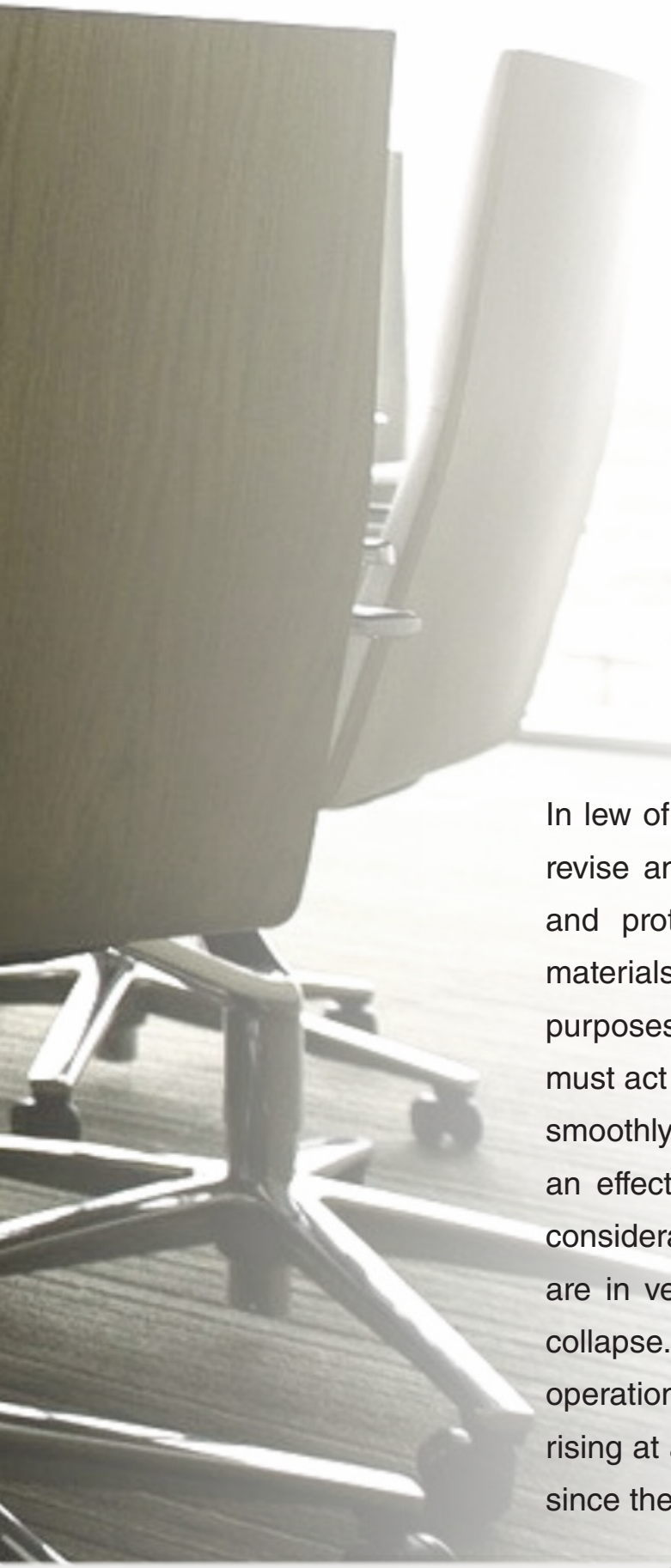
The Evolution of Supply Chain Management into a Holistic Risk-Based Approach Supply Chain Network

April 2022 Newsletter

17th Edition

RMG

Table of Contents



INTRODUCTION

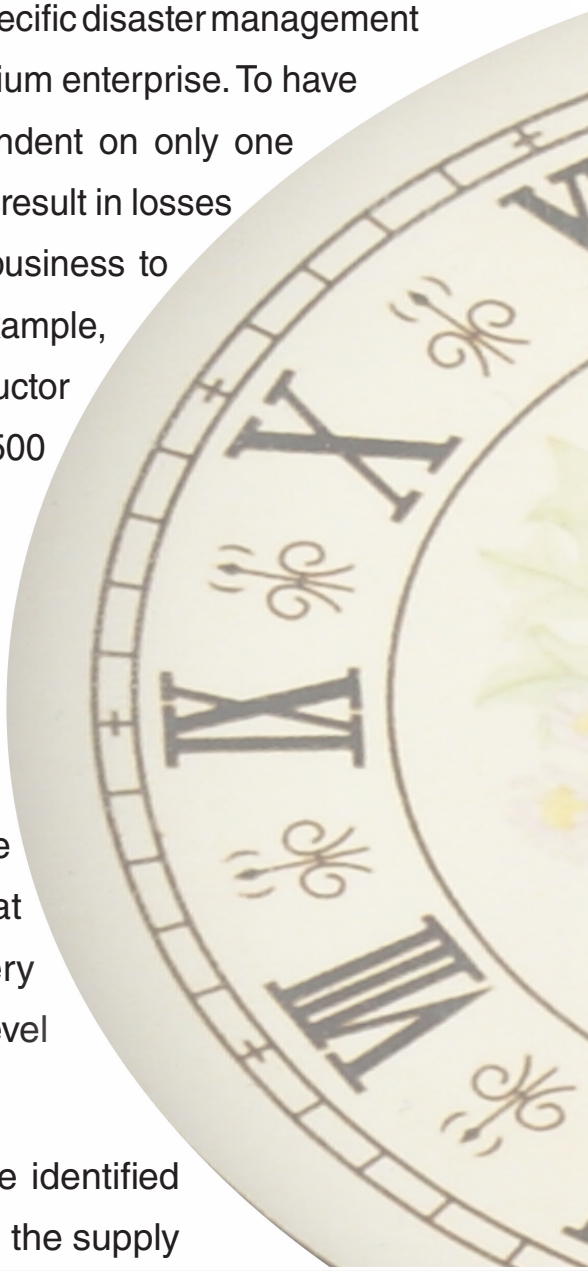
In most industries, an interconnected network of businesses is involved in the ultimate provision of products and services to consumers. Upholding and maintaining the supply chain network is the foundation for mitigating commercial crime risks related to such. In terms of choice, loyalty is slowly being replaced with compliance, as security replaces trust. Digital platforms that are being considered the norm of the technological revolution limit person-to-person contact to mitigate risk and to serve as a tool for a better overall risk profile.

In lew of current events, businesses are advised to revise and strengthen all risk mitigation processes and protocols that consider secure sourcing of materials and products for both retail and production purposes. These supply chain risk mitigation controls must act as buffers to keep the organisation running smoothly. Organisations that have not yet devised an effective risk management plan that takes into consideration the implications of supply chain risks are in very real danger of sudden and irrevocable collapse. Alongside the internal risks faced in daily operations, the number of external risk factors is rising at an alarming and exponential rate, not seen since the start of the 1940's.

IDENTIFYING SUPPLY CHAIN MANAGEMENT RISKS AND THREATS

Winston Churchill spoke about letting advance worrying become advance thinking and planning. This is true in the world we are facing now as conflict situations cause international havoc amidst a worldwide pandemic. Recognising probable risks and scenarios before they take place is essential for the future survival of an organisation.

If the demand for a specific item skyrocket or if a supply route is no longer a viable option, it is necessary to facilitate effective disaster management and recovery plan to control the action plan if these events happen. Having a supply chain specific disaster management and recovery plan would be beneficial to any large or medium enterprise. To have a future, the organisation cannot be symbiotically dependent on only one supplier or producer of certain goods. This may potentially result in losses that would require reparatory action on the part of the business to make up for the revenue of non-deliverable items. For example, a Deloitte report stated that for the past 2 years semiconductor shortages have resulted in revenue misses of more than $500 billion worldwide for both suppliers and customers.



Considering the amount that was lost in just 2 years, a risk management plan is essential for any organisation that deals with supply chain networks. Should it be an office that is sourcing paper from an unethical source or suppliers who give false credentials to be more eligible for tenders and contracts, planning for events that may disrupt the normal production of goods or delivery of services is an integral part of higher and mid-level management.

Precoro has a recommended list of threats that can be identified within an organisation that may have adverse effects on the supply

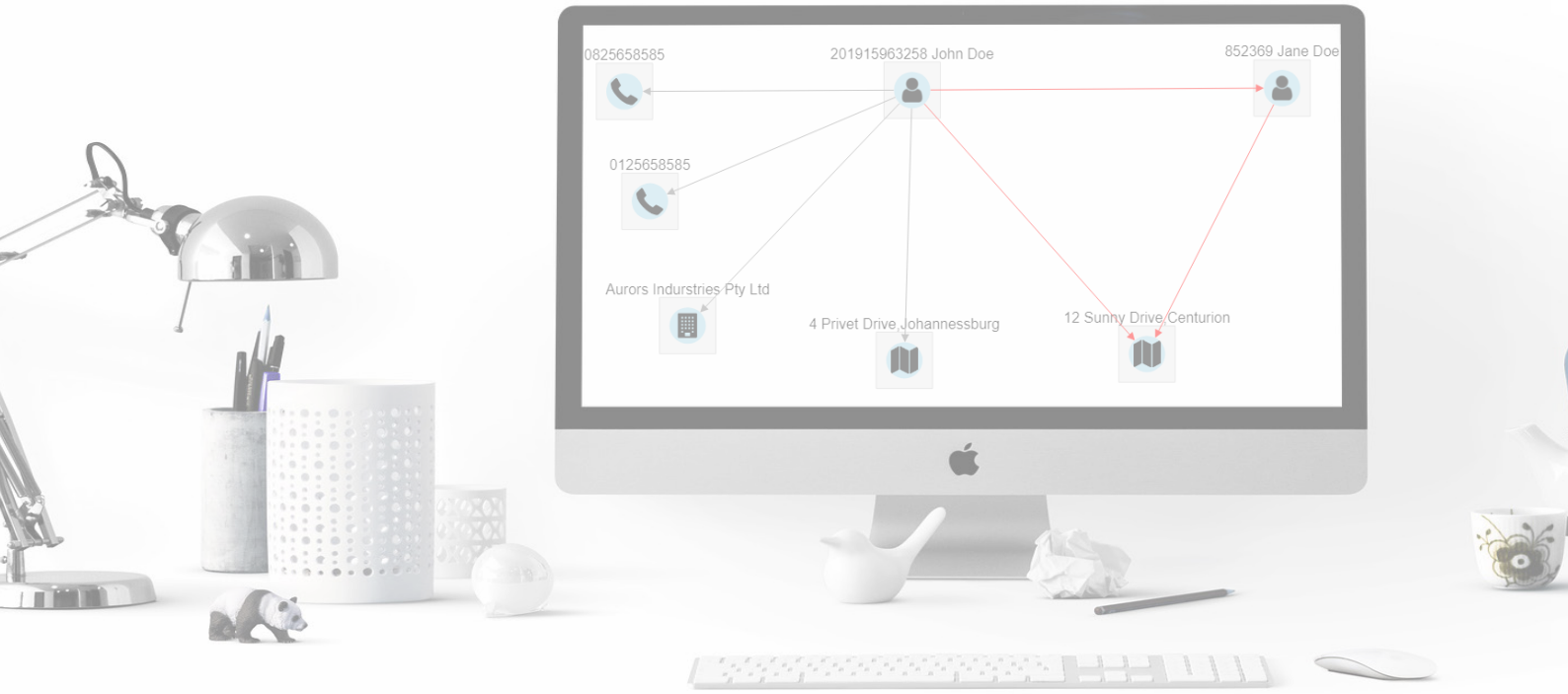
chain management of the business. The service delivery of the business is after all the way it survives. Examples are given for financial risk scenarios that may arise from sources such as budget overruns, constructive changes, and missed financial milestones, all of which may result in additional funding being required. Financial risks must be pre-planned carefully, with care taken for certain scenarios. Regardless of how improbable they may seem at the time.

Scheduling changes can cause any organisation headaches in a way that is known to only a rare few. Large-scale logistical enterprises can be compromised by acts of nature and natural disasters. However, poor quality of work resulting in timeline setbacks and compliance issues can threaten the projected timeline of a project or products' delivery. Scope risks can occur due to changes when the initial statement of work becomes unworkable or due to technical changes taking place within the market.

Organisations may experience supply chain complications through the legal risks that often relates to disputes or different interpretations of contractual obligations, or from requirements not met to client satisfaction. Any intellectual property are considered a legal risk, especially where patent infringement is a possibility. Legal action against a supplier in the case of legislative non-compliance may have adverse effects on the organisations that it provided goods or services if the scandal becomes public knowledge.

Ecological awareness must be at the forefront of supply chain risk management as the digital age has introduced a new level of freedom of information. Environmental risks

that must be considered are the impact of both the organisation itself and its suppliers' negative impacts on water, air, and soil because of discharges, emissions, and other waste. Difficulty adapting to new regulatory systems and socio-political changes poses a significant risk to supply chains if there is no contingency plan in place if a supplier is proven to be non-viable.



Physical planning errors and other human behavioural risks are the most difficult to assess. Bad judgement, even with the purest intentions, can be detrimental to the overall health of the organisation. Illnesses and injury, even departures of key personnel must be considered when assessing the risks involved in supply chain management. Human error and oversight can furthermore contribute to a data leak or authorisation breach resulting in cyber-attacks that may affect specific systems or ransomware that could result in data losses if secure backups are not available.

Of utmost importance are commercial crime risks that are posed to organisations without proper supplier vetting controls in place, or worse – loopholes within their procurement policies and procedures. Repeatedly making use of the same supplier should raise questions within the procurement department, while making use of a supplier for work outside of their field of expertise should alert red flags and initiate an investigation. While many companies outsource supplier vetting to an independent,

objective, and impartial third party, there are still organisations that perform 'quick in-house due diligence assessments', ultimately resulting in contracts with substandard suppliers or suppliers whose intention is to defraud the organisations they work with.

Thus, an effective risk management plan for supply chains must include both internal and external risk factors and scenarios that must be considered and consistently evaluated. Corporatecomplianceinsights.com predicts that 2022 and beyond will require robust oversight and a more holistic understanding of the supply chain itself. Including looking beyond traditional partners, methods, and technologies.

Furthermore, organisations that make use of suppliers must ensure that the supplier will be a good, compliant, and competent partner that is open to working together to identify, address and mitigate threats along the supply chain. It is only by asking the correct fundamental questions and looking into more holistic approaches that an organisation has any hope of sustainability as digital trends can cause instantaneous reputational damage. Security from suppliers is just as important as compliance. As cargo theft and piracy have been steadily increasing, there is a higher number of disruptions to supply chain networks reported. If those risks are not addressed in time organisations may face revenue loss, reputational damage, and even legal action from unsatisfied consumers.

SYNOPSIS OF REAL-LIFE TRANSGRESSIONS AFFECTING SUPPLY CHAIN NETWORK

Commercial crime risks can be posed by external parties, internal parties, or a combination of both internal and external parties. Working within the risk identification and management industry, RMG has noted trends relating to procurement fraud. In our professional opinion, it is both the lack of efficient procurement policies and the absence of diligent application of procurement procedures that enable the perpetration of criminal activities.

One example of such relates to the impersonation of a large and well-known retail distributor by a criminal syndicate. The criminal syndicate was able to defraud South African companies of millions of rands worth of stock before being discovered and apprehended. The criminal syndicate was able to complete multiple transactions before being discovered. Had proper due diligence been performed at the inception of the business dealings, the criminality of the organisation would have been brought to light. Furthermore, had strict control measures been in place to follow up with outstanding debtors, the number of transactions would have been much less and saved the company hundreds and thousands of rands.

Larger companies require stricter control measures, as it is oftentimes difficult to retain control over every aspect of business, especially when responsibility has been handed over to employees. It may be detrimental when those employees look after their own best interests before that of the company. RMG has investigated irregularities with regards to the use of one supplier across multiple business spheres, for various clients – which indicates that this loophole is relevant to a broad spectrum of industries. A supplier specialising in, for example, plumbing, would be contracted to complete other maintenance work, such as electrical or building. Not only does this open the company to substandard service as they are making use of a supplier who is working outside of their field of expertise, but more often than not, there is collusion between the supplier and an employee within the procurement or finance department. Collusion

results in undue benefits. Segregation of duties is an incredibly useful control measure that can be used in various business silos, but especially within procurement. Having more than one employee responsible for business decisions, and splitting business transactions into smaller parts assigned to employees across the procurement department drastically reduces the chance of collusion with suppliers and limits the commercial crime risk posed.

We maintain that reporting procedures and whistleblowing are vitally important, especially in larger organisations. The presence of such motivates and encourages employees as well as outsiders to report incidents of suspected or actual commercial crime incidents.

To demonstrate the value of proper due diligence assessments, RMG recently conducted a due diligence for our client before any contractual agreements were signed. Through our assessment we discovered that two of the Directors had been found guilty the month before of crimes relating to tender fraud and were awaiting sentencing. It was our submission that the criminal elements were planning on swindling our client in a similar fashion. The impartial and independent due diligence ultimately saved our client millions of rands.

If these real-life scenarios have piqued your interest, visit our website for further reading: www.rmgforensics.com

SUPPLY CHAIN RISK MANAGEMENT STRATEGIES

As is true with many forms of risk, prevention of risk is better than treating risk after the fact. Thomson Reuters (tax and accounting) states on their webpage that there are multiple strategies that both large and small organisations can apply to mitigate any supply chain related risks that they may foresee. Dangers from supply chain disruptions have been rising, thus organisations are attempting new supply chain risk management strategies, reportedly in the areas of trade compliance, import/export screening, supplier evaluation, and post-entry audits.

It is reported that only one in six organisations carry out proper due diligence on all key suppliers at the procurement stage, and a quarter fails to do so until after contractual obligations have been made. Companies that fail to comprehend all aspects of their supply chain are inviting risks through the door, by not comprehending all stages of their product or service an organisation faces risks such as fines, penalties, loss of import/export privileges, cost overruns, damage to reputation and loss of consumer trust. Getting visibility into compliance documents and financial statements of a supplier can assist in conducting predictive financial reporting on potential suppliers.

Supplier evaluation and selection is a crucial element of effective supply chain risk management plans, organisations must know who their business partners are and whether they represent risks to the current supply chain. Supplier evaluations must consider the public perception of the supplier, the location of the supplier (both in terms of logistics as well as environmental and socio-economic factors), and

if any risks that can be identified can be mitigated by an agreement. Thomson Reuters furthermore states that many consumers do not distinguish between a brand and its suppliers, resulting in the erosion of public perception of sometimes innocent parties whose only oversight was that proper supplier due diligence was not carried out.

To avoid any mishaps and oversights that may occur, organisations are advised to develop a comprehensive supply chain risk assessment programme. This can include policies, processes, procedures, protocols, and software that will aid in taking out the guesswork of supplier compliance and possible risk. In addition, some companies specialise in risk management and supplier vetting that make use of denied-party screening software that allows management to identify potentially problematic suppliers before a contract is signed. In the digital age, solutions are everywhere, but sound due diligence must be carried out on the said risk management solution and its providers to ascertain that it is fully licensed and has access to relevant personal information required to vet compliance.

Cyber-criminals are increasingly infiltrating third-party software. To maintain system security, it is advised that compliance checks for third-party software must be issued to mitigate this risk. In addition, companies that provide comprehensive training for employees about cyber-security protocols will be less at risk as employees can be on the lookout for phishing emails, malware, and other anomalous Internet of Things devices communications. Efficient employee training empowers employees with the knowledge to identify commercial crime risks and to report such instances to the correct parties.

Even with the best software and risk management plans in place, there is never a full safeguard against supply chain disruptions. Supply chains are at constant risk of border declarations, international legislation changes, licenses, and change in product

classification. Each link in a supply chain is of importance and a risk analysis must be conducted on each participant in the supply chain. After the product is delivered or produced further risk analysis and quality control are strongly advised.

Post-entry audits can help an organisation identify previously unknown risks and vulnerabilities in the supply chain, by giving a detailed insight into the true dynamics of the supply chain.

Thomson Reuters recommends that an organisation builds a strongly screened, internal team with the right and competent skills under the guidance of senior management to carry out projects. An internal risk analysis team, or even an externally allocated company, can have the task allocated of making risk evaluation an essential part of the supplier on boarding process.

The supply chain risk management plan must be able to tie supply chain mapping to threat data logically and on geographic points to foresee and visualise potential issues, for example, political unrest or tariff changes. Using a risk-based approach with a clearly defined methodology instead of simple checklists is a useful technique to root out potentially undesirable suppliers that may cause supply chain disruptions. Continuity of these risk mitigation practices must be carried out consistently and precisely to be effective. As new threats rise to replace mitigation controls the supply chain risk management plan must constantly be evaluated and updated based on current risk analysis trends.

Supply Chain Digital has recommended the PPRR risk management model. The characters represent Prevention, Preparedness, Response, and Recovery.

This will spur organisations to take Preventative action and Prepare contingency plans in case of a risk scenario taking place, be able to effectively execute a risk mitigation Response to nullify any immediate threats and Recover to a level that enables normal operations or production to resume as soon as possible.

Not only must these protocols be practiced externally but internal errors within an organisation can harm the well-being and sustainability of the business model. Candidate screening, employee evaluations, and team-building exercises are powerful techniques that senior management can employ to find undesirable candidates in the workplace and retire those unwanted elements. Desirable candidates must express ethical attitudes that will lead to a positive work environment and higher levels of productivity. To paraphrase a term from the turn of the previous century: happy workspace, happy employee.

Internal risks are grouped by a research gate paper to be able to fit into 5 broad categories.

Manufacturing risks	caused by disruptions of internal operations or processes
Corporate risks	caused by changes in key personnel, changes in business processes and changes in communication or reporting channels
Planning and control risks	Caused by inadequate assessment of the risks in the supply chain processes. This can stem from the mismanagement of resources or employees.
Mitigation and contingency risks	caused by not having adequate alternatives or contingency plans in case of a risk scenario taking place

Cultural Risks

caused by an organisation's internal ethical culture's attitude toward hiding or delaying negative information. This slows the risk mitigation reaction and can result in a delay in the supply chain processes or even financial losses on the part of the organisation.

CONCLUSION

With the information at hand, it is impossible to argue that a relaxed attitude towards supply chain management is advised. It is essential that businesses adopt a risk-oriented company culture that protects themselves from threats not only in terms of supply chain management but also from external and internal commercial crime risk factors. Controls must be in place to mitigate commercial crime risks at all levels throughout the organisation and higher management needs to have a clear and precise prescription of the plan of action to follow in a risk scenario. To safeguard against commercial crime risks that tomorrow may bring, it is best to have the plans to deal with those risks in place yesterday.

BIBLIOGRAPHY

capacityllc

supply chain dive

precoro

corporate compliance insights

thomson reuters

supply chain digital

researchgate

supply chain quarterly