

HR & Security

The new norm

What employers need



The employers need!

- *Security team must be situationally aware and can identify besides comprehend the fast-changing vulnerability landscape.*
- *Proactive & investigative minded team*
- *Team uncovering new crime or identifying loopholes.*
- *Improved reporting from the ground with all the reliable and truthful information.*
- *Awareness of Profit Protection*
- *Manage multi-cultures efficiently.*
- *Awareness of Radicalization*
- *Implement Solutions or protocols efficiently and effectively*
- *Getting the best results from their investment into technologies.*

What security people do

Security practitioners find the crime and stop it, protect sites and save lives. They must out-think and outsmart perpetrators because they manage life impacting and deadly incidents. They find the crime and stop it – protect sites and save lives. We saw this, when Security managed the flow and behaviour of the population as we saw during the covid-19 biothreat besides by using biothreat security protocols that were specially designed for covid-19, besides mucormycosis and MPOX. They also managed the litigation or lowered the level of collateral damage related to the threat.

Security practitioners use technologies and the workforce to litigate or limit the level of collateral damage. Some of these advanced technologies such as software platforms for the management of risk, emergencies, incidents and investigation are cognitively driven that demand specific skills to get the results that are required to justify the investment.

The New Norm

With multiple threats in theatre such as biothreats, wars, climate change has led to the economic meltdowns that have contributed to the mass migration of people. Apparently, in Sweden there is a predication that in two generations time, there will be more immigrants aborded into their community than the home-grown inhabitants.

The current situation globally has seen a major change in their societies whereas pro-nationalist extremists, pro-revolutionary extremists and religious extremists becoming more vocal and active besides higher crime levels besides a wider variety of crimes being committed.

An entity or company is only as good as its people

There is more HR in Security than in HR itself. Unfortunately, there are security managers that report to HR but when the Security Manager knows exactly what they do - then the HR will trust and respect the security manager's intellect as they have much in common. This also holds true with the financial department because the emphasis is now on profit protection.

Profit protection

During a pandemic, war, economic meltdowns with increased crime levels

Cross-skilling and training of key people is vital because of viral sicknesses besides demonstrations and riots.

- Consider the costs of hiring people when it involves placement agencies, screening and training of permanent staff or even temporary staff during biothreats or during uprisings.
- Consider the costs regarding and related to sick leave increasing impacting on production, missing performance deadlines or any issues that are in-line with the train of thought.
- Avoid reputational damage when crime such as jobs for sex or money becomes an issue or when mobs, demonstrations or riots attack a site.

We must include corruption in the fold. Subsequently, oversight and governance of all staff besides the decision-making hiring chain should be considered as vital.

Selecting the right people and why

HR should be aware that security practitioners experience individuals or groups that could be aggressive which could manifest into violent behaviour. This means that security do handle life impacting and deadly outcomes therefore, the new norm must consider to the layering of manpower by skillsets and character traits of the individuals.

Multicultural management. Based on research within Critical Thinking the X Factor for security, criminology, risk one can find leadership and project management of multicultures. Also, view security managers strategic protocol guide for biothreats that talks to such subject.

- People that are bias; will display their emotions in their tone of voice and in their body language. This could fuel tensions therefore employing people that are bias towards any political body, religious beliefs or moral code could spike increased aggression. This talks to the importance of using lie, deception detection and critical situational interviewing regardless of culture.
- We must also now bring into this the new norm because there could be an increase in terror attacks and demonstrations based on recent changes in the global dynamics that may prompt the question: "*Could the worker or applicant be radicalized?*" We do know that there have been radicalized security officers that have murdered others, resulting in major reputational damage. It is not good to point fingers because any security company could experience this dreadful scenario.
- Again, we repeat - The HR and Security should adopt certain skills below could be capable of uncovering the true feelings of people or a change in a person's character besides using other forms of intelligence gathering methods.

Escalated crime and New Crime related to the threat

HR should know that with the economic meltdown, people could break their moral code and resort to despicable behaviour. Therefore, HR should know that security considers the crime related as in,

- Increased corruption, bribery, the selling of company secrets, extortion, to mention but a few. Keep in mind that people have phone video recorders and if a bribe or aggression and violence is captured then social media will have a field day resulting in *reputational damage*. This could impact the profits because customers that avoid going to site - means that no money is going to arrive at the front door.
- During recessions of sorts - the illegal economy grows. There could be attempts by transnational, local organized crime, gangs or lone wolf criminals to infiltrate or hijack companies, departments, desperate employees or assets. These criminals or groups prey on desperate people, and one may need to identify the silent victim that could be working on their own voluntarily or in concert with others under duress.

Therefore, do attempt to discover the silent victim as organized, local gangs or lone wolf predators target such people under duress to work in concert with them.

Certificates and Skills

HR would be considering the regulators criteria for certain job functions. Certificates could prove a person is educated in certain knowledge, *but it is the skillsets that make them relevant.*

The HR must now seriously acknowledge that security sector is fast changing with current threats and is highly volatile that requires the mix of security knowledge and skills is required to maintain relevancy from here on into the future.

Managing the people and finding the crime

Consider the simple facts:

There are millions of criminals trying to outsmart or out-think the security system (tech and manpower).

- People do lie, hide or volunteer information. *The security practitioner cannot afford to be misled. Professional practitioners that are gullible and naïve to the fact that people do such simply heightens the risk factor. Therefore, if they can prove the fact that they have had some form of education relating to reading people and the situation - then that is excellent.*
- Crime or Criminology-Risk Situational awareness. Critical Thinking (security styled) is imperative to educate for software platforms related to managing incident, emergencies, investigations or risk besides compliance.

Based on the principle " Security success depends on the level of situational awareness of the people on the ground and their reaction speed" (Kirsten J, 2018).

As said, it is people that cause crime. The crime investigator gets called only after an incident. The security practitioner must be able to find the crime, the person or people involved before it becomes an issue.

Therefore, the follow ingredients form the most important skillset.

- **Critical Thinking Security Styled to** out-think and outsmart perpetrators besides to effective use specific technologies that are cognitively driven.
- **Multi-culture** management.
- **Lie, deception detection and critical situational interviewing** regardless of culture meaning that the assessment must be done within seconds.
- **Criminology-Risk knowledge** means that one has to know where, how and why to look for distinct crime especially new crime.
- **How to identify the silent victim.**
- **Emotional intelligence** to identify a person or people that are being anxious and the ability of calming people down. These skills could be found in leadership skills, conflict management and strangely enough in lie, deception detection and critical situational interviewing as its based-on emotion management of different cultures.

Character Traits of a substantial security applicant

- Balanced empathy and ego drive
- Investigative minded
- Studios

Knowledge Relevancy

The above hopefully paints a picture of this new norm for this moment in time as security obviously does more.

This is not a one size fits all kind-of-thing.

Consequently, the above document gives guidance to the HR and Security to research their location and field of interest to determine their situation, the position that they are in and what needs to be done.

Note: plagiarism in any aspect of this document or methodologies will be dealt with accordingly.