



# Security Newsletter

OCT 2017 | ISSUE 2

Welcome to the second edition of the OMNIRISC Security Newsletter where we will continue to discuss items of interest to the security industry in Macau and examine security issues elsewhere in the world that have implications for all of us.

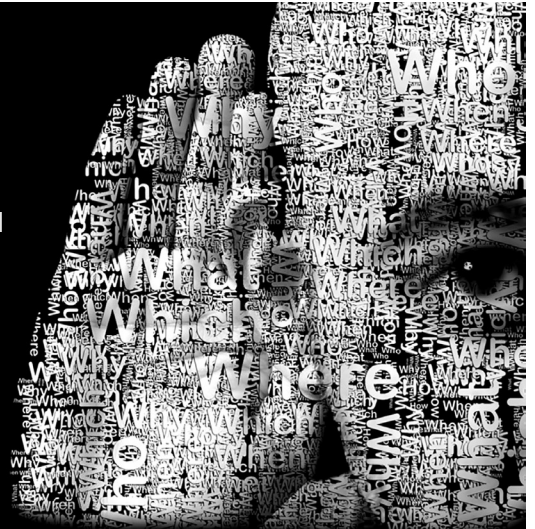
## What we can do to help you:

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.

James Langton, is an advisor to "OMNIRISC." He has over 40 years of experience in the security and law enforcement industries and is a consultant in security, risk, crisis and emergency management working throughout SE Asia and Australasia.

## Management of Public Access Areas

The August terror attack on Barcelona's Las Ramblas and the tragic loss of life resulting from the attack on an open-air music festival in Las Vegas this month reminds us of the risks currently posed by extremist elements. It also draws the attention of facility owners and security organizations to the risks involved in the management of public access space within their areas of responsibility.



## Terrorism

The attack on the pedestrian precinct of Las Ramblas using a light commercial vehicle resulted in 13 people being killed and many injured. This was the latest terrorist attack targeting pedestrian areas using vehicles.

## Security Nightmare

By contrast, the attack on the music festival in Las Vegas carried out from a nearby hotel room by a deranged individual with access to a significant number of weapons enabling him to open fire on the crowd below, killing 59 people and injuring at least 600 people.

## Interventions

The authorities tasked with preventing such tragedies are now increasingly making use of permanent and temporary barriers in order to counter these types of incident.

In addition, cities are often making use of private security companies to bolster police coverage of these areas, to ensure public safety.

**Companies involved in this type of security coverage need to ensure that they are fully prepared for the risks involved.**

## Aftermath

As the investigation into the incident progresses and the subsequent litigation begins, many questions will be asked of the organizer and security company responsible for the event and of the hotel's security organization.

1. Was the security plan adequate?
2. Was the security organization properly prepared?
3. Was a vigorous risk assessment conducted prior to the event?
4. How did a guest manage to bring such a large quantity of weapons into the hotel?
5. How did housekeeping miss a large number of guns in the room and if they were denied access for a period, was this reported to hotel security?

**Again the hotels risk management procedures will have to be examined closely.**

# RISK & RISK MANAGEMENT

Both of these issues raise adequacy of the Risk Management procedures.  
So let's examine Risk and Risk Management?

**Risk** can be defined as the potential for loss, damage or destruction of an organization's assets [human, physical, financial or reputational], as a result of a threat.

## Risk Management

is a range of activities designed to identify, assess and prioritize threats to your organization followed by the application of resources to minimize or control those threats.

### STEPS in the RISK MANAGEMENT PROCESS

1. Identify the Risks
2. Analyze the Risks
3. Evaluate or Rank the Risks
4. Treat the Risks
5. Monitor and Review the Risks



## Identify the Risks:

1. What risks are we likely to face?
2. What happens if we are hit by a typhoon or we lose power for several days?
3. What can hurt us?

Once threats or hazards are identified how do we prioritize our actions in order to prepare for them?

## Analysis the Risks

Use of a Risk Matrix (see Table 2 for a sample risk matrix) used during a risk assessment to identify the level of risk, by considering the probability or likelihood of a particular risk occurring, plotted against its severity of consequence to your particular organization. This is a useful mechanism to increase visibility of risks and assist in management decision making.

		CONSEQUENCES				
		Almost Certain	Marginal	Minor	Moderate	Major
LIKELIHOOD	Almost Certain	M	H	H	C	C
	Likely	M	M	H	H	C
	Possible	L	M	M	H	C
	Unlikely	L	M	M	M	H
	Rare	L	L	M	M	H

## Evaluation or Rank the Risks

We evaluate or rank the risk by determining its magnitude. The use of the risk matrix will rank the organization's risk by likelihood of occurrence against its consequences, shown by the color coding in Table 2. Risks colored red [e.g. almost certain likelihood of occurrence and severe consequences] would be a top priority for urgent action.

## Risk Treatment

Having determined the priority of the threats we face we can then make informed management decisions regarding those risks we plan to treat or modify. As shown below, we have a number of risk treatment options to choose from.

1. Avoidance, such as not performing the activity that attracts the risk.
2. Reduction, that involves reducing the impact of any loss by preparing risk reduction plans and procedures.
3. Sharing, where the risk is transferred to a third party or retention where the risk is accepted as part of business operations and expenses.

It is important to remember that risk reduction plans and procedures should also be adopted by your key stakeholders to prevent external vulnerabilities.

## Monitor and Review

Finally the whole process needs to be regularly monitored and reviewed in order to ensure that it is current and remains fit for purpose.

## Coming Up

In next month's newsletter we will discuss Emergency Management and Crisis Preparedness and Response.