# MARSH RISK CONSULTING

Cybersecurity Consulting
and Advisory Practice

# MANAGING THIRD PARTY/VENDOR CYBERSECURITY RISK

The Marsh Risk Consulting (MRC) Third Party/Vendor Cybersecurity Risk Management service provides a cost-effective way of continuously monitoring and managing the cybersecurity risks that third parties may present to your enterprise. Cyber-attacks on third parties with authorized access to your network, systems, or data can seriously affect your operations through interruption of the services on which you depend, entry of malware that can migrate to your systems, compromise of your valuable data, and other actions and outcomes that can harm your business. We can help by:

- Offering an efficient alternative to the poor economics and scalability of trying to perform ongoing cybersecurity risk assessments on a large number of third parties and vendors.
- Highlighting the third parties and vendors most likely to experience a cyber event that could threaten your enterprise with malware, business interruption, or loss of data.
- Assessing aggregation risk by examining common "fourth party" dependencies of your third parties and vendors that can increase your risk exposure.

## A THREE-STEP PROCESS

MRC's Third-Party/Vendor Cybersecurity Risk Management service is tailored to your business needs and objectives and is implemented in three steps.

### 1 Program Design

- Conduct data discovery through in-person interviews with procurement, cybersecurity, risk management, and others to understand your existing enterprise vendor management framework and related processes.
- Understand the business requirements that drive third-party connections to corporate resources.
- Integrate MRC's continuous monitoring service with your enterprise vendor management program.

### 2 Third-Party Inventory and Baseline Assessment

- Comprehensively inventory and tier third parties, if a complete third-party inventory is not available.
- Create a baseline by analyzing the cybersecurity risk posed to your enterprise by each third-party through non-intrusive monitoring and assessment.
- Identify specific risk aggregation sources across third parties.

## 3 Ongoing Monitoring

- Provide monthly (or quarterly) reports with in-depth analysis of both primary and aggregate third-party cybersecurity risk.
- Aid in due diligence of potential new third parties and vendors prior to onboarding.
- Add vetted and onboarded new third parties and vendors to the monitoring service.
- Identify recommended actions and a detailed protocol for addressing third-party risks.

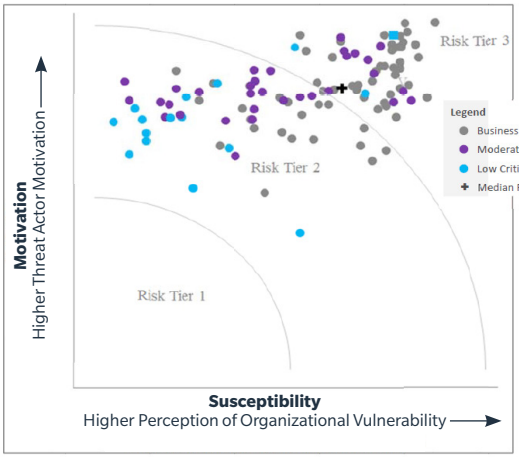
## BIG DATA CYBERSECURITY RISK ANALYSIS TOOL

MRC uses a Big Data cybersecurity assessment tool developed by Cyence, a leading cybersecurity analytics services provider, which provides predictive indicators of the overall likelihood of being successfully targeted by internal or external threat actors. This proprietary assessment tool continuously aggregates a multitude of data sets for over 200,000 firms in a non-invasive fashion yielding a measure of a company's cyber risk.

### Primary Risk

Our analysis of **primary risk** is based on data on your third parties' and vendors' risk levels.

Vendor Risk Ratings




### Aggregation Risk

Our analysis of **aggregation risk** is based on the risk posed to your enterprise by the use of common service providers by your third parties and vendors.

Shared Service Provider Matrix (Showing the number of service providers shared between High Risk-Business Critical vendors)

| | Vendor 90 | Vendor 91 | Vendor 92 | Vendor 93 | Vendor 94 | Vendor 95 | Vendor 96 | Vendor 97 | Vendor 98 | Vendor 99 | Vendor 103 | Vendor 108 | Vendor 110 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vendor 90 | | 11 | 4 | 7 | 10 | 7 | 4 | 8 | 5 | 9 | 5 | 10 | 9 |
| Vendor 91 | 11 | | 6 | 8 | 13 | 7 | 6 | 10 | 6 | 11 | 6 | 10 | 12 |
| Vendor 92 | 4 | 6 | | 2 | 8 | 4 | 2 | 4 | 5 | 4 | 3 | 4 | 5 |
| Vendor 93 | 7 | 8 | 2 | | 15 | 5 | 3 | 9 | 7 | 7 | 6 | 9 | 11 |
| Vendor 94 | 10 | 13 | 8 | 15 | | 7 | 6 | 13 | 10 | 12 | 10 | 13 | 15 |
| Vendor 95 | 7 | 7 | 4 | 5 | 7 | | 6 | 9 | 4 | 6 | 6 | 8 | 8 |
| Vendor 96 | 4 | 6 | 2 | 3 | 6 | 6 | | 7 | 3 | 6 | 5 | 5 | 6 |
| Vendor 97 | 8 | 10 | 4 | 9 | 13 | 9 | 7 | | 5 | 10 | 7 | 10 | 11 |
| Vendor 98 | 5 | 6 | 5 | 7 | 10 | 4 | 3 | 5 | | 6 | 6 | 7 | 13 |
| Vendor 99 | 9 | 11 | 4 | 7 | 12 | 6 | 6 | 10 | 6 | | 10 | 11 | 16 |
| Vendor 103 | 5 | 6 | 3 | 6 | 10 | 6 | 5 | 7 | 6 | 10 | | 8 | 11 |
| Vendor 108 | 10 | 10 | 4 | 9 | 13 | 8 | 5 | 10 | 7 | 11 | 8 | | 15 |
| Vendor 110 | 9 | 12 | 5 | 11 | 15 | 8 | 6 | 11 | 13 | 16 | 11 | 15 | |

*Sharing Threshold = 12*

## WHY MARSH?

Only Marsh provides clients with award-winning and industry-leading expertise in: technical cybersecurity, forensic accounting, economic modeling and analytics, and cyber insurance broking.



### Who it's for

Organizations that have:

- External service providers and market partners (third parties/ vendors) that require access to corporate information resources.
- Limited visibility into the cybersecurity controls of their third-parties and vendors.
- Little fact-based insight into where the biggest third-party cybersecurity risks lie.
- Limited or no ongoing monitoring of third-party cybersecurity posture over time.
- No insight into "fourth party" aggregation risks.

### What you get

- Regular analytical reports based on independently acquired data.
- Comparative ratings of the cybersecurity risk of all third parties.
- Identification and baselining of risks from common dependencies.
- Ongoing monitoring.
- Prescriptive advice on how to improve the cybersecurity risk inherited from third parties.

**Additional information can be found on www.marshriskconsulting.com and on www.marsh.com, or:**

THOMAS FUHRMAN
Managing Director
+1 703 731 8540
thomas.fuhrman@marsh.com

BRANNAN JOHNSTON
Managing Director
+1 212 345 9698
brannan.johnston@marsh.com

JAMES HOLTZCLAW
Senior Vice President
+1 202 297 9351
james.holtzclaw@marsh.com