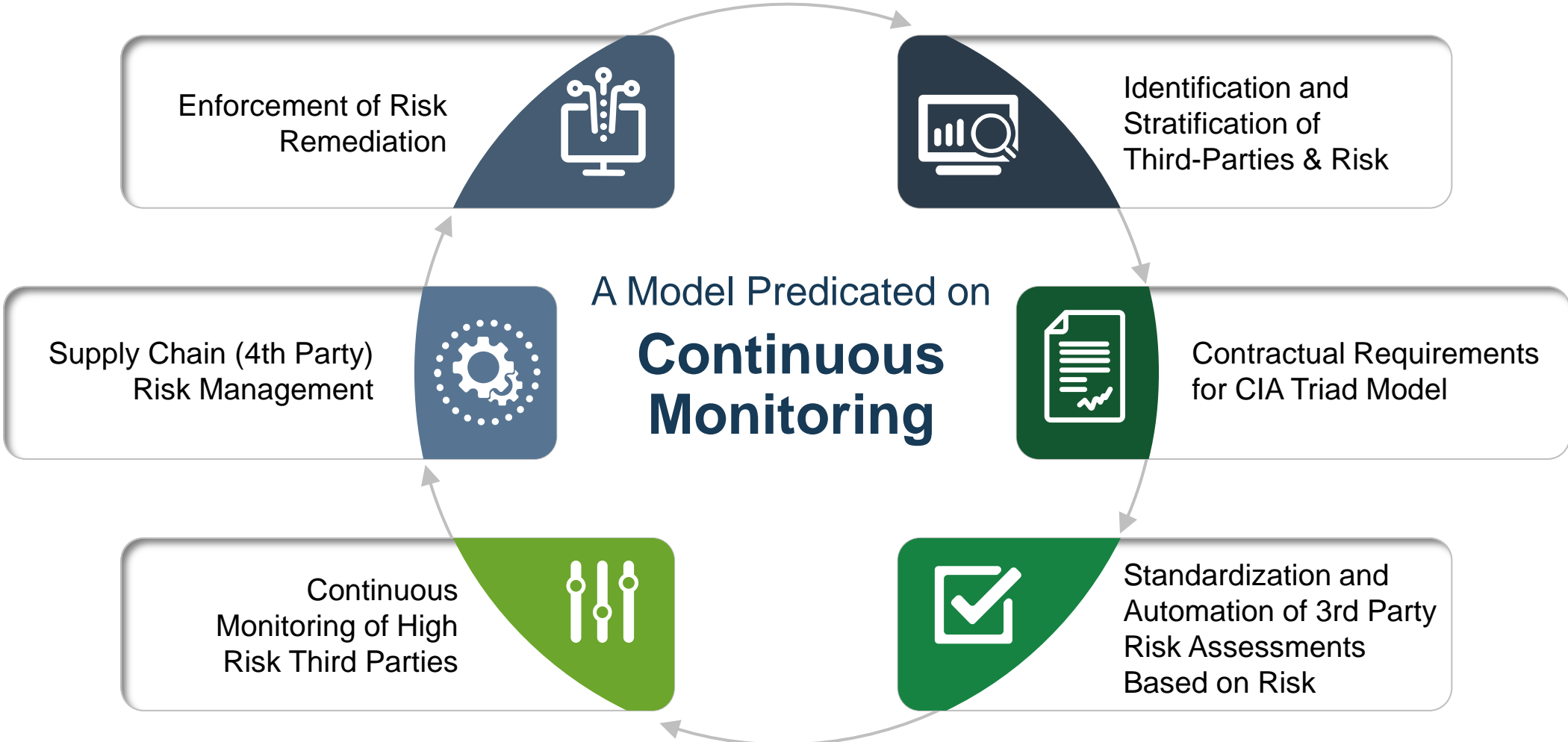
Implementation and Results



“The ability to tune policies and measure risk to that threshold across our vendor portfolio solved a lot of problems.”

- Set custom risk policies to track highest risk issues for critical vendor tier.
- Leverage alerting and action plans to notify vendors of critical vulnerabilities as they occur.
- Manage vendors to action plan performance.
- Track the closure of specific issues.

Operationalizing Into a Continuous Monitoring Approach



Key Drivers for Adoption

- **CISO drove investment in Third-Party Vendor risk**
- **Program required improvements to vendor risk accuracy**
- **Complete GRC integration**

Measuring Risk Outcomes

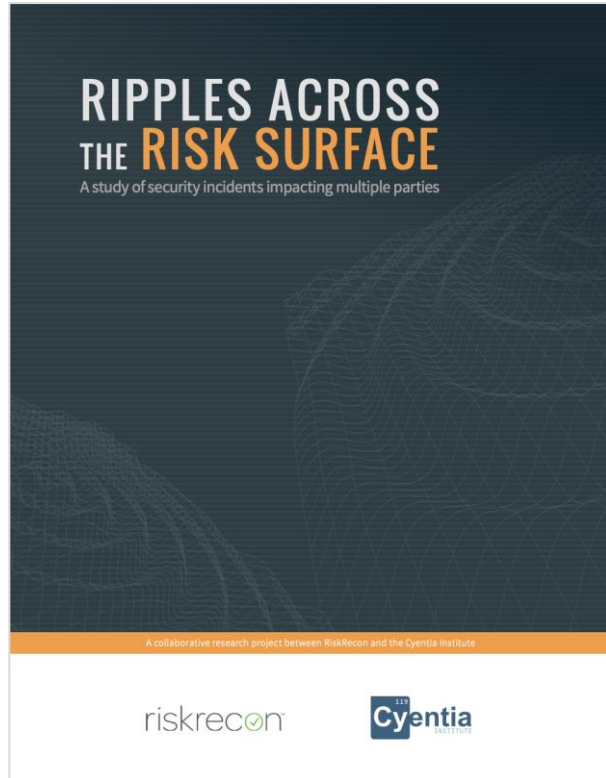


- **\$633K Annual Savings** (People, Process and Technology)
- **Lowered Annual TCO**
- **35% Productivity Increase**
- **35% Increase in Organizations Annually Assessed**
- **Full Implementation in Three Weeks**



A 50% Risk reduction has been realized annually as reported by their Risk Management team's aggregate 'Risk Radar' internal score.

Our Research and Tools



<https://www.riskrecon.com/ripples-across-the-risk-surface-tbm>



<https://www.riskrecon.com/aws-assessment-toolkit>



Thank you.