THE SECURITY INSTITUTE

INTRODUCTION TO SECURITY MANAGEMENT

(Mandatory Module)

A study guide and source of reference for Security Managers on the SyI Certificate in Security Management

September 2013

This publication, 'Introduction to Security Management', is designed primarily to provide students with the necessary study material in preparation for one of the mandatory modules forming part of the Security Institute's assessment in Security Management at Certificate level and on which detail it is based.

Students and security practitioners are recommended to read additional publications, including statutes, as appropriate on these subjects to achieve greater understanding. However, it must be clearly understood that all assessment questions for the module will be based on the contents of this particular publication unless otherwise directed.

The content of this publication, together with the other module publications – shown below – are considered to be an indispensable source of reference and practical guidance to any professionally motivated security manager.

The full range of publications in this series and relative to the modules of the same name that comprise the SyI Certificate in Security Management are shown below. The Guides are available either separately, or as part of a comprehensive Security Management Compendium. The actual award of the Certificate requires students to undertake study and pass assessment in the three mandatory modules as well as three elective modules.

Introduction to Security Management	*(Mandatory)*
Security Department Management	*(Mandatory)*
Information Security	*(Mandatory)*
Health and Safety	*(Elective)*
Retail Security	*(Elective)*
Terrorism Awareness and Management	*(Elective)*
Risk, Crisis, and Disaster Management	*(Elective)*
Strategic Security	*(Elective)*
Physical Security	*(Elective)*

Quotations from statutes are reproduced with the permission of the Controller of Her Majesty's Stationery Office

First published: September 2013

CONTENTS

1 Introduction to Security and Risk Management

In a hundred years' time, when the history of the 21st century comes to be written, the first decade of the century may well be called 'The Age of Security'. Although security has been a fundamental consideration since the beginning of human history, security has come to play an increasingly central role in all aspects of our lives in the recent past. This has affected, amongst other things, the way we live, how we travel, how we communicate and the way we move money around.

The role of the modern security manager has also had to adapt to the emergence of new threats and challenges. The traditional role of the security manager was often seen as being limited to ensuring that windows and doors were locked, and preventing goods from being stolen. However, the modern security manager faces a wider range of tasks and challenges. It is not uncommon for security managers to be called upon to deal with situations involving terrorism, cyber-security, crisis management and the personal protection of senior executives, as well as more traditional tasks around physical security (fences, lighting, locks, CCTV, access control systems, alarm monitoring and control room design).

1. As well as that, the modern security manager also faces the need to operate in a tight financial environment. Unfortunately, security is often seen as a 'non-productive cost', and security managers need to fight their corner at Board room level to ensure that their assets, personnel and budget are fit for purpose.

2. However, whilst the security manager faces increasing challenges due to the changing nature of the world, there are also increased opportunities. It was not so long ago that the corporate security manager (who in those days would invariably be a man) would be a retired police officer who found work through the "Old Boys" network, and who mainly saw the work he was doing as an extension of their police activities. The modern security manager, however, is expected to be able to demonstrate the same level of professional development and technical excellence as any other senior expert in the company.

3. The purpose of this programme is to ensure that, wherever you are in your security career, you will develop a full understanding of all of the major issues in modern security management. Whatever your present level of operation or future aspirations may be, this programme is designed to give you the basic framework that will allow you to understand how the various components of modern security management fit together. All of the Modules can be approached as stand-alone subjects, but just as in security itself, you will find that many of them use the same basic concepts of security management, and there may be areas where the language and concepts overlap.

2 Security, Freedom, Threat: The Three Basic Concepts of Security Management

The Great Wall of China and Castle Moats show that security is something that has always been at the forefront of human social management (see Figure 1 below).

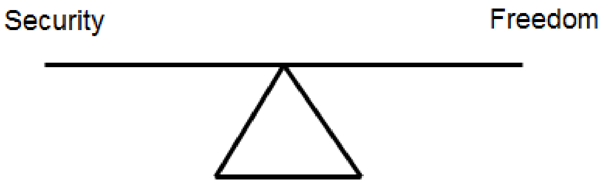
Figure 1: Classical Security Systems

If we want to find an all-encompassing definition of security, one that would be valid under any circumstances, it would be something along the lines of: *'The purpose of security is to create a safe environment where routine activities can be carried out in as normal a way as possible, in accordance with the perceived level of threat'*.
By using this definition, we are introducing the three basic concepts that are the foundation of all security management programmes, namely:

- Security
- Freedom of Action
- Threat

These concepts apply whether you are locking your bicycle to a railing, putting defensive fencing around a nuclear power station, protecting a VIP or using an access control system into a multi-usage commercial building. The first two concepts, Security and Freedom, are inseparably linked. If you want more security, you will pay for that in freedom (see figure 2). If you decide you need to have more freedom (for example to move in and out of a building without showing a pass, to use a private laptop in the workplace, or to allow cars to park near your building), then that will inevitably mean that you will have a lower level of security than if those things had not been allowed.

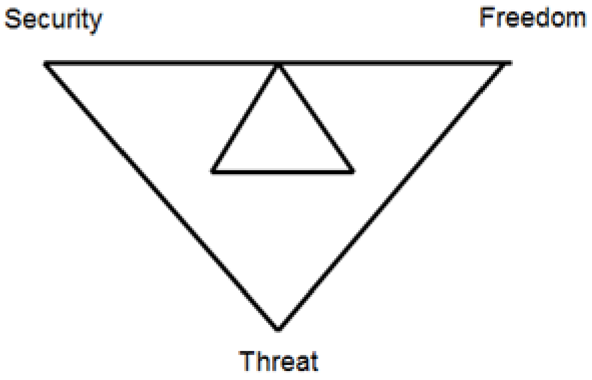
Figure 2: Linkage between 'Security' and 'Freedom'



Security and **Freedom** are inversely linked. The greater the security, the less freedom, and conversely, the more freedom, the less security.

Therefore, the question that all security managers need to address is 'How much security do I need?' In order to answer this seemingly simple question, we have to ask another question in return: 'What is the threat?' Unless we have an understanding of what is the level of threat, we have no way of assessing what level of security would be considered appropriate (see figure 3).

Figure 3: The Security Management Triangle: Security, Freedom and Threat



The appropriate balance between ***Security*** and ***Freedom*** can only happen once we have assessed the level of ***Threat.***

Airport security checks are an excellent example of this principle. The perceived high risk of attacks against airlines has led to governments across the world increasing the levels of security at airports. However, this has had direct impact on our freedom, for example we cannot take liquids and other material onto planes, and / or we have to undergo what might be considered as intrusive security checks, including removing belts and shoes and, more controversially, undergoing full-body x-rays.

Given the potential impact of a successful terrorist attack, it is not surprising that there have been fierce debates concerning the correct balance between security and personal freedom. Arguments made in 2006, following the attempt to use 'chemical bombs' on ten airliners travelling from UK to United States and Canada saw politicians, who wanted to introduce laws such as identity cards and extended periods of detention with arrest for suspected terrorists, clash with judges, who felt that these new rules were outside the normal British legal system, and disproportionate to the actual level of threat. UK Home Secretary John Reid made a speech that stated that Britain was 'now facing the most sustained period of sustained threat since the end of the second world war' (2006). Reid went on to state that critics of the government anti-terror legislation were putting national security at risk. The Court of Appeal disagreed with this, and stated that there was no justification for the declaration of a state of public emergency, and that therefore 'Terrorist violence, serious as it is, does not threaten our institutions of government or our existence as a civil community'. In the same judgement, Lord Hoffman, made his famous announcement that 'The real threat to the life of the nation . . . comes not from terrorism but from laws such as these' (2004).

As a security manager, one of your fundamental roles will be to assess the actual level of threat, and strike the appropriate balance between the freedom required by your organisation and personnel to carry out their normal duties, whilst monitoring or controlling those activities in order to ensure the right level of security cover is provided.

3 Risk Management Strategies

Although the overriding objective of Security Management could be encapsulated in the slogan 'Reduce Risk, Increase Safety', deciding which is the most appropriate approach is dependent on a wide range of factors, including the operating environment, organisational risk culture, resources, management support , potential loss and other (competing) strategic objectives. For example, it may be part of the company's strategic objectives to develop operations in new markets in Eastern Europe or Africa. There would obviously be a risk associated with these moves that would not be applicable in working in a UK or a developed western European market such as Zurich or Hamburg. However, it may be that these additional risks may be considered as acceptable by the company's management within the context of the business development project, and it would be the responsibility of the security manager to develop an appropriate strategy to manage those risks in line with the company's wider strategic objectives.

Given that it is impossible to completely eliminate risk altogether, there comes a time when there must be an acceptance of a certain level of risk – or at least, uncertainty. In order to keep risk management relevant to situations in the real world, there is a recognised concept of 'As Low As Reasonably Practicable' (ALARP). This means that whilst we have a responsibility to both identify and manage risk, we cannot be expected to try and eliminate every single conceivable risk, however low its possibility might be.

There are a number of ways that potential risk management strategies can be categorised, though most models generally consist of between four and six different approaches. Here are five of the most widely accepted options. As you work through the study course, you will recognise these as coming up time and again within different security management contexts.

Avoid This is done by acknowledging the risk, and changing your own activities in order to avoid the possibility of an incident occurring. Examples might include not moving into new markets in the example above, banning the use of personal computers in order to minimise the possibility of an electronic virus contaminating the company computer system, or keeping visitors to a production facility restricted to certain areas, in order to avoid industrial espionage or potential accidents.

Reduce This is done by introducing protocols to minimise the possibility of an unwanted event happening, and to minimise the impact of any unwanted event that does happen. For example, if a company had lone workers who were visiting outside sites, and had identified that as a potential risk, requiring them to log their movements ahead of time with the HR or security department, and then calling in both before and after the visit would limit the potential harm if something did happen (by allowing the HR or security team to become aware of the situation at the earliest possible moment). Similarly, introducing a 'Meet & Greet' process at the front gate reduces the risk of potentially unwanted visitors gaining access to a building.

Share Many of the risk management strategies that have been accepted within the wider security management framework originally started in Supply Chain Management. It is a feature of SCM that each player is dependent on the link before them in the chain, so that the final 'customer' who is waiting delivery of the vital piece of stock is relatively powerless to control that process. The concept of sharing the risk is actually more concerned with sharing potential loss. Under this system, each person would face financial penalties if they did not deliver according to agreed terms. Within a wider security management context, sharing risk can be seen as a way of minimising potential liabilities.

Transfer An example of risk transfer that would be familiar to most people is insurance, where the payment of a relatively small fee transfers the risk of the cost of a potential incident to the third party, in this case the insurance company. By transferring risk, you are in effect outsourcing the responsibility for the management of the risk, and any possible consequences. The retention of a specialist crisis management agency to handle crisis situations overseas is an example of sharing the potential liability for emergency evacuations, in a situation where it would be irresponsible to ignore the potential risk, but unfeasible to manage it in-house. Another example would be the decision as to whether to use a car-leasing company for the company fleet, or to own the cars outright. By using a fleet-hire system, the management of the risks – breakdowns, accidents, servicing, etc - is transferred to the leasing company. One advantage of this system is that there is a clearly defined cost to this particular option – the fee you pay to the agency for the service that they provide.

Retain There are two reasons for retaining risk. One is because the potential likelihood or potential impact is so low as be deemed acceptable – the 'We will deal with it if it happens' approach. This is actually a very effective means of dealing with low-level risks, as long as the potential consequences of such risks are well understood, and there are clear protocols in place for dealing with them. For example, if in the example above the company decides to own their own cars rather than lease them, then the risks associated with that decision would be accepted as part of the greater risk management process, but there would also be clearly defined protocols in place for when those situations did occur.

The other reason for retaining risk is if there is no feasible way of managing it though any of the other strategies listed. For example, the risk of an executive being kidnapped is one that would need to be managed if they were working in Somalia or Sudan, where such risks are a realistic part of operating in that region, but would not necessarily be part of the risk management strategy in New York or Zurich. It may be decided that the low likelihood of such an incident occurring there outweighs the prohibitive cost of insuring against such a situation.

3.1 Summary

Modern security management has grown beyond traditional concepts of merely protecting property, services and personnel. The range of present-day risks is creating challenges that require a fully integrated and professional approach to security management that is on par with every other aspect of an organisation's operation management. The modern security manager needs to have a strong understanding of the underlying principles that create the foundation for effective security management, and this programme will introduce those principles in a structured way over coming modules.

In summary:

- Security Management is always a balance between Freedom and Security
- Appropriate levels of security can only be discussed in terms of the *perceived Risk / Threat*
- There is no such thing as total elimination of Risk, the best we can aim for is *'As Low As Reasonably Practicable'*
- Major RM strategies include Avoid, Reduce, Share, Transfer, Retain

3.2 Self-assessment exercises

Self-assessment 1: Choose an organisation, and outline some of the main functions and responsibilities of the Security Manager within that particular risk environment

Self-assessment 2: Give an example of three situations where a change in the level of Risk Perception has caused a change in the level of security control (for example, being searched at a nightclub, having to show ID to get into an Embassy, having to wear a student ID card to get access to campus buildings).

Self-assessment 3: Take one of the examples, and discuss whether, given the perceived level of threat, you think that they have got an appropriate balance between security and freedom, and why you think they have made that decision.

Self-assessment 4: Give an example of each of the five security management strategies listed above, and show how the appropriate use of each can add to the overall security of an organisation or operation.

4 Risk Management

For any security manager, whatever their role and whatever the size of operation that they are responsible for, there are three fundamental issues that they will be dealing with, and it is likely that the vast majority of their daily work can be clearly classified as belonging in one of those three categories:

1. 'What are the problems that I need to deal with?'
2. 'What should I do about it?'
3. 'What do I do if something goes wrong?'

To put this into more technical terms, we are talking about **Risk Assessment**, **Risk Control** and finally **Contingency Planning**. This module introduces these three basic concepts, and shows how they act as the foundation for all security management operations.

4.1 Three-Stage Risk Management System

Stage 1: Risk Assessment

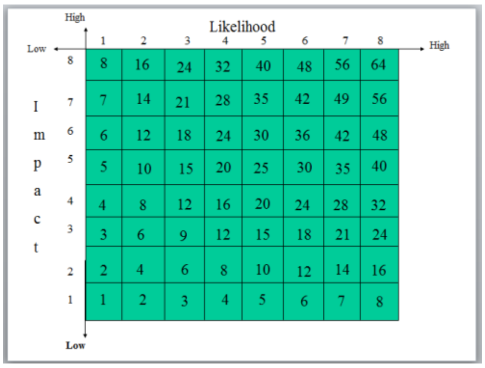
The purpose of the ***Risk Assessment*** is to take all of the thousands of possible or potential risks that might occur, and to give them some kind of comparative value. This will allow us to decide which of them is more serious, and which need to be actively managed. The truth is, that if we take any simple situation – walking from our home to the train station, or delivering a package from your warehouse to a client, for example - there are literally hundreds of possible scenarios that could be considered as risks, from the road being closed or the tube being disrupted, to a twisted ankle or being mugged, and even a major terrorist attack.

As an example, a risk assessment carried out in a factory might identify realistic possible threats such as workers stealing goods; an electrical breakdown that would stop the production line; a hole in the fence; a phoned-in bomb threat; suspicious activity outside the main gate; a major terrorist attack somewhere nearby, but which would lead to the police putting a cordon around our factory so that no-one could get in, or a breakdown in the access control system.

This is the first stage of a ***Risk Assessment***, in that we have ***Identified Potential Threats***. However, that is only the first part of the process, because we then need a way of putting them into some sort of order.

The accepted way of doing this is to create a ***Risk Matrix***, based on two measures: ***Likelihood*** (the likelihood of an event occurring) and ***Impact*** (the disruption that event would have on our operations if it did occur). Both of these measures can range from Low (unlikely, low impact) to High (very likely, high impact) See Figure 4 for two different versions of a risk matrix.

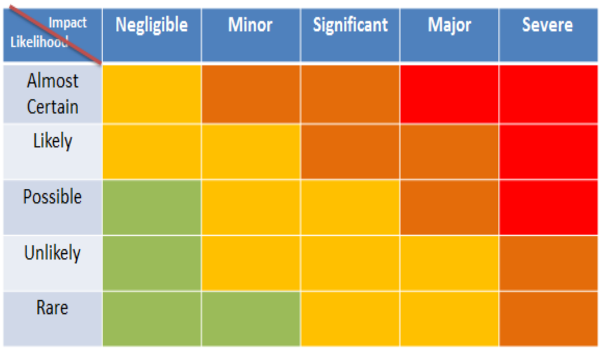
Figure 4: Two forms of a Risk Matrix. By using this system, we can give different threats different values based on diffeent combinations of ***Likelihood*** and ***Impact***.



Likelihood

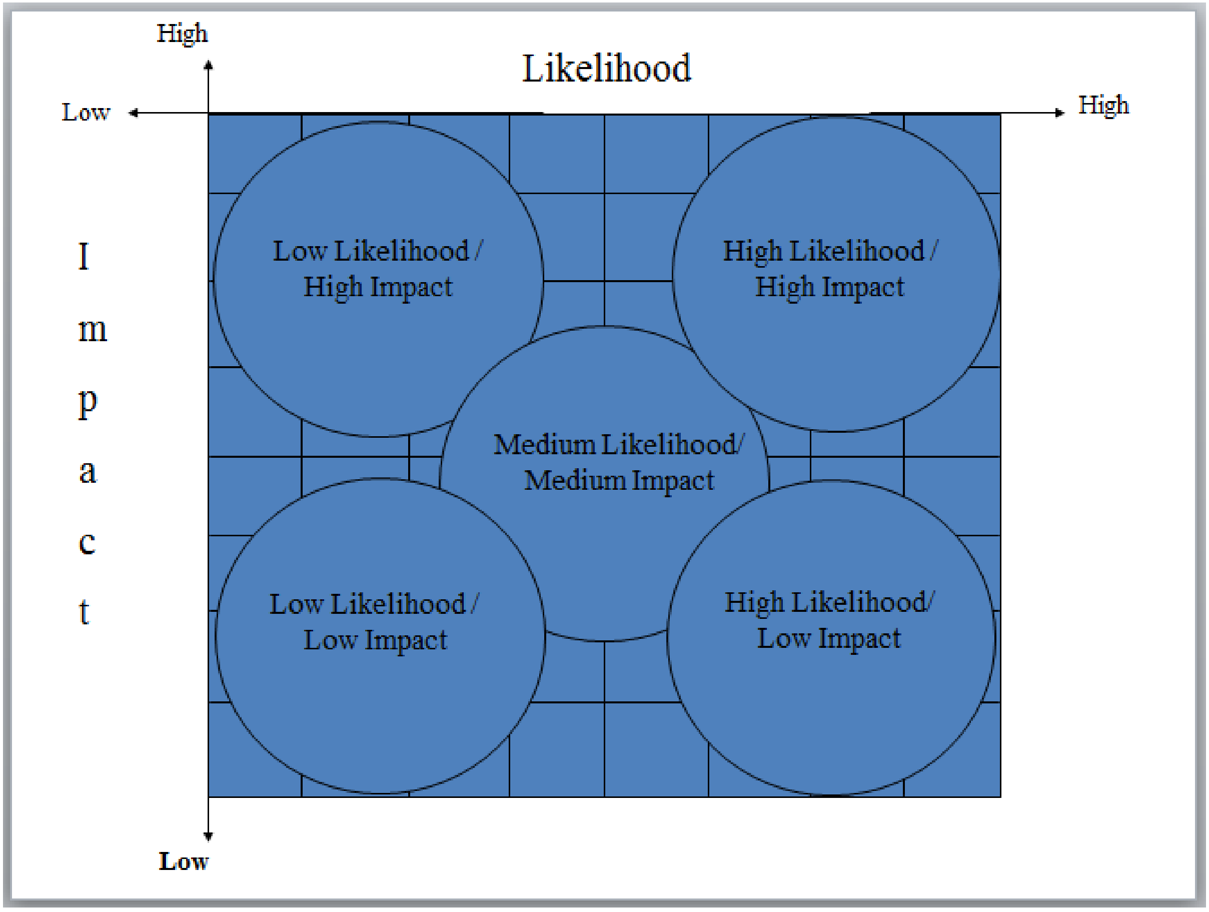
Impact	1	2	3	4	5	6	7	8
8	8	16	24	32	40	48	56	64
7	7	14	21	28	35	42	49	56
6	6	12	18	24	30	36	42	48
5	5	10	15	20	25	30	35	40
4	4	8	12	16	20	24	28	32
3	3	6	9	12	15	18	21	24
2	2	4	6	8	10	12	14	16
1	1	2	3	4	5	6	7	8

High
Low
High
Low



Impact Likelihood	Negligible	Minor	Significant	Major	Severe
Almost Certain	🟨	🟧	🟧	🟥	🟥
Likely	🟨	🟨	🟧	🟧	🟥
Possible	🟩	🟨	🟨	🟧	🟥
Unlikely	🟩	🟨	🟨	🟨	🟧
Rare	🟩	🟩	🟨	🟨	🟧

Figure 5:Risk Zones Within the Risk Matrix


High
Likelihood
Low
High
Impact
Low Likelihood / High Impact
High Likelihood / High Impact
Medium Likelihood/ Medium Impact
Low Likelihood / Low Impact
High Likelihood/ Low Impact
Low

The Risk Matrix (see figure 5) has been divided into five distinct Risk Zones, based on the Likelihood / Impact values. Each of these areas would identify a different class of problems, which would require different forms of solutions.

Figure 6: Characteristics of the Five Risk Zones

Risk	Effect	Example
Low Likelihood / Low Impact	This is not likely to happen, and even if it does, it will not affect us.	Bus strike in city
Low Likelihood / High Impact	It is not likely to happen, but if it does, it will have a major impact. This can be described as a 'Rare Event'	Major Terrorist Attack Earthquake
High Likelihood / Low Impact	It happens on a regular basis, but it should not affect our operation	Someone forgets their ID card
High Likelihood / High Impact	There is something wrong with our system that is creating the possibility of something potentially disastrous going wrong	Regular failures of the fire alarm systems
Medium Likelihood / Medium Impact	These are the problems that we are dealing with as part of our normal security mangement activities	Report of suspicious person on the premises

Each risk zone would identify a different class of problem, each of which would require a different approach in risk management

Stage 2: Risk Control

The purpose of Risk Control is to minimise the likelihood of any identified unwanted event occuring, and minimise the impact of any unwanted event that does occur.

Once we have identified the risks and given them a **Comparative Risk Value**, we can then identify those risks that can be most easily managed through our security systems. For example, if we have identified that the lack of access control means that unauthorised people are walking around our premises, the introduction of a Reception Desk and / or an entry-phone system could be one way of solving that problem.

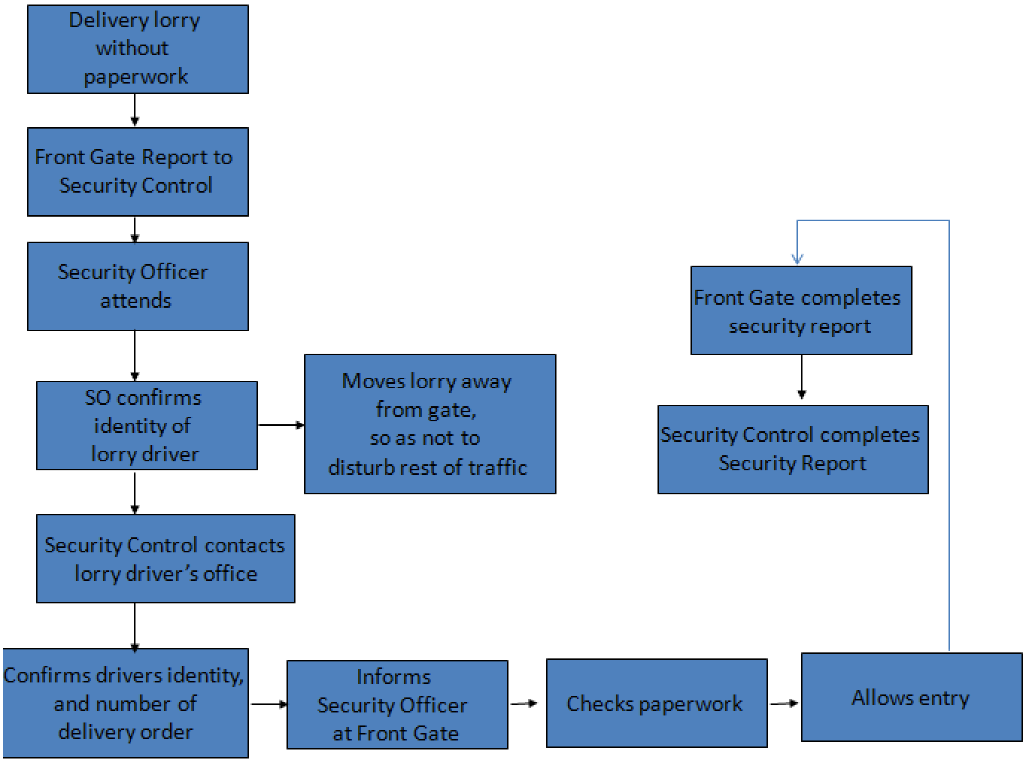
In order to ensure that the most effective **Risk Control** measures are put in place, each identified threat should lead to the introduction of a specific **Security Protocol** / **Procedure**.

For example, if you are working in a situation where the possibility of a parcel or letter bomb is considered greater than normal, this would be identified during the risk assessment process. As part of your risk control measures, you would then develop specific security protocols to maximise the likelihood of identifying a letter-bomb, and to minimise the effect if any letter bomb that might be sent. This might involve screening all incoming mail at a separate location away from the main offices. You might also have ensured that all mail-room and reception staff had undergone specific training to teach them how to identify suspicious packages and what to do if they were found. Reception staff would also need to undergo the training in case someone hand-delivered a suspicious package, either themselves or using one of the major logistical companies. If a suspicious package was found, you could then isolate the area whilst a specialist police team was called. As this was identified as a high-likelihood potential threat during your Risk Assessment , you should have developed good relationships with the police units, who would be aware of the threat and may well have taken part in joint-exercises with your staff to respond to a suspect package. All of these actions would be developed in response to the initial identification of a high-impact threat.

There have been a number of examples of letter bombs in the UK, and a company might be targeted because it is working in the pharmaceutical industry, or it may be associated with political or national issues that increase the likelihood of attack. In 2007, a single person sent seven letter bombs in the UK to companies associated with DNA testing and various traffic organisations. The Animal Liberation Front have also used letter bombs, as have Arabic organisations targeting both Jewish and Israeli targets, as well as Arab-language newspapers in the UK.

A security protocol is a set of guidelines outlining how a person should behave in the event that a specific incident was to occur. Figure 7 provides an example of a security protocol that could be used in the event that a delivery lorry arrived at the front gate, but without the appropriate paperwork.

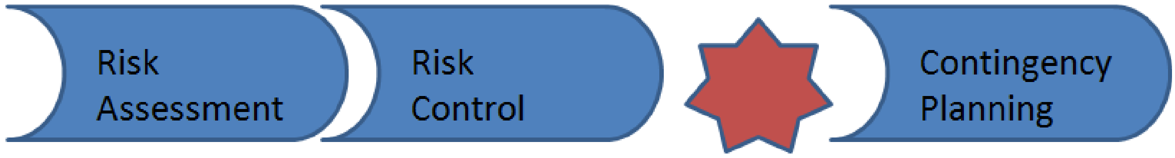
Figure 7: An Example of a Security Protocol


Delivery lorry without paperwork
Front Gate Report to Security Control
Security Officer attends
SO confirms identity of lorry driver
Moves lorry away from gate, so as not to disturb rest of traffic
Security Control contacts lorry driver's office
Confirms drivers identity, and number of delivery order
Informs Security Officer at Front Gate
Checks paperwork
Allows entry
Front Gate completes security report
Security Control completes Security Report

This is an example of a Security Protocol if a delivery lorry arrives without the necessary paperwork. The reason it is important to log this in the Incident Book is that this will help identify if there is a pattern of behaviour, and one particular company is regularly sending drivers without the paperwork.

The first two stages of any risk management programme, namely **Risk Assessment** and **Risk Control,** are designed to prevent an incident occuring. The third stage, **Contingency Planning**, prepares you to react and respond as effectively as possible when something does happen. In some American risk management models, the difference between the proactive Risk Assessment and Risk Control stages, and the reactive Contingency Planning stage is described as 'Left of Bang' and 'Right of Bang' (see figure 8).

Figure 8: Left of Bang / Right of Bang



This demonstrates how Risk Assessment and Risk Control are pro-active security management measures that are designed to be put in place to prevent an incident occuring. Once an incident has occured (the 'bang'), then Contingency Planning is used to try and regain control of the situation and to restore the situation to normal operational status.

Stage 3: Contingency Planning

The purpose of Contingency Planning is to allow the security team to regain control of the situation, and return to to normal operational status, as quickly and effectively as possible.

Once an incident has occurred, it is clear that it will have a negative impact on the normal running of the operation, whether it is someone forgetting the key to the front gate, disruption of your normal supply chain, or a water-pipe bursting in the office above, and flooding your whole control room. (Thii s last example is exactly what happened at the main police control room just before the 2012 London Olympics….).

Some of the issues involved in responding to a 'Right of Bang' situation will be covered in more detail in the Crisis Management module, but it is worthwhile noting that when something does go wrong, your response will almost certainly consist of a mixture of pre-planned options and responses that you create 'on the hoof'. As the nature of the problem becomes clearer, and you gather more information, the effectiveness of the pre-incident preparation will start to kick in. Effective crisis management is based on the ability to manage the transfer of information around a number of different stake-holders, make decisions under pressure, deploy teams and then receive information from them once they have assessed the situation for themselves.There is also the need to deal with **Secondary Consequences**, that is, the knock-on effects from the initial problem that will in themselves become problems for your incident management team.

The ability to respond effectively to an unexpected event is, in many ways, the ultimate test of a security manager's effectiveness.

4.2 Summary

The role of the Risk Management procedure is to give the security manager the tools to create viable and realistic risk management programmes capable of responding to the thousands of potential incidents that could possibly occur. The truth is that the vast majority of a security manager's time is taken up dealing with the same few situations that occur on a recurring (and often daily) basis. An effective security management programme should be able to identify the predictable normal incidents that can be dealt with using Standard Operating Procedures, those that need a higher level of management input and decision-making, and those that can be classified as crisis and which could potentially impact significantly on the wider organisation and its activities.

In summary:

- Risk Management has three component parts: Risk Assessment, Risk Control, Contingency Planning
- Risk Value is based on Likelihood and Impact
- The *Risk Assessment* identifies possible *Risks*, and gives them a *Risk Value*
- *Risk Control* consists of *Protocols* introduced to manage the risks identified in the Risk Assessment
- *Contingency Planning* is concerned with the *Reponse Options* that would be triggered if an unwanted event did occur
- Contingency Planning is also concerned with *Secondary Effects* that can impact on the organisation as a result of the unwanted incident

4.3 Self-assessment exercises

Self-assessment 1: Choose any organisation, identify ten potential threats that they might be facing, and then put them into a Risk Matrix based on the likelihood of those events occuring, and the impact it would have if they did occuur.

Self-assessment 2: Take three of the situations you have identified in Exercise 1, and produce a Risk Control protocol to prevent them from occuring, and which would also allow you to respond effectively if they did occur.

5 Creating a Safe Organisation

'The purpose of security is to create safety, not respond to danger'.

One of the most effective ways of developing security management systems is to look at how other organisations manage their security programmes, and to learn from how they have managed to balance the various aspects that we have covered in previous sections. This section introduces two organisations that are widely accepted to have developed world class Best Practices for dealing with widely differing threat profiles: one is tasked with managing mass-access but low-threat amusement parks, whilst the other has developed its own security management practices in the face of international terrorism for over forty years. The principles that they have developed to create security management capability across their organisations will be of value for anyone involved in any aspect of security management.

5.1 Total Security Management

Although the 'Creation of a Safe Organisation' is the ultimate objective of any security manager, there are still many differing (and in some case, conflicting) ideas of how that can be achieved.

One of the common models of security management has been 'Threat-Based Management' which was covered in the three-stage Risk Assessment – Risk Control – Contingency Planning model introduced in Section 1.2, which is based on the idea that if you identify all possible threats, and then develop methods ('protocols') to prevent them from happening, you will then have created a safe organisation. The problem is, of course, that you will never run out of possible threats, and the likelihood is that however many threats you think of, the world will throw a new one at you that you hadn't taken into consideration.

However, another method is to approach the problem from the other side, namely by concentrating on creating security as an integral part of the organisation, and then trusting that any potential problem that might become a threat to the organisation will be identified early enough to manage and deal with before it has the opportunity to escalate into an actual danger. One phrase used to describe this approach is 'Total Security Management'. Although TSM was originally coined to describe the management of vertical risk – that is, through the different levels of supply chain management, so that the end-user was not dependent on the effective management of the previous links in the supply chain that were outside of their control, it can be equally used to describe the total control of territory that comes under a security manager's responsibility. In this way, security management can be seen as a proactive measure designed to create safety, rather than a reactive system that responds to risks, threats and dangers only after they have been detected.

There are two organisations that are widely recognised to have integrated best-practice security and risk management into every aspect of their wider management operations, one dealing with the issue of normal, daily low impact high-likelihood scenarios, and the other dealing with potentially more serious low-likelihood-high impact threats.

The first is Disney World, which has created a self-contained Kingdom within which one of the main selling-points for potential visitors is its safety. Although Disney World is designed to deal with a massive amount of people with the freedom to choose to do a massive amount of different activities, the underlying management system is one based on total control of their territory, so that once you are inside Disney World you are actually experiencing a totally managed experience. The second organization is El Al, the Israeli national airline, which since the first political hijacking of a plane on 21st June 1967 of an El Al plane from Rome to Tel Aviv airport (following the end of the 6-Day War), has maintained security in its airports and planes across the world for 45 years. Despite a couple of notable exceptions, specifically the killing of 26 people in an attack on Lod Airport (now Ben Gurion) in 1972 by members of the Lebanese-trained Japan Red Army, El Al is still considered as perhaps the most effective security management system in the world, and its methodologies are widely accepted as setting the bench-mark for securing mass access public areas. Although Disney World and El Al are seemingly faced with radically different threats, the methods they have devised to manage them are remarkably similar.

The first concept common to both systems is Territory. Territory is that space over which you have control, and for which you take responsibility. For both Disney World and El Al, their territory begins a long way before you reach any actual buildings. In Orlando, Florida, there are signs welcoming you to Disney World from 30 miles away, telling you what documents you will need, informing you of what attractions are available, telling you what radio station to tune to for Disney world information. In Israel's Ben Gurion airport, the first check points are 2Kms from the actual airport, and are designed to give you the positive feeling that you are entering a safe zone, one where possible threats and problems have been identified and effectively mitigated. This First Point of Contact (FPoC) has two purposes. The first is to clearly mark the territory where you accept responsibility for creating and managing a safe space. The second is to allow the FPoC to act as an initial filtering system, allowing the initial security team to identify people who will not move through the system smoothly, who can then take be taken to the side and dealt with on an individual basis, without disrupting the main flow of business.

The concept of Control of Territory is continued once the visitor is 'inside'. There is nowhere within Disney World, or within an Israeli airport or airline section, that is not under the control of someone who has the specific responsibility for maintaining the safety of that area. One writer told how his daughter developed a blister during a visit to Disney World and removed her shoes and socks. She was immediately identified and confronted. When told that this was not allowed 'for the safety of visitors', and that failure to replace her footwear would result in them being escorted from the grounds, she decided that the she would undergo the pain in order to be allowed to remain within the funfair.

The second concept common to both organisations is the fact that 'Everyone is involved in security'. It is reasonable to presume that a small security team cannot maintain control and 'eyes on' to every possible situation that might develop. However, if everyone within the organisation is security aware, then the likelihood is that someone will become aware of a potential problem before it escalates into an actual threat, and that information can be passed on to the security team, who can then intervene in the most appropriate manner. This is not only relevant to traditional security threats, but is valid for any actions that could threaten the organisation. Although it seems that this is a simple principle, you only need to read the papers each day to see how organisations are putting themselves into danger because simple problems are allowed to develop into major threats, because although people are aware of them, no-one has taken the responsibility to inform someone in authority.

The third principle of security management that both systems are based on is that of 'Tight Management'. Writing security manuals and lists of protocols is easy. Delivering and maintaining them at an effective level over time is almost impossible. The truth is that most security programmes fail because the policies that have been put into place are not adhered to, and then a culture of laziness or ignorance becomes embedded into the organisation. Both of the organisations discussed here have a very strong management system in place, so that there is a clearly-defined organizational culture that security management is important, everyone understands what they have to do, and control systems are in place to ensure that they do so. If you want to test the system, drop a chewing gum wrapper on the floor at Disney World and see how long it takes for someone to pick it up, and then inform you that littering is not allowed.

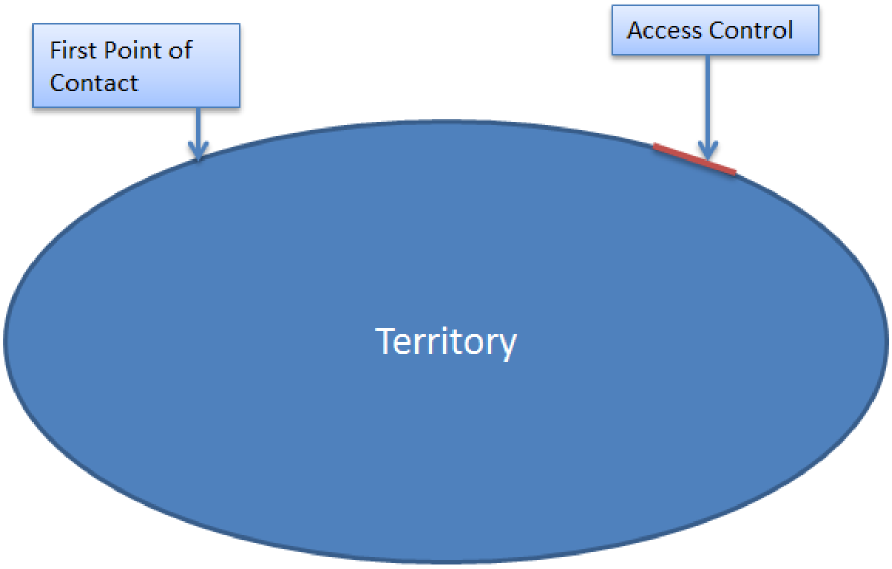
The question therefore, is how can we adapt the lessons learned from these global security leaders, and introduce these highly effective security management models into our own organisations? Here are some of the basic security concepts that are common to both Disney World and El Al, and which can be easily applied to any operational situation.

5.2 Principle 1: Territory: Security in Depth

Territory is not just 'Space'. For example, if you were the manager of a factory with an attached car park, but you had no information about what was happening within that car-park, it could not be considered your 'Territory'. Even if you had information about the car-park – for example, through use of CCTV monitored from a central Control Room – but could only observe what was happening without being able to do anything about it, you would still not be able to consider that area your territory. So, one definition of Territory is 'that area over which you have both information and control'.

Once the concept of Territory as a function of information and control is accepted, the next question concerns exactly where our territory starts. This is a critical question in the process of developing an effective security management capability.

Figure 9: The Attributes of Territory



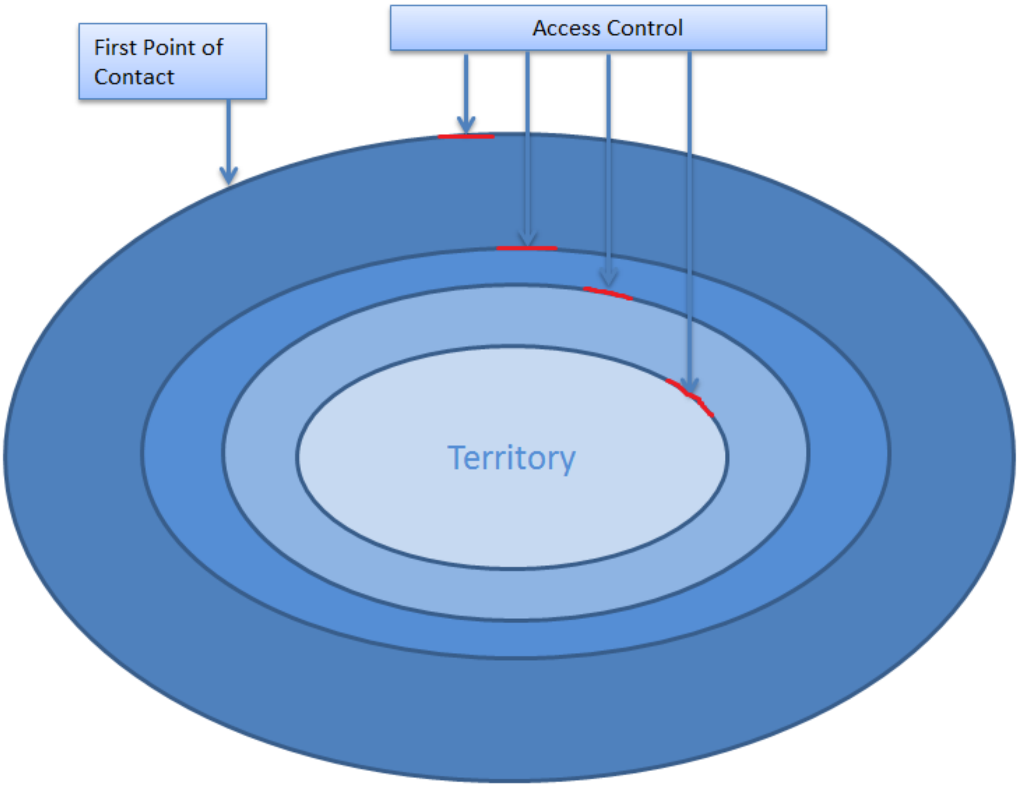
Territory is defined by a Boundary. This is where the FPoC is made. Access Control allows easy entry to that territory for those who pose no problem, and gives the security system the opportunity to identify potential problems before they are able to make an approach to higher-risk areas deeper within the system (see Figure 9).

Any Territory is defined by Boundaries. It should be clear to anyone coming into your territory that they are now coming under your control – though that should be done in a friendly, welcoming way, rather than an officious, impersonal way. The Boundary is marked by the FPoC. Although the FPoC might be overtly security-based, as in a government building or military base, depending on the general threat environment it can also be seen in terms of 'Meet and Greet'. This form of security as 'customer care' can be seen in hundreds of different situations where security managers want to clearly mark the beginning of their territory, such as bars, where there is a Door Supervisor outside the door, 5-star hotels, where there is a doorman waiting to greet you, corporate headquarters, where there are security personnel who will show you to the reception desk, or shopping centres, where there are (or at least, should be!) security personnel at the main entrance.

There is always a balance between Freedom and Security. One way that we can calibrate the level of security is the distance between the FPoC and the thing that we are securing, and the number of barriers you need to pass to get there. As a basic rule, the greater the distance between the FPoC and the target, and the greater the number of barriers, the safer you are.

Additional security can be created by increasing the distance from the FPoC and the main area that is being protected, and by the introduction of additional barriers. The basic principles behind Security in Depth (figure 10) are the same whether it is limiting access to the backstage area at a concert, the VIP room of a club, the Chairman's office in a major corporation or the research laboratories in a technology company.

Figure 10: Security in Depth



5.3 Principle 2: Total Cover: Everyone is Responsible for Security

One of the fundamental principles of both Disney World and El Al is that security is not just a single event – you show your pass to someone, and then the security checks are finished - but that security is in-built into every aspect of that organisation's functions. For example, whilst the security teams in both systems are highly-trained, extremely professional and well-resourced, they are not the only people responsible for security. The car park attendants, the toilet cleaners, the peanut-sellers, the people taking the rubbish out of the kitchen are all considered to be part of the security management programme. In this way, it is possible to have total cover of an organisations' territory, where someone will be bound to spot any potential problem before it becomes an actual danger. The role of that person is then to inform the security team that something is not quite right, and they will then be able to respond in an appropriate manner, assess the situation and take the necessary actions.

5.4 Principle 3: Tight Management

David Veness, the former head of Metropolitan Police Special Operations Unit, who was later a Special Adviser to the United Nations Commission on Security, used to have only one sign on his desk. It read 'Security is the management of complacency'. Any effective security management programme has to be one which can be maintained over time, without any loss of capability. Although this is a simple idea to put into words, it is possibly one of the hardest aspects of security management to actually control.

People are lazy, systems that are considered too intrusive are switched off, good practices are left to wither, systems are not maintained, and often after a certain amount of weeks or months, things return to how they were. It is well recognised that to create genuine organisational change is one of the hardest things to achieve, and yet to a large degree that is the purpose of the security manager. After all, if everything was OK, there would be little need for the security manager in the first place.

Although there are often limits in what a security manager can achieve (it is often true that the security manager is relatively low in the organisational power chain), there are a number of basic rules that will make it easier to achieve organisational change, and introduce an effective security management system that will at least move towards the creation of a safe organisation.

The first is that it is better to have a few rules that everyone follows, rather than many rules which are mainly ignored. The purpose of the security management programme is to support the overall activities of the organisation, so any rules that are introduced should be simple, easy to adhere to and understood by everyone. If there is a system of access passes, that should be used by everyone. If there is a rule that lone workers should log where they are going to be, and then confirm that all is well in a final call before they go home, that should be adhered to.

The second rule is that the security management system needs to be supported by everyone, from the Chairmen to the toilet cleaner (as outlined in principle 2, above). Security is not just the responsibility of the security team, but is one of the basic functions of everyone who works within that organisation.

And the third rule is that security is for ever. It is the role of the security management to ensure that the level of security awareness and readiness is maintained, and that standards are not allowed to slip. The Second Law of Thermodynamics (also known as Entropy) states that unless extra energy is put into a system, it will tend to slow down, lose effectiveness and generally come to a halt. This is equally true of security management. Effective security management is not a natural state. It is the role of the security manager to ensure that the necessary protocols are adhered to, just as much as writing the initial security management programmes in the first place.

5.5 Kaizen….

Having taken two examples from American and Israeli organizations, we can finish off this Module with another concept, this time from Japanese management systems. Kaizen is the idea of 'Continuous Improvement', and has become one of the leading general management theories in the last twenty years. In its simplest terms, Kaizen is built on the principle of incremental improvement – identify a weakness, find a way of improving it, implement it. It is a philosophy as much as a method, and believes that everyone has expert knowledge of their own field – the car-park attendant is as expert at being a car park attendant as the chief scientist is as being a research manager. They might also be aware of ways in which the security of the car park might be improved which no one else in the organisation has. Arsene Wenger, the Arsenal manager, put it another way: 'If you improve a hundred things by one per cent, you get a hundred per cent improvement'. Whilst this may not be strictly true from a mathematical perspective, it is an excellent way of managing security ***kaizen***.

5.6 Summary

Security has to begin and end somewhere, and that point is decided by how we define the territory that we accept responsibility for. Security in Depth describes the way that we can utilise our own resources in order to create progressively more secure environment. These simple principles of security management are used by two of the most well-respected organisation in global security management, each of which is facing completely different potential threats.

These principles are easy to understand, simple to implement, and can be adapted to almost any security situation.

In summary:

- *Total Security Management* (TSM) allows you to be proactive in developing a safe organisation, rather than responding to individual risks / threats
- *TSM* can be *Vertical* – as in Supply Chain Management – or *Horizontal* , through control of Territory
- *Territory* is *Space* which is defined by *Boundaries*, and for which you have *Information* and *Control*
- Safety is increased by *Security in Depth,*
- *Everyone* in an organisation is part of the Security Management Programme
- *Kaizen* allows for a culture of continuous improvement across the organisation

5.7 Self-assessment exercises

Self-assessment 1: An organisation has been identified as being involved in an oil spill in Alaska. The Board have decided that the security system around its HQ offices on the 13th-20th floors of an office block in Canary Wharf need to be reviewed, and if necessary improved. Using the principles covered in this module, what recommendations could you make to the Board?

Self-assessment 2: Your Chairman has returned from a visit to Japan, where he has heard about Kaizen. He has requested you give a presentation to the next Board meeting, identifying how Kaizen can be of use to the overall security management of the organization. Put together a PowerPoint briefing (about twenty minutes), that could be given to the Board, together with notes that could be distributed to the Board at the meeting.

Self-assessment 3: Your company has taken over a production factory in Ukraine. It stands in its own area within a larger industrial park. As Head of Security EMEA, you are going to visit the facility to assess the level of current security, and to identify possible areas that might need improvement. Put together a checklist of points that you would need to cover during your visit to the facility.

5.8 Further Reading

Reducing Terrorism Risk at Shopping Centres:
An Analysis of Potential Security Options
http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR401.pdf

6 Gold, Silver, Bronze Operations Management System

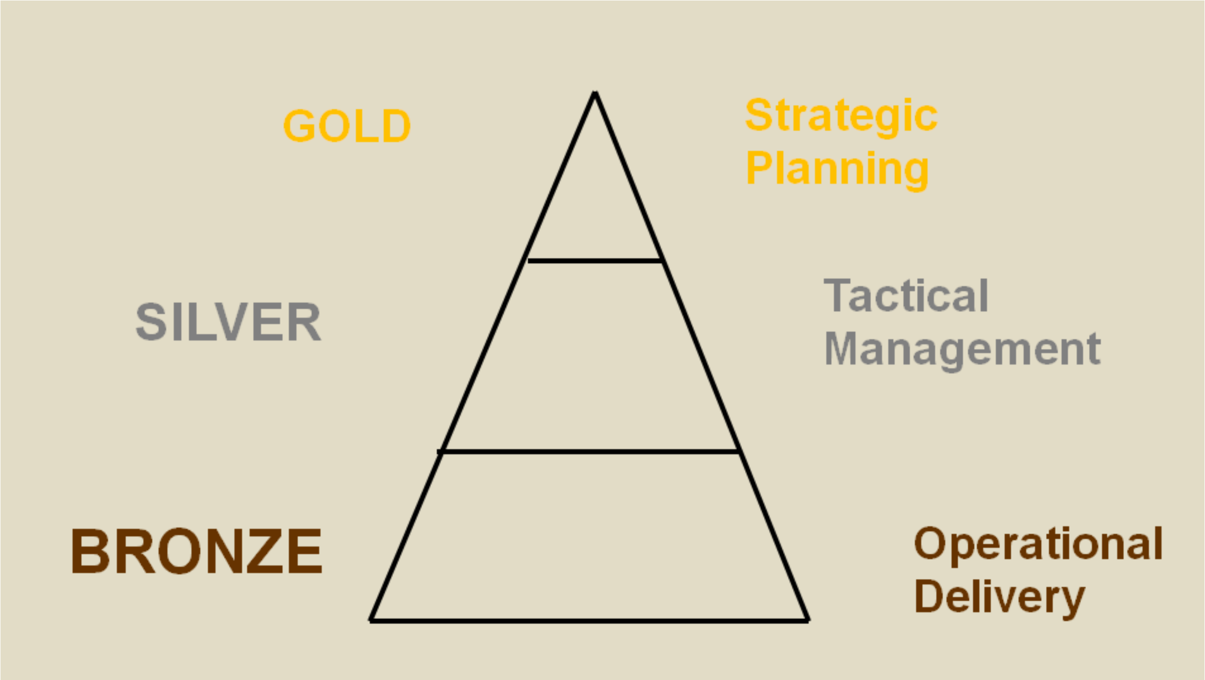
The Gold, Silver, Bronze (GSB) command system is used across the world to manage any sort of operation that involves multi-team coordination. Multi-team operations inevitably create issues of command and control, communication, information transfer, and integration with other teams, and possibly other outside organisations. This chapter introduces the basic concepts behind the GSB command system, as well as giving examples of where the GSB system has been used in real-life situations. An understanding of the GSB system will give the security manager the skills to design more complex security operations, safe in the knowledge that they will be able to function effectively and with a high degree of coordination and adaptability in the widest range of possible scenarios.

6.1 Gold, Silver, Bronze – Creating Operational Capability

One of the basic problems in security management is turning good ideas into operational capabilities. Unless it is little more than a one-office operation, the likelihood is that the security management operation will consist of various teams, each with their own duties and responsibilities, and which might well be based in different sites, geographical areas, or even countries. The security manager will be passing instructions on to other people, often Team Leaders, who will then be expected to carry out those duties. As such, it is likely that there will be the need for a Command and Control (C&C) Structure that will allow effective daily operations to take place. This module looks at the most common form of C&C Structures, and is designed to give you an understanding of the various components and functions of the system that will enable you to design the most appropriate C&C system for your own organisation.

The three-tiered management structure is common to almost all operational management programmes, whether it is in government, military, emergency services or corporate organisations. It consists of Gold, Silver and Bronze Command levels, each of which have their own duties and functions, and it is designed to allow information to pass speedily up the chain, commands and instructions to cascade down the system, and over all a high-level of coordination between the different teams and other units involved in the command structure (see Figure 11). If designed correctly, the C & C system should be able to deal equally effectively with standard daily activities, minor incidents that might require immediate response, and crisis management situations that demand a high level of coordination and organisational resilience.

Figure 1 1: The Three-Tiered Security Management System



Almost all security management systems are based on a 3-level management system, Gold (Strategic Management), Silver (Tactical Management) and Bronze (Operational Management).

Bronze Command level denotes the lowest level of the command chain, and consists of the people, and teams who complete the task on the ground. This is often called the Operational Command. This could mean interfacing with the public, as in a hotel security team, the security teams in an airport or the door supervisors in a pub. The Bronze level teams are the people on the ground, so they will often be the first people who are aware of changes in the immediate situation. As such, as well as carrying out their individual functions, their role is also to be the ears and eyes of the Silver and Gold Commanders, and to pass information up the command chain as required.

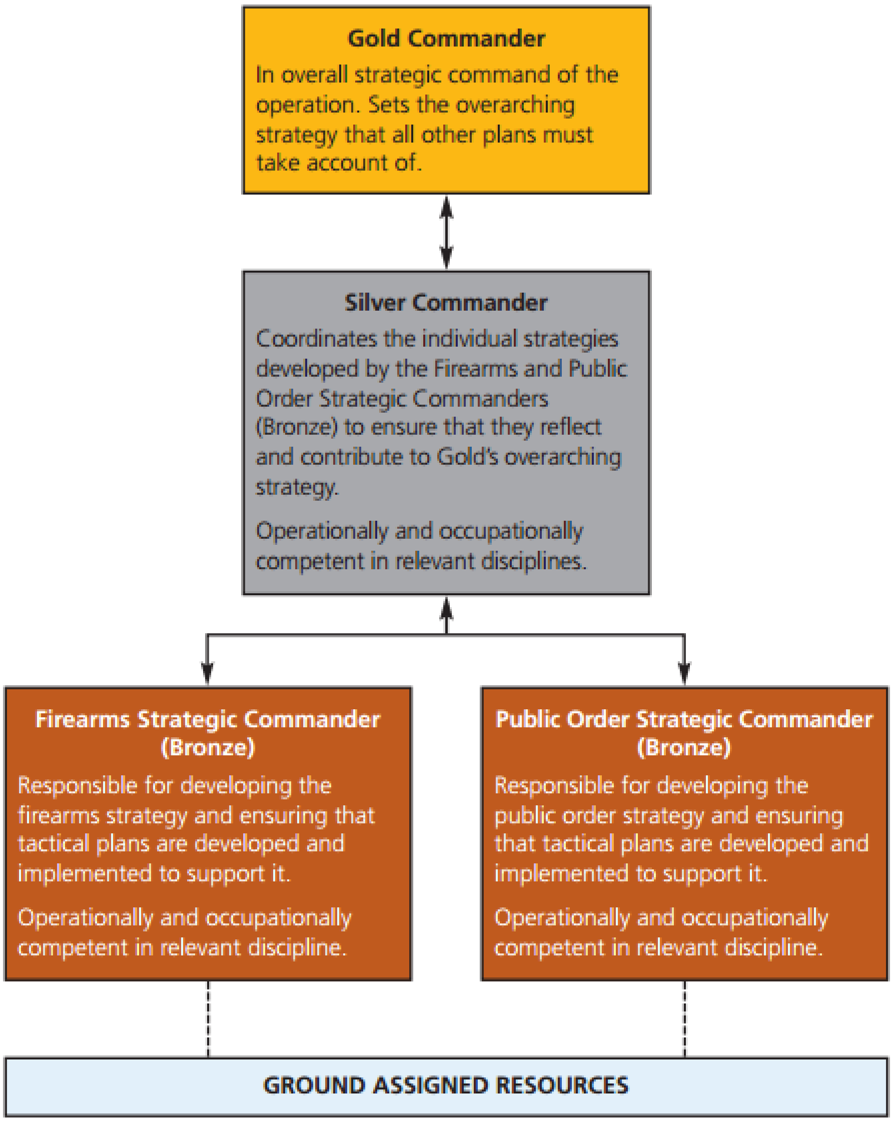
Silver Command is the level of command responsible for making sure that that work is carried out effectively, and is often known as the Tactical Command level. Tactical Command could involve defining roles and responsibilities, creating working protocols, delivering training programmes, ensuring that the correct equipment and other resources are in place, and in general ensuring that operational capability is at the required level. The Silver Command level may well be on charge of a number of Bronze level teams, and one of the functions of the Silver Command is to coordinate the work of the individual bronze teams so that they can respond in the most effective manner to any incident that might occur.

Gold Command level is responsible for creating the overall strategy, so that each team knows where they fit into the overall command structure, and how their roles contribute to the overall success of any operation.

As an example in a hotel chain, the Gold Commander might be the regional security manager, who is responsible for ensuring that there are clear security policies within each hotel, that there is sufficient training and resources to allow the security teams to carry out the functions, and who would review the security operations on a regular basis. The Silver Commander would be equivalent to the hotel security manager, who is responsible for ensuring that the hotel, its staff, guests and general operations are kept safe, and that all appropriate steps are taken to ensure that those processes are adhered to. The Silver Commander would also be responsible for managing the response to any situation that would come outside 'normal daily activities', such as a complaint from a guest, a report that a member of staff was stealing from rooms, or a tree falling down in the car park. The Bronze Commander would be the person acting as Shift Manager or Team Leader, who would be actively interacting with staff and guests as their first point of contact, and who would be the people actually responsible for the on-going safety and security of the hotel.

Figure 12 provides an example of an operational command system as set out by the National Police Improvement Agency (NPIA) Guidance on Command and Control
http://www.acpo.police.uk/documents/crime/2009/200907CRICCG01.pdf

Figure 12: Example of a 3-Tier Command Structure for Complex Operations


Gold Commander
In overall strategic command of the operation. Sets the overarching strategy that all other plans must take account of.
Silver Commander
Coordinates the individual strategies developed by the Firearms and Public Order Strategic Commanders (Bronze) to ensure that they reflect and contribute to Gold's overarching strategy.
Operationally and occupationally competent in relevant disciplines.
Firearms Strategic Commander (Bronze)
Responsible for developing the firearms strategy and ensuring that tactical plans are developed and implemented to support it.
Operationally and occupationally competent in relevant discipline.
Public Order Strategic Commander (Bronze)
Responsible for developing the public order strategy and ensuring that tactical plans are developed and implemented to support it.
Operationally and occupationally competent in relevant discipline.
GROUND ASSIGNED RESOURCES

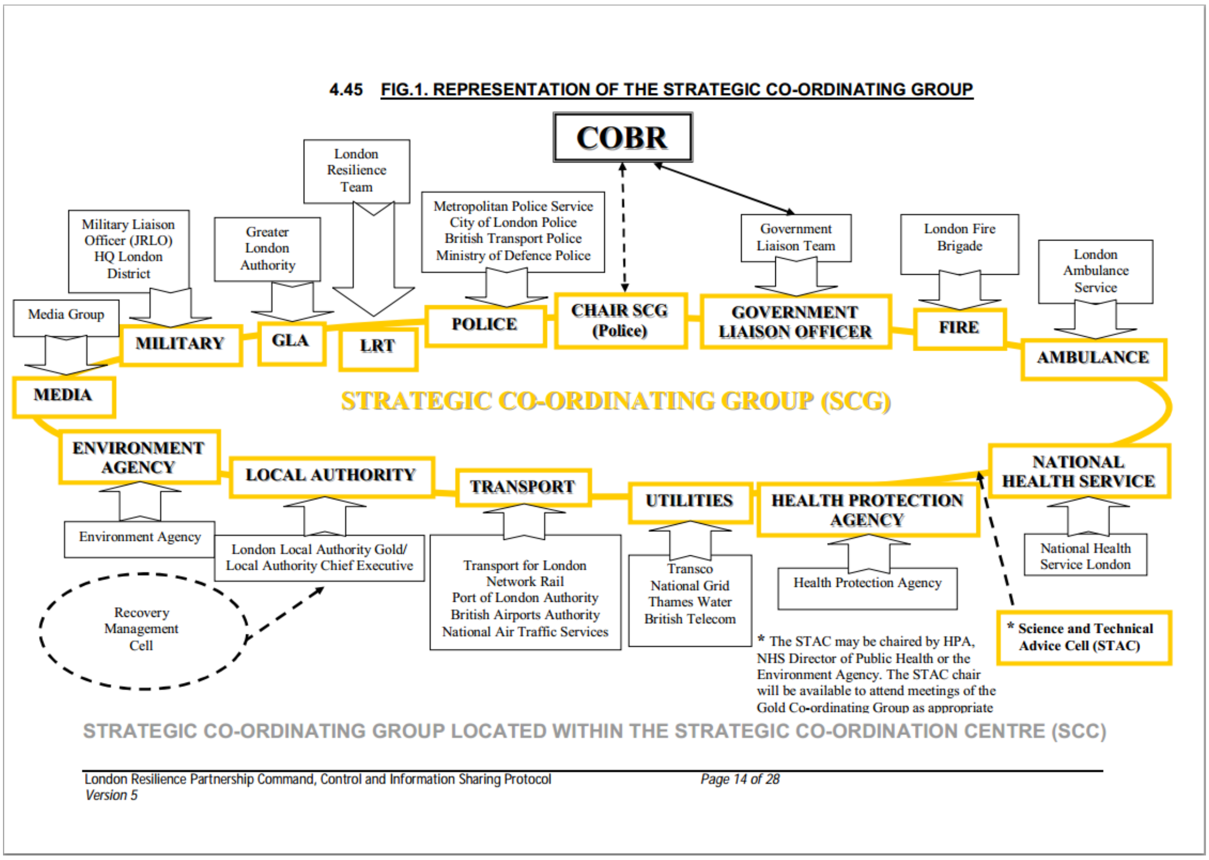
6.2 Advantages of the GSB System

One of the advantages of the GSB system is that it allows different Bronze Commanders, Silver Commanders or Gold Commanders to coordinate their actions with similar-level commanders in different systems, so as to create effective multi-team working groups. This is the basis of the most 'senior' of the GSB Command system in the UK, COBR, which is the government-level crisis management system. COBR stands for Cabinet Office Briefing Room, and is used when there is the need to coordinate a large number of different organisations for a national crisis, such as terrorism, health scare or natural disaster (such as flooding).

The COBR Strategic Coordinating group is comprised of Gold Commanders of various representative groups, each of which comprises organisations which have their own Gold Commanders. This is an extremely effective system for allowing a large amount of information and expertise to be brought together into one meeting, as well as allowing orders and requests to cascade down the command chain extremely quickly and efficiently.

Figure 13 is an example of a Gold Strategic co-ordinating group.

Figure 13: This example of a Gold Command Strategic Coordinating group.



4.45 FIG.1. REPRESENTATION OF THE STRATEGIC CO-ORDINATING GROUP

COBR
London Resilience Team
Metropolitan Police Service
City of London Police
British Transport Police
Ministry of Defence Police
Government Liaison Team
London Fire Brigade
London Ambulance Service
Military Liaison Officer (JRLO) HQ London District
Greater London Authority
Media Group
MILITARY
GLA
LRT
POLICE
CHAIR SCG (Police)
GOVERNMENT LIAISON OFFICER
FIRE
AMBULANCE
MEDIA
STRATEGIC CO-ORDINATING GROUP (SCG)
ENVIRONMENT AGENCY
LOCAL AUTHORITY
TRANSPORT
UTILITIES
HEALTH PROTECTION AGENCY
NATIONAL HEALTH SERVICE
Environment Agency
London Local Authority Gold/ Local Authority Chief Executive
Transport for London
Network Rail
Port of London Authority
British Airports Authority
National Air Traffic Services
Transco
National Grid
Thames Water
British Telecom
Health Protection Agency
National Health Service London
Recovery Management Cell
* Science and Technical Advice Cell (STAC)
* The STAC may be chaired by HPA, NHS Director of Public Health or the Environment Agency. The STAC chair will be available to attend meetings of the Gold Co-ordinating Group as appropriate

STRATEGIC CO-ORDINATING GROUP LOCATED WITHIN THE STRATEGIC CO-ORDINATION CENTRE (SCC)

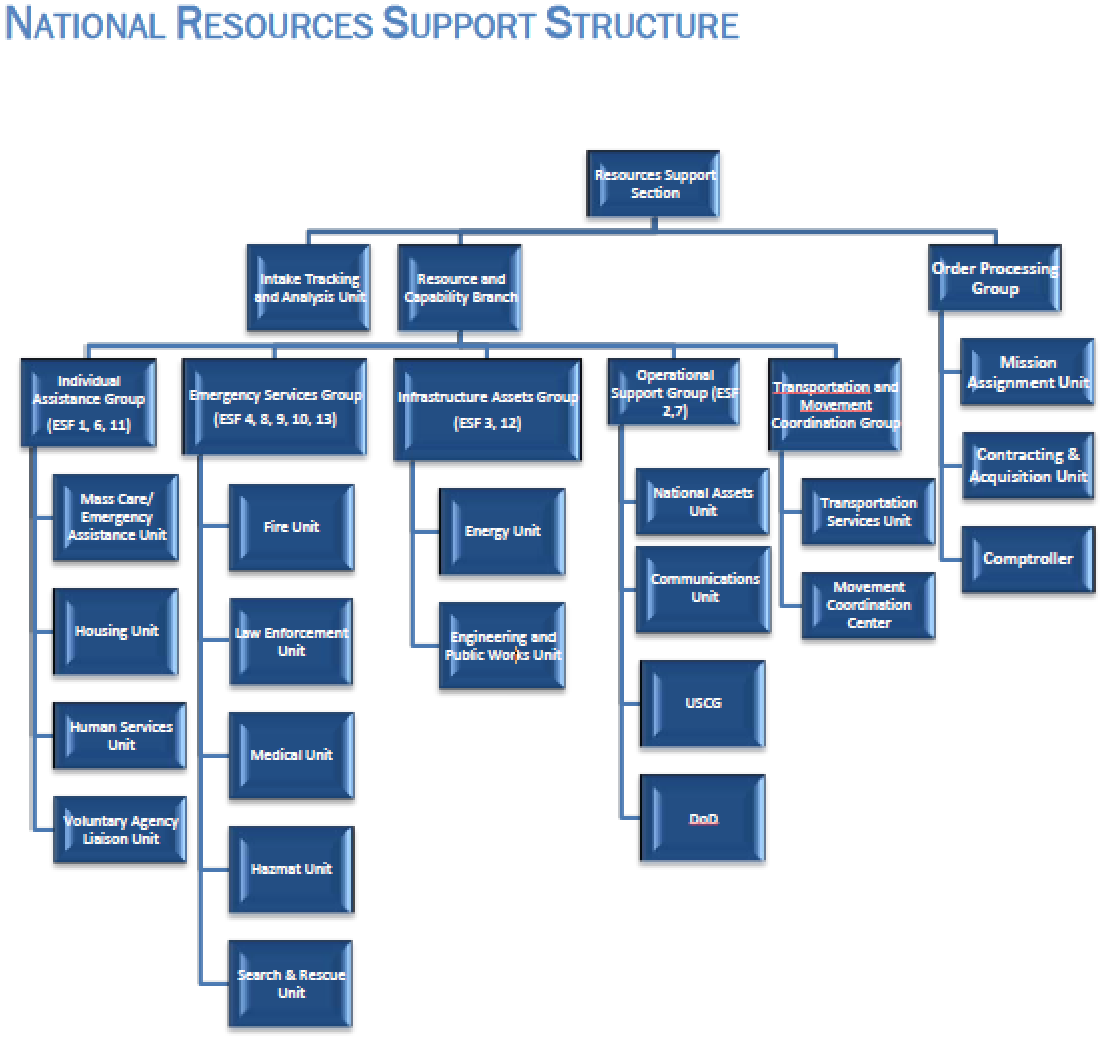
London Resilience Partnership Command, Control and Information Sharing Protocol Page 14 of 28
Version 5

From http://www.london.gov.uk/sites/default/files/Command-and-control-protocol-v5.pdf

This outline gives an indication of the number of stakeholders that need to be included in a strategic coordination team. However, this is an extremely effective way of getting senior decision-makers together, allowing fast decisions to be made that can then be cascaded down through a variety of chains of command.

Figure 14 provides an example of a System Cascading into Increasingly Specialist Sub-Units.

Figure 14: System Cascading into Sub-Units

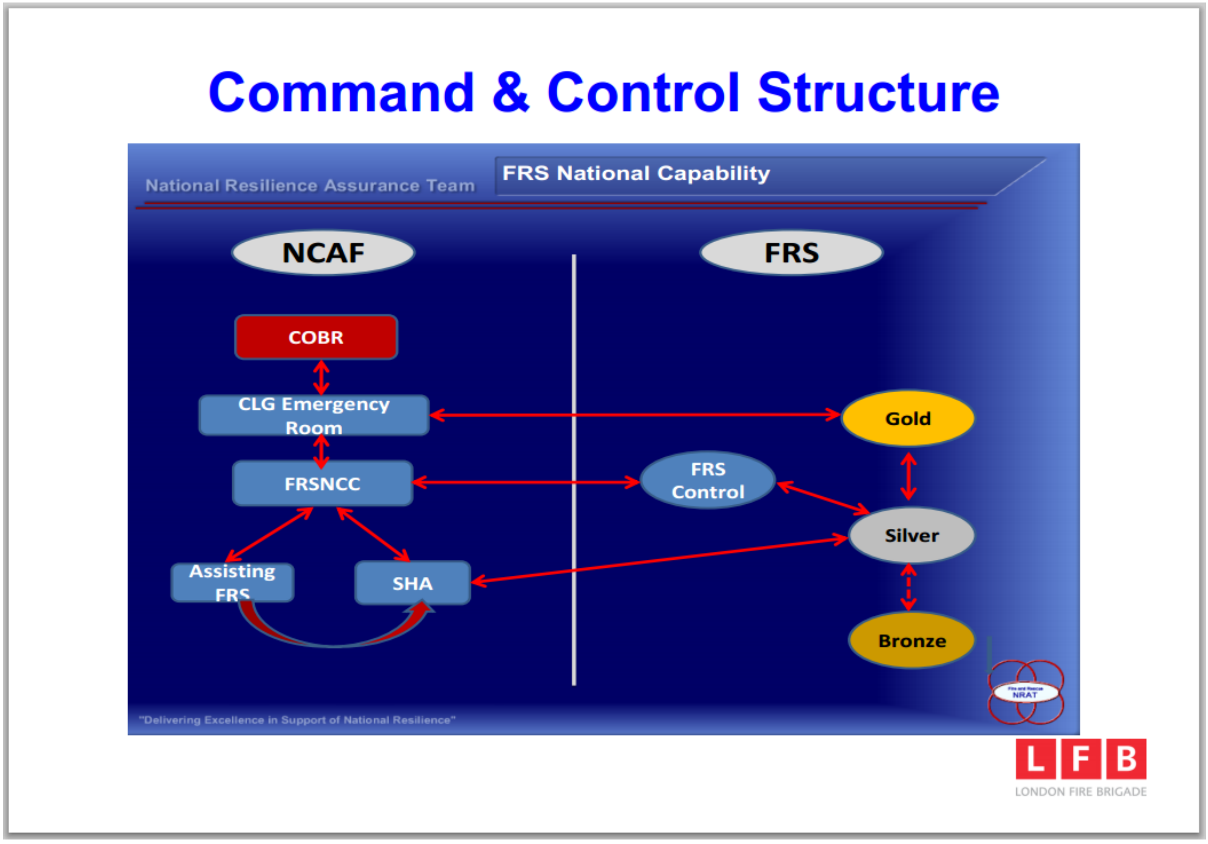

NATIONAL RESOURCES SUPPORT STRUCTURE
Resources Support Section
Intake Tracking and Analysis Unit
Resource and Capability Branch
Order Processing Group
Individual Assistance Group (ESF 1, 6, 11)
Emergency Services Group (ESF 4, 8, 9, 10, 13)
Infrastructure Assets Group (ESF 3, 12)
Operational Support Group (ESF 2,7)
Transportation and Movement Coordination Group
Mission Assignment Unit
Contracting & Acquisition Unit
Comptroller
Mass Care/ Emergency Assistance Unit
Housing Unit
Human Services Unit
Voluntary Agency Liaison Unit
Fire Unit
Law Enforcement Unit
Medical Unit
Hazmat Unit
Search & Rescue Unit
Energy Unit
Engineering and Public Works Unit
National Assets Unit
Communications Unit
USCG
DoD
Transportation Services Unit
Movement Coordination Center

From US FEMA National Incident Support Manual (p 30) http://www.lrc.fema.gov/em_doctrine_fema_nismanual.html

This is the Command Chain of a sub-section of an overall operation – in this case, the Resources Support Section in the US government Federal Emergency Management Agency. As in previous examples, the purpose of such a system is to create an effective chain of command that allows communication and commands to be passed down the system, and relevant information to be passed up the system.

Figure 15 is a slide from a London Fire Brigade presentation showing the connection between COBR and the LFB Gold / Silver / Bronze Command system for the 2012 London Olympics.

Figure 15: Gold/Silver/Bronze Command System for the 2012 London Olympics


Command & Control Structure

National Resilience Assurance Team

FRS National Capability

NCAF

FRS

COBR

CLG Emergency Room

FRSNCC

Assisting FRS

SHA

FRS Control

Gold

Silver

Bronze

"Delivering Excellence in Support of National Resilience"

LFB

LONDON FIRE BRIGADE

(Presentation available at http://www.sefip.gov.uk/viewDocument.jsp?document=3027)

6.3 Potential Problems with the GSB Command Structure

Although the Gold, Silver, Bronze (GSB) Command Structure is recognised as being the most effective way to manage security operations that are bigger than a one-team operation, there are a number of potential problems that are repeatedly identified as causing problems both in the planning and development stages of security management, as well as in actually responding to incidents.

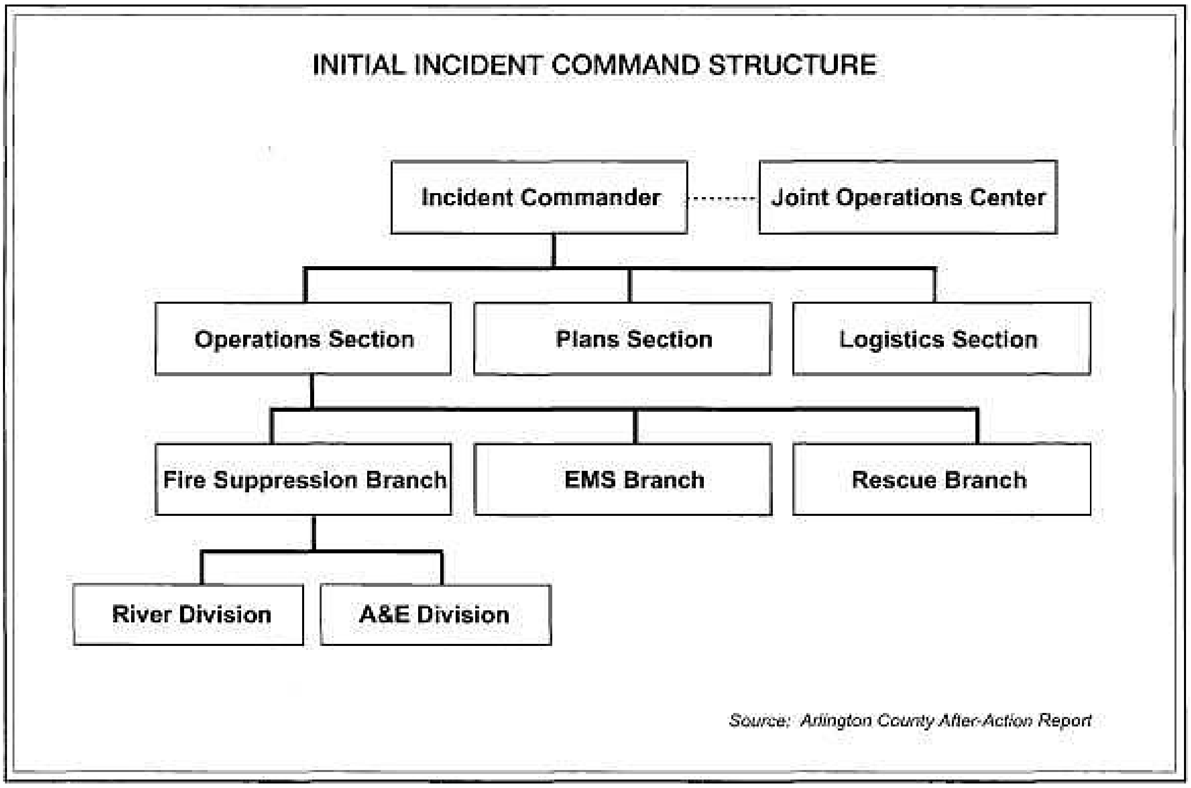
The first potential problem, and one that is almost always identified as one of the critical causes of operation failure, is communications. More precisely, it is the failure of the transfer of complex information under pressure. Carl von Clausewitz, the great Prussian strategist, coined the phrase 'Fog of War' in 1837 to describe the general chaos and uncertainty that almost always accompanies operational activity. As organisational complexity increases, due to more levels of command and a greater number of different teams, the pressures created by responding to unfamiliar or unknown situations whilst having to operate with less than full information creates an environment where information can be easily lost, misheard or misunderstood.

This can be the case even when the security operation is run by the best trained operation managers in the country. The Jean Charles de Menezes incident in 2005, when an innocent Brazilian student was mistakenly shot by armed police counter terrorism teams, was in a large part due to a misunderstanding as to the nature of the threat. Was it a 'normal stop', or was it part of Operation Kratos – a stop with possibility of a 'critical shot' to prevent the immediate detonation of a suicide bomber'? Despite the clear national threat, and a whole range of briefings, there was still lack of agreement in the report given by one of the officers who made the critical shot, and Commander Cressida Dick, who was acting as Gold Commander at the time, and who had denied giving any order that would have triggered 'Operation Kratos'. The report into the de Menezes incident by the Independent Police Complaints Commission gives a good insight into some of the issues of command and control in the pressures of immediate incident response. (See http://www.ipcc.gov.uk/en/Pages/reports_stockwell.aspx for as full copy of the report).

An associated problem with the transfer of information is stove-piping, or when different departments don't share information with each other. This can be because there is simply a lack of available channels to exchange information, or can be because different departments see other departments as possible rivals for influence, and therefore see the control of information as a way of maintaining their own power position. This was certainly the case in the run up to 9/11, when the lack of open communication between CIA and FBI (on both an official and informal, personal basis), meant that information that was known and on the record was not shared.

Figure 16 shows the initial GSB command structure at the US Pentagon immediately following the 9/11 attack. This shows how even the most complicated operation can be simplified based on clear chains of command.

Figure 16: GSB Command Structure



Source: http://www.history.navy.mil/library/online/pentagon_9-11.htm (p74)

A third problem connected with a hierarchical GSB command system is that often the situation being dealt with demands an immediate response, but the command system means that it takes a long time to transfer information to the decision-makers, who then spend time discussing the situation, and only then start issues instructions as to how to respond. This is true whether the situation is a national disaster such as Hurricane Katrina or snow blocking UK airports, or a local office complaining that the road to their warehouse is blocked, and they need to make alternative arrangements. In most cases, the most effective use of the GSB system is to devolve authority to the lowest appropriate level. In other words, if one level of decision maker has the ability to make the decision, there is nothing to be gained by having to go higher up the command chain to receive authority for that decision.

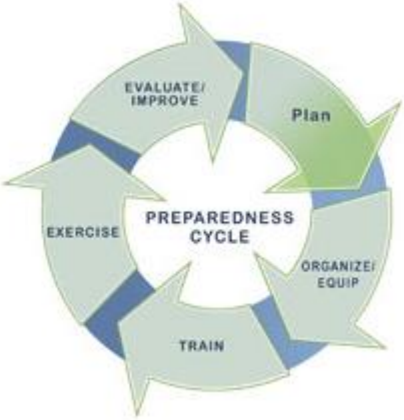
6.4 And finally….

As in all security management programmes, the success of the system lies not in drawing pretty command plans with boxes and arrows, but in ensuring that everyone involved in the operation knows what they are doing, understands what they are trying to achieve, and are able to exchange information and make decisions on an on-going basis.

The GSB command System works best when there are three criteria that are met. Firstly, that all of the groups within the system share the same basic culture and 'risk recognition'. Every security manager knows the frustration from talking with Head Office administrators who don't understand the seriousness or immediacy of a problem! Secondly, the different people involved in the organisation know each other on a personal basis, and are able to work together effectively for a common cause. And thirdly, that the various teams have worked together in training situations, either with table-top exercises for the team leaders and commanders, or in real-time with the different operational teams.

Creating multi-team operational capability is not something that can be left to chance, or can be established once a crisis situation has occurred. The development of such capabilities is something that must be managed over time in a continuous cycle of learning, reviewing and improvement. Figure 17 shows one method of achieving this, namely the preparedness cycle.

Figure 17: The Preparedness Cycle



Source: www.fema.gov/plan

6.5 Summary

As soon as a security management system involves more than a single person, then a Command and Control structure will need to be in to ensure that all aspects of the security management programme are coordinated and controlled in an effective and professional manner. The Command & Control Structure should be able to manage Routine Activities, Minor Incidents and Crisis Situations, and should allow information to be passed up the command chain from front-line responds who have information on any situation and instructions to be passed down the command chain from managers who may well be located far away from the incident site. The ability to create effective command chains is at the heart of effective security management, and it is almost always the case that it is failures in command chain management that is one of the major causes of most security management failures.

In summary:

- A three-level command system – Gold, Silver, Bronze – can be applied to any security operation, and clearly sets out the responsibility associated with each command level
- The purpose of any command system is two-fold: to allow information to be passed up the command chain, and orders and directions to be passed down
- If a command system fails, it is almost always because there has been a break-down in communication
- Additional complexity increases the likelihood of failure
- Command systems work best when all of the people involved in the operation know each other, have worked together before, and share a common organisational culture
- The more you train together, the more successful the response operation will be

6.6 Self-assessment exercises

Self-assessment 1: Draw out an Organizational Plan for a multi-level, multi-team organisation, identifying the Gold, Silver and Bronze Commanders in each section.

Self-assessment 2: Create a Response Programme for three separate incidents, one involving local teams within an organisation, one involving teams from across the organisation, and one involving teams from both inside and outside the organisation.

Self-assessment 3: Write a report for the CEO of your company, explaining the arguments for the introduction of a GSB command system within the company security department. (Make sure that they system you are describing is large enough to support the GSB system).

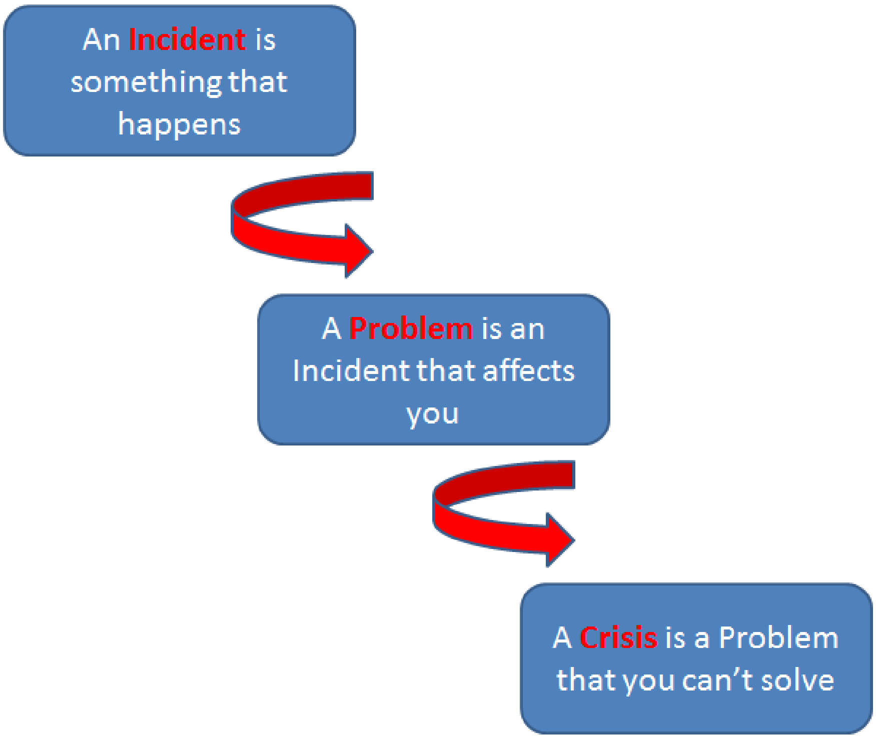
7 Maintaining Sustainable Capability

As has already been mentioned in previous sections, the secret of creating effective security management capability is to ensure that whatever programmes and protocols are introduced are not seen as one-off events, but are embedded into the organisation so that they become a natural part of its operating procedures and its organisational culture. For many security management systems, this is the hardest part of the management process. Protocols can be written, programmes designed and personnel trained, but to create organisational change is one of the hardest things for any manager to achieve, and even if they have succeeded in doing so, the natural tendency is for organisations to revert to previous practices. This section will introduce some ideas as to how security managers can self-audit their own organisation, and can identify areas where weak practices or lack of management oversight are likely to produce vulnerabilities that could allow small scale potential problems to develop into genuine problems.

7.1 Effective Protocols

There is often a desire in security management to try and identify every possible problem, and then to introduce increasingly detailed and situation-specific protocols to try and manage those scenarios. The problem is that if the control systems become too intrusive and disruptive, the natural reaction is to ignore them or to switch them off. This is then not just a problem with that particular situation, but creates a culture where it is not only permissible, but is accepted practice to ignore guidelines and directives. The purpose of the security management team should always be to support the overall operations and objectives of the organisation, and though it may be tempting to introduce more and more controls, that is self-defeating in the long-run. It is better to have a few guidelines that are accepted and adhered to, rather than a whole raft of directives that are ignored.

Figure 18: From Incident to Crisis



An **Incident** is something that happens

A **Problem** is an Incident that affects you

A **Crisis** is a Problem that you can't solve

7.2 Crisis Cognition

It is a basic rule in life that the earlier you are aware of a potential problem, the more likely you are to be able to deal with it smoothly, effectively and with the minimum of disruption to the rest of the operating network. If you allow that problem to go unmanaged, it is likely to escalate to a level where it sets alarm bells ringing, at which point the system takes notice and responds, but will often need a much higher level of intervention to deal with the situation than if it had been detected and managed earlier in the escalation cycle.

- By becoming aware of a potential problem earlier rather than later in its development cycle:
- You have more options to deal with it
- You can respond with a lower level of intervention
- You are safer from both a personal and organisational perspective

By being unaware of a potential problem, or by ignoring a problem you are aware of:

- You will have less options to deal with it
- You will need to respond with a higher level of intervention
- You will be in greater danger from both a personal and organisational perspective

7.3 'Normal Accidents'

In most situations, crises do not just happen. They are only the final stage in a long process of gestation and development. In most situations, the reason that a major problem occurs is not because of an outside event, but rather because there is a lack of ability to respond effectively. In almost all situations, there will have been warning signs that the conditions that will allow the crisis to develop are in place, and there are what have been called 'Normal Accidents' that occur on a repeated basis, which highlight the organisational weakness that is allowing those situations to occur, but which are ignored or accepted.

7.4 Complexity

Many organisations are complex – that is the nature of our inter-connected world. However, it has been well-recognised that organisational complexity itself creates an increased likelihood of problems arising - or even catastrophic failure, which threatens the continued existence of an organisation. Although the issue of organisational complexity is a subject in itself, from the security managers perspective there are two clear consequences of an organisation's over-complexity which may well (actually, undoubtedly will) create avoidable situations that have the likelihood of developing into genuine and serious problems.

7.5 Information Transfer

One of the clearest signs of harmful organisational complexity is if there are regular breakdowns in the transfer of information. This can either be because the lines of communications between different sections of the organisation are ineffective, or because different sections of the organisation are unaware of the need to pass information across to other sections. An example that many security managers might recognise is if the Business Development section creates plans to open a new office or factory in a country where there is genuine risk, whether political, social, criminal or health based. These are problems that the security department would be well aware of, and could highlight if they were part of the business development process. A Risk Analysis of any new country (or even city) should be a natural part of the business development process, but this is dependent on the working relationship between the different divisions. A similar example would be if the HR department is responsible for booking flight tickets for travelling executives, but doesn't inform the security department if one of the company's managers is travelling to what could be perceived as a high-risk area. If the first time that the security department is aware of a problem is when the HR department contact them because that executive's wife has called them because she hasn't heard from her husband in five days, then there is clearly a breakdown in organisational communication and planning.

7.6 Clear Lines of Responsibility

One of the hidden effects of organisational complexity is that it blurs lines of responsibility. In some cases, complexity is introduced specifically to allow people to avoid individual responsibility for decisions and policies that they know to be questionable, flawed or even illegal. Many of the major incidents that hit the national headlines are a direct result of organisational over-complexity that left a vaccuum where clear responsibilty and leadership should have been. This includes the Federal Emergency Management Agency (FEMA) response to Hurricane Katrina (2005), the Japanese government's response to the Fukushima disaster (2011), the BP response to Deepwater Horizon Gulf iof Mexico oil spill (2010), the G4S failure to supply security personnel to the London 2012 Olympics (2012) or the BBC's failure to adequately respond to the issue surrounding Jimmy Savile and accusastions of child abuse within the organisation (2012).

The problem with complexity is not just a theroretical problem, but is reflected in almost every aspect of operation management. The more complex an operation becomes (especially if the additional complexity seems to be unnecessary), the more liley it is to lead to serious, and perhaps catastrophic, failure. Txample of how the break-up of British Rail into separate companies, each of which had the responsibility for a separate asepct of the over-all operation, is just one example of how additional complexity can lead to management breakdown and eventual disaster.

7.7 Case Study: Railtrack – Complexity and Disaster

One of the clearest cases of the conenction between complexity and loss of organisational control was Railtrack, the company that was created after the privatisation of the railway system by the Conservative government in 1996. Formerly known as British Rail, the nature of the railway network was already extremely complex, with a high degree of inter-conenctedness and mutual systems-dependency - (10,346 miles of track and signalling, 40,000 bridges and viaducts, 50 tunnels, 2,508 stations, 1500 signal boxes, 9000 level crossings). Altrhough there were organisational problems with BR before the break-up, at least there was one organisation that was responsible for the entire system, and which had clear lines of responsibility for its maintenance and management.

After nationalisation, different section of BR were broken up into autonomous organisations, each responsible for a specific area of operations, and often developing a competetive or even adverserial relationship with other areas of operation. The trains and rolling stock were owned by three separate companies, that in turn leased them out to twenty-five different train operating companies. Railtrack owned the track, but its role was purely administrative. Responsibility for the maintenance of the track (a critical factor in the operation) was sub-contracted to other companies, which although they were then tasked with the responsibility for the maintenance of the track, in turn sub-contracted it out to other companies to actually deliver the work. Railtrack did not have its' own engineering department, and did not have the technical knowledge within the company to oversee the maintenance work, or even to gauge whether it was being delivered effectively.

Another consequence of the break-up of BR was that rather than acting as a single entity with different divisions, each division acted in order to maximise its own profit and minimise any potential liablility. This meant that the highy critical and immensely complex network of relationships between the new companies were controlled by detailed contracts, each of which tried to micro-mange extremely complex operations. There were 224 separate legal agreements covering freight contracts, and apportioning responsibility for delays was based on 1,900 checkpoints, 204 predefined delay causes, and 1,300 delay-attribution points. Railtrack employed fifty people just to account for delays in the Southern region alone. These contractual relationships led to increasingly bitter legal actions between the various companies, which in turn led to a break down in over-all service delivery. Although the government still held nominal responsibility for overseeing the running of Railtrack, that was equally murky, with a raft of different organisations involved in the oversight, including the Office of Passenger Rail Franchising, the Office of the Rail Regulator, Her Majesty's Railway Inspectorate, the British Railway Board, the Rail Passengers Council, and the Transport Secretary. It will be no surprise that rather than working cooperatively and collaboratively, these government agencies often saw each other as rivals for power and influence, and spent more time trying to out-manoeuvre each other than concentrating on the actual objectives.

The consequences of this organisational complexity became tragically clear on the morning of 17th October 2000, when an Intercity train travelling at 115 miles an hour was derailed near Hatfield, with the death of four passengers and over seventy injured. Subsequent enquiries found that the cause of the derailment was the failure to repair damaged tracks, despite the fact that the damage and potential consequences were known. The official review into the incident laid the blame for the accident squarely on the lack of clear responsibility for the management of the tracks. This accident led to massive disruption of national rail services (with an estimated loss to UK businesses of £6 million per day), and ultimately caused Railtrack to go into administration in 2002.

7.8 Regular Reviews

One of the fundamental developments in security management since 9/11 has been the realisation that rather than something that is limited to a security department, security management should be an integral part of every aspect of an organisation's operations and culture. In a similar way, security protocols are no longer seen as static things that are written and then forgotten, but are living documents that develop and evolve in the same way that any other part of the organisation would develop and evolve. Regular reviews of every aspect of the security management system play an important role in ensuring that security management capabilities are maintained at the highest possible level. As well as reviewing existing protocols and documentation, regular reviews also allow the security managers to develop their relationships with managers and personnel in other divisions or departments, which in turn helps facilitate the personal relationships which underpin effective security management at every level of an organisation.

7.9 And Finally….

In many ways, security management fulfils a different role from every other activity within an organisation. Whilst mistakes in most other divisions are recoverable, and can often be resolved by way of a simple apology, mistakes made in the security department can often have much more significant consequences, are not recoverable, and may, in the worst circumstances, lead to death, injury or catastrophic impacts. The responsibility of the security manager is to create the correct balance between freedom of movement and activity on the one hand, and safety and security on the other, but also to ensure that lessons are learned, mistakes rectified and the overall system strengthened and improved on an on-going and continuous basis. Security management in its fundamental form is a simple art, but it is the ability to maintain standards, and to manage them effectively over time, that is the ultimate test of the success or otherwise of the security management system.

7.10 Summary

It is almost certain that the front page of the newspaper you brought this morning carries an example of where failures in security management have had significant impacts, and quite possibly have led to actual disasters. The likelihood is that these failures did not happen because of some catastrophic outside event, but are the result of a breakdown of what should be basic management controls. The reasons for these failures are usually predictable and well known, but have in some way been ignored or side-stepped. The issues covered in this chapter will give any security manager the ability to audit their own operations, and to identify problems that have a high likelihood of leading to significant operational failures.

In summary:

- You can't always prevent Incidents – but you can take responsibility for how you respond to them
- Incidents and crises don't 'just happen'. They develop over time, and the earlier you are aware of potential problems, the more effective you will be as a security manager
- Complexity is the enemy of clarity. Do not allow your systems to become overly complex – especially if that doesn't add to your operational capability
- Even the largest and most high profile operations fail for simple reasons – breakdowns in communications, breakdowns in command structures, lack of leadership
- Security management is not a single event, but is a never-ending process – review your own operations on a continuous basis, and keep on improving them

7.11 Self-assessment exercises

Exercise 1: Identify an incident that has been the direct result of organisational complexity (it can be one of the incidents mentioned in this module, or another one of your own choosing), and analyse how and why the incident happened, and what steps could have been taken to prevent it.

Exercise 2: Take an organisation that is known to you, and design an Annual Security Review that will allow you to assess the level of security within the organisation, identify potential weak spots, and allow you to make recommendations as to how the system can be improved over the next management cycle.

Exercise 3: Identify three ‘Normal Accidents’ that could be indicators of systemic weakness within the security management programme, and show how the underlying causes can be dealt with in order to prevent those Normal accidents from occurring, and potentially escalating into full-blown crisis status.

7.12 Further Reading

How Privatization Became a Train Wreck Eric Morris. Access, Issue 28, pp 18-25, (2006)
http://www.uctc.net/access/28/Access%2028%20-%2004%20-%20How%20Privatization%20Became%20a%20Train%20Wreck.pdf

8 Adding Value

As should already be clear from the previous sections of this module, for security management to be truly effective it should be embedded into the very heart of an organisation, intricately connected with every aspect of its' operations and general management culture. However, the truth is that in many, if not most, organisations security management lacks the status of other aspects of the organisations management processes, and in many ways is seen as being something that can be considered once a year at an annual review. There are a number of reasons why that happens, which will be touched upon in this section, but it is certainly the case that the way that security management represents itself often causes it to be seen as a 'poor cousin', one lacking the status and respect that it deserves. In many organisations, security managers are seen as being involved with operational matters, rather than strategic decision makers. As such, they are considered in the same group as facility managers, fleet hire managers and other members of the 'back room staff'. If security management is to be given the central role that we believe it should, then security managers in turn must make sure that they have the skills and capabilities that will allow them to fulfil that role in an effective and appropriate manner.

8.1 Cost or Investment?

One of the fundamental reason that security is not given the place it merits at the directors boardroom is that, rather than being seen as 'adding value' to an organisation, it is considered to be a 'non-productive cost'. This, in turn, causes it to become a 'grudging spend', rather than a well-supported investment. Security management is undoubtedly spend-driven – there is a need for a high level of technology, whether CCTV, fencing, lighting, control rooms, vehicles, personnel, etc, which needs to be both maintained and upgraded on a regular basis. However, there is also a case that could be made that effective security management can rationalise the security management programme, and especially in a larger organisation where security functions are spread across different sites, and can find effective cost savings without compromising security. In many cases, there is a business case to be made that by upgrading and taking advantage of newer technology, real savings can be made across the organisations' security spend.

8.2 Business Manager

The power of the above argument demonstrates another basic truth about the modern security manager – he or she is a Business Manager of a significant division within the organisation, and therefore should be able to bring all of the skills to the business management aspect of their role as would the equivalent head of any other division. This should be reflected in the language used to describe the value of the security division to the organisation, the way that it is presented and the supporting material that is produced. The security manager should be able to identify strategic objectives for their department, recruit the right people, develop effective protocols and manage the budget, at all times being aware of how that fits in with the wider strategic objectives of the company as a whole.

8.3 Competitive Advantage

In many situations, security management is seen as a business inhibitor rather than an opportunity enabler. For many people within the organisation, the only contact they have with the security operation is when they arrive in the building in the morning, or have a problem with their pass card. However on a wider perspective, the security management programme should be a business enabler, allowing the organisation to gain a competitive advantage over its competitors. This may be because they can gain 'First Mover Advantage' by expanding into new markets where their competitors cannot – this is especially true in what might be seen as high risk areas that could be an inhibitor to business development by organisations with less well-developed security management capabilities.

A Risk Management Framework such as shown in Figure 19, allows an organisation to assess whether it is viable to develop operations in a high-threat environment: (note the use of terminology previously covered in this module: risk assessment, likelihood and impact, avoid or transfer risk, acceptance of risk, standard operating procedures, regular review, contingency plans).

Figure 19: An example of a Security Risk Management Framework

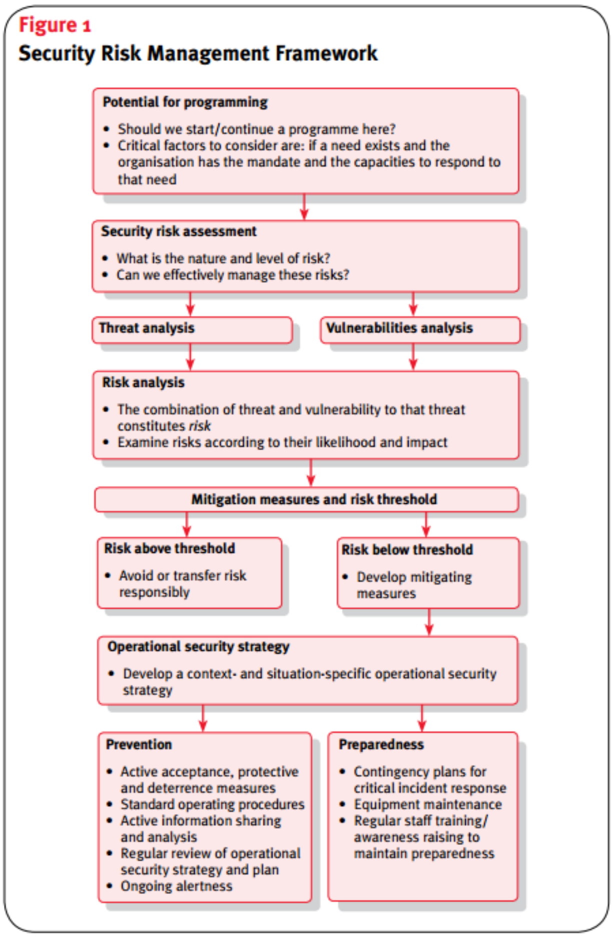


Figure 1

Security Risk Management Framework

Potential for programming

- Should we start/continue a programme here?
- Critical factors to consider are: if a need exists and the organisation has the mandate and the capacities to respond to that need

Security risk assessment

- What is the nature and level of risk?
- Can we effectively manage these risks?

Threat analysis

Vulnerabilities analysis

Risk analysis

- The combination of threat and vulnerability to that threat constitutes *risk*
- Examine risks according to their likelihood and impact

Mitigation measures and risk threshold

Risk above threshold

- Avoid or transfer risk responsibly

Risk below threshold

- Develop mitigating measures

Operational security strategy

- Develop a context- and situation-specific operational security strategy

Prevention

- Active acceptance, protective and deterrence measures
- Standard operating procedures
- Active information sharing and analysis
- Regular review of operational security strategy and plan
- Ongoing alertness

Preparedness

- Contingency plans for critical incident response
- Equipment maintenance
- Regular staff training/ awareness raising to maintain preparedness

Source: Van Brabant, K. (2010a) 'Good Practice Review - Operational Security Management in Violent Environments', London: Humanitarian Practice Network. http://acceptanceresearch.files.wordpress.com/2010/10/2010-good-practice-review-81.pdf

8.4 Subject Matter Expertise

The security manager's role has traditionally seen to have been relatively unskilled when compared to the level of professional capability expected from the heads of the finance division, business development division, marketing and branding division, etc. This is a hangover from the era when security managers were traditionally hired on the basis of their previous police experience, and the function that they fulfilled was often little more than in-house policeman. However, that has been changing over the last ten years, and there are now a wide range of professional and academic security management training programmes available. If the security manager is to achieve the same status as comparable managers in other divisions, it is necessary for them to show that they are able to bring the same level of expertise and professional development as their equivalents would. The security manager should expect to be the point of reference for all issues relating to security within their organisation, whether it is personal, as in foreign travel, operational, as in day to day management of security operations, or strategic, as in contributing to the organisation's continued growth and development.

8.5 Proactive Risk Management

Whilst a large part of a security manager's function will naturally be involved with managing the routine tasks associated with the security team, it is also necessary for them to become part of the 'Over the Horizon' thinking that is an essential part of any strategic management project. The nature of the present world means that the risks and threats facing any organisation are radically different than those that would have been faced in previous generations. Whether it is natural disasters, technological breakdowns, political upheavals, or the 'unknown unknowns' that could strike at any time, the role of the security manager is to bring these threats to the attention of strategic decision makers and to ensure that appropriate risk management procedures are in place.

8.6 Crisis Management

In the event that a genuine crisis does occur, it will be the security team that will be expected to draw up immediate response plans, to explain these to the rest of the organisation, and to take responsibility for the delivery and management of these programmes in order to realise a successful conclusion to the situation. The success or otherwise of such solutions will depend on the development of previous crisis management plans that will allow appropriate options to be created and managed in the face of high-pressure, potential catastrophic losses, breakdowns in normal communication and lines of command, and possible total disruption of normal operating capabilities. Crisis management capability is something that is developed, maintained and improved over time, through training, exercises and a high level of personal connection between the significant take-holders within an organisation. This is one area where the competent security manager can demonstrate real value to an organisation.

8.7 Business Continuity Management (BCM)

One of the clearest aspects of a security manager's function in relation to crisis management is to ensure that the organisation has the capability to maintain viable functionality even at the time of greatest disruption. Although this is not limited to the security management team, and will require genuine multi-division collaboration, it should be a function of the security managers to contribute their specialist expertise in terms of risk management, contingency planning and general project leadership. BCM is widely recognised as being a significant indicator as to the general level of effective organisational management, and is one place where the security management team can rightfully claim to have a level of expertise unmatched in any other division in the company.

8.8 Education and Training

Given that security awareness is something that should be an integral part of every aspect of an organisation's operations, it is clear that the security division has a role to play in developing both the appropriate corporate culture as well as specific skills and capabilities. It is the security manager's responsibility to ensure that everyone within the organisation is aware of their security role, how they can contribute to general organisational safety, and what specific steps should be taken in the event that potential threats are detected or actual incidents occur. Whilst it is easy for these up-skilling programmes to become tick box exercises, if they are seen as genuinely contributing to the development of a more effective organisation, then they will be valued as an integral part of the organisation's on-going corporate development process.

8.9 Point of Contact

As well as proactively raising the role of the security division, an effective security manager will develop the relationship with other divisions that will allow them to approach the security team for advice and guidance in areas where otherwise they might just have made a best guess and carried on. To a large extent it is a sign of a successful security management system if managers from other divisions feel comfortable dropping in to have a chat.

8.10 Summary

You have now completed the first, introductory module of this programme. Rather than giving detailed analysis of the specific skills that are an integral part of an effective security manager's portfolio, which will be covered in the following modules, the purpose of this module was to provide a basic understanding of the fundamental concepts that are the foundation of any security management programme. The concepts covered here will come up time and again in the rest of the course material, often within different contexts or with slightly different labels. However, if you understand the relationship between risk and security, understand how to create an effective command structure, can interact with the other divisions within the organisation, and perhaps most of all, can clearly demonstrate the added value that you bring to any organisation that you might be associated with, then you can be confident that you will be able to play a full part in creating an effective security management system that will provide the appropriate level of protection for the people, assets and operations in your company.

It may well be that as you go through this course there might be specific areas that take your interest. It could be in risk analysis, security auditing, overseas development, facilities management or crisis management. Whatever it might be, it is the duty of the modern security manager to be able to offer a level of knowledge, experience and professional capability that will be at least equal to the equivalent experts in every other division of the organisation.

In summary:

- In order to add value to the overall organisational management structure, the security manager must have the same level of personal and professional capabilities as any other senior manager of equivalent division.
- To make an effective contribution to the organisations security, and long-term success, he security manager should be seen as part of the strategic decision-making process, rather than 'merely' as part of the back-room support staff.
- In order to be valued, the security manager should be able to demonstrate that they are adding to organisational capability, and competitiveness, rather than being an unproductive cost.
- Security managers should be valued for the level of subject matter expertise that they offer, in the same way that the managers of other business divisions would be.
- Security managers should be seen as making a contribution to the success of every other division within the organisation, rather than being isolated as a separate, and relatively unimportant, adjunct to the organisation.

8.11 Self-assessment exercises

Self-assessment 1: Identify four other divisions within the organisation, and demonstrate how closer association with the security division could be to their advantage

Self-assessment 2: Write a report to be distributed to the heads of every other division within the organisation, explaining the importance of an effective Crisis Management capability, and explaining how this would be developed over the next six months.

Self-assessment 3: Prepare a PowerPoint presentation (about twenty minutes) that can be given to the General Board on the function of the security division, and how an expanded role will increase general effectiveness and capability across the organisation.