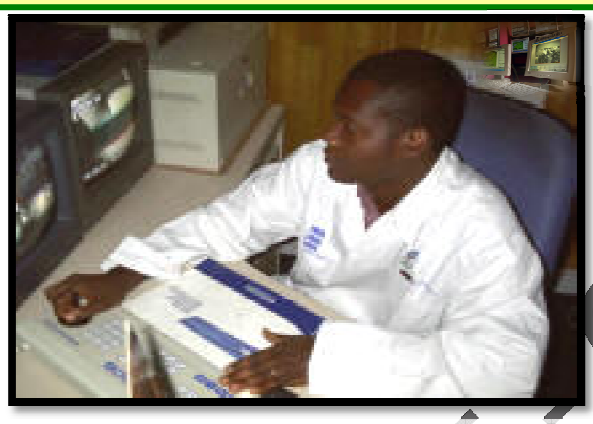
TransAfrica2000

[CCTV SECURITY PROJECT]

Network, Remote & Central Control Monitoring
Building Home Grown Digital Security Solutions in Convergence
AFRICAN HOMELAND SECURITY CONCEPT



Mission Statement

To demonstrate and prove the concept of integrated surveillance monitoring within your business environment, it is important that management fully understands the needs and benefits of centralised monitoring control. These controls are not only for crime related issues but also for general human management within. The Project will add on to the already almost completed infrastructure resource that will enable the management and designated personnel witness the real and true value of modern control methods.

Disciplines

With current digital technology plus the advent of the internet it is now possible to transmit and communicate speech, data and video to virtually every corner of the globe. It is possible to interface the entire gamut of modern security technology & communications into a national or international web. For the purposes of this exercise the disciplines will be limited to Closed Circuit Television Surveillance technology, Remote Ethernet Interface and Command Communications Infrastructure.

Background & History

For some, crime is a scourge that can be cut out of society as a surgeon would do with his scalpel. For others, it is an inevitable part of the sociological structure that needs to be addressed and coped with – because it is inherent within the make of man. It is not the purpose of this document to debate that issue.

It is the purpose of this document, however, to directly address the inevitable consequences of crime within a structured organisation run by human beings and the rule of law.

There is an endless catalogue of reasons for how and why crime occurs in any given demographic configuration and environ. There are two fundamental underlying causes and they are greed and necessity.
The types of crime, of course, are universal. The list of crimes including theft, fraud, robbery, corruption, negligence, smuggling, indifference, is a catalogue that has remained unchanged since time immemorial.

Where Next?

The introduction of modern technology and State of the Art communications will send out a very powerful message not only to the criminal fraternity within its organisation but to those criminal elements in the society.

Creative and lateral thinking based on sound intelligence and statistics is the only way forward to counter the modern criminal and the ever increasingly sophisticated methods they employ. It is a battle of wits. Complacency is a device of the devil and the bell tolls for those who fall into the trap!

That message will be, "Do not mess with us – or else".
You WILL be detected.
You WILL be tracked and monitored.
You WILL be arrested.
You WILL be prosecuted
You WILL go to prison

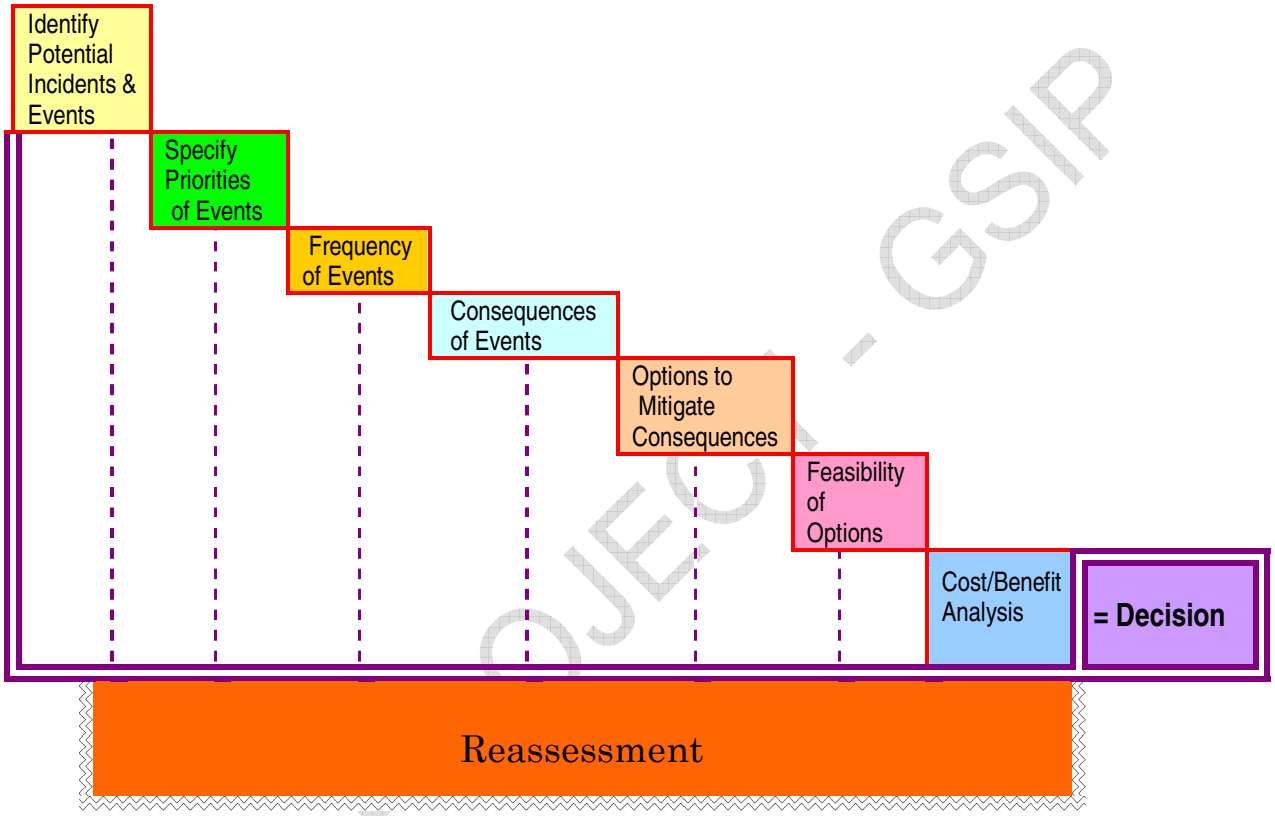
Good policing in association with the latest methods, systems and technologies is the only way forward to fight and counter the rising levels of crime within business organisation. Methods and systems of CCTV detection are well proven to be massively successful in Europe & the USA. The United Kingdom in particular, which probably has one of the most sophisticated and efficient monitoring, control and communications networks in the world, is, without doubt, at the forefront of the application of technology in the fight against crime related issues.

Deployment

The priority – should it be Detection or Deterrence?
If your business has the ability to detect does it not therefore follow that inherent within the technology is the key deterrent factor?
Systems deployed within the UK have proven time and time again that the deterrent factor can have as much as a 70% reduction affect on the levels of crime and patterns of behaviour.

By creating a high profile technological presence those who would have been committing offences within the fields of surveillance will think twice before attempting to commit any act in areas that are monitored. The efficiency of the detection and monitoring systems, as a result, become massively effective in being able to concentrate on more manageable levels of crime and anti-corporate behaviour. It becomes a “targeted” operation not a random one.

[Assessment Critical Path]



Method

Undertake a complete and detailed risk analysis of the geographic areas under consideration.

- ◄ Establish & identify real needs within geographic areas – Levels and types of Crime – traffic patterns, flows and densities – usage of areas Industrial, commercial, accounts, cash office, storage, spare parts) etc
- ◄ Establish types of human movements and vehicles.
- ◄ Establish relationship to Police Stations, Emergency Services.
- ◄ Determine suitability for correct location of Cameras & Poles.
- ◄ Determine availability of power supplies and ups.
- ◄ Establish suitability of proposed command Control Centre.
- ◄ Train and fully educate personnel not only in the mechanics of operating the systems but also in all the relevant techniques of Identification of Suspects, Body Language, Behavioural Patterns, Risk and Threat Potential, Human Flow Management, Command Centre and Communication Protocols, Correct use of Radio Behaviour, Information Management Techniques.

Information Sources for Determining Loss Risk Events & Incidents

1. Organisation internal documents (e.g., Security incident reports of local companies or other government bodies & institutions
2. Prior complaints from the public or commercial companies.
3. Prior civil claims for consequences of inadequate security
4. Intelligence from local, state or national law enforcement agencies about potential threats & history
5. Industry related trends about trends
6. General economic conditions in the area
7. Presence of a “crime magnet” (e.g., popular night clubs, restaurants, banks, high value retail units, ATM’s, regular cash collection services, presence of armoured security vehicles, presence of vagrants, property in disrepair.

[Solution]
Closed Circuit Television Technology

Modern policing is not just about efficient methods and management techniques but is also about adopting creative measures to counter the rising levels of crime. It is imperative that management adopt creative and innovative solutions and learn to think laterally to produce those creative solutions. Staid and traditional methods must only be retained where they have a direct relevance to new wave thinking.
Deploy the most advanced and sophisticated technology that can be afforded. Quality is the key, not quantity. Better to have a few of the best rather than many of the average.

The implementation of a critically honest risk assessment is therefore absolutely imperative at the outset to determine the most effective plan for the location and type of infrastructure.

The decision in respect of what types of cameras to deploy and where, can only be taken once the Risk Assessment is completed. Fixed, Domes, traditional Pan & Tilt types (the much favoured solution) and Number Plate Recognition – all have their place but only in relation to the Priority of Events.

THE SPECIFICATION

What are the key considerations?
What are the specific risks currently identified?
What risks *have not been* identified or highlighted?
Where are the risks?
What personnel are dominant within the risk area and why?

Is the risk security or health and safety?
How are the risks currently being managed?
Will monitoring or securing of the risk relocate the problem somewhere else or even create a new one?
Does the defined risk have a financial or logistical base?
What are the wider implications of not addressing any given risk?
Given the risk is correctly identified and a solution adopted what contingencies need to be applied in the event of component failure (however caused)?
Is there a wider requirement to exchange data, information or video signals in respect of the security systems with other government agencies?
What key benefits will be derived by the operator in the resolution of the defined risks?

OBJECTIVES - Revisited

1] **Maximise** deterrence against All Criminal Activity (The right equipment).

2] **Maximise** information for dissemination to all departments and individuals -on a strictly need to know basis. (Mutual understanding).

3] **Maximise** Proof of Evidence for prosecution. (Capture of criminals).

4] **Maximise** safety and welfare of all including members of the public.

5] **Maximise** comfort, well being and information systems for the benefit of Customers & VIP's.

6] Maximize lines of communication. (Two Way Radios)

7] **Maximize** efficiency of management and supervisory structures for incident response, monitoring procedures and operational control (More effective time management that will lead to greater individual and group motivation & identity).

8] **Maximise** knowledge, awareness and potential of all airport staff and employees. (Knowledge = Confidence + Individual Responsibility will lead to a more easily managed workforce more ready and able to identify with their work place =Greater Loyalty which in turn will lead to a more efficient and self motivated workforce).

9] **Minimise** opportunities for collusion and disaffection. (Cohesiveness of systems coupled to a greater sense of identity and loyalty, hopefully will lead to greater cooperation).

10] Minimize opportunities for fatal human error.
(Integration of all electronic monitoring and surveillance systems).

THE EQUIPMENT

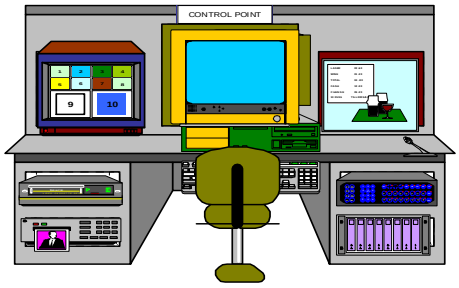
CCTV

What are cameras required to monitor and why?
Distance to target?
Is target stationary or moving? If moving how fast relative to target distance?
How much detail and definition is required of target?
Are devices to be monochrome or colour?
If monochrome devices are specified detail of risk must be re-defined through lack of definition and detail within target field.
Is cover to be Daylight only or 24 hour coverage?
If 24 hour coverage what artificial lighting support is available?
Will additional lighting be required or will the option of Infra Red Projectors be needed?
How will heat and light affect performance of devices?
Note: If locations are southern facing housings will require extended sunlight screening and will also need cooling fans.

CONTROLS

Analogue or Digital?
Will recordings be required for evidential purposes in a Court of Law?
Will other departments or agencies require access to recordings or have these recordings transmitted by telephone line, microwave or some other medium?
How many monitoring points will be required?
Will monitoring points be required to act as a contingency stand by in the event of failure of central control (by any means) or exchange information between each other?

Will the central control room (or any of the satellite centres) have any physical line of sight of the complex?
Who will operate the system?
How will operators be trained and by whom?
How much expansion capability will need to be built into the system?
Will camera heads need facility for pre set automatic control patterns?
What level of security is anticipated to limit access of unauthorised personnel to the control room?
Note: It is essential that only strictly authorised personnel have access to control centers.



TRAINING & AWARENESS

Given the systems are correctly specified, properly installed and working – then what?

There is the matter of achieving the proper levels of operational competence, awareness and professionalism. The team responsible for the technical overview and selection MUST also consider the wider implications of the management of the systems. There must be an operational and management structure within which they are required to perform and by which their performance is measured.

Performance is about people! ! ! Everyone, but everyone from the cleaner right through the entire management structure MUST be working within a clearly defined strategy; a strategy within which every individual must be held personally accountable.

There must be a clearly defined mission statement in respect of the purpose of the electronics systems. Systems are not about electronic gadgets – they are about the effectiveness of the levels of professionalism and awareness of the people who operate them and those who are ultimately responsible for their on-line effectiveness.

Comment: The package of security measures must include for the training and education of ALL personnel in respect of expectations of their contribution within the overall performance strategy.

In a modern world where so much is expected, in so little time, how do you cope with the key question of how to effectively protect your company's assets, its property, its people and its stock?

Murphy's 1st Law of Integration: Whenever you set out to do something – something else must be done first.