September 2022

PROTECTIVE INTELLIGENCE NEWSLETTER

Advanced Security Risk Management Ltd.

Proactive Security Risk Management - Selecting CIT Providers, It's all in the details

The death of the two Security Officers and the injury of another in the gruesome daylight robbery involving Allied Security, Cash In Transit (CIT) team on Monday 19th September, 2021, is still quite difficult for me to accept as Security Consultant. It is quite difficult to accept, because it is my expert opinion that their deaths could have been avoided by simply making them 'hard-targets'. A hard-target is "a person who, due to his/her actions and/or appropriate protective measures, is able to minimize existing risks and thus most likely represents an unattractive target."

The objective of this article is to provide Corporate Clients/Business Owners like yourself with an insight into managing risks associated with CIT operations.

The two main takeaways are as follows:

1.A list of factors to consider prior to selecting a CIT Provider

2.The correlation between the selection of a CIT Provider and safeguarding your businesses, customers, employees, and assets during CIT operations.

History of CIT robberies in Trinidad.

The robbery of CIT vendors is not new to Trinidad and Tobago. However, the modus operandi, use of brute force, observed in the recent incident was outside the norm. There have been multiple reported incidents over the years in which Business owners lost large deposits/withdrawals. However, 99% of those incidents were non-violent robberies where, in most of those incidents, the cash was transported by employees (baton Security Officer, Office Assistants and Drivers) who are surveilled, followed and robbed. This is ongoing and is more prominent in southern and eastern Trinidad.

There have also been various attacks on the registered CIT providers over the years:

·**November 2013,** armed robbers attacked a Sentinel Security Services CIT crew and stole $17 million in local currency and US$150,000. A Security Officer was killed in the incident.

·**December 2017,** Amalgamated Security Services Limited's CIT were robbed of $6 million at the Piarco Airport

·**September 2018,** G4S Secure Solutions' CIT crew was robbed of firearms and an estimated $1.6 at Republic Bank's ATM machine at St Helena, Piarco.

BY FIONA PERKINS - CEO

September 2022

PROTECTIVE INTELLIGENCE NEWSLETTER

Advanced Security Risk Management Ltd.

On 20th September, 2022, The Guardian Newspaper quoted Ms. Rebecca Ranger, Estate Police Association's (EPA) Allied Security Services Branch Secretary, saying "We have been begging Allied Security for over seven years for proper vehicles to do CIT (cash in transit) pick-ups. Allied has not provided that. What they did is continue to increase in their pick-ups and give us vehicles that are not suitable," It is indeed the general expectation that all CIT providers would utilize armored vehicles. This however is not a guaranteed practice as demonstrated in the fatal attack in which Allied Security utilized a pick up as opposed to an armoured vehicle for cash collection from Pennywise. Similarly to other countries, Trinidad and Tobago has a number of Security Companies and private individuals who provide Cash In Transit (CIT) services on behalf of Corporate Clients/Business owners/Public Entities. Some of these CIT providers have employed international best practices, including but not limited to, operational quality assurance and technical specifications as outlined in ISO 9001, 2015, ISO 18788 2015 and Trinidad and Tobago's Occupational Safety and Health (OSH) Act.

I anticipate that the above incident would have created the platform for further deliberations among CIT providers, the government, and the Estate Police Association on the implementation of controls in the field of private security.

However, it is also important that Corporate Clients/Business Owners examine the risk associated to CIT operations and take reasonably practicable actions to minimize exposures/losses: loss of life, assets and the impact on your businesses. This requires each Corporate Client/Business owner to proactively manage your CIT security risks by doing the following:

1.Understanding your CIT process and exposures
2.Becoming highly engaged in the selection of your CIT providers
3.Conducting ongoing reviews of your CIT providers/services

CIT Processes and Exposures to Corporate Clients /Business Owners

CIT operators serve multiple clients throughout the island, moving cash between Businesses, Financial Institutions and Cash Processing Centres. They visit their clients' locations to both collect and deliver cash and other valuable items. In most cases these armed officers operate during their client's business hours, thus arriving at and being on your compounds with firearms in the presence of your customers. This therefore means that both your employees and customers could be exposed the risks associated with a CIT robbery.

The risks CIT operations present to Corporate Clients/Business Owners include but is not limited to:

- Injury/Loss of life (employees, customers, CIT Officers, etc.)
- Loss of Assets
- Reputational Risks (which may affect your customer base and profitability)
- Financial Loss
  - Lost Man Hours (as injured or traumatized employees may require time off)
  - Cost to address Reputation Risk through costly Public Relations Campaigns
  - Civil Actions (from injured parties)
  - Fines via the OSH Authority (if found guilty of failure to implement effective security and safety controls)
  - Increase in Insurance Premium
  - Legal cost
- Ongoing court attendance (which can be stressful for employees and result in lost man hours)

Some business owners have addressed the CIT risks by acquiring Public Liability Insurance or Comprehensive Crime Coverage Insurance. However, it is also recommended that you conduct a thorough due diligence before employing the services of a CIT Provider. This simple act is an effective cost management tool.

Managing Risks and Minimizing Losses - The importance of a CIT Due Diligence

It is recommended that Corporate Clients/Business Owners become more engaged in the selection of your CIT Provider by conducting a through due diligence. As mentioned above, conducting a CIT due diligence is a component of your Proactive Security Risks Management process, aimed at minimizing losses. It provides you with an opportunity to ensure that you select a reputable CIT provider that is capable of Securing your assets; Securing their Officers; and Minimizing your losses.

It is important that as Corporate Clients/Business Owners you can decide whether your CIT provider has implemented the necessary Security Governance Structure and Physical Protection Systems to proactively manage security risks and effectively respond to attacks. One way of verifying the CIT Providers' readiness is to request that they demonstrate how they will achieve the following:

1. Proactive -Security Management Risk Strategy

Prevent attacks
Delay attacks
Detect threats
Assess threats

2. Security Incident Management Strategy

Assess Attacks
Contain/Eliminate Threats
Improves Response and Recovery to Incidents
Enables/Supports Business Continuity

If as a Corporate Client/Business Owner, you believe that you are not equipped to conduct such an assessment, it is advised that you utilize the services of an independent security consultant/company. Your Security Consultant should be engaged to conduct a Security Vulnerability Risk Assessment of the CIT provider. The final report shall address the following:

·Threat Events;
·Threat Source;
·Description of Control Activities;
·Likelihood of Attack/Occurrence;
·Impact of the attack based on the effectiveness of the CIT Providers Security Systems;
·Consequence of the Loss from these attacks.

Minimum Expectations of a CIT Provider

1.**CIT Operating Procedures and Policies.** CIT Providers should provide evidence of their existing processes aimed at minimising your exposure. This may include a procedural overview on officer selection and training, pick-up and delivery plans, vehicle tracking, parking arrangements etc.

2.**CIT Technical Specifications**: In the absence of formally written international CIT Standards, the vendors must show proof of implementing international best practices to ensure adherence to technical specifications in the design of its CIT vehicles; operations centres and other technical requirements such as GPS tracking.

The CIT Provider should utilize armoured vehicles with an internationally accepted Ballistic Protection Level. Ballistic protection Level indicates the extent to which the armored vehicle (glass and metal) can provide protection against bullets/attacks. Several CIT providers in Trinidad and Tobago utilize armoured vehicles with the correct ballistic levels for both glass and opaque areas. These vehicles are designed to deter, delay and prevent loss of assets and lives through attacks. Others similarly to Allied Security, utilize what is called soft skin vans, that I like to call Bread Vans because they lack the necessary protection.

There are several standards of ballistic protection. Kindly refer to the following:

1.

LEVELS OF CAR ARMOUR

BALLISTIC PROTECTION	BULLET TYPE	THICKNESS ESPESOR
B4 Handguns and Shotguns 	• 9mm • .38 Secial • .357 Magnum • .44 Magnum	
B5 Riffle protection - AK47 	• 7.6X33/.30 CAL Carbbine • 62X39/AK-47	• 32 mm
B6 High Power Rifle Protection 	• 7.62X51 mm/M-80 • .380 Winchester FMJ • 5.56X45mm/M-16/193	• 41 mm
B7 Armour Piercing Rifle Protection 	• 30.06 AP (Armor Piercing)	• 78 mm

3. **Adequacy of Physical Facility and Equipment** (in instances where the CIT Provider holds your cash overnight): Crime Prevention through Environmental Design should be incorporated into the design of the vendors' Cash In Transit Operations Centres. This includes implementing the physical and psychological barriers to deter would be assailants, outfitting the location with the necessary electronic security and structural reinforcement eg. CCTV Systems, Access Controls, Reinforced walls, and armed Security Officers.

2.**Maintenance of Equipment:** It is important to acquire proof of the vendor's vehicle and firearm service schedules to ensure they operate at their optimum.

3.**Schedule and Route Planning:** It is important to recognize that you could be a victim of a robbery and ensure that your CIT provider takes the necessary precautions to minimize the chances of you being targeted. This means that CIT providers should vary their routes and the times that they conduct collection and delivery of your cash/assets. It is also important that the same CIT drivers/crew do not visit your location repeatedly as this minimizes the chances of collusion among CIT Officers and members of organized crime.

4.**Ongoing Training and Uniform Guideline:** The CIT Provider should provide proof of ongoing Officer training in areas including but not limited to: CIT, Security, Use of Force and Firearm Training. Officers must also be outfitted the required PPE such as bullet proof vests.

5.**Emergency Response and Business Continuity:** Emergency Response and Business Continuity Plans must be institutionalized by your CIT provider. This includes having alternate operations sites, spare appliances, written response plans and proof of assimilation based on incidents/threats. Most importantly, they should provide an overview on their response to various attacks at your locations.

Utilizing the services of a CIT Provider that is unable to provide the above may save cost in the short run but as demonstrated above, will ultimately be quite costly.

Advanced
Security Risk Management Ltd.

www.advancedsrm.net
info@advancedsrm.net
1 (868) 688-4345