Global third-party networks are crucial for businesses but pose unique threats

Reliance on **Third Parties** – suppliers, vendors, contractors, outsourced teams, service providers, alliance partners, subsidiaries and affiliates – poses the threat of disruption to business should a third party fail to meet expectations.

Types of potential risks incurred by third parties

- **Business disruption**: a key third party failure can prevent a business from delivering with due speed and quality to its own customers.
- **Reputational**: failures/transgressions of third-parties will reflect on the prime business.
- **Regulatory**: Regulators frequently hold prime contractors accountable for the actions of third parties.
- **Financial**: Market share/revenue loss and/or financial sanctions can accompany above threats.

Potential benefits

- **Increased performance** – if companies’ third-party networks become more dependable they can deliver with more quality and consistently for their own customers without being hindered by lack of crucial supplies/services, potentially generating more demand in the marketplace.
- **Increased market share** – additional lead time generated for planning around third party needs can allow clients more time for due diligence in leveraging third parties. Missteps by under-vetted third parties can damage a company’s reputation and incur penalties that may affect a client’s standing in marketplace.
- **Increased profitability** – companies avoid costs related to scrambling to fill third-party product/service gaps in the event of disruption by prudent planning enabled by advance intelligence.
- **Decreased burden on resources** – enhanced governance that doesn’t require added resources at a cost-efficient price point. Less disruption means fewer ‘fire drills’ that tie up existing resources.
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

1. Accurate and timely third party intelligence to identify and address threats?
2. Enough lead time around potential third-party disruption?
3. The right tools to properly govern third parties’ activities?
4. Backup plans in place to quickly neutralize threats once identified before they become harmful to the organization?

Questions for Senior Management

1. How do we ensure our third parties are less vulnerable to disruption?
2. How do we conduct the appropriate level of third party risk monitoring, both geopolitical and financial?
3. How can we anticipate third party or supply chain disruption in enough time to act?
4. Do we have the appropriate tools in place to monitor third parties around the world, whether public or private?
5. Do we get timely and actionable risk alerts so that pre-emptive action can be taken before it is too late?

What is required?

— Ability to anticipate supplier disruption
— Consistent access to data for all third parties
— Efficient data acquisition model
— Ability to define risk metrics and thresholds
— Robust data analytics
— Risk monitoring and alerts
— Workflow processes to facilitate timely risk reviews

What value it brings to you?

— Intelligence you can act on to mitigate risk
— Actionable intelligence for both public and private third parties
— Ongoing third-party threat monitoring
— Data-driven decision support
— Ability to track and close reviews

What actions could the Board consider?

Ensure that our management team have evaluated and addressed gaps in our organization’s third party governance process
Consider technology solutions to uncover insights about our suppliers and evaluate options for mitigating current and future risks