OMNIRISC
REDEFINING SECURITY

Security Newsletter

NOV 2017 I ISSUE 3

Welcome to the third edition of the OMNIRISC Security Newsletter where we will continue to examine items of interest to the security industry in Macau and security issues elsewhere.

What we can do to help you...

We believe that by being risk conscious and developing a culture of security awareness, we can provide better protection for an organization's people, assets and key infrastructure. To effectively address this issue, OMNIRISC has invested in developing its people in Security Risk Management culture as a focus for operational strategy and risk interventions. We provide bespoke consultations for businesses and organizations on various levels of vulnerability and risk assessments.

About the Author

James Langton, is a Security & Risk Management advisor to "OMNIRISC".

In the next newsletter we will review unexpected events that require Crisis Management.

In the last issue of this newsletter, the management of risk was outlined. In this issue we will examine hazards and emergency management. **In most organizations 'security' has now a greater span of responsibilities than previously allocated to them. Increasingly, additional responsibilities such as health and safety, customer relations and emergency management are being added to the more conventional functions expected of security departments.**

Hazards

Are the events that can harm our businesses, our people, our physical assets, our stakeholders, our reputations and our brands. They are usually categorized as either natural or human-made. The list of potential hazards is extensive and ranges from typhoons, floods, fires, tsunamis and even volcanoes in the natural category, to terrorism, industrial accident, loss of power, industrial action, criminal action and IT disruption in the human-made category.

From the extensive list of potential occurrences, each differing organization needs to identify the specific hazards that they have faced or are reasonably likely to face. They then need to closely examine how these particular threats impact on their vulnerabilities.

In Macau, we do not face all hazards but the ones that we may possibly face are:

- Typhoons
- Fire
- Loss of Power
- IT Disruption
- Health
- Staff Issues
- Flood
- Bomb Threat
- Supply Disruption
- Criminal Activity

This list is by no means exhaustive and each different organization must complete its own specific list of likely hazards.

Once the threats that can possibly impact your business have been identified, you need to determine your specific vulnerabilities to them. How do they impact upon your employees, your physical structures, your IT systems, your communications, your Intellectual property, your stakeholders, your supply chain, your brand and reputation and on members of the public using your facilities?

The way to effectively deal with these known hazards and vulnerabilities is through effective emergency management.

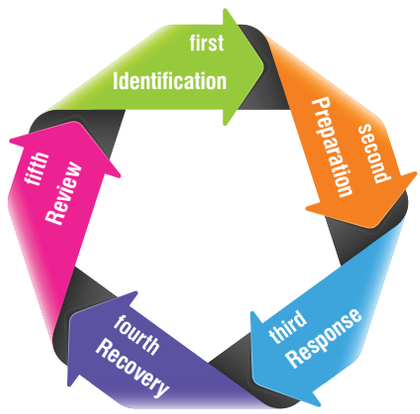
OMNIRISC SECURITY SERVICE (MACAO) LTD. 26 Avenida De Marciano Baptista, Chong Fok Comercial Centre, 12/H, Macau
Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com

Management of Public Access Areas

The recent terrorist incident in New York on 5th November, where a rented vehicle was used to kill and injure pedestrians in a public thoroughfare is yet another reminder of the risk of terrorism and the responsibilities which also fall on security organizations that control public access spaces within their properties. The increasing use of vehicles in these types of incident means that countries which have a lower risk of guns and explosives usage must now take the possibility of terrorist use of vehicles much more seriously.

Emergency Management [EM]

Is the process of preparing for emergencies by management of the resources and responsibilities required to deal with them. There are a number of components of the EM process. These are:



Identification

In order to commence the EM process you need to identify the specific hazards that your organization is likely to face.

In basic terms, we can use fire as an example. Let's say that the possibility of fire affecting your organization is fairly high. What then are your vulnerabilities? Possibly these are your employees, your building(s), your records, your equipment, and your reputation.

Once you have identified fire as a potential risk you then need to prepare to deal with it. The same procedure holds for all threats you have identified.

Preparation

These are actions taken prior to an emergency to facilitate readiness and effective response.

They include hazard mitigation measures incorporated into facility design and creating emergency plans for each threat. Once created, the various stakeholders need to be informed about the plan, staff must be trained and simulation exercises conducted, to ensure that staff are familiar with their responsibilities. Using our example of fire, we would have considered fitting fire alarms, fire suppression systems to reduce damage to facilities, provided firefighting equipment, ensured that vital records and IT backup are secured safely at an offsite location, created a fire response plan to make sure staff know their role during a fire and created evacuation routes to move staff to areas of safety. Staff should be aware of the plan, their responsibilities, if any, during the emergency and actions they need to take when the fire alarm sounds. Training in the plan is vital and taking part in simulations and drills must occur if the plan is to run effectively during an emergency.

If the preparedness stage is properly planned and managed the response stage will flow effectively.

Response

Is the action taken during emergencies to save life and property.

In the example of fire, this can include, what to do if discovering a fire, initial fire fighting prior to the arrival of professional fire services, fire marshals ensuring safe clearance of sections or floors of your facilities, evacuation of staff to predetermined safe holding areas, identification of missing staff members, initial first aid prior to arrival of paramedics and the presence of your organizations PR representative to deal with the media. Someone also needs to be given the responsibility within the plan to liaise with arriving emergency services to enable a better external response.

Recovery

Actions are taken after an emergency to restore and resume normal business operations.

These would include cleaning and repairing damaged facilities, replacing damaged equipment and communication systems, where necessary, relocation to temporary premises, recovery of records and IT equipment, ensuring the PR department is protecting brand and reputation, reconnecting with supply chain organizations and major stakeholders.

We will examine the more specialist area of Business Continuity arrangements in a later newsletter.

Review

Is important after any activation of an EM plan or after the plan has been used in a simulation exercise.

Lessons learned must be incorporated into revisions of the plan so that plans are maintained, updated and current.

Effective emergency management procedures, show staff, customers and other stakeholders that the organization is prepared to deal effectively with foreseeable emergencies. It generates confidence inside and outside the organization. It saves life and property and shows corporate responsibility.

We've seen a lot of interest in the community of late and increasing awareness of corporate responsibility when it comes to emergency management. For example last month we were invited to conduct a presentation for the France Macau Chamber of Commerce on the subject of risk, emergency and crisis, where we introduced the various processes that help prepare businesses for emergencies.

OMNIRISC
REDEFINING SECURITY

Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com