Organised Crime in the Petroleum Industry

SAPIA Security Committee
Risk Assessment

2022

sapia | South African Petroleum Industry Association

Organised crime risks

1. Bulk fuel theft (PN)
2. Truck hijacking (JW)
3. Pipeline theft (SM)
4. Depot robbery (BB)
5. RTC theft (FM)
6. Illegal imports (BB)
7. Cyber fraud (AL)
8. Cyber ransom attack (AL)
9. ATM bombings (WN)
10. Violence/injuries, fatalities – impact on people (WN)
11. Business extortion (JN)

Likelihood assessment

DESCRIPTIVE RATING	SCORE	PROBABILITY	LIKEHOOD DESCRIPTION
ALMOST CERTAIN	5	>50%	Expected to occur in most circumstances and has occurred several times in the industry.
LIKELY	4	31-50%	Probably to occur in many circumstances and has occurred a few times in the industry.
POSSIBLE	3	16-30%	Might occur at some time and has occurred once in the industry.
UNLIKELY	2	1-15%	Could occur or has occurred in the industry.
REMOTE	1	<1%	May occur only in exceptional circumstances and has never occurred in the industry.

Impact assessment

FINANCIAL IMPACT RATING

Impact levels / Impact Perspective	Insignificant (Rating 1)	Minor (Rating 2)	Moderate (Rating 3)	Major (Rating 4)	Severe (Rating 5)
Direct financial loss to industry					
Indirect financial loss to industry					

NON-FINANCIAL IMPACT RATING

RATING	Insignificant (Rating score 1)	Minor (Rating score 2)	Moderate (Rating score 3)	Major (Rating score 4)	Severe (Rating score 5)
Loss of stakeholder trust	Trust questioned -but recoverable speedily	Trust dented - recoverable with time and good PR	Trust diminished recoverable at considerable cost	Trust severely damaged - never fully recovered	Trust completely lost - not recoverable
HSE-People	Slight injury	Minor injury	Major injury Major Health Effects	Single fatality Total Disability	Multiple fatalities Permanent Total Disability
HSE-Asset	Slight damage	Minor damage	Local damage	Major damage	Extensive damage
HSE-Environment	Slight impact	Limited impact	Considerable impact	Major national impact	Major international impact
HSE-Reputation	Slight impact	Limited impact	Considerable impact	Major national impact	Major international impact
Security	Stable environment where business operations are uninterrupted	There are incidents in the area, which may require higher security level	Incidents/events are escalating which requires constant security monitoring of further developments	Incidents/events escalating to a point whereby business operations are disrupted	Incidents/events have direct impact on the security of staff (injuries/fatalities) or operations (Corporate crimes)

Financial Impact contextualisation:
RSA Petroleum Industry Economic Contribution

Value chain segment	Head office	Feedstock and imports	Refining and Manufacturing	Distribution and storage	Wholesale	Retail	Total
GDP	R9.3 bn 5.7%	R2.5 bn 1.5%	R63.3 bn 38.9%	R12.1 bn 7.5%	R51.6 bn 31.7%	R23.7 bn 14.6%	R 163 bn 100%
Jobs	21,775 8.8%	4,167 1.7%	64,121 25.9%	27,021 10.9%	32,364 13.1%	98,324 39.7%	247,772 100%
Capital expenditure	R21.6 bn 23.0%	R3.3 bn 3.5%	R32.1 bn 34.2%	R18.1 bn 19.3%	R13.9 bn 14.8%	R5.0 bn 5.3%	R94 bn 100%

Source: SAPIA FTI Economic Assessment Report 2021 (2019 data)

Risk assessment summary

Detailed risks

1. Bulk fuel theft

Risk description:

Theft from storage facilities

Current risk rating (matrix) LOW

causes	Impact on industry	Key mitigations	vulnerabilities
Internal collusion Weak controls	Financial impact low	digitization	Weak law enforcement support Human element
Legitimate wholesalers purchase ULP93 and sell-off as ULP95 – add green dye to product.	Not volume loss, but value. Economic impact Indirect impact on industry	Check, double check 3rd party vehicles loading at your gantry	If found out, reputational damage to industry and possibly supplier.
Misrepresentation / fraud Collusion between internal & external parties		digitization Inventory management	Smaller players might be behind in terms of technology and controls

Detailed risks

2. Truck Hijacking

Risk description:
Truck hijackings in general have increased over the past years and show a significant jump in the 2022 crime statistics. This increase also shows in the petroleum industry, where various sources report a marked increase with the increasing fuel prices.

Current risk rating (matrix): high

causes	Impact on industry	Key mitigations	vulnerabilities
Organised crime	Operational impact Feeds illicit trade High risk for injury and fatality Product loss	Operational interventions: • Convoy driving • Night curfews • Etc.	Poor law enforcement support
		Security technology	Smaller player security standards
		Intelligence-driven mitigation	No petroleum industry – specific intelligence sharing
		Charges under Criminal Matters Amendment Act section 3.1 A and B (crime code 3200)	

Detailed risks

3. Pipeline theft

Risk description: Increase in the number of pipeline theft incidents in the TPL pipelines system which is impacting the security of fuel supply.

Current risk rating (matrix): EXTREME

causes	**Impact on industry**	**Key mitigations**	**vulnerabilities**
Organised crime • Depressed economy	• Security of fuel supply • Financial (high cost of bridging, investments in gantry capacity) • Environmental (product spillage to rivers and protected swamps	• TPL must invest in advance security measures using technology (drones) • Greater collaboration with the key stakeholders (SAPIA, Police, NPA and the army) • Stiff prison sentences to those convicted to ensure deterrence • Arrest the kingpins	• Police inability to nab the kingpins behind the pipeline attacks • Slow process of the court processes thus the deterrence factor is diminished • High cost of recovery operations (environment and pipeline repairs)
• Alleged involvement of the police	• Diminished trust on the police response and action	• Police management to reinforce the police responsibilities and prosecute the corrupt elements	• Entrenched corruption culture within the law enforcement agencies
• Alleged internal collaboration within TPL		• Proper vetting of staff in critical pipeline operations	• Intelligence on role-players and arrested persons/organisations
Syndicates duplicate action currently in			Incapacity of depot owner / TPL to trace

Cla

Detailed risks

4. Depot robbery

Risk description: ARMED ROBBERY AT STORAGE FACILITIES – FUEL THEFT

Current risk rating (matrix): HIGH

Causes	Impact on Industry	Key mitigations	Vulnerabilities
Depots are relatively easy targets for OCGs – low number of staff, industrial areas often remote	Financial losses, disruption of supply, reluctant workforce, high mitigation costs, high potential for safety incidents	Improve delay mechanisms such as fences, detection mechanisms such as remote video monitoring, response mechanisms such as armed response, stop certain products, relocation	Weak Law Enforcement in certain areas, remote locations, demographic changes at legacy terminals, high risk to people - staff and contractors
Insider collusion – contractors and staff can be approached by OCGs to supply information, local employees easily targeted	Costly integrity testing programs, staff relocation with associated costs, costly mitigations easily circumvented,	Regular integrity testing, recruitment from remote communities, reduce staff level by automation/digitalization Target hardening tank and loading infrastructure	Trust – controls easily breached/overcome by insiders, staff/contractors offended by integrity testing, high risk recruiting from local communities

Detailed risks

5. RTC theft			
Risk description: **TFR collects loaded and sealed RTCs from various coastal points to deliver inland. Theft of product happens between the pick-up and delivery points as they arrive with missing or broken seals. Sometimes RTCs do not arrive at all** **Current risk rating (matrix): Minor / Moderate**			
causes	**Impact on industry**	**Key mitigations**	**vulnerabilities**
RTC take long period on the road passing various points to build a train	Security of supply is negatively impacted, and delivery costs increase as road deliveries are considered to avoid running dry	TRF to be approached collectively by the Petroleum industry to address delivery challenges such as Security of RTCs, time taken to deliver RTCs, Payment of claims etc	RTC structure in terms of securing product(opening and closing valves, dome covers, leaking tankers)
TFR yards are not properly secured – no lighting, fences, access control, cameras and are not well maintained	Sustainability is affected as TFR does not honour claims (timeously)	Access to Transnet tracking system Effective Technology to secure product while on route	Weaknesses in Transnet structures / security
Tampering with Rail infrastructure- causing unplanned stoppages were criminals syphon RTCs	TFR reluctant in signing binding contracts to avoid liability	Shortening period of RTCs on the route (For TFR to find a better system to build their trains and ensure a more effective delivery process based on route alignments)	

Detailed risks

6. Illegal import

Risk description: Fuel products are imported in various ways (Bond to Bond/Under-declared/wrongly declared) with the knowledge of government officials, and sold into the local market at margins that are not feasible for the legitimate fuel industry.

Current risk rating (matrix) EXTREME

Causes	Impact on industry	Key mitigations	Vulnerabilities
Org Crime Groupings (OGC) financially strong; buy product, setup storage facilities and own their own transport, sell at uncompetitive rates	Industry cannot compete with reduced rates, lose distribution channels and customers, lower earnings lead to lower taxes	Engage with SAPIA and the DMRE, investigate sources of uncompetitive pricing, report known incidents to SAPS	The complexity of Org Crime is above the capability of smaller police stations, local government officials complicit in many cases, no official channel to report known incidents to the HAWKS and/or the NPA.
Collusion with Customs officials	Fuel is imported free of any duties, OGCs flood market with cheaper fuels,	Report known incidents to SAPS/SARS/NPA	No official channel for reporting known incidents to SARS .
Huge demand for cheaper fuels	Shrinking market, erratic supply depending on availability of fuels in the market can lead to shortages	Monitor sales to customers, report % drop in sales volumes to SAPIA for analysis, Report findings to the DMRE	Impact of OCG are not known or appreciated as there are little research done on this threat
		Real-time data analysis of retail site	Diesel price not regulated

Detailed risks

7. Cyber fraud

Risk description: Digital media used:

1. **For the identity theft of individuals, companies and assets (trucks) to submit fraudulent requests to open fuel accounts and place fraudulent orders on existing or newly fabricated customer accounts.**
2. **To perpetrate cyber frauds, particularly various forms of phishing, specifically relating to financial transactions and the release of goods.**

Current risk rating (matrix): HIGH

Causes	Impact on industry	Key mitigations	Vulnerabilities
Economic climate & poor criminal consequence management driving opportunity and greed Insufficient company internal control environment Employee negligence or complicity	Cyber fraud will be perpetuated as Internet-based activity is central to business worldwide	Regular review of the anti-cyber fraud control environment – internal and external (customers, vendors, business partners) Ongoing awareness to employees who are key to mitigating cyber risk. They are our “human firewall”	The nature of cyber means we will always be vulnerable to cyber fraud risk as online trading is central to business Human greed and poor “tone from the top” in society and business will always contribute to business being vulnerable to cyber fraud risk

Detailed risks

8. Cyber ransom attack			
Risk description: Ransomware is a form of Malware used to encrypt data so that it is unusable to the organisation. It then requests a ransom from the organisation typically in cryptocurrency to decrypt the data. This trend of cyber extortion is increasing locally and globally. **Current risk rating (matrix): EXTREME**			
causes	**Impact on industry**	**Key mitigations**	**vulnerabilities**
Organised cyber crime syndicates motivated by money. Typically initiated via phishing emails.	Many ransomware cases reported locally and globally.	User awareness around phishing emails. Cybersecurity technical layered defenses. Back-up of immutable copies of data.	Ransomware is an increasing form of cyber extortion as it can be done remotely with ease by threat actors motivated by financial gain.
Nation states, competitors and activists use ransomware as part of cyber attacks.	Major impact on industrial industries disrupting organisations, forcing operations to be halted, causing financial impact and lack of service to customers.	User awareness around ransomware threats from Board to end-users. Deploy technical cyber defenses in OT networks.	Old outdated technology can be exploited remotely by cyber threats.
			Inadequate state resources to investigate/mitigate

Detailed risks

9. ATM/CMS Bombings

Risk description: Criminal syndicates are using explosives to blow up cash management systems (safes) as well as Automated Teller Machines (ATMs) at retail sites to access cash. These incidents occur mainly at night.

Current risk rating (matrix): EXTREME

causes	**Impact on industry**	**Key mitigations**	**vulnerabilities**
Availability of explosives in the black market	Damage to property including devices and shop and loss of revenue	Security aids including alarms, armed response, staff awareness training. Stronger safes with plastic bags.	After hours trading
Declining Socio-Economic conditions	Increased incident rate around the country	Revised opening hours	No control over the external threat environment
Inside information or good understanding of the vulnerabilities	Repeated attacks on sites		(no) collaboration with banking industry

Detailed risks

10. violence

Risk description: Increasing violence against retail staff by criminal gangs during armed robberies and ATM or CMS bombings.

Current risk rating (matrix): HIGH

causes	Impact on industry	Key mitigations	vulnerabilities
High crime rate due to declining socio-economic conditions	Injuries	Security awareness training	No armed security personnel on sites
Use of weapons during robberies	Fatalities	Bullet resistant cashier booths	Most sites do not have offsite monitoring
Frustration caused by mitigating measures		Smoke solution (?)	

11. BUSINESS EXTORTION

Risk description:

There are groups in varies forms, it can either be political affiliations and/or localized formations confronting the business demanding to get a share on operations, projects and sometimes monthly payments.

There is a thin line between localization and business extortion.

Current risk rating (matrix): Extreme

causes	Impact on industry	Key mitigations	vulnerabilities
Lack of knowledge by communities on how to do business with well established corporates.	Tension's between corporates' and local communities, negatively affecting corporate image and branding.	we mostly engaged community leadership, and structures where this erupted and also gave them high-level procurement processes.	Threat to burndown business infrastructure by unrested related to these demands.
Localization Government Policy misunderstood.	Communities and local business forums up font demanding 30% on industry projects	In the main, we have since asked our appointed contractors to sub-contract local companies on jobs that are not technical in nature.	If this communities, no local business is appointed, the project is halted and delayed.
Assumption that goods and services are rendered by people/contracting companies that are not local where work is done.	Unwanted tensions between industry and local communities. Business infrastructures damages Delays on the project, work that might be done by unskilled people/subcontracting companies	We have since asked appointed contractor by the industry to at least appoint the CLO, and local community members were possible in non technical skilled duties.	.

Detailed risks

11. Business extortion			
Risk description: **Criminal elements that takes advantage of the socio-economic advantage of our people, crime and demanding to offer businessowners, dealers and contractors security to can operate or do business in their gangsterism territories. ('construction mafia')** **Current risk rating (matrix) EXTREME**			
causes	**Impact on industry**	**Key mitigations**	**vulnerabilities**
Organised Crime levels in the country	This creates fear on business operators, dealers and contractor	SAPS has since formed a task team on business extortion and we report to SAPS	On professional businesses that are audited, they can't account on such transactions.
Gangsterism	Aggression towards business operators, dealers and contractors.	Private Security Companies deployment. Open a case with SAPS	Law enforcement support
Drugs		Deployment of Close Protection Officers	Death threats

#	risk	trend
1	Bulk fuel theft	↔
2	Truck hijacking	↑
3	Pipeline theft	↑
4	Depot robbery	↑
5	RTC theft	↔
6	Illegal imports	↑
7	Cyber fraud	↑
8	Cyber ransom attack	↑
9	ATM bombings	↑
10	Violence/injuries, fatalities – impact on people	↑
11	Business extortion	↑

Industry actions

- DMRE/SAPS/TPL/TFR engagement
- Setup a combined fuel industry project with the NPA, HAWKS, and SARS
- Engage TFR for improved service, security and claim processes
- National Priority Committee for Extortion and Violence at Economic Sites is set by Business Against Crime (BAC); the Petroleum Industry is taking part.
- Business Guidelines set to engage with SAPS on Extortion.
- Shared security intelligence platform with road freight industry & insurance Cos
- Initiate industry-related cyber ransom expert discussion at SAPIA level
- Engage SABRIC