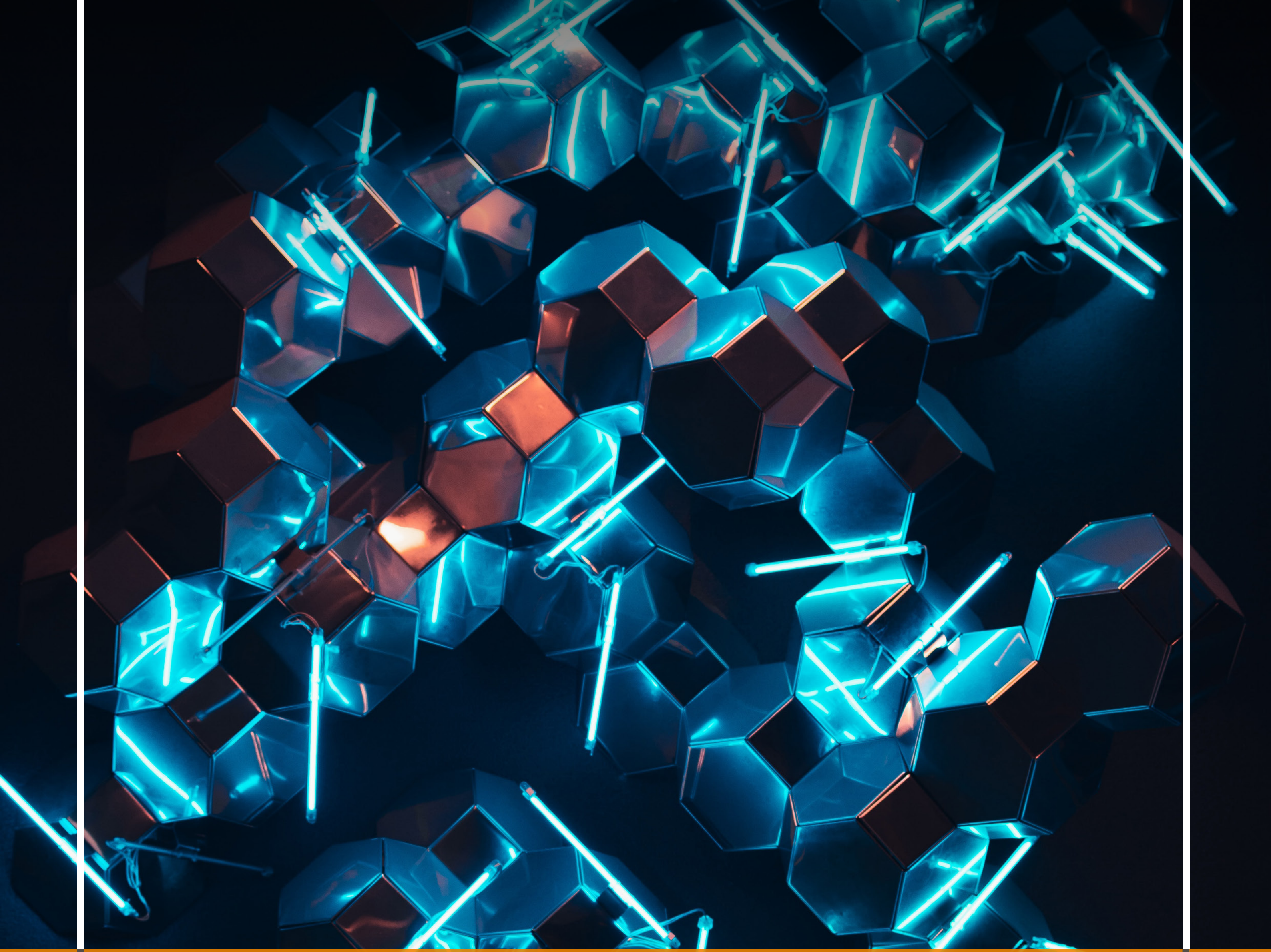
CIONET What's next. | whyaye! | interos



A FINANCIAL SERVICES EVENT ON 2ND MARCH 2023

ELIMINATING SUPPLY CHAIN RISKS

IN THE FINANCIAL SERVICES SECTOR

Roger Camrass
CIONET UK

Discussion Documents March 23

A Financial Services event on 2nd March 2023

Eliminating supply chain risks in the financial services sector

A discussion dinner was held on the 2nd March, sponsored by Interos and Whyaye and attended by senior executives from the financial services sector including AXA, Deutsche Bank and Northern Trust. The title of the event was 'Eliminating supply chain risks in the financial services sector' and was moderated by Roger Camrass, Research Director of CIONET International.

As leading organisations within the financial services sector adopt multiple cloud-based infrastructures and SaaS services they become increasingly reliant on third parties across their 'digital' supply chains. Such dependencies can increase business risk and threaten information security.

Short term, digital supply chain insights can allow organisations to mitigate immediate risk allowing the right supplier and spend management decisions to be made. Longer term, it's the cultivation of a stable environment for resource management, customer experience and the ability to pre-empt risk. This will empower organisations to innovate knowing they possess a stable supply chain to help drive organisations forward.

Context for the discussion

Each delegate was asked to describe their supply chain issues. These included:

- How best to analyse risks such as cyber, due to third parties across digital supply chains.
- Can regulation help or hinder supply chain risk, and does this limit agility and profitability?
- Who is ultimately on the hook for supply chain risks – the COO, CFO, CIO or other?
- What are the latest techniques relating to risk assessment and mediation?
- How is data sovereignty affected across connected supply chains, and who owns the data?
- What happens when your firm is acquired and integrated into a larger organisation?

Whyaye explained that conditions have changed over the past two years with the introduction of global regulations focused on operational resilience / vendor risk management, including fourth and fifth level partnerships. Cloud has opened new areas of risk as it encourages users to spin-up applications with little supervision.

Gaining visibility of risk

According to delegates, the task of monitoring and assessing risk becomes increasingly complex in a multi-cloud world. Dependency on third parties is growing rapidly in areas such as Software as a Service. The question posed to the round table was 'who is responsible for managing the risk, and do they have sufficient information to meet internal and regulatory standards and responsibilities?'.

One delegate pointed out that third party risk is growing at unprecedented rates with dependence on up to 18,000 vendors in the case of large airlines. Such external dependencies include reservation systems, credit cards and hotel systems. Some vendors such as Salesforce have developed risk templates to help their customers manage complex supply chains.

For some organisations around the table, dependence on large server farms of varying vintages can obscure risk levels at the core infrastructure level. Building applications on top of such legacy platforms introduces yet more uncertainty. Becoming proactive around risk management requires a new generation of tools and processes. Many delegates emphasised the need for 'real time' measures to anticipate and mitigate risks.

Mergers present another form of supply chain risk, especially when systems and partnerships differ between parties. In the case of one delegate, his acquired organisation was well in advance of the acquirer. This has caused alignment problems which may take years to resolve.

Managing third party risk

One delegate from a global bank commented that organisations need to understand and assess the level of risk within supply chains and establish their own appetite for this risk. In this case, elaborate procedures are in place that require an 18 month vendor evaluation of third party risk. This sets a limit on who can be trusted as many smaller vendors cannot endure such a lengthy evaluation period. It also limits the ability of the firm to get a timely and insightful view of vendor risk and business innovation which depends on speed.

A second delegate emphasised that you can outsource your operations but you cannot outsource your risk. The organisation remains accountable for risk regardless of external arrangements. Relying on large cloud vendors such as AZURE and AWS has the effect of concentrating risk into small clusters.

Regulators are not capable of staying ahead of technology developments. They can help establish 'safe' operating standards between countries, but they will always remain behind the curve in areas such as Cyber and Cloud. One delegate suggested adopting open-source software as a means of controlling risk levels in areas of application development.

Who should be responsible for risk?

Delegates made several suggestions about who should manage risk. These included the COO, CIO, head of procurement and CISO. However, everyone was clear that regulation (such as the Senior Manager Regime in Financial Services) provides guidance on accountability. Regardless the business should be actively involved in managing the risk and incorporating supply chain risk into the corporate risk register. The main imperative here is to protect the brand and increase profitability. Any obstacles in the way of these objectives need to be surfaced at the most senior executive levels.

Businesses need to express their desired outcomes or KPIs as they relate to profit and resilience. Risk will influence these outcomes. Regulators are often too concerned about inputs rather than outputs and can be blockers to business innovation and growth.

As one delegate stated, if you cannot measure risk, you cannot manage it. Tools and platforms such as those provided by Interos and ServiceNow are essential instruments to enable those accountable to do their jobs effectively. IT has a central role in implementing such techniques, but must work closely with the business to ensure full alignment of goals such as efficiency and profit.

In addition to technologies, all delegates considered integrated processes and aligned cultures as essential ingredients for success. As with cyber, every member of an organisation bears a responsibility for managing risk.

What can you do to improve third party risk?

The discussions surfaced some vital pointers on how to best manage risk across digital supply chains. These included:

- dentifying who is accountable for risk management, and specifically vendor risk management, within the business.
- Understanding how this individual can be supported with appropriate tools and platforms. This will allow them to identify supply chain risk in a timely manner and be able to collaborate internally and with vendors on actions to mitigate risk.
- Establishing and communicating what individuals can do to reduce risk across the organisation and outside.
- Developing collaborative and transparent relationships with key vendors to tackle risk management across complex supply chains.

For further information on how ServiceNow and Interos can help identify supply chain risk in real and improve how you manage this risk, please contact Tanya Morris at Interos and Stuart Birnie at Whyaye

Roger Camrass
Lead researcher

A pioneer of today's Internet as an ARPA research fellow at MIT in the seventies, Roger has spent over forty five years helping corporations harness the power of new technologies such as cloud, mobile communications, e-commerce, voice recognition and satellite. He was a partner at EY responsible for e-commerce during the dot.com boom. He is a graduate of Cambridge University and MIT, and a visiting professor at the University of Surrey.

See **rogercamrass.com**

CIONET

What's next.