BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

August 16, 2021

Storm Clouds on the Horizon: Accelerating Challenges in Complex Supply Chain Risk Management

By Bob Jones

In today's world organizational success is most often dependent upon an increasingly large network of external relationships. If we accept the expression that a chain is only as strong as its weakest link, assessing risk in supply chains is impossible when links in the system are invisible. The challenge of managing supply chain risk where unknown 4th, 5th, and Nth parties support critical activities is exactly what risk management professionals face on a daily basis.

This report will discuss four complex supply chain challenges:

- Accurately understanding the length and depth of supply chains and determining appropriate due diligence techniques
- The ramifications of sudden shifts to work-from-anywhere (WFA) environments
- Ethical sourcing challenges in supply chains
- Confronting ransomware in the supply chains

Board members cannot and should not manage the enterprise's supply chain. However, they can be cognizant of and sensitive to the impact that ineffective supply chain management will inevitably have on their enterprise's performance, increasing financial, security, and reputational risks.

The purpose of this report is to provide board members with information they require to ask management more pointed questions about:

- Their organization's identification and prioritization of supply chain risks
- Their organization's ability to confirm that risk management programs are congruent with the enterprise's culture and risk appetite

---

THE CHALLENGE OF MANAGING NTH PARTIES - HOW FAR DOWN THE SUPPLY CHAIN DO YOU GO?

Third parties are increasingly reliant on subcontractors to help them accomplish their responsibilities to their customers, a cross sectoral trend exacerbated by the use of cloud service providers (CSPs) during the pandemic. That subcontracting can extend far down the supply chain (one financial services regulator referenced 20 suppliers in a single chain, FSB), sometimes without the upstream participants' knowledge. Single points of failure can be managed through the application of sound due diligence and assessment only if they are identified. The failure to understand the complete structure of complex supply chains can lead to several significant risks:

- **Concentration Risk:** Multiple participants contracting with the same provider increases concentration risk both within firms and across sectors. Updating vendor inventories to include all supply chain participants has become increasingly important.
- **Incomplete Due Diligence:** An incomplete understanding of supply chain complexity can create a wide range of risks because of missed due diligence. Outsourcers should contractually require third parties to report their subcontracting arrangements (including scope of work, rationale for sub outsourcing, etc.) to outsourcers. Contracts can (and should) require third parties to levy the same security requirements downstream. Outsourcers can assemble a comprehensive inventory (register) of vendors, an important first step in identifying, assessing, and managing supply chain risks.
- **Regulatory Coherence:** An additional complication has emerged in the financial services business where regulators hold different expectations about an outsourcer's due diligence obligations in complex supply chain management. A stark example is a recent (November 2020) outreach in which the Basel-based Financial Stability Board noted that "most…authorities expect FIs to retain responsibility, and manage risks relating to the subcontracting of services provided by third parties… which can involve fourth parties, fifth parties and beyond." (FSB, page 24). But in newly issued (March 2021) guidance the Bank of England said quite plainly that it "does not expect firms to directly monitor fourth or fifth parties." (BOE, page 30).

Questions Boards Should Consider:

- Does management contractually obligate its organization's third parties to:
  - Report the identity of their third parties' subcontractors and the scope of their work?
  - Perform assessments of those subcontractors and share the results with you?
  - Grant rights to accept or reject any subcontractors?
  - Require their subcontractors to place the same conditions on their sub-contractors, and so on?
- Has management completed a vendor inventory?
  - Does that inventory include fourth, fifth, and Nth parties?
  - How often is the inventory updated?

ESG IN YOUR COMPLEX SUPPLY CHAINS

ESG is a headline issue around the world. News items appear whenever organizational activities have negative environmental or social effects on stakeholders, often with significant reputational, financial, and - increasingly – regulatory consequences.

The practice of ethical sourcing is inextricably linked to knowledge of the Nth parties in any sourcing relationship. Yet one recent study found that although 46% of firms surveyed had a formally documented ESG program, only 14% comprehensively considered ESG metrics in their supplier analyses (ESG Planning and Performance - OCEG). Many firms are just beginning their ESG journeys and are bewildered by standardized ESG metrics that are still works in progress and due diligence regimes that are incomplete. It's no wonder that so many of these companies are looking for a workable path forward.

Some organizations have found initial success in the adoption of an ESG Code of Conduct, used both internally and with suppliers (for example, see Aurelius Group).These codes are often excerpted from more wide ranging conduct codes used internally, and they function best when they are incorporated into vendor contracts. Suppliers are required to agree in writing to conduct business in accordance with the code and may be asked to certify compliance on a periodic basis. When a third party subcontracts

processes on behalf of an outsourcer, parties down the line are asked to subscribe to the same code of conduct, assuring continuity of practice. Some organizations undertake periodic site visits to confirm that the outsourcer's ethical standards are being met.

ESG Codes of Conduct vary – sometimes significantly - from organization to organization, industry to industry, and country to country. That's okay. Codes can be an extremely efficient way to move forward at a time when ESG metrics are unsettled and there is an increasing stakeholder expectation for progress in ethical sourcing.

Because preventing bribery and corruption is such an important component of an organization's ethical sourcing practices, compliance with the Foreign Corrupt Practices Act (15 U.S.C. §78dd-1), enacted in 1977, which applies broadly to all US-based corporations and their supply partners [1], no matter where they operate, is key.

Questions Boards Should Consider:

- Does your organization have a comprehensive set of ESG policies and are they actively socialized within the organization and to your suppliers?
- Does your organization have and abide by an ESG Code of Conduct?
- Does your organization ask suppliers to formally agree to abide by your ESG Code of Conduct?
- Does your organization take steps to ensure supplier code of conduct adherence?

THE CHALLENGE OF ENSURING SECURITY HYGIENE IN HIGHLY DISPERSED SUPPLY CHAIN WORKFORCES

Pandemic-related logistical and hygiene considerations of a work-from-anywhere (WFA) environment forced organizations in nearly all sectors and at all supply chain levels to meet unprecedented challenges in managing information security and human resources while maintaining appropriate employee privacy.

- **Bring Your Own Devices (BYOD) in Unprotected Environments:** BYOD control issues aren't new. What is new, however, is the proliferation of the types and locations of devices brought into the work environment, including routers connected to home networks of phones, tablets, smart speakers responding to voice prompts; and the plethora of Internet of Things (IoT) devices managing appliances, security cameras, etc., common in "smart" homes. Computers used for work may be used for personal purposes in spaces shared by other family members.
- **Invisible Subcontractors:** Work From Anywhere challenges may be harder to detect in subcontractors towards the end of a supply chain, and risks are magnified if the outsourcer either doesn't know they exist or does not adequately understand the environment in which those risks lie.
- **Protecting Your Crown Jewels:** Management has an obligation to protect the organization's sensitive information by monitoring WFA environments, not just internally, but throughout its critical supply chains. At the same time, organizations are obligated to protect employee privacy, and achieving both goals simultaneously produces friction.

Questions Boards Should Consider:

- Does your management understand which suppliers (including subcontractors) are being most impacted by their newly dispersed workforces?
- Has management taken appropriate steps to mitigate any disruptions exacerbated by newly dispersed workforces, including protecting IP assets?
- What has management learned about anticipating the possibility of short-term dispersed workforce environments in supply chains moving forward?

THE CHALLENGE OF RANSOMWARE

While most press reports focus on single victim attacks, ransomware can (and does) play havoc with supply chains. Many organizations are not equipped to deal with a downstream provider who, when attacked, is unable or unwilling to pay a ransom.

On July 3, 2021, Kaseya reported that its servers, which provide central authentication and authorization services for Windows-based computers, had been successfully attacked, taking down the servers of its customers. These customers include managed service providers (MSP's) that provide IT infrastructure services to their customers.

According to Kaseya, 60 of its direct customers and approximately 1500 of their customers, many of which had probably never heard of Kaseya, were affected. The impact included network-connected devices, including point-of-sale networks. The attackers demanded a $70 million ransom for the decryption key. Kaseya stated it had refused to pay. One full week later, on July 12th, Kaseya's networks were largely restored.

Approving a ransomware response policy is probably among the thorniest challenges a board will be asked to address.

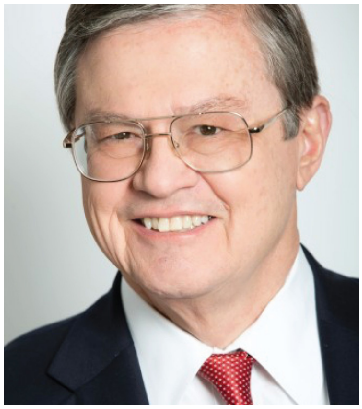
Questions Boards Should Consider:

- Is your organization prepared to respond to ransomware attacks?
  - Should your organization adopt a strict pay or no pay policy? Should your organization step in on behalf of a supplier if it cannot pay a ransom?
  - Does your organization's cybersecurity insurance policy include ransomware coverage? Does your organization require suppliers to have cybersecurity insurance including ransomware coverage?
  - How does your organization and firms in your supply chain resolve the friction between "official" government policy and the need to restore timely service to your customers?
  - How does your organization deal with a critical downstream provider financially unable or unwilling to pay a ransom?
  - What tactics is your management taking to diminish the impact of ransomware attacks?

---

[1] The Act applies to all US - based corporations, their foreign subsidiaries, foreign companies with US subsidiaries or do business in the US, any company having transactions going through the US banking system, and any US or foreign citizen working for any of those entities.

ABOUT THE AUTHOR



Bob Jones, Senior Advisor, Shared Assessments
Bob has 50 years of experience leading fraud risk management and risk management strategy programs. At Shared Assessments Bob facilitates the Best Practices Awareness Group and UK/EU TPRM Strategies Group. Both have a current focus on supply chain risk management. Bob is Adjunct Professor Emeritus of Economic Crime at Utica College. His articles have appeared in the RMA Journal and the Journal of Economic Crime Management.
Contact: Bob@santa-fe-group.com

WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.