Situational Awareness:

Profit Protection (Security Style)

Preamble

The Accountants set the budgets taking into consideration the HR needs and the security department (that is if the security practitioners are reporting to the HR or perhaps another person within the company).

Accountants consider security as an expense which in-fact 'old school mentality'. Furthermore, HR may be unaware of the power of security training and also may look down upon the security practitioners.

When the security practitioners earn trust and respect by educating both the accountants and HR on security methodologies then the working relationship improves. Keep in mind that the accountants are also investigators because they need to find fraud, sometimes they may assist in discovering the losses and are fully aware of being compromised by computer viruses. Security practitioners could impress the accountants with their investigative knowledge and their efforts in protecting reputation because there is no insurance to mitigate reputational damage.

There are certain fields of interest whereas loss prevention through theft is reducing the profits. Let us keep in mind that each field of interest has its own unique issues of concern for example,

- A vehicle mechanic could not only steal parts but also time. They may tell the client to purpose just the parts and then after working hours the mechanic could install the parts are a reduced rate.
- Hotel's biggest expense is related to theft by guests as well as staff. Also keep in mind that staff could be selling rooms. They could be using physical keys so that they can 'bypass' the computer system that records the times when doors and opened and closed.
- We can go further into the hotel sector whereas the office that sells time sharing could be pocketing a larger share that is disclosed to the ownership of the hotel.

These above examples simply give the idea that these crimes could be draining revenues that the accountants may be unaware of. Providing such information to the accountant could enhance the level of trust and respect for the security department.

Overview

The threats from 2020 till present along with the massive development of technologies provide the security industry the comprehension and methodology to profit protect themselves and their client base.

It would be wise to assess the financials before and after covid 19. The unexpected expenses, for example, increased sick leave, increased costs related to screening and employing temporary staff, equipment, technology, besides any loss of revenue relating to crime be it insider threat. There could also have been loss of business relating to reputational damage.

Then consider the threat implications from early in January 2022 because of the Russia Ukraine war impacting energy and food security. There could have been increased costs relating to transportation of staff, electricity costs and perhaps others that impacted the business.

The two or more economic meltdowns running back-to-back is compounded to the extent that the inflation levels elevated besides increased lines of the jobless could lead to increased crime levels never experienced before where some countries could shift into various levels of anarchy. It is best to keep an eye on the daily inflation rates besides the common crime levels and any crime related to a specific field of interest. The speed of intelligence gathering specially from reliable resources is vital for many reasons that will in-turn protect the profit margins.

Situation

Evaluate your location and field of interest. There may be clients that could reduce the size of their guard force. Some even may shop around for cheaper prices and select services from unregistered so-called security companies or/with unregistered security officers/guards. This will open the door to organized or gang crime besides other financial losses.

The cost to live increasing could dictate that lower income security officers/guards. This could lead to a greater insider threat and therefore budgets must be set for stronger governance management using manpower and technology.

Profit protect considering the Workforce and Technology.

Expenses to budget now to service unexpected expenses.

- Multi-skill or Cross-skill Key people. Do keep in mind that covid has variants that may not be deadly, but people could get re-infected because of the changing genomes that seem to be highly infectious and could be more deadly. Therefore, this will impact all expenses related to the sick leave and hiring of staff. The more experienced the staff – the higher the cost.
- Mpox in certain countries, cities and sites of concern dictate that additional PPE would be required such as **gloves** besides the masking and additional sanitising expenses in relation to such as it is different to covid. (view updated security officers managing bio-threat booklets on HIM because it addresses current threats that could demand eye protection.

Using Technology to Profit Protect

Reduce the level of incidents, speed up appropriately emergency response and effectively manage investigations-based utilizing technology and workforce.

- Reduce false alarms by utilizing PSIM or VMS that could use AI, IoT and other means to identify the threat and discharge it immediately if is not a threat.
- If it is a threat, then the technology could alert appropriate people to respond instead of wasted time with irrelative personnel. Time costs money. Travel expenses cost money therefore deploy the right number of appropriately skilled people.
- Litigate certain crime speedily using technology without having to use personnel on the ground (View using AI and technologies identify crime and concerns).
- Use technology for governance management besides compliance (Getting the most out of AI on HIM)
- It must be said that effective incident reporting software connected to the technologies would service identifying crime, comprehending the hot spots that would require frequent intervention besides identify staff on the ground that may need to be upskilled or changed

because of higher levels of aggressive and violent behaviour incidents.

- When customers are fearful of walking through the doors – then there is no revenue entering the site. It has to be professionally managed by layering the workforce by skillsets, constant monitoring and supported with the appropriate technology.

Urban and Rural Security

When people are starving or unable to pay for their electricity bill besides others that may need life giving medicine then they are desperate. Desperate people can break for their moral code when their basic needs and wants are compromised. There are sites that are high-risk and any attack on such sites that lead to the burning down of the sites or the stock levels are heavily compromised. The predictions of such in some countries are inscribed in the security managers protocol guide for bio-threats because the crime related to the threats led to some countries going into anarchy.

The Rural Security issues are covered for Catastrophe Security in the Critical Thinking the X factor in criminology security and risk. The types of invasions and methods of theft can be litigated by using automated drones along with (if necessary) armed with non-lethal means.

Most Importantly – Loyalty Bond the Client

- The client will trust and respect the security practitioner that uses specific security concepts and language besides using security soft skills to get the most out of their business negotiations.

When the client trusts and respects suggested measures to be used for profit protection then they would not change suppliers. In-fact the relationship could turn into more of a method of partnership to identify threats and opportunities.

The reason being is that critical thinking methodology uncovers loopholes, damning issues and opportunities. The security sector is able to define the topic ‘critical thinking’ and prove such. Find on HIM