Main purpose of security management flashcard

To need security management we first have to identify a threat because without a threat we can’t fully understand or comprehend the task at hand, Management is how we go about implementing our principals of management that we have learned throughout our careers and personal approaches to the systems that have been proven over the years in successes and also failures.

The Management section of any security organization must start at the top from the security director down, It makes no difference if you have a security section of ten or a thousand the command structure must be adhered to because if it doesn’t things can rapidly deteriorate quickly, we have these structures in place as a fallback system to determine where things have failed and also to stop it progressing to the next level.

The thing that usually differs with security management and the other corporate management sections is the others are usually put in place to increase the financial yield of an organization, The Security section although a very important part of an organization is sometimes found to be a costly financial burden which is sometimes seen as an extravagance but necessity. As the old adage says security is everyone’s concern and should be emphasized throughout the whole organization.

Today security can be under an umbrella of many guises ranging from information security, physical security, investigations, forensics, screening and crisis management to name a few. To combat against the threat the security Director/manager must have a good security and risk plan.

Michael Belly (2008) describe that a Security Director/ Manager should be embedded into the organizations planning team, assisting with the establishment of task requirements, management, and conduct.

All available sources should be utilized when compiling the plan from the perceived threat, military missions, humming and historical intelligence. For a security plan to work you first have to compile the risk assessment elements Of the assessment may be captured within an introductory section of the contingency plan in order to define the nature of the risks facing a company or organization. This is useful for those entirely not up to speed with the impact of certain risks.

The risks can be categorized into five sub sections but are not exhaustive to the following Risk Avoidance- Does is really need to happen, Risk transferal- Could we mitigate the risk by subcontracting the task, Risk Sharing- Where we need to have an element of our own people n the ground but we could share with other companies, Risk mitigation- Where the risk is deemed acceptable for the potential gains and Risk Acceptance – Where the short term gains are viable against long term losses.

Where there is a risk assessment incorporated in the plan should always be the contingency plan which is basically the procedure of the organization in the event of a situation or emergency, Its main objectives are to ensure to containment of damage or injury or loss of personnel or property the organization.

In corporate into the plan due diligence must be considered cause it is a significant service requirement within the security sector, as confirmation of

the suitability of key hire positions within the organization it also important to confirm or refute any allegations of criminal or questionable business practices prior to business activities being initiated and contracts agreed.

The statement that security measures must be commensurate with the threat has to be thought logically and clearly before we can begin to answer the question we must fully understand the word “ commensurate” which reinstates to (corresponding in size or degree) which broken down in layman’s terms of security our security measures must at least be as good but preferably better then the imposed threat against us.

For us as security managers to begin to dissect the threat we must go back to the Risk and threat assessment as stated in (Risk and Security management 2008) the threat assessment specifically defines the scope, nature and impacts of risk the company may face during the life span of the operation. It should be written in the context of both the risk environment and the company’s risk learners, as these will define what risks are considered noteworthy and which fall within acceptable ranges for a project or organization.

The Security Director should not assume that the initial threat assessment will be read in conjunction with the intelligence review. Therefore the key elements from the intelligence review should be included (if) to clarify the environment in which the organization will operate. The threat assessment can be conducted in isolation of a site visit, although specific risks associated with the project will e difficult to ascertain without firsthand knowledge through an actual visit.

Secondary threat assessment may be done concurrently with, or as part of the security survey to provide the final specifics for the organization itself, as opposed to the more overarching initial assessment. The Risk assessment will be a vital part of the whole security plan which is a document which basically covers the whole spectrum of the overall risk that could affect the everyday running of the organization. The main focus of the plan is to look at the bigger picture from the outside in only then can you rasp the full facts of what you have to achieve.

The plan has to include but not exhaustive to the following , the standing operating procedures (SOP, S)the evacuation plan , the attack procedures from internal as well as external threats, and the overall incident procedures theft associated to the organization. We must always remember that plan has to be constantly updated as the threat is continually evolving and changing and wee as a security organization must take on board these issues and be prepared to alter things as we see fit.

This isn’t always an easy thing to do because of the changing threat to the organization it may be an added financial burden on resources not only monetary but also man power etc but for us to control the status quo We must convince the stakeholders that this must be done to make sure that (security measures must be commensurate with the threat). Security Management like any other type of management must be based on past proven principles as published by Peter Trucker (Management by Objectives) MOB deals with a certain type of interaction, specific to a manager and his employee.

MOB is based on the thinking that various hierarchies within need to be integrated. There was a need for commitment, responsibility and maturity.

There was a need for a common challenge. Here MOB becomes a process by which the objectives of an organization are agreed to and decided between the management and the employees, this way the employees understand what is expected of them and help set their own individual goals. Therefore they attain both their personal goals and the organizations targets.

The Goals are expected to be SMART, Specific, Measurable, Achievable, Realistic and Time Bound. Like any system sometimes its trial and error which can only then identify what works best for your personal organization because what worked at one time may not work now, this can be due to the ever changing threat and risk. It has to be a continues cycle of the following but not exhaustive to 1 Identify the threat, combat the threat, Monitor the threat, Evaluate the threat and review the threat.

As long as we are continuously aware of the evolving threat around us and act accordion Nagy we can stay one step ahead of the game. Successful management of security and risk is required throughout the projects lifespan or organizations ongoing viability. As long as we (DO the right things right). From my personal experience the stakeholders/Directors are businessmen who want to see the most profit and to increase the bottom line.

Depending on the environment of our business that can usually happen with a bit of forward thinking and common sense. In one initiative was involved in was going to take over one million dollars to purchase a piece of machinery

that was only going to save a coo plea of minutes of waiting time obviously this was a security measure that was not commensurate with the threat.

And from there could allocate resources to a better and more appropriate security initiative.