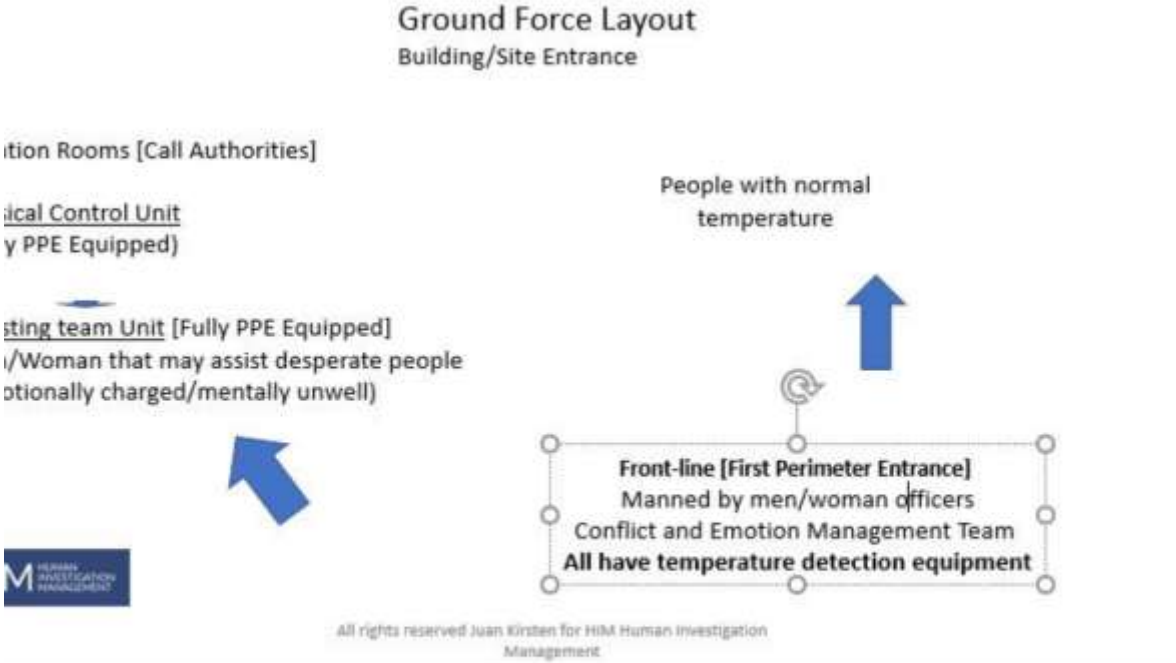
BIOLOGICAL THREAT SECURITY

SECURITY MANAGER'S STRATEGIC OPERATIONAL & PROTOCOL GUIDE TO MANAGE BIOTHREATS

LEVEL OF DANGER: PRIORITY ONE

[LIFE IMPACTING & DEADLY OUTCOMES]



SECURITY SUCCESS TO LIMIT BIO THREAT COLLATERAL DAMAGE DEPENDS ON THE LEVEL OF SITUATIONAL AWARENESS OF THE DECISION-MAKERS ON THE GROUND AND REACTION SPEED

Index

Contents

Dedication

Thank you to all security practitioners, be it the academics and consultants, the owners and executives of security companies, the heads of corporate security, risk mitigators, investigators and security officers on the ground.

Many are behind the scenes and are just as important as the first responders on the ground.

Thank you again for your service.

Reviews 2020

Larry Barton, Ph.D., Distinguished University Professor of Crisis Management and Public Safety, University of Central Florida, USA states ‘’action steps and considerations that employers must take now, before rancour and situations of aggression and harm emerge in the workplace. While all of us want to be optimists, we must be realists- the health check of employees in so many employment environments globally *do not meet a "one size fits all standard.*" If, employers’ race to bring back employees without thinking about the many nuances that the ‘paper’ outlines, they do so at their own peril.

Prof. Rommel K. Manwong, PhD "Managing COVID-19: Strategic and Operational Guide" is an excellent criminological tool for security and safety managers in packaging their industry-based pandemic protocols. It contains a unique formula in dealing with the current and future threats of public health crisis. The author creatively shared the most necessary direct options to counter COVID-19. A great source in formulating your own counter pandemic formula

Capacity Building 2021

In December 2020, HIM was endorsed by ISIO | International Security Industry once the biothreat security protocols for Covid-19 were published. Thereafter in January 2021, CAPSI | Central Association of Security Industry, IFPO | International Foundation for Protection Officers and SASA Security Association of South Africa (Now representing together 10.2 million security practitioners) joined the mission to contribute globally to lowering the level of collateral damage)

Addressing 2021-23 Mucormycosis, MPOX & Marburg Virus

Foreword

The population of the world went through security from the beginning of the covid19 pandemic until different countries decided to end the health protocols that dictated that people had to wear masks, maintain social distancing and satanized.

It is the public and private security industry that took temperatures using thermal imaging cameras or electronic thermometers besides managed the flow and behaviour of people and that ensured they sanitized.

Subsequently, protocols had to be considered for taking temperature using technology and devices, besides strategically layering the workforce on the ground because security manage life impacting and deadly incidents as they handle aggressive and violent behaviour.

Also, the security practitioners did more because there is crime related to the threat and its tailing threats.

This work provides a formula to identify and uncover unknown issues which is a methodology to discover formations of key issues and suggestions to limit collateral damage. The research is to provide historical context for Covid19, but we will continue to update this work as time goes on to maintain its accuracy so as to provide a chronology of research.

In 2021 in some countries because of a climatic condition *a parallel life impacting and deadly biothreat* Mucormycosis (black fungus/mold) took advantage of covid-19 can caused major issues. Furthermore, the situation impacted increased crime levels by sole traders, street and organized crime gangs.

Mpox presented itself in 2022 and is now addressed in this updated edition. Some protocols that was considered for Covid19 are highly relevant for Mpox however Mpox does have unique character traits that is addressed herein one of which is that the major threat is to pregnant woman where one in four has a healthy baby.

Consequently, we address

- airborne viruses (Covid19)
- black fungus transmits airborne and through water droplets (Mucormycosis – a parallel life impacting and deadly threat in certain countries)
- viral liquid transmission (MPOX- Alert for pregnancy)

Furthermore, this work addresses the tailing threats. Meaning, that this work could give direction to managing a bio-threat besides highlighting specific crime and other issues to profit protect the security industry and the global economy at large.

Introduction

In early 2020, the entire world was in a state of shock when watching the wave of the pandemic destruction rapidly moving invisibly through the world. When watching the news channels, one could just think of the factual reality that, whatever was planned and hoped for by many, just became null in void. In

companies, all financial planning was just wiped clean; human resources could lose irreplaceable people; and the security department needed to protect and limit the collateral damage using all means possible.

To base this work on something in the past – a search was made of something similar that happened before. In 1918, the Spanish Flue hit the world leaving between 50 and 100 million dead. It would have been beneficial for a security manager to have compiled a 'security' incident report on the collateral damage to their location and/or their field of interest. There was nothing recorded that a security practitioner could begin to work with based on something that was truly unknown.

It must have been by universal design or just plain coincidental that previous articles published over the past months made even more sense for this moment in time. For example, "the security practitioner's biggest nightmare in not knowing what is truly happening on the ground."

Considering also, that *certain terms and formulas* have become more relevant and noticeably clear, such as, "security success in limiting the collateral damage would depend on the level of situational awareness of the people on the ground and their reaction speed." Reaction speed is paramount.

Most importantly, the related truisms are also applicable, such as "we live in a fast-changing world where the vulnerability landscape can change at a moment's notice could invite unique collateral damage." Subsequently, we would need to "uncover loopholes and damning issues besides opportunities (methods and protocols) to limit or mitigate the collateral damage."

Other terms used elsewhere in the Human Investigation Management (HIM) works are highly relative now, such as, "it is not the weapon that will causes mayhem, it is the people. The virus is the weapon – the *issues are related to the people*." The issues related to identifying, managing, and isolating infected people would be the major issue. Furthermore, people could react desperately and physically whereas, former methods of policing people may not be appropriate. Accordingly, "*skills must be relevant to the threat.*"

Moreover, "*technology and equipment are only as good as the users*." With minor adjustments on some equipment and/or technology would turn into a formidable necessity for handling life impacting threats and, some users could get even more benefit out of the technology and equipment than others.

Now, the time has arrived to collate all past research and knowledge to productively construct and contribute towards the plan for COVID-19 disablement. The realization of the size of the problem demanded that all practitioners on the ground must work using the same method by, either duplicating methods used elsewhere and/or, could design their own unique approach. This situation could occur because each person could experience a different impact by working on a

different timeline and/or in an environment that was appropriate where only some or all of the others could experience the same.

The security industry is foundational in disabling COVID-19

The building blocks for success must begin by obtaining information from ground level. In all countries there are more private security officers than there are police officers. The security practitioners that have had training in situational awareness besides many have had some form of conflict management training.

Consequently, there is a huge force of millions of security practitioners on the ground that have basic relevant training. This huge force could smoothly be upskilled to litigate the unique threats and could be activated real time on the ground. They should all work together toward the same goals using the same principles.

These millions of security practitioners are HIGH-RISK first responders in one way or another. They are the ones that could more than likely experience dangerous and highly confrontational interactions with others more so than any other force. Especially, the practitioners that are on the ground and physically working in direct contact with the public. This statement calls to the protocols, a strong form of oversight, and a daily vetting regiment.

This means that the officers must have their temperature checked when walking on and off shift. They should be "safely travelling to work" and physically and mentally equipped. This will be elaborated upon below.

No country can afford to have 50 000 Security Officers infected. The 'power of two' infection rate would multiply exponentially the viral infections. In 2021, ISIO formed a MoU with CASPI (India) and SASA (South Africa) brining over 9.150 million security practitioners on biothreat security mission.

Next COVID-19 stage impacting some countries

The predications of each stage must be realized. The implications of which would be that what happens in one country will impact others.

There are already a few countries already that are on the knife's edge. Within a matter of days, they could be in a state of anarchy which would consequently deliver unimaginable collateral damage. The term 'unimaginable' is used because now more so than ever because desperate people will do desperate things which they would never previously think of doing.

There are many informal settlements, townships, and slums. These are aside from the poor population living within villages, towns and cities. These people are densely amassed, where they live, eat, and take transport together.

They are inter-dependent on one other, while also dependant on menial (low-paid ad hoc employment) jobs which are paid daily or weekly. It would be impossible

for them to lockdown for days on end as they would starve to death. Their situation would drive them to commit acts of desperation.

Moreover, there are 'invisible' people working in high-risk sites who function as the foundation of the support services which keep the system functional. For example, people applaud the surgeons, doctors and nurses. But what about the cleaners, cooks and maintenance workers that keep the hospitals running? What about the security which safeguards the critical infrastructure? When one or more become infected, the entire chain of support may need to be re-manned. The re-training of security officers consumes valuable time and impacts the smooth running of the system.

The following may not sound applicable to practitioners in some countries. However, the situation would vary according to the length of time it takes to create a cure.

Situation

- Increased numbers of starving people due to loss of jobs.
- People desperate for basic needs including, food, water and shelter.
- Many will be desperate for protective gear.

Implications

- Increased theft in every form. From insider threats to forced intrusions.
- Mob attacks on warehouses which stock food and medicines. These attacks will also be directed at providers such as outlets in malls, hospitals, pharmacies, nursing homes, or even street vendors.
- Attacks of logistical supply chain of food and medicine.
- Increased home invasions.
- Many more weaponized people without sufficient training.
- Many more people suffering from psychological disorders.
- *In some countries various levels and types of anarchy could be displayed for various reasons.*

Problems

It is doubtful that countries can afford to sustainably provide free food and housing to the masses. Once people being to starve, especially children, their reactions could become aggressive and hostile

COVID-19: Even though some human trials began, it will take a significant period of time for a cure and vaccination to be discovered, become approved, manufactured on a mass scale, and distributed world-wide.

Concept of disablement

There is a saying in Africa that, "one could eat an elephant when one eats a small bite at a time." Eventually the entire elephant will be eaten.

Security practitioners on the ground must build their own secure structure by taking four steps working with the protocols for each step. These protocols share the same principles but are implemented variably according to each context. Then, the elephant will initially use the trunk to let others know what and where there is a danger, until the day will come when all trunks trumpet victory together. We consider the elephant because it has a huge memory. People tend to forget very quicky once a major threat is manageable. This cannot be the case for practitioners in this field because we manage life impacting and deadly incidents.

This is for the practitioner (elephant) on the ground

- Weaponize the team with knowledge to identify and report the threat.
- Collect the reporting and attain an understanding of one's own big picture using a visual incident management system, be it on a black/white board or using data capture software.
- Plug the holes/fill in any gaps.
- Repeat the cycle again, this time with more relevant knowledge from own experiences as each location or field of interest may have unique issues.
- Then lift that trunk and let others know what was uncovered and what worked effectively!

Where to begin

This may break the flow of the reading but is important to insert here. All practitioners must wear face shields or goggles besides masks because the eyes are just as porous as the mouth! This is specifically important for practitioners that have a *high probability of managing aggressive and violent behavior.*

The Security Department needs the money to update the equipment, get the technology and skill the staff accordingly to the threat. The problem was is that the financial controllers believed that security was an expense besides all others undervalued the security department and the capabilities of the security practitioner. Crazy as it sounds, the security practitioners may not have reported to top management but was seconded to report to the HR Department or accountant or even the chief engineer. It was imperative to now display the thinking ability of the security practitioners who must out-think and outsmart for the forever thinking criminals.

On February 28th, the first article from HIM| Human Investigation Management (powering ISIO,) was published in the security media and on LinkedIn was urging security managers to have a conversation with the human resource manager and the financial department. The reason for calling such a meeting was because the financial department considered security as an expense and that security personnel themselves were undervalued by other departments.

It was imperative for the security officers now to take the initiative and motivate such a meeting, in order to earn trust and respect by their peers. This meeting was meant to enlighten all on the implications of the pandemic from the security point of view. Sure, the finance and HR departments would consider budgeting for

- sick leave
- cross-skill training; and
- all expenses related to employing temporary staff.

However, the Security Department had to make their position clear to consider a different mind-set and collaboration by their peers for a sufficient budget. The security manager had to consider equipment, technology and to determine the type of skills that would be required to limit the collateral damage.

Concept of protocols

Initially, one must consider that what could happen in one location or field of interest could be replicated in another or have its own unique brand of collateral damage.

The fundamentals had to be understood by comprehending the true nature of this beast. Distinct sectors could be impacted initially greater than others such as the tourism related sector.

Having just completed mentoring a learner using hotel security as a hypothesis, which was again coincidental and timely because there was sufficient insight to construct protocols related to such. The first step was to comprehend the beast and how to identify it. *Subsequently all practitioners heighten their situational awareness to identify the features of the threat by considering what could be seen or heard, being coughing, and displaying flu-like sickness.*

Therefore, if a person went to a room they would first listen at the door for any sounds, then follow the protocols that are outlined in the hotel security protocols. The same protocols could be used for old-aged retirement homes, ships, rehabilitation centers or for any pandemic being COVID-19 housing management.

Tracing back to the roots

Considering now that before the person inside (perimeter), they may have already gone through some layered security system, by being viewed on CCTV and, passed through some form of access control *when walking through the parking area or even was seen or heard by a security officer.*

The problem is that people could walk around acting like normal without displaying symptoms for a few days before they became ill. Therefore, the next best thing would be to identify the threat in theater by using what we knew being, the symptoms of high fever and coughing.

To identify an infectious person being in high-threat status would be by the only reliable method being the measurement of someone's temperature. *Temperature fever detection settings must be known,* for example - ensure settings for temperature and fever detection only begins at **37.8**. ***Avoid ciaos by knowing the core temperature of a person.***

Equipment and tech: There are now many more technology providers joining the cause with some not providing the correct solutions for a specific application. There are also some that are driving product with false information. This is due to technology designers that are uneducated and unaware of the characteristic traits of the threat and therefore highlight attention to specific unrewarding benefits or use wording that misinforms the buyers. The following ''technology testing group'' is highly recommended to *evaluate the product performance that complies with the health community or measuring temperature*, be it thermal imaging cameras and thermometers software and/or equipment for various purposes, namely IPVM (http://www.IPVM.com)

Do view the FDA for protocols related to non-contact electronic thermometers and thermal imaging cameras. US FDA(https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/non-contact-infrared-thermometers) Thermal imaging for mass-screening people can be viewed on https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/thermal-imaging-systems-infrared-thermographic-systems-thermal-imaging-cameras. There is ongoing research into mass screening thermal imaging testing because of a high number of false negatives or false positives. It is advised to keep in-touch with such testing via FDA and IPVM.

The instruments are only as good as the users: Ensure that authentic goods are purchased and the users on the ground know exactly how to use such and follow the protocol instructions. Furthermore, and very importantly, ***where to place and the installation of technology*** because the background light or the temperature from outside could linger in the doorway. Also consider, the distancing of objects or person from the equipment must be for accurate readings.

There is some equipment that cannot read a person's forehead through someone's hair or when wearing a hat. There is advanced equipment that reads the temperature near the inner eye and not the forehead which is more accurate. ***The point is, that the user must be educated on the equipment that is selected and therefore requires proper training***. There is good examples and knowledge on IPVM (e.g., in nursing home).

Explaining the formula [Octopus]

To explain the formula, do consider another animal being added to the formal, namely, *the octopus.* This is a highly intelligent creature that makes complex cognitive decisions. All tentacles (legs/ arms) working together coordinated with each reporting to the brain that strategically directs each entity (tentacle) towards the desired outcomes. In this case, the tools being equipment, technology and manpower on the ground will be working in concert. Bringing together all of these aspects will provide a big picture (landscape view) to the practitioners. The vulnerability landscape can change at a moment's notice which speaks to the

importance of data from the ground must be updated and interpreted with urgency.

The formula

"The success in limiting the collateral damage of a pandemic would depend on the level of situational awareness of the decision-maker *and their reaction speed." Reaction speed is vital.*

- Situational Awareness

Different security practitioners relate to the term situational awareness. For this situation, it is a question of knowing something and identifying the threat. If one does not know that it exists, then one will not be able to become aware of it, unless they were told that, it is what they do not know - is what they need to discover. Therefore, critical thinking situational awareness is understanding what you do not know with the knowledge that you do know. Therefore, all practitioners would use distinct information being relative. For example, the officers on the ground would be looking for signs of sickness or the manager would use it to consider the layered security positioning of officers on the ground.

The equipment integrated with AI analytics (artificial intelligence) software connected to the equipment could link for incident management assessment which would serve for analysis to heighten situational awareness.

- Decision-makers

The decision-makers are all people on the ground. When you see it – react, either by consulting with the senior or if they are not around, then do what you think is appropriate, and do it immediately.

Reaction Speed: This is vital. Elaborated above, in another situation, it would be to follow the chain of command for distinct reason. In this situation, reaction speed is everything. The virus has no conscience, does not make decisions – simply acts and infects. Making mistakes is not important – simply do what must be done – REACT NOW!

Actions

In order for societies to survive this pandemic, all must realize the simple formula that security success to limit the collateral damage will depend on the level of situational awareness of the people on the ground (all are decision-makers) and their reaction speed. *The key to such is specific knowledge (new era skills), situational awareness and reaction speed!*

In addition, society as a whole must obtain substantial and reliable data from the people on the ground to prioritize the necessary actions that must be taken. *Lack of information and unreliable delivery of* relevant information from the people on

the ground will cripple strategy, and waste precious time. *Every second that ticks over another life could be taken.*

Situation – The people
COVID-19 Emotion Management

X-Factors in the situation: Thoughts motivate people

The practitioners are now dealing with mass hysteria of people that are scared, angry, insecure, desperate, and reacting quite differently from their norm. There would also be more mentally unwell people that could perceive actions differently to others and react accordingly. One must also consider that the number of suicides, for various reasons, will increase.

Keeping in mind that there are already people that are *unknowingly* infected.

The focus in this case is working with something that is known - *the knowing person that should be in self-quarantine. There are many more reasons why people would break quarantine curfew,* namely:

The infected person may desperately need something for themselves and/or their family and break quarantine. A simple solution could solve this problem.

There are infected people that may *have* cabin-fever and just needs to get out because they feel claustrophobic. Perhaps there are some have their personal desires overcome their caring for themselves or others and they need to *indulge their pleasures.* Yes, there are people that are unable to control their desires besides the ones with compulsive obsessive behaviour disorder. It may even simply be jealously as the motivation that could cause *someone to break quarantine.*

There also could be infected people that are mentally unwell and/or in emotional turmoil. Some people may even believe that they are going to die and need to find closure by settling issues with others.

To ensure that people are in quarantine and must stay in quarantine for good reason, the authorities may lay down a law that people will be arrested and charged for attempted murder. That threat is going to add fuel to the fire because they would need single cells to hold masses of people. This action would multiply the number of infections exponentially.

Step 1 (Who and what to educate)

It begins with the security practitioners that have had training in situational awareness, and they must just be upskilled quickly relying upon, and in addition to, their previous training. Many have been trained on physical intervention, but

by adding further knowledge which will take from an hour to a few of training depending on their experience and character traits.

There are those who have had some form of leadership or conflict management training and their upskilling would be quicker than those skilled only with physical intervention training.

This dictates that skills must be relevant to the threat in theatre. One must adapt to this moment in time where the vulnerability landscape has changed. Even if people believe that they are sufficiently skilled and do not believe that they require upskilling, then their ego would inhibit their performance. The 'all-knowing person' realizes that the knowledge from the past may be insufficient and not be relevant for this type of pandemic threat.

Gathering information from more than one source could strengthen the foundation. This is where we use AI (Artificial Intelligence), which would include the equipment and technology in concert with the new era skills of the practitioners on the ground. Let us take this further, where people that have information could be the heads of departments or HR who obtain information from people that may report in sick. This includes the temperature detection equipment which identifies a person that has an elevated temperature. *All of this data must be gathered quickly and reported using a simple method of reporting into a common database.*

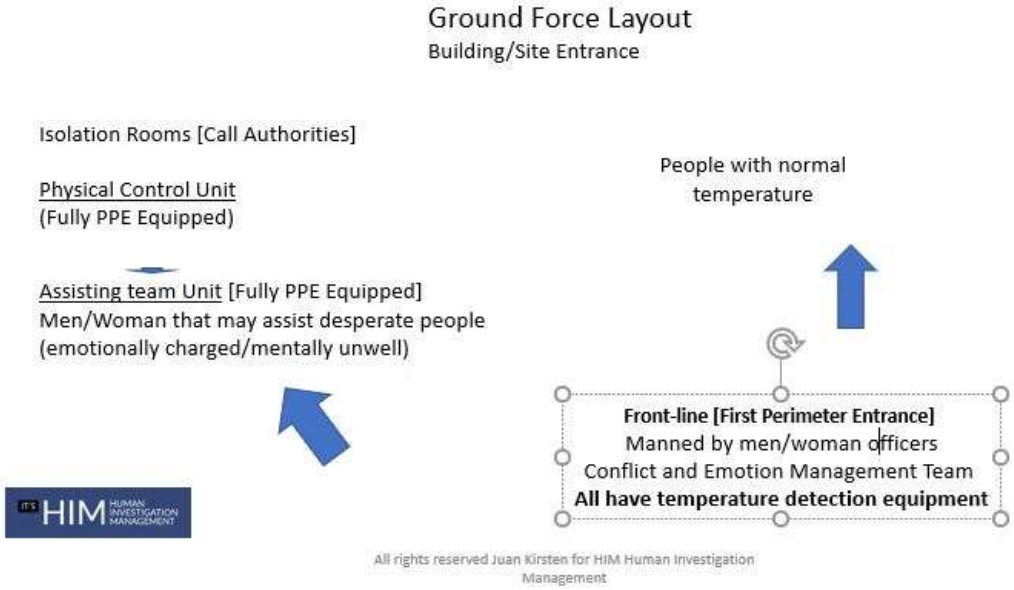
Character of the person

This pandemic could drive people to react and do desperate things that may be out of their norm. The practitioner on the ground must be a people-person, who has a balance between empathy and the ego drive. It will not help matters if the practitioner is just driven and focused on using physical force as it will cause further chaos.

Furthermore, they cannot be biased in any sense of the word because their thoughts will be displayed in their verbal and non-verbal body language which causes others to instinctively react with mistrust and disrespect.

'We must layer the security team by character traits and skills'

The practitioner must calm people down and bring them to their senses in order to encourage co-operation. One cannot afford to confront aggressive behaviour and must manage such accordingly. This could easily be trained using 1-hour virtual recordable meeting as each scenario could demand specific highlighted points. Note – using the term recordable means that the user must watch the clip multiple times in order to embed the knowledge, which allows them to react instinctively.



Step 2 [What to look for]

Initially, by using temperature detection technology and the situationally aware people on the ground, "people of concern" could be identified quickly. If the "person of concern" refuses to voluntarily take themselves out of the equation to self-quarantine, then summon authorities immediately.

This must be done by professionally trained personnel that are fully clad in relative protection gear, for example – if it is an air-borne virus then eye protection ware is just as important as masking up when managing aggressive behaviour.

For MPOX, Practitioners must wear gloves because the poxed skin is carrying viral liquid that is highly infectious.

Crime related to COVID-19

Criminals wearing masks may not be easily identified or not at all by CCTV. Also, the wearing of masks gives criminals a confidence boost because they feel they could get away with the crime. Subsequently, one may not rely on facial recognition software. [Research on the manufacturers is discussed in the work.]

The primary need of humans, and especially the poor and hungry, is food and water. Therefore, any outlet could be raided, even stockists of alcohol.

Protection consideration for security of food**,** medicines, protection gear and equipment from Pharmacies, Hospitals, Old Aged Homes, Rehabilitation Centres or from Hotels [that could be repurposed into ICU (Intensive Care) or Quarantine centres]. Consequently, the protocols for the protection of such must be considered besides methods to mitigate shoplifting.

The Warehousing and Logistics of food, medicines, oxygen, protection gear and equipment could be targeted by criminals and call for distinct security services.

Furthermore, this work takes into consideration the Financial Crime and Fraud which is committed to raise funds to sustain people as well as the protection suggestions of pawn shops, which purchase goods for cash.

This list of crimes related to COVID-19 when reported or discovered will be uploaded onto ISIO or HIM. This could be new crimes as it is uncovered or evolved copycat crime discovered.

Step 3 [What to do with the information retrieved]

The data collected could then be access by the practitioner on the ground so that they are able to address and manage access to their region of responsibility. *Furthermore, they are also providing information* when they identify a "person of concern" that may be refused entry or when the person is re-routed to another entrance. For example, at a hospital where there could be dedicated and distinct entry points.

The pharmacist in a mall would attract compromised people. These people could have already tested positive and/or exhibit state high temperatures, where hopefully they have already been flagged and dealt with accordingly at the entrance to the mall. Keeping in mind, one must accept the fact that desperate people will do desperate things and may use the backdoor to get into the mall. This calls for the pharmacist to have security practitioners at their own entrances. This is an example of *layered security* that may be required for other businesses on the ground.

Once a "person of concern" is identified because of technology or critical situational interviewing (as the person was lying or hiding information) in addition to refusing to co-operate, then the authorities must be summoned. This must be done immediately because people that are "weaponized" could infect others with this highly contagious virus.

Implications

The situation could eventually lead to going to the mall, catching a bus, train, ship or even a taxi shortly will involve some form of equipment or technology for human health assessment. At all access control points there will be some form of temperature detection, be it by hand swiping over a temperature reader panel or

CCTV temperature detection, in conjunction with the handheld device. These could be linked to mass data incident management systems.

Step 4 [Repeating the cycle with more new knowledge]

Actions

- Ensure that all forms of reporting are loaded into the incident management system. Do not discriminate because something that may seem irrelevant now could become prevalent at another stage.
- This manager/analyst must be able to follow the dots to comprehend the big picture and the formation of any structures taking shape, which in-turn could become a damning issue to contend with.
- Most importantly, the manager/analyst must keep their eyes fixed on all issues from around the world, paying attention to the timeline in relation to the incidents. These could occur in the location or field of interest of the manager/analyst and therefore, must be addressed when considering the methods to limit the collateral damage.
- Apply new or updated protocols as necessary to the new issue which is in theatre and/or amend an existing protocol to comply with the remedy.

Considerations

Again, reaction speed is vital: Reporting quickly is necessary

The speed of accurate reporting is key, therefore, if a practitioner is on the ground and they confront a "person of concern," regardless of whether or not they co-operate, then they will need to furnish details through any device. Their findings must be captured into the incident management system. *There are security incident management systems for small companies, not just for larger institutions. These could be cloud-based, meaning that it would be easy to acquire and derive remote on-line support.*

There are communities that more than likely do have systems in place, such as the critical infrastructure of multi-national companies, who are highly dependent on security products or services that would have incident management systems in place. These spaces may consider that they have what it takes, however, there may be additional added software or modules that must be considered. They may need to add a technology, there may be other quick training methods introduced or software editing to include specific knowledge or tags to be included.

The key point is that all equipment and technology must be updated and relevant to the threat in theatre

Recognition and Habitation of the habitual contaminator

The biggest problem with a pandemic is the human factor when a "person of concern" will not abide by the rules and regulations. The speed of locating and isolating a moving threat is vital to reduce the speed of viral transmission.

Technology for containment

As stated earlier, a temperature detection connected to some form of access control, besides facial recognition, that could also be connected to access control.

Cell-site tracking. Once the "person of concern" is registered, their mobile phone can be monitored. If quarantine is broken, the authorities, fully clad in protective gear, can either escort the person back to their location or send them to a more secure centre. Thus, ensuring that they are contained. Alternatively, on-site reporting can occur, when a "person of concern" is identified as having broken quarantine, using thermal imaging/fever detection technology

At a centre for quarantine containment, the "person of concern" could have a location monitoring device attached to their body. Furthermore, given that reaction speed is key, surveillance technology and access control which are functional and interconnected with an alert system will support a better result.

Regardless, simple incident management systems for small companies or large data centres is crucial. The managers on duty and/or analysts must be able to detect a pattern occurring in order to identify an evolving threat or the formation of a structure where the threat will become more difficult to contend with. They may also be able to uncover an existing loophole that needs to be plugged quickly. This knowledge can also be trained quickly depending on the person's familiarity with security investigation, which differs slightly from crime investigation. More information can be found through HIM [Human Investigation Management].

Reaction Speed

The nature of the beast.

A pandemic or endemic that knows no bounds and does not make decisions, nor does it discriminate. There is absolutely no room for procrastination – this demands immediate action!

Black Fungus (Mucormycosis) and protocols

In May 2021, the researcher detected that India black fungus infection levels jumped from +3000 to +7000 cases.

Black Fugus can be found in specific countries that has a climate conducive for it to grow and thrive.

Black fungus has a mortality rate of 50 percent with the balance of infections leading to either one eye, both eyes and the top jaw having to be removed to save the lives of patients.

Immediately, all security practitioners were notified worldwide to look for such in damp building and rooms and arrange for it to be appropriately removed.

Furthermore, the research went into the crime related to the threat and uncovered the fact that the fungus could be in *old industrial oxygen cylinders*, the tube as well as in the valves. Also, this fungus could be in assisted breathing machines and humidifiers, therefore if a security company is protecting a client that re-sells such equipment, then they should notify their clients of the implications or the authorities if they clients do not comply with the health protocols by ensuring the equipment is fit for purpose.

Subsequently, any corruption related to refuelling old cylinders, or re-selling and using *old industrial oxygen bottles besides* old assisted-breathing machines that could be contaminated with black fungus is of concern.

Consequently, in May 2021, CAPSI was notified to inform the Policing authorities to the facts and to consider that some entrepreneurs may be involved out of naivety, or gang and organized crime could be involved. In August, the cases rose to +42000 cases.

The Black Fungus experience dictates that it is imperative for security practitioners to fully investigate their location as well as keep their eyes on global incidents that occur. The implications of not paying attention as we well know with black fungus is the life impacting issues besides the elevated rate of deaths.

A remedy would be that the departments of health and safety should televise to the populations in all countries that the compliance standards for manufacturing, bottling, distribution, refilling and selling oxygen using oxygen cylinders must be adhered to for distinct reasons. Any contravention of such that leads to life impacting or deadly incidents should be held accountable accordingly.

Mpox

January 2022 Mpox made its debut and is similar to HIV/Aids by initially targeting the gay and bi-male community first. This could be because males are more promiscuous than females, but rest assured it will grow as it did with HIV/Aids through all sexes. It is also similar to HIV/Aids as the method of transmission is the same however it is MORE INFECTIOUS but NOT AS deadly as HIV/Aids.

The Mpox infected person oozes viral liquid though cuts, sores, lesions and blisters. When the skin falls off an infected person then that skin is still contagious therefore it is highly transmissible by touch to the extent that the person changing the bedding could contract the virus. Subsequently, when security practitioners that touch 'poxed' people then they could contract the virus by touch besides if the viral liquid enters the eyes or mouth. Consequently, the front-line staff that could experience aggressive or violent behaviour must GLOVE UP besides MASK UP.

The high-risk sites initially are where gay or bi-sexual males meetup which could be entertainment sites, saunas, gyms, etc.

Technology such as facial recognition with 'pox' identification could deny access. Also, the technology could inform the workforce to identify and assist a person of concern off a site besides informing that workforce to suit up for the job especially if an aggressive situation could or is taking place with the person of concern is involved.

Manpower: The layering of manpower is the same as covid19 by character traits and skill sets.

The Mpox quarantine is set for 21 days and the same high-risk protocols for such must be considered.

Other tailing threats: The economic meltdown resulting from covid and compounding on the costs to live because of the Russian Ukraine war will increase the threat levels.

Mpox may regionally impact the same because there are many that were not inoculated in their country and have migrated elsewhere or the new-born generation less than 3 years old being not yet inoculated because some countries did not initiate such during the covid period.

Keep in mind that covid is not yet over and my not be for years to come. It is not a question of what one knows but also who one gets to know. All security practitioners must know the fundamentals of biological threat security as we have all experienced the speed and damage. Security practitioners always plan for the worst and hopes for the best. It is the way – we do things in this field.

There is more that could be found on HIM that talks to practitioners that are using new-age technology for incident and emergency management software or technology besides the new crimes related to the threats.

General Protocols

- Keep your mind in theatre (situational awareness) because you could experience life impacting or deadly outcomes
- Keep calm regardless of the situation
- Look for black fungus that could be in damp places, e.g., on ceilings, walls or in the tubes, valves in old oxygen cylinders. This can be also found also at fertilizer plants or any site that uses water along with anything that decays. When it is found, summon the cleaners that must use chemicals to destroy the fungus. This black fungus can be deadly or life impacting if one loses their eye/s or top jaw.
- Do not accept any bribes or participate in corruption - Look for any type of crime and report immediately!
- Make sure you know how to take temperature and use the equipment properly just as good as a nurse or doctor.
- Switch off alarms or flashing lights off thermometer or thermal imaging camera that could cause panic
- Do not shout or get into a verbal argument with any other person
- When you are in the front line wear a facial shield and especially goggles if there is a high probability of handling aggressive behaviour. *With a poxed person definitely use gloves besides mask*.
- Physical restraint officers must comprehend that they need to lower their exposure rate by reducing face to face confrontation.
- Front line must work in teams (+2 or more)
- Larger groups must have security observers on the side lines.
- Identify high-risk stores. Do have an emergency entrance that could serve as a secondary dedicated entrance or people located near outlets what could services basic needs of man and may attract desperate or aggressive people for example, a chemist, a bottle store or a dispenser of oxygen or sellers of oxygen cylinders and assisted breathing machines.

Mpox Protocols

- ***People of concern*** regarding Mpox or any pox for that matter ***are pregnant woman***. Therefore, pregnant security officers or security officers that have pregnancy in their life space should not work on the frontlines in certain countries, cities and specific sites where Mpox has landed. There is good reason for such warning based on the research. Apparently in a study in the Democratic Republic of Congo in October 2017[1], one in four pregnancies are successful. *Two of the pregnancies miscarried and one born dead.*
- Get into a professional mindset for the job at hand as heightened situational awareness is required.
- *Officers that are pregnant or have pregnancy in their lives must not be on the frontlines at high-risk sites at the moment in certain countries or cities. Check your location's health ministry.*
- Mpox can be transmitted by the skin that could contain viral liquids such as pus or blood. ***Skin can fall or viral liquid*** *the bedding, on a person's clothing or on a chair subsequently all must be sanitized. People need to be gloved-up.*
- If a person that has Mpox coughs or sneezes the skin particles or viral liquids or droplets could go fly into ones' eyes or mouth. The eyes are just as porous as the mouth and therefore eye protection wear is just as important as masking up.
- When Mpox is identified then manage the person of concern calmly with gloves at all times
- All staff besides security that are working at sites which could be medical clinics, chemists, hotels, besides gay clubs, saunas, gyms and such like must be considered high-risk, and all staff must glove up. There must be backup support staff that could be summoned to manage aggressive or violent behaviour and kitted out with the appropriate PPE.

  There are distinct protocols for housing people that could contract Mpox such as staff that deliver room service as well as those that clean such apartments or rooms.

Focused biothreat threat detection by Security Managers

[1] Oct 2017 Maternal and Fetal outcomes among pregnant women Placide K Mbala, John W Huggins, Therese Riu-Rovira, Steve M Ahuka, Prime Mulembakani, Anne W Rimoin, James W Martin, Jean-Jacques T Muyembe https://academic.oup.com/jid/article/216/7/824/4348689

2023. In different counties there are different viruses that rear up from time to time. Marburg is a deadly virus that has no cure. Ebola apparently has vaccines that seem to be working to which take Ebola off the list of incurable diseases. There are cases of Black Fungus (Mucormycosis) in many countries that vary in life impacting outcomes or deadly incidents.

Subsequently, the security managers should investigate their location and keep watch for any change in infection besides keeping their eye on the world in case a global virus emerges which is possible as we all have experienced with Covid19.

Marburg Virus

A few days ago (March 23, 2023), we identified Marburg Virus with two deaths in Equatorial New Guinea (now 7 dead) and needed to determine if it would be localized. Unfortunately, it jumped to Ghana (2 dead) and Tanzania (5 dead).

Apparently, there are currently 20 cases with a mortality rate of over 80-90 percent. There is no cure yet despite that it is part of the Ebola Virus that has two vaccines that are apparently working. Subsequently, we trust that a vaccine could be discovered shortly.

The biggest nightmare is that the incubation period is 2 - 21 days. The implications of such mean that one could visit and exit those countries and infect many before it is discovered in other countries. Secondly, it is not easy to detect as the initial symptoms are similar to many non- life threating viruses.

Use the Security Biothreat Protocols for covid19 as well as for MPOX. Layer the workforce by skillsets, manage the flow and behaviour of people besides ensuring they sanitize. Wear gloves, eye protection and ensure that all clothing, bedding, beds or anything that was touched by the patient is burnt. Marburg virus is transmitted by bodily fluids.

The sites where patients are situated would be under the WHO and Ministries of Health so we trust that the security teams protecting such sites will be provided the necessary PP equipment and will be under strong supervision by the oversight and governance unit.

The point of inserting Marburg into this booklet is that biological threats could always emerge and impact the globe. These viruses do mutate and could unleash even greater collateral damage than covid19 did. Security Practitioners must always prepare in plan for the worst.

Acknowledgements

To Dr. Larry Barton (Prof) and Dr. Rommel Manwong (Prof), thank you for the continuous supply of encouragement and acknowledgement, besides the relevant, insightful pieces of work that inspires these works.

Dr Katerina Poustourli, your invaluable input brought this work to a fully stocked and completed piece of work because of your design thinking. Jean-Pierre Roux MPhil, thank you for your editing contribution for this work besides the sounding-board chats.

Presented by HIM | Human Investigation Management (HIM e-Connect Tools endorsed by many organizations.