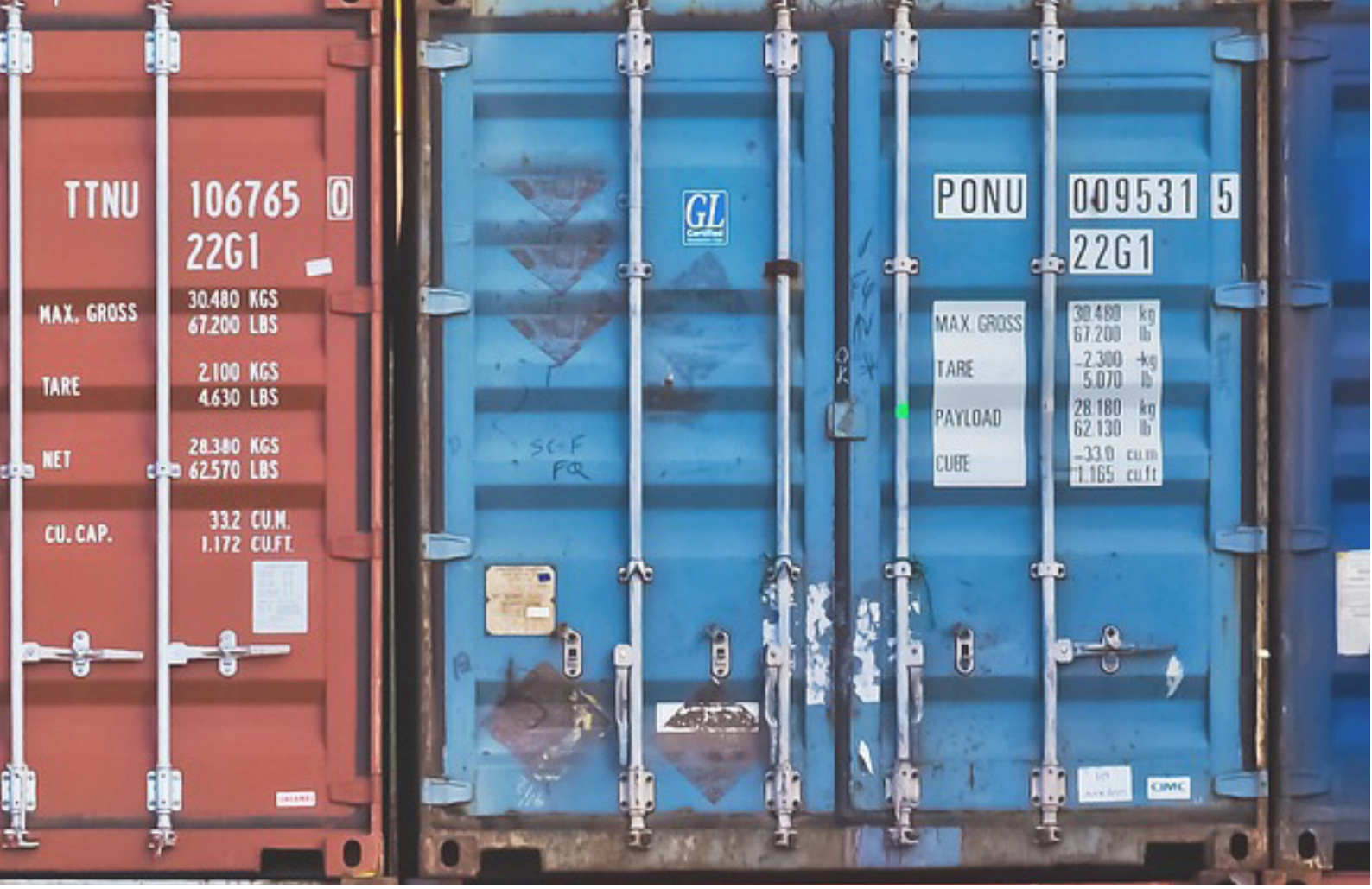

SUPPLY CHAIN CONSTRAINTS TO AVOID COMMERCIAL CRIME AND SUPPLY CHAIN PITFALLS

June 2023 Newsletter

21st Edition

RMG

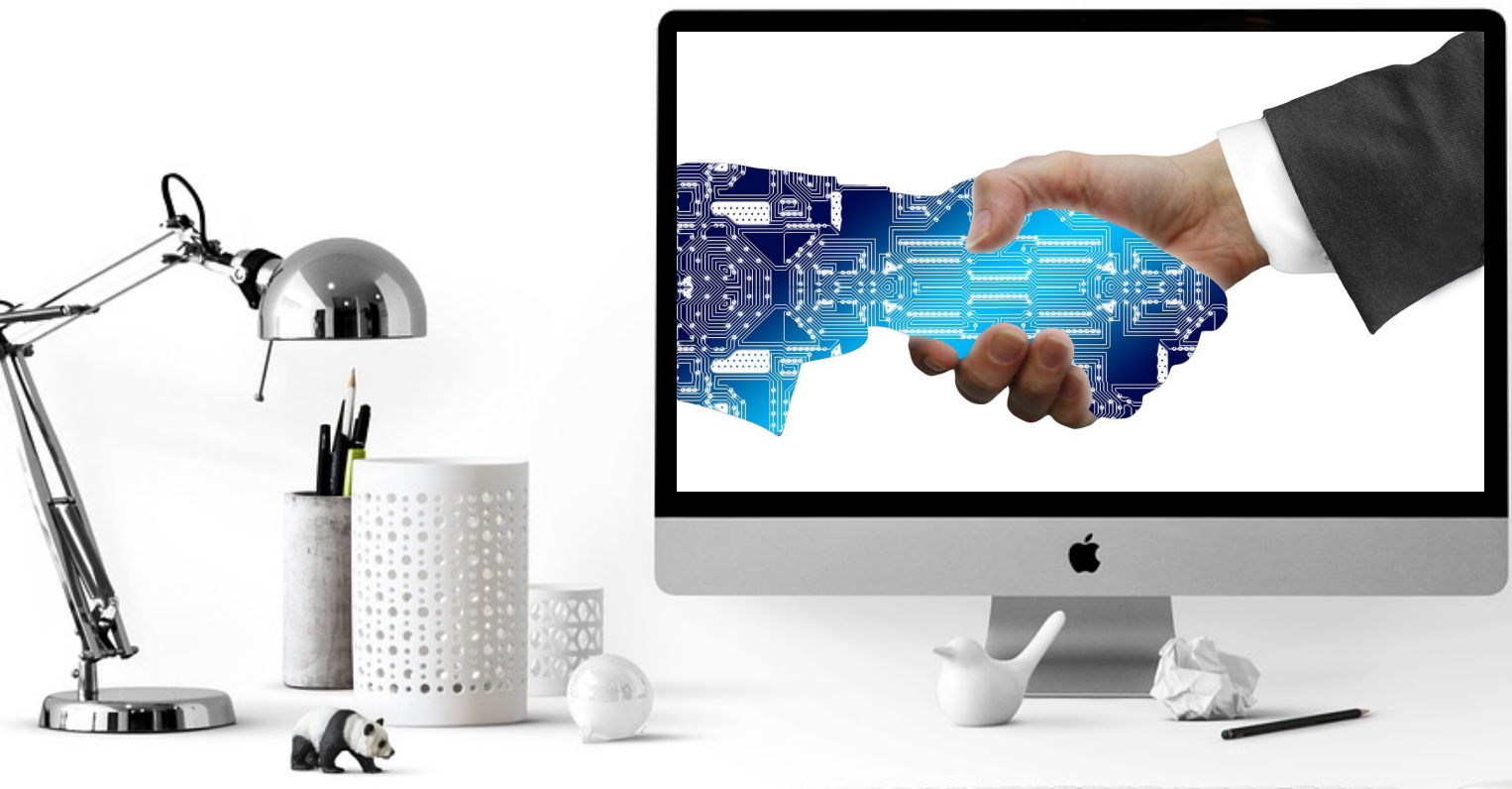

TABLE OF CONTENTS

INTRODUCTION

Supply Chain Risk Management ("SCRM") is the process of identifying, assessing, and mitigating commercial crime risks associated with an organisation's supply chain. For many businesses, the procurement of goods and raw materials is one of the most important functions contributing to the enterprise's success. KPMG has predicted that supply chain disruptions will continue well into 2023 and beyond. However, it is not the issues of the organisation that influences the success of the organisation, but rather the business's response to issues that will define the relativity of success. As stated by the business entity, Planergy, there are more powerful disruptors and more dangerous commercial crime risks that affect the supply chains of organisations than ever before, and effective commercial crime risk mitigation methodologies are critical to protecting business continuity and operational efficiency. The business entity, Precoro, lists a study done by the Business Continuity Institute where researchers have calculated that supply chain disruptions have gone up by approximately 48% in recent years.

SUPPLY CHAIN DISRUPTIONS HAVE GONE UP BY APPROXIMATELY 48% IN RECENT YEARS.

THREATS TO SUPPLY CHAINS

If contingency plans are not in place and do not specifically address commercial crime risks, the business is at greater risk for financial risks (such as fines for non-compliance or loss of revenue due to supply constraints) and for reputational risks (whether by allowing negative publicity on the company on publicly accessible platforms or through adverse media that links the business with undesirable elements). Aside from the commercial crime risks posed by suppliers, employees who seek to exploit internal weaknesses may result in nepotistic

relationships, stock losses, monetary losses due to poor performance, and the falsification of supply chain data (fraud). All the above-mentioned must be dealt with harshly and with zero tolerance as opening the window for commercial crime is as good as an open invitation to the criminal element.

KPMG states that possible disruptions to supply chains are widely attributed to new or existing geopolitical conflicts and sanctions, inflationary pressures and the recessionary environment, and climate change and extreme weather events. These factors not only restrict the flow of raw materials and goods from one economic sector to the next, but can create port holdups, reduce the availability of containers and freights, and may lead to a surge in prices throughout the supply chain lifecycle. The business's supply chain further needs to be responsive and agile enough to manage unexpected threats and disruptions. For a business to track incident investigation and mitigate the recurrence of similar incidents, collaboration amongst roles within the procurement sphere is essential.

Cybercriminals have become more sophisticated in recent years regarding infiltrating supply

chains to damage or steal data from a business entity. Vulnerabilities in the supply chain of a business provide opportunities for exploitation to cybercriminals to gain access to large-scale operations. The *modus operandi* of cybercriminals has evolved alongside the controls that are in place to reduce the impact of cybercrime, as criminals can use basic warehouse equipment such as barcode readers and various Internet of Things ("IOT") devices to hack into the supply chain network.

Supply chain constraints can have a trickle-down effect that can cost billions of rands overall, such as the 2021 Suez Canal obstruction by the ship Ever Given. As reported by the BBC, this event cost an estimated $9.6 billion (R185 billion). There was evidence that poor supply chain management in the healthcare sector attributed to the inadequate distribution of healthcare products and vaccines during the early stages of the COVID-19 pandemic. As many entities had been unprepared for such a large-scale disaster, it was evident that supply chain commercial crime risks had been poorly identified and the plans in place to deal with these risks had not been up to par.

SUPPLY CHAIN RISK IDENTIFICATION

Previously, SCRM was an afterthought for many large-scale organisations, but has evolved to one of the top priorities to the Board of organisations, as organisations lose money on non-compliance fines and loss of brand reputation, leading to a loss in consumer range and consumer trust. Identifying specific commercial crime risks is the first step in any commercial crime risk management process, and categorising commercial crime risks can assist with how the organisation prepares and responds to specific incidents. The following is a list of common categories of commercial crime risks that can be considered during a supply chain commercial crime risk assessment:

- **Financial Risks** are varied and can range from a change in consumer interest, to a change in exchange rates, or supplier bankruptcy. Financial risks to consider include budget overruns, constructive changes, and missed milestones that require additional funding. Changes in the scope of work can be grouped as a financial risk as this may affect the total cost of labour in comparison to the amount of compensation offered by the client.

- **Scope of Schedule Risks/Production Risks** can overlap with financial and reputational risks, these risks threaten the timeline of work. Both human error and natural disasters can affect the delivery and processing of goods and materials. These risks include changes that are required when the initial Statement of Work ("SOW") becomes unworkable or due to technical changes in the market. Project Organisational Risks are grouped under Schedule Risks, as not having the correct employees or equipment can adversely affect delivery time. Production or manufacturing risks stem from potential technical failures or shutdowns in the supply chain process flow.

- **Legal Risks** arise from disputes or different interpretations of contractual obligations, or from not meeting the requirements included in the terms and conditions of service. The misuse of intellectual properties and patents is additionally grouped as a legal risk to the supply chain.

- It is imperative to evaluate the **environmental risks** that are created by suppliers or contractors. Businesses must be wary of suppliers that have a larger than average negative impact on water, air, and soil because of discharges, emissions, or morally grey resource gathering.

- **Socio-political Risks** arise from a change in the regulatory environment in response to governmental changes and to an increasing awareness of inequitable social conditions. Sourcing efforts can be affected by these changes, as sanctions and other socio-political factors can cause irreparable damage to the reputation of the business.

- **Human Behaviour Risk** requires businesses to prepare contingencies in case of employees being ill, injured, or leaving the company. The business is further obliged to audit and evaluate work done by employees to identify avoidable mistakes in the supply chain process. Internal control measures should be implemented to mitigate the risk of employees perpetrating commercial crime or colluding with external parties at the detriment of the organisation.

INTERNAL CONTROLS TO ASSIST WITH COMMERCIAL CRIME RISK MITIGATION

Businesses must concede that the organisation's cybersecurity strategies often stop at the borders of the native enterprise. Therefore, co-operation is the key to identifying the strategies that will be inclusive of all participants in the supply chain to mitigate procurement cyber risk. It is advised that these strategies are robust and provide adequate commercial crime risk governance across third-party contracts. As human behaviour risk is the most prevalent risk to cybersecurity, businesses are advised to automate technology and to conduct a cyber assessment for all functions and activities utilised in supply chain management using various devices (this includes data storage, managing inventory, and goods tracking), to identify and resolve vulnerabilities that can act as a gateway to wider system access.

Hitachi Solutions recommends that businesses make use of the PPRR Risk Management Model, which is a risk management model used globally in supply chain risk management strategies. The PPRR stands for:

- Prevention: Take precautionary measures for supply chain risk mitigation.
- Preparedness: Develop and implement a contingency plan in case of emergencies.
- Response: Execute the actions of the contingency plan to reduce the impact of the disruptive event.
- Recovery: Resuming operations and getting the supply chain process flow running at normal capacity as soon as possible.

It is important to have full visibility and ongoing monitoring throughout the supply chain process. The following strategies can be used by businesses as internal controls to improve SCRM:

- Multi-sourcing describes having multiple sources to procure goods, services, and materials from, allows for flexibility in the supply chain should a disruption occur or if a supplier becomes embroiled in a publicly known scandal. Businesses are advised to find alternative suppliers to act as a contingency plan in case of disruptions, reputational damage, or supplier business failure.

- Nearshoring encourages businesses to look for suppliers and distributors closer to their centres of operation. Additionally, cutting delivery times and looking for alternative suppliers can reduce projected time spent on product and service delivery. Although regional suppliers can be more expensive, reducing the points of travel will reduce physical security risks.

- Inventory Buffering can be described as planning and stockpiling of goods and materials to reduce delivery occurrences, and to retain products during major supply chain constraints. Inventory buffering is an effective method to determine the number of materials required on hand to meet the current economic demand from the business.

- Product and Plant Harmonisation describes the use of identical technologies for different components in the supply chain to give greater flexibility during production, packaging, or distribution in the event of a disruption. Using the same software throughout the network, such as cloud services, reduces the shortcomings of the siloed business approach and additionally allows better communications between systems and departments.

The business must take steps to ensure that internal controls are in place during the onboarding phase of new suppliers. By performing a supplier commercial crime risk assessment with proper due diligence that incorporates public domain research prior to contractual obligations the commercial crime risk posed to the business can be significantly reduced. Establishing compliance standards that suppliers must comply with will reduce the commercial crime risk posed through relationships with such suppliers as the suppliers will be responsible for maintaining the compliance status or commercial crime risk of losing revenue if it is not selected for services by secondary entities.

Businesses should ensure that employees are well educated in cybersecurity protocols to protect them from social engineering, phishing, and ransomware attacks. Appointing data stewards or custodians to assign the availability of data to specific employee clearance levels is an important step to safeguard data, and these custodians should be well versed in best practices for data systems, which includes knowledge of anti-virus programmes, anti-spyware solutions, and firewall software solutions. Businesses can use internal controls such as data-back-ups and insurance to assist with shielding the business from financial and legal liabilities that may arise due to inability to fulfil contractual obligations, and internal losses that can impact delivery time.

SUPPLY CHAIN RISK MANAGEMENT TOOLS AND SERVICES

To simplify SCRM, many organisations outsource the function to capable, reliable, and efficient third-party organisations. To make an informed decision on the suppliers and vendors that are used, vetting services must be regularly benchmarked to ensure that the solution meets the business needs, and that the solution holistically addresses the statutory compliance of suppliers and vendors, as well as incorporating bureau information from multiple national and global sources such as TransUnion and Experian while remaining legally compliant regarding consent and data privacy. It must be understood by businesses that conducting supplier and vendor vetting only during the onboarding process is not sufficient, as continual supplier and vendor vetting will allow businesses to detect any potential commercial crime activities or non-compliance of suppliers and vendors. Visit www.rmgforensics.com for

more information The benefits of continuous supplier and vendor vetting include reduced exposure to reputational risk, informed decision-making, reduction of fraud, corruption, and unethical business practices, assisting directors with fiduciary duty, and achieving actual bottom-line savings. Businesses are advised to use solutions that assist with administrative and financial reporting and to ensure what information is being verified to avoid compliance pitfalls. It is equally important to consider that adverse media searches must be conducted on suppliers regularly to ensure that there is no underlying reputational risk that SCRM tools do not compensate for.

CONCLUSION

Exacerbated supply chains can have an impact on the rise of both commercial and physical crimes. To cultivate a positive company culture and to introduce ethical decision-making, it is important that all entities of the supply chain are held at strict compliance levels and are vetted regularly through due diligence and adverse social media checks. By outsourcing the SCRM function to capable third parties, organisations are well on their way to sustainable growth, and they can effectively manage their business, benefit from a competitive edge, retain and satisfy their customers, and comply with legal requirements - especially when their reputation is on the line.

BIBLIOGRAPHY

KPMG.com

Precoro.com

Planergy.com

global.Hitachi-Solutions.com

SupplyChainBrain.com

BBC.com

Jaggaer.com

BeroeInc.com

RMG Forensics.com