cybervadis

How to manage the Cybersecurity footprint of an expanding network?

Agenda

- Context

- Challenges in running an effective TPCRM program

- Solutions to those challenges

- About us

Context

56%

Percentage of security incidents that result from indirect attacks (third party)

Study - Ponemon Institute - 2020

71%

Percentage of companies that consider themselves immature in their management of third-party risk
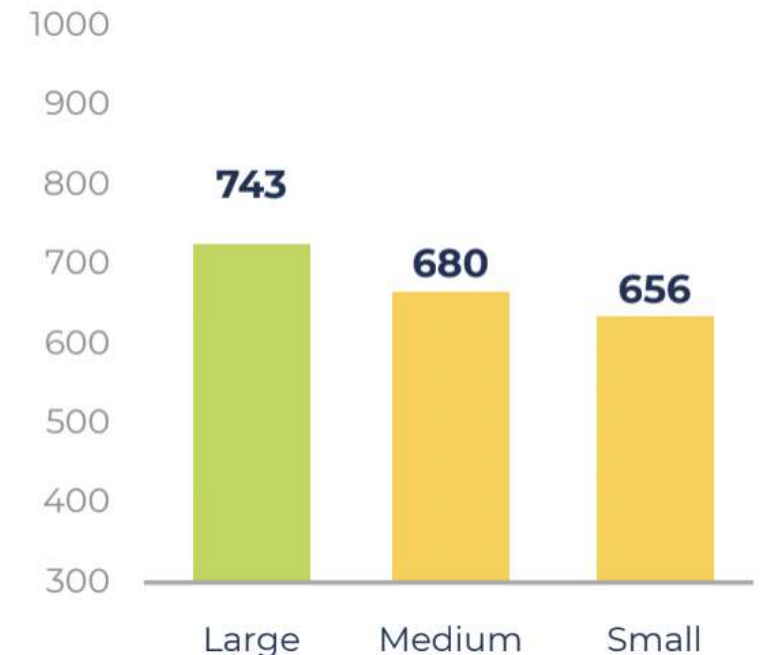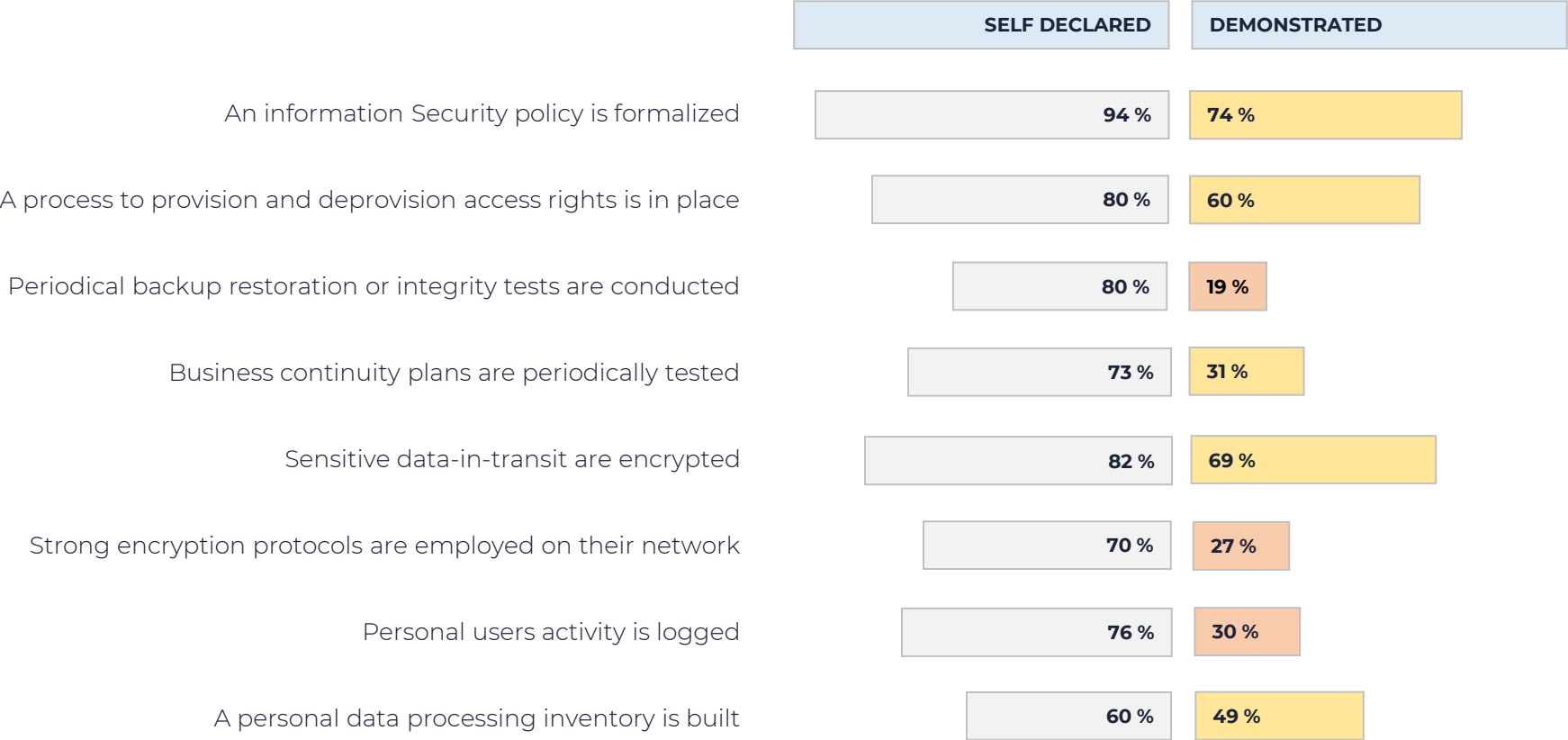
Study - Ponemon Institute - 2020

Your suppliers need you

- Small & Medium Size Companies maturity is lower than larger companies

  ○ quite often don't have Information Security resources

  ○ they are the main source of risk and preferred hackers targets

- Larger organisation have a role to play in increasing overall ecosystem maturity and to better protect themselves

  ○ Provide meaningful feedback to suppliers

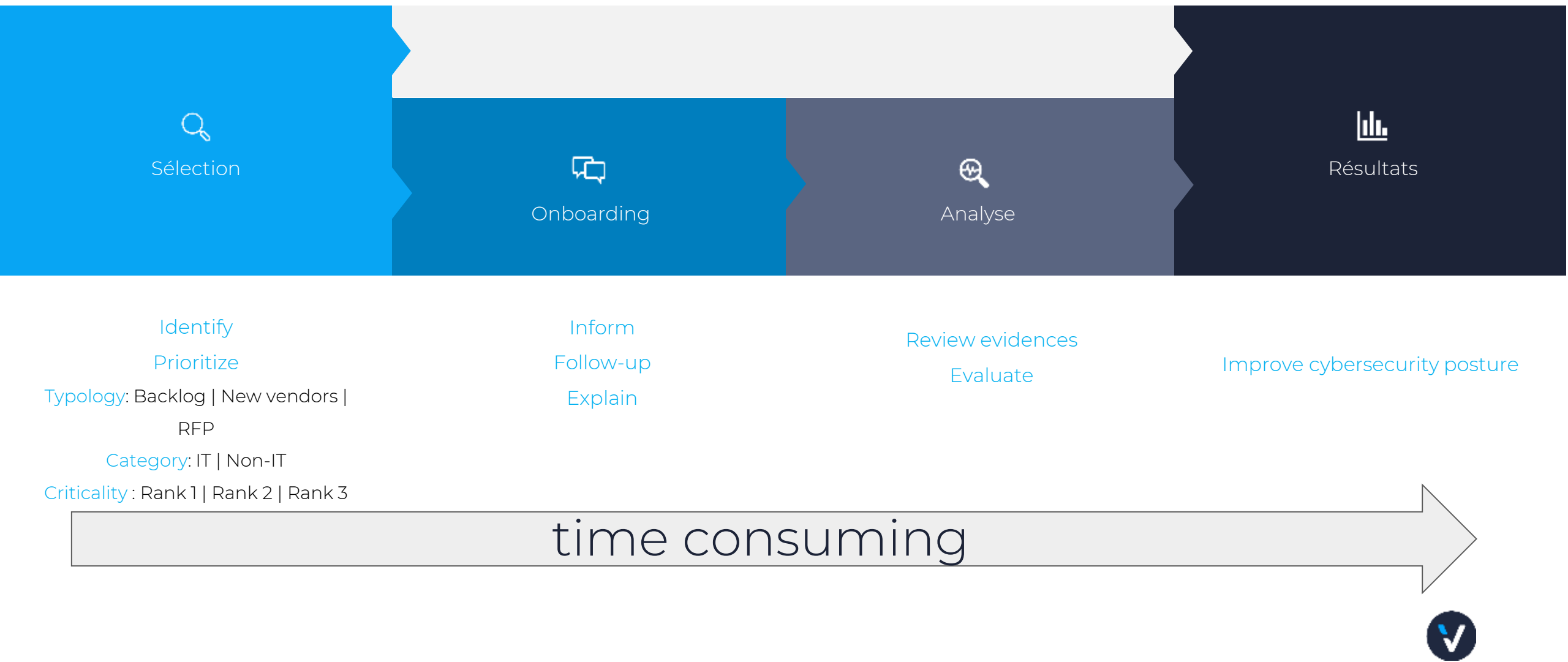 ○ Provide detailed analysis and improvement plan

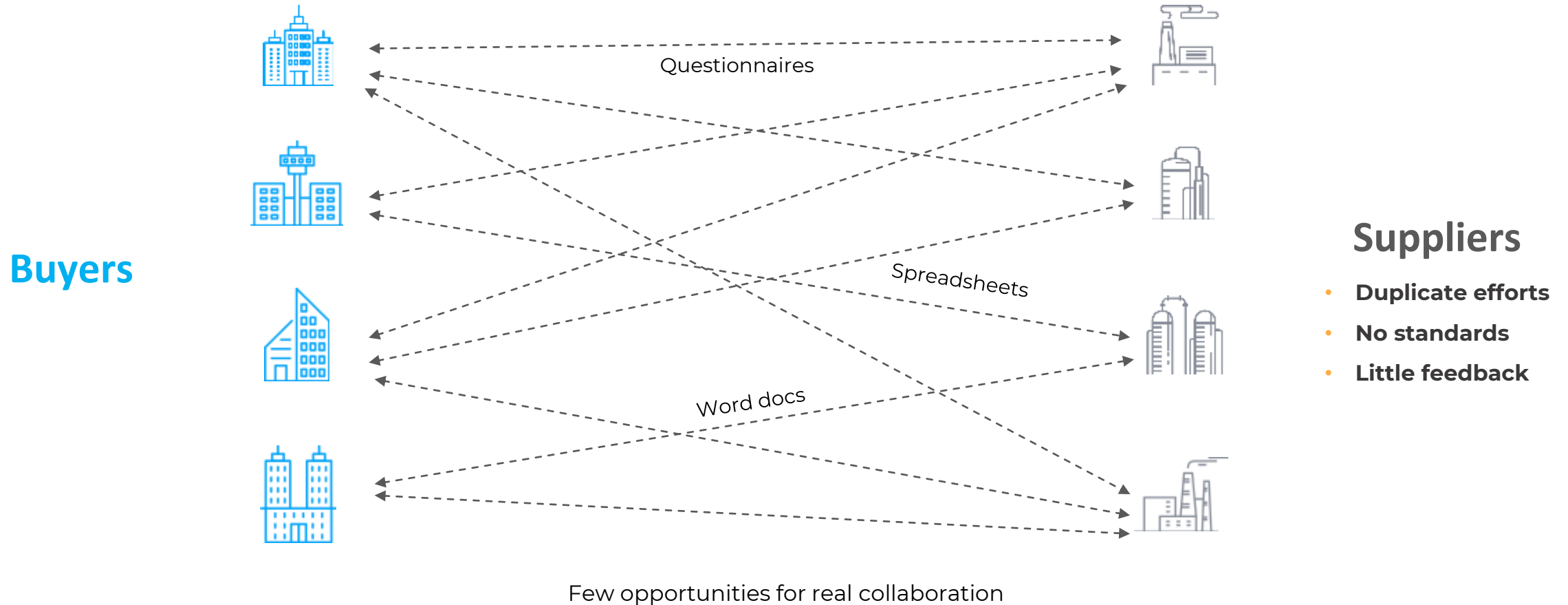**Average maturity score by company size (out of 1,000)**

Source: sample of Cybervadis assessed companies

Getting **reliable assessments** is a challenge

	SELF DECLARED	DEMONSTRATED
An information Security policy is formalized	94 %	74 %
A process to provision and deprovision access rights is in place	80 %	60 %
Periodical backup restoration or integrity tests are conducted	80 %	19 %
Business continuity plans are periodically tested	73 %	31 %
Sensitive data-in-transit are encrypted	82 %	69 %
Strong encryption protocols are employed on their network	70 %	27 %
Personal users activity is logged	76 %	30 %
A personal data processing inventory is built	60 %	49 %

Resources are a challenge

| Sélection | Onboarding | Analyse | Résultats |

Sélection

Identify
Prioritize
Typology: Backlog | New vendors | RFP
Category: IT | Non-IT
Criticality : Rank 1 | Rank 2 | Rank 3

Onboarding

Inform
Follow-up
Explain

Analyse

Review evidences
Evaluate

Résultats

Improve cybersecurity posture

time consuming

Solutions to these challenges

Challenge 1: Getting reliable assessments

Accuracy & Reliability

Evidence-based assessments - for ALL vendors

Based on cyber security industry international standards

Performed by expert cybersecurity analysts

Challenge 2: Time & resources

Managed Services

Assess an unlimited number of vendors for a fixed level of investment

Team of experts conducts onboarding and analysis for you

Focus on risk mitigation

Challenge 3: Multitude of assessments
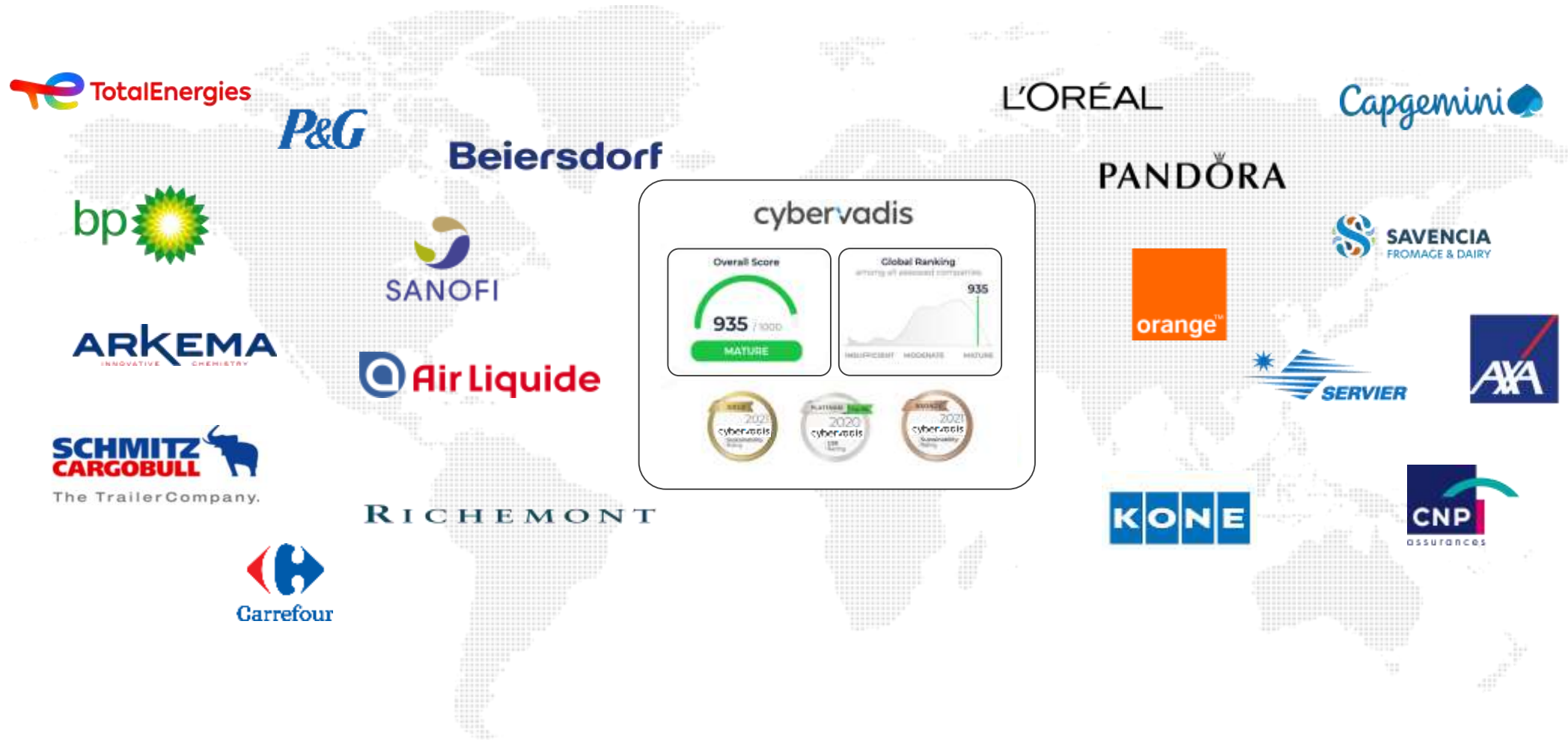
Sharing assessments

Shared-value business model

Vendors go through one single assessment to share with all their clients

Company has access to previously assessed vendors

Some of our clients

cybervadis

Thank you for your attention!

Contact:

Michael Kern

mkern@cybervadis.com